ADVANCED ALGEBRA

ADVANCED ALGEBRA

BY

S. BARNARD, M.A.

FORMERLY ASSISTANT MASTER AT RUGBY SCHOOL, LATE FELLOW AND LECTURER AT EMMANUEL COLLEGE, CAMBRIDGE

AND

J. M. CHILD, B.A., B.Sc.

FORMERLY LECTURER IN MATHEMATICS IN THE UNIVERSITY OF MANCHESTER
LATE HEAD OF MATHEMATICAL DEPARTMENT, TECHNICAL COLLEGE, DERBY
FORMERLY SCHOLAR AT JESUS COLLEGE, CAMBRIDGE

MACMILLAN AND CO., LIMITED
ST. MARTIN'S STREET, LONDON.

MACMILLAN AND COMPANY LIMITED
London Bombay Calcutta Madras Melbourne

THE MACMILLAN COMPANY OF CANADA LIMITED
Toronto

ST MARTIN'S PRESS INC
New York

First Edition 1939
Reprinted 1953

PRINTED IN GREAT BRITAIN

PREFACE

THIS volume is a continuation of the *Higher Algebra* by the same authors, and is intended for the mathematical specialist. Its scope has been determined by what is necessary for Honours degrees at the Universities: and we think that such parts of Advanced Algebra, as Matrices, Sets of Points, etc., should be dealt with by experts in these subjects in special texts.

Sections on Homographic and Linear Transformations, Cross Ratios, Involution, Projection and Plane Perspective are given: the authors think that the contents of these sections are more suitably given in texts on Algebra, rather than in those on Geometry.

Theory of equations is continued from *Higher Algebra*, and leads to sections on Elimination, Invariants, Covariants and Canonical Forms. Also the Theory of Infinite Series is continued in two chapters on (i) Double Series, (ii) Uniform Convergence: these include articles on Quotient of two Power Series, Reversion, Multiplication, Differentiation and Integration of Power Series, Bernoulli's Theorem and Euler's Constant.

Quadratic residues and primitive roots lead up to Euler's Criterion, Gauss's Lemma and Lange's proof of the Law of Quadratic Reciprocity: there are also articles on the sums of two or more squares and methods of factorizing large numbers.

For convenience, a chapter on the expression of a Quadratic Surd as a Continued Fraction is repeated from *Higher Algebra*; and this leads to a discussion of the general solution in integers of the Indeterminate Equations of the Second Degree: there is also a chapter on the general theory of Continued Fractions, including Gauss's Transformation for the quotient of two Hypergeometric Series.

Other subjects discussed are the Complex Variable, Exponential and Logarithmic Functions, Probability of Causes, Life Contingencies and Insurance, and Gauss' solution of $x^n - 1 = 0$.

Some theorems, and certain simplified proofs, such as the $\Sigma(a_n a_{n-1}/b_n)^{\frac{1}{2}}$ test for continued fractions, and the expression for, and evaluation of Euler's Constant, are original: but so much has been done in the last few years, that the authors hesitate to claim such theorems or proofs as new.

Most of the examples are from the Mathematical Tripos, Parts I and II, and Examinations for Oxford Senior and Junior Mathematical Scholarships; but a considerable number are original, these being usually of a type leading up to the former. Some of those on Probability are taken from Whitworth's *Choice and Chance*; while many of the most interesting are due to Dr. G. T. Bennett, to whom the authors are also under deep obligation for much valuable advice and assistance throughout the work.

Among the books to which the authors have made reference are: Bromwich, *Theory of Infinite Series*; Chrystal, *Algebra*; Whitworth, *Choice and Chance*; Hardy, *Pure Mathematics*; Gauss, *Recherches Arithmétiques*; Salmon, *Higher Algebra*; Serret, *Algèbre Supérieure*; Tannery, *Leçons d'Algèbre et d'Analyse*; Wertheim, *Anfangsgründe der Zahlenlehre*.

Best thanks are gladly given to Sir Richard Gregory for his helpful advice; and to Messrs. Macmillan and Messrs. MacLehose for the great pains they have taken in the difficult task of illustrating and printing a book of this kind.

In working out solutions to such a large number of Examples, the authors cannot hope that all answers will be correct: they would esteem highly notification of errors, or of misprints in either the text or the answers.

S. BARNARD.
J. M. CHILD.

CONTENTS

The numbers in brackets refer to pages.

ADVANCED ALGEBRA

CHAPTER I

THE HOMOGRAPHIC RELATION

1. Homographic Substitution. (1) Let the variables z, Z (which may be complex numbers) be connected by the equation

$$z = \frac{lZ+m}{l'Z+m'}, \quad \text{.....(A)}$$

which is the same as $l'zZ + m'z - lZ - m = 0$. .....(B)

If $l' \neq 0$, this may be written

$$\left(z - \frac{l}{l'}\right)\left(Z + \frac{m'}{l'}\right) = -\frac{lm' - l'm}{l'^2}. \quad \text{.....(C)}$$

When z, Z are complex variables, we may represent them by points z, Z in two planes oxy, OXY. If $z = l/l'$, then $Z = \infty$, and the point Z may be any point on the line at infinity in the Z plane. If $Z = -m'/l'$, then $z = \infty$, and the point z may be any point at ∞ in the z plane.

Apart from these special cases, a single value of Z corresponds to any value of z, and *vice versa*. Thus, if the point z describes a curve in its plane, then Z describes a corresponding curve in its plane.

Equation (A) is called a *homographic* (or *bilinear*) *substitution*; the change from the variable z to the variable Z is a *homographic transformation*.

(2) *A homographic substitution, which changes z_1, z_2 into Z_1, Z_2 respectively, is of the form*

$$\frac{z - z_1}{z - z_2} = k \cdot \frac{Z - Z_1}{Z - Z_2}, \quad \text{.....(A)}$$

where k is a constant.

For if the substitution is $z = (lZ+m)/(l'Z+m')$, then

$$z - z_1 = \frac{lZ+m}{l'Z+m'} - \frac{lZ_1+m}{l'Z_1+m'} = \frac{(lm'-l'm)(Z-Z_1)}{(l'Z+m')(l'Z_1+m')},$$

with a similar value for $z - z_2$. Hence

$$\frac{z-z_1}{z-z_2} = k \cdot \frac{Z-Z_1}{Z-Z_2} \quad \text{where} \quad k = \frac{l'Z_2+m'}{l'Z_1+m'}.$$

(3) *The homographic substitution which changes* z_1, z_2, z_3 *into* Z_1, Z_2, Z_3 *is*

$$\frac{z-z_1}{z-z_2}\cdot\frac{z_3-z_2}{z_3-z_1}=\frac{Z-Z_1}{Z-Z_2}\cdot\frac{Z_3-Z_2}{Z_3-Z_1}. \quad \text{.....(B)}$$

For the value of k in equation (A) is obtained by putting $z=z_3$, $Z=Z_3$.

2. Double Points of the Substitution. (1) Let z and Z be connected by the equation

$$z=(lZ+m)/(l'Z+m'). \quad \text{.....(A)}$$

Suppose that the z and Z planes coincide and that the points z, Z are referred to the same axes.

In general, *there are two points which are unaltered by the substitution.* These are called the *double, or self-corresponding, points,* and they are to be found by putting $Z=z$ in equation (A), giving the quadratic

$$l'z^2-(l-m')z-m=0, \quad \text{.....(B)}$$

whose roots α, β correspond to the double points.

(2) *If the double points* α, β *are distinct, the substitution* (A) *can be written in the form*

$$\frac{z-\alpha}{z-\beta}=k\cdot\frac{Z-\alpha}{Z-\beta}, \text{ where } k \text{ is a constant.} \quad \text{.....(C}$$

The value of k *is given by* $k=\dfrac{l'\beta+m'}{l'\alpha+m'}=-\dfrac{l'\alpha-l}{l'\alpha+m'}=-\dfrac{l'\beta+m'}{l'\beta-l}$.

This follows from Art. 1, (2), on putting $z_1=Z_1=\alpha$ and $z_2=Z_2=\beta$.

Again, equation (C) may be written

$$k\left\{1+\frac{\alpha-\beta}{z-\alpha}\right\}=1+\frac{\alpha-\beta}{Z-\alpha},$$

and since $1-k=l'(\alpha-\beta)/(l'\alpha+m')$ and $\alpha\neq\beta$, this is equivalent to

$$\frac{k}{z-\alpha}-\frac{1}{Z-\alpha}=\frac{l'}{l'\alpha+m'},$$

which is the same as

$$\frac{l'\beta+m'}{z-\alpha}-\frac{l'\alpha+m'}{Z-\alpha}=l', \quad \text{or} \quad \frac{l'\alpha-l}{z-\alpha}+\frac{l'\alpha+m'}{Z-\alpha}+l'=0. \quad \text{.....(D)}$$

(3) *If the double points* (α, β) *coincide, the substitution* (A) *can be written in the form*

$$\frac{1}{z-\alpha}-\frac{1}{Z-\alpha}=c, \text{ where } c \text{ is a constant.} \quad \text{.....(E)}$$

The value of c *is given by* $c=2l'/(l+m')$.

For equation (D) holds however small $\alpha-\beta$ may be, and the form of the equation shows that it also holds in the limiting case when $\alpha=\beta$,

and then from equation (B), $2l'\alpha = l - m'$ and $2(l'\alpha + m') = l + m'$; which gives the result in question.

3. Special Transformations. (1) *A homographic substitution converts a circle c in the z plane into a circle C in the Z plane or, in a special case, into a straight line.*

Choose a pair of points z_1, z_2 which are inverse with regard to the circle c, and let Z_1, Z_2 be the corresponding points. The substitution can be expressed in the form

$$\frac{z-z_1}{z-z_2} = k \cdot \frac{Z-Z_1}{Z-Z_2}.$$

If z is any point on the circle c, we have

$$\left| \frac{z-z_1}{z-z_2} \right| = k',$$

where k' is a constant, for the left-hand side is the ratio of the lengths zz_1, zz_2, therefore

$$\left| \frac{Z-Z_1}{Z-Z_2} \right| = \frac{k'}{|k|}.$$

Therefore the ratio of the lengths ZZ_1, ZZ_2 is equal to $k'/|k|$. Hence the locus of Z is a circle of which Z_1, Z_2 are inverse points, unless $k' = |k|$. In this case Z describes the perpendicular bisector of Z_1Z_2.

(2) *A circle c in the z plane is converted into a straight line by the substitution*

$$z = \frac{lZ+m}{l'Z+m'} \qquad \text{(A)}$$

if, and only if, the point $z = l/l'$ lies on the circle c.

For any point at ∞ in the Z plane corresponds to the point $z = l/l'$. Hence the Z locus has a real point at ∞ when, and only when, the point $z = l/l'$ is on the circle c. In this case the Z locus cannot be a circle, and is therefore a straight line.

(3) *If the substitution* (A) *converts a circle c into a circle C, then the part of the z plane inside the circle c corresponds to the part of the Z plane inside or outside the circle C according as the point $z = l/l'$ is outside or inside the circle c.*

Let p be any point inside c, and let P be the corresponding point. Suppose that the point z moves along a continuous path from p to the point l/l'; then the point Z moves along a continuous path from P to some point at ∞. If the z path crosses the circle c, the Z path crosses the circle C. Hence P is inside or outside C according as the point $z = l/l'$ is outside or inside c.

(4) *If the substitution* (A) *converts a straight line u into a circle C, then the part of the z plane on the side of u remote from the point $z=l/l'$ corresponds to the part of the Z plane inside the circle C.*

The proof is similar to that in § (3).

4. *If a figure s is converted into a figure S by the substitution $z=lZ+m$, then s and S are directly similar and the magnification is $|1/l|$.*

Also if l is real and positive, the figures are similarly situated.

For, if z_1, z_2, z_3 are any three points in s, and Z_1, Z_2, Z_3 are the corresponding points in S, then

$$(z_1-z_2)/(z_1-z_3)=(Z_1-Z_2)/(Z_1-Z_3);$$

and the triangles $z_1z_2z_3$, $Z_1Z_2Z_3$ are directly similar. (*H.A.*, p. 80, Ex. 14.)

Moreover, $z_1-z_2=l(Z_1-Z_2)$; therefore the length z_1z_2 is equal to $|l|$ times the length Z_1Z_2, that is to say, the magnification is $|1/l|$.

Again, if l is real and positive, $\mathrm{am}(z_1-z_2)=\mathrm{am}(Z_1-Z_2)$, therefore corresponding lines in s and S are parallel and are drawn in the same sense.

Therefore the figures are similarly situated.

EXERCISE I

1. Prove that the substitution $z=1/Z$ converts the straight line $ax+by+c=0$ into the circle

$$c(X^2+Y^2)+aX-bY=0.$$

Show also that the part of the z plane, on the same side of the line as the point $z=0$, corresponds to the part of the Z plane outside the circle.

[Put $x=X/(X^2+Y^2)$, $y=-Y/(X^2+Y^2)$.]

2. If z is any point on the circle $x^2+y^2=a^2$, then

$$|kz-a^2|=a\,.\,|z-k|,$$

where k is any real number except 0 or a.

[The points $z=k$, $z=a^2/k$ are inverse points.]

3. The substitution $z=(Z-1)/(Z+1)$ transforms the circle $x^2+y^2=a^2$ into the circle

$$X^2+Y^2-2\frac{1+a^2}{1-a^2}X+1=0,$$

or, if $a=1$, into the Y-axis.

4. Show that the substitution $z=\iota(Z+1)/(Z-1)$ transforms the circle

$$x^2+y^2-x=0$$

into the circle

$$X^2+Y^2+2X-2Y+1=0.$$

5. Express the relation $z=(5Z-4)/(2Z-1)$ in the form

$$\frac{z-\alpha}{z-\beta}=K\cdot\frac{Z-\alpha}{Z-\beta},$$

where α, β, K are constants.

6. With regard to the circle whose equation is $3(x^2+y^2)=4x$, prove that $z=1$, $z=2$ are inverse points, and that if z is any point on the circle, then

$$|z-2|=2|z-1|.$$

Hence show that the substitution $z=(5Z-4)/(2Z-1)$ transforms the circle into the circle whose equation is $35(X^2+Y^2)-68X+32=0$.

7. In questions 3, 4 and 6, show that the part of the z plane inside the first circle corresponds to the part of the Z plane inside the second circle.

8. Given two directly similar figures $z_1, z_2, \ldots$ and $Z_1, Z_2, \ldots$, prove that

(i) The first may be transformed into the second by a substitution of the form

$$z=aZ+b.$$

(ii) The point $z=b/(1-a)$ may be regarded as belonging to both figures, and is called the *double point* or the *centre of similitude*.

(iii) Prove the following construction for the double point S: Take two pairs of corresponding points z_1, Z_1 and z_2, Z_2. Join z_1Z_1, z_2Z_2, meeting in C, then the circles z_1z_2C, Z_1Z_2C meet in S.

[Take any other pair of corresponding points as z_3, Z_3. Let ABC be the triangle formed by the lines z_1Z_1, z_2Z_2, z_3Z_3. The 'point 0 theorem' shows that the triangles Sz_1Z_1, Sz_2Z_2, Sz_3Z_3 are directly similar.]

9. If z is any point on the circle

$$x^2+y^2+2gx+2fy+c=0,$$

then

$$\left|\frac{z+k(g+if)}{z}\right|=\sqrt{1-k},$$

where $k=c/(g^2+f^2)$, unless $g=0$ and $f=0$.

[The points $z=0$, $z=-k(g+if)$ are inverse points.]

5. Imaginary Points and Lines. In order that the correspondence between the language of geometry and that of algebra may be more complete, we extend the meanings of the words 'point' and 'line.'

(1) *Points on a line.* The reader is familiar with the mode of representing real numbers by points on a line. This notion is extended as follows:

Definition. To every complex number (x) there corresponds a point (P) on a given line. This point P is real or imaginary according as x is real or imaginary.

(2) *Points on a plane.* A point P in a plane is determined by its coordinates x, y, referred to given axes, rectangular or oblique. If $ax+by+c=0$, the point (x, y) lies on a straight line, of which this is the equation.

These ideas are extended as follows:

Definitions. To every pair of numbers (x, y) there corresponds a point P in a given plane. This point is *real* if both x and y are real, and *imaginary* if one or both of x, y are imaginary. The *coordinates* of P are x, y. If a, b, c are constants, the equation $ax+by+c=0$ represents a straight

line which is the aggregate of all the points, real or imaginary, whose coordinates satisfy the equation. The line is *real* if both c/a, c/b are real, and *imaginary* if at least one of them is imaginary.

(3) If (a, a'), (b, b'), (c, c'), (d, d') are the coordinates of four real points A, B, C, D which are in the same straight line, then

$$\frac{AB}{CD} = \frac{b-a}{d-c} = \frac{b'-a'}{d'-c'}.$$

We take these equations as defining the meaning of the ratio of two collinear segments AB, CD when any of A, B, C, D are imaginary.

6. Conjugate Points and Lines. (1) If a, b, c, a', b', c' are real, the points

$$(a + \iota a', b + \iota b'), \quad (a - \iota a', b - \iota b')$$

are called *conjugate points*, and the lines

$$ax + by + c \pm \iota(a'x + b'y + c') = 0$$

are called *conjugate lines*.

(2) *An imaginary line contains only one real point (which may be at infinity). This point also lies on the conjugate line.*

For the equation to the line is of the form

$$ax + by + c + \iota(a'x + b'y + c') = 0.$$

The only real point on it is given by

$$ax + by + c = 0, \quad a'x + b'y + c' = 0.$$

Also, this point lies on the conjugate line.

(3) *One and only one real line passes through an imaginary point, and this line contains the conjugate point.*

For if the line $px + qy + r = 0$ contains the point $(a + \iota a', b + \iota b')$, where p, q, r are real numbers, then

$$p(a + \iota a') + q(b + \iota b') + r = 0;$$

$$\therefore \; pa + qb + r = 0 \quad \text{and} \quad pa' + qb' = 0;$$

$$\therefore \; \frac{p}{b'} = \frac{q}{-a'} = \frac{-r}{ab' - a'b}.$$

Therefore the only real line through $(a + \iota a', b + \iota b')$ is

$$b'x - a'y = ab' - a'b,$$

and this contains the point $(a - \iota a', b - \iota b')$.

Ex. 1. *If two imaginary lines l, m meet at A and the conjugate lines l', m' meet at A', then A, A' are conjugate points.*

For the equations of l', m' are derived from those of l, m by changing ι into $-\iota$.

7. The Circular Points at Infinity. The points at infinity on the circle $x^2+y^2+2gx+2fy+c=0$ satisfy the equation $x^2+y^2=0$. Therefore every circle is to be regarded as passing through two fixed points, namely the points at infinity on the lines $y=\pm ix$.

These are called the *circular points at infinity*.

8. The Harmonic Relation. Let A, B, A', B' be points on a line corresponding to the numbers α, β, α', β', no two of which are equal.

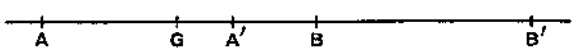


FIG. 1.

We say that AB is divided *harmonically* at A', B' if

$$AA'/A'B=-AB'/B'B. \quad \text{.....(A)}$$

This equation may be written in any of the following forms :

$$A'A/AB'=-A'B/BB', \quad \text{.....(B)}$$

$$(\alpha-\alpha')(\beta-\beta')=-(\alpha-\beta')(\beta-\alpha'), \quad \text{.....(C)}$$

$$2(\alpha\beta+\alpha'\beta')=(\alpha+\beta)(\alpha'+\beta'), \quad \text{.....(D)}$$

$$\{\alpha-\tfrac{1}{2}(\alpha+\beta)\}^2=\{\alpha'-\tfrac{1}{2}(\alpha+\beta)\}\{\beta'-\tfrac{1}{2}(\alpha+\beta)\}. \quad \text{.....(E)}$$

Comparing (A) and (B) we see that *$A'B'$ is divided harmonically at A, B*. Again, equation (D) is symmetric with regard to α, β and with regard to α', β', therefore *the relation still holds if we interchange either A and B, or A' and B'*.

From equation (E) it follows that, if G is the mid-point of AB, then

$$GA^2=GA'.GB'. \quad \text{.....(F)}$$

Also from equation (C),

$$\frac{1}{\alpha-\beta}-\frac{1}{\alpha-\alpha'}=\frac{1}{\alpha-\beta'}-\frac{1}{\alpha-\beta} \quad \text{or} \quad \frac{2}{\alpha-\beta}=\frac{1}{\alpha-\alpha'}+\frac{1}{\alpha-\beta'}, \quad \text{.....(G)}$$

and therefore

$$\frac{2}{AB}=\frac{1}{AA'}+\frac{1}{AB'}, \quad \text{.....(H)}$$

showing that *AB is the harmonic mean between AA' and AB'*.

The relation (A) is expressed by saying that *the pairs* (A, B), (A', B') *are harmonic, or that the 'range'* $(AB, A'B')$ *is harmonic, or that A, B are harmonic conjugates with regard to A', B'*.

Conversely, if no two of α, β, α', β' are equal and any one of the above equations holds, then $(AB, A'B')$ is harmonic.

9. Cross-ratios. (1) Let A, B, C, D be four points in a straight line, corresponding to the numbers a, b, c, d.

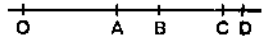


FIG. 2.

The *cross-ratio* denoted by (AB, CD) is defined as the ratio of the ratios in which the points C, D divide the segment AB; which is the same as the ratio in which the points A, B divide CD. Thus

$$(AB, CD) = \frac{CA}{CB} \div \frac{DA}{DB} = \frac{AC}{AD} \div \frac{BC}{BD} = \frac{(a-c)(b-d)}{(a-d)(b-c)}.$$

More generally, if z_1, z_2, z_3, z_4 are numbers which may be complex, or the points represented by them, the cross-ratio (z_1z_2, z_3z_4) is defined by

$$(z_1z_2, z_3z_4) = \frac{z_1-z_3}{z_1-z_4} \div \frac{z_2-z_3}{z_2-z_4} = \frac{(z_1-z_3)(z_2-z_4)}{(z_1-z_4)(z_2-z_3)}.$$

The points in question may be real points in the plane Oxy (Fig. 3), or they may be real or imaginary points on an axis.

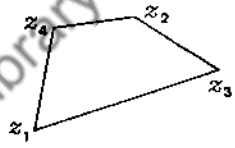


FIG. 3.

(2) It is easily verified that (z_1z_2, z_3z_4) *is unaltered by the interchange of any two of* z_1, z_2, z_3, z_4, *provided that the other two are also interchanged.* Thus

$$(z_1z_2, z_3z_4) = (z_3z_4, z_1z_2) = (z_2z_1, z_4z_3) = (z_4z_3, z_2z_1).$$

Hence corresponding to the 24 permutations of z_1, z_2, z_3, z_4, *there are 24 cross-ratios which may be arranged in six groups of four equal cross-ratios.*

Also it should be noticed that *the single interchange of* z_1, z_2 *or of* z_3, z_4 *converts* (z_1z_2, z_3z_4) *into its reciprocal.*

10. Relations between the six different Cross-ratios. We have

$$(z_2z_3, z_1z_4) = \frac{(z_2-z_1)(z_3-z_4)}{(z_2-z_4)(z_3-z_1)} = \frac{(z_2z_3+z_1z_4)-(z_3z_1+z_2z_4)}{(z_2z_3+z_1z_4)-(z_1z_2+z_3z_4)}.$$

Let $\lambda = z_2z_3 + z_1z_4$, $\mu = z_3z_1 + z_2z_4$, $\nu = z_1z_2 + z_3z_4$, and observe that the process of changing 1 to 2, 2 to 3, 3 to 1 (called the *cyclic substitution* (1 2 3)) changes λ to μ, μ to ν, ν to λ.

Denoting any one of the cross-ratios, (z_2z_3, z_1z_4) say, by ρ, we have

$$(z_2z_3, z_1z_4) = \frac{\lambda-\mu}{\lambda-\nu} = \rho, \quad (z_3z_1, z_2z_4) = \frac{\mu-\nu}{\mu-\lambda} = 1 - \frac{1}{\rho}, \quad (z_1z_2, z_3z_4) = \frac{\nu-\lambda}{\nu-\mu} = \frac{1}{1-\rho},$$

and, interchanging the first two numbers in each of these,

$$(z_3z_2, z_1z_4) = \frac{1}{\rho}, \qquad (z_1z_3, z_2z_4) = \frac{\rho}{\rho-1}, \qquad (z_2z_1, z_3z_4) = 1-\rho.$$

Hence *if any one of the six cross-ratios is denoted by* ρ, *the complete set (in the above order) is*

$$\rho,\ 1-\frac{1}{\rho},\ \frac{1}{1-\rho},\ \frac{1}{\rho},\ \frac{\rho}{\rho-1},\ 1-\rho.$$

It follows that *if one of the cross-ratios of* z_1, z_2, z_3, z_4 *is real, then all are real, and if one is imaginary, all are imaginary.*

11. Special Cases of great importance arise if two of the set of six cross-ratios mentioned in Art. 10 are equal.

Let $\rho=(z_2z_3, z_1z_4)$, then it will be found that all possible cases are included in the following:

(1) Let $\rho=1/\rho$, so that $\rho=\pm1$.

If $\rho=1$, the values of the six cross-ratios in the order of Art. 2 are respectively

$$1,\quad 0,\quad \infty,\quad 1,\quad \infty,\quad 0.$$

And since $(z_3z_1, z_2z_4)=0$, it follows that $z_2=z_3$ or $z_1=z_4$.

If $\rho=-1$, then (z_2z_3, z_1z_4) is harmonic.

We conclude that *if* (z_2z_3, z_1z_4) *is unaltered by the interchange of* either z_2, z_3 or *of* z_1, z_4, *then either* (z_2z_3, z_1z_4) *is harmonic or else one of the pairs* (z_2, z_3), (z_1, z_4) *consists of coincident points.*

(2) *Let* $\rho=1-\frac{1}{\rho}$, then $\rho^2-\rho+1=0$ and $\rho=-\omega$, where ω is an imaginary cube root of unity. In this case, the values of the six cross-ratios in the above order are

$$-\omega,\quad -\omega,\quad -\omega,\quad -\omega^2,\quad -\omega^2,\quad -\omega^2,$$

and the system z_1, z_2, z_3, z_4 is said to be *equi-anharmonic.*

12. Homographic Substitution. (1) *If* z_1, z_2, z_3, z_4 *are any four values of a variable* z, *the value of* (z_2z_3, z_1z_4) *is unaltered by the homographic substitution*

$$z=(lZ+m)/(l'Z+m').$$

For if Z_1, Z_2, Z_3, Z_4 are the corresponding values of Z, as in Art. 1,

$$z_1-z_3=\frac{(lm'-l'm)(Z_1-Z_3)}{(l'Z_1+m')(l'Z_3+m')},$$

with similar equations. It follows that

$$(z_1z_2, z_3z_4)=(Z_1Z_2, Z_3Z_4).$$

(2) If a cross-ratio of A, B, C, D is equal to a cross-ratio of A', B', C', D', then any two corresponding cross-ratios are equal, and we say that *the two sets of points are equi-cross.** This is indicated by writing $(ABCD)=(A'B'C'D')$.

* Also called equi-anharmonic by some authors.

13. The Biquadratic. *If ρ is any one of the six cross-ratios determined by $\alpha, \beta, \gamma, \delta$, the roots of* $u = ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0$,

then $$I^3(\rho+1)^2(\rho-2)^2(\rho-\tfrac{1}{2})^2 = 27J^2(\rho^2-\rho+1)^3, \quad \text{.....(A)}$$

which is equivalent to

$$4\Delta(\rho^2-\rho+1)^3 = 27I^3\rho^2(\rho-1)^2. \quad \text{.....(B)}$$

For suppose that

$$\rho = (\beta\gamma, \alpha\delta) = \frac{(\beta-\alpha)(\gamma-\delta)}{(\beta-\delta)(\gamma-\alpha)} = \frac{\lambda-\mu}{\lambda-\nu},$$

where $\lambda = \beta\gamma + \alpha\delta$, $\mu = \gamma\alpha + \beta\delta$, $\nu = \alpha\beta + \gamma\delta$.

It follows from *H.A.*, XII, 10, that $\rho = (t_1 - t_2)/(t_1 - t_3)$, where t_1, t_2, t_3 are the roots of

$$4t^3 - It + J = 0. \quad \text{.....(C)}$$

Let $z = \rho + \rho^{-1}$, then using the equations

$$\Sigma t_1 = 0, \quad t_1t_2t_3 = -J/4, \quad 4t_1^3 = It_1 - J,$$

it is easy to show that

$$z + 2 = \frac{36t_1^3}{8t_1^3 - J} = \frac{9(It_1 - J)}{2It_1 - 3J},$$

and therefore

$$t_1 = \frac{3J}{I} \cdot \frac{z-1}{2z-5}.$$

Substituting this value for t in equation (C), we find that

$$\frac{I^3}{4(z-1)^3} = \frac{27J^2}{(2z-5)^2(z+2)} = \frac{I^3 - 27J^2}{27(z-2)}.$$

Since $z = \rho + \rho^{-1}$ and $\Delta = I^3 - 27J^2$, equations (A) and (B) follow at once.

Hence the following conclusions:

(i) *If $I = 0$ and $J \neq 0$, then $\rho = \omega$ or ω^2, and the points $\alpha, \beta, \gamma, \delta$ are equi-anharmonic.*

(ii) *If $J = 0$ and $I \neq 0$, then $\rho = -1$, 2 or $\frac{1}{2}$, and the points $\alpha, \beta, \gamma, \delta$ are harmonic.*

(iii) *The cross-ratios are all real or all imaginary according as $\Delta \gtrless 0$, and in the first case the points $\alpha, \beta, \gamma, \delta$ lie on a circle or they are collinear.*

For t_1, t_2, t_3 are all real or only one is real, according as $\Delta \gtrless 0$.

14. Ranges and Pencils. A set of collinear points is called a *range*: the line on which they lie is the *axis* of the range.

A set of concurrent lines is called a *pencil*: the point at which they meet is the *vertex* of the pencil.

15. Cross-ratio of a Pencil. (1) *If the pencil of four lines*

$$y=\mu_1 x, \quad y=\mu_2 x, \quad y=\mu_3 x, \quad y=\mu_4 x$$

is cut by any transversal $ax+by+c=0$ *at* P_1, P_2, P_3, P_4, *then*

$$(P_1P_2, P_3P_4)=(\mu_1\mu_2, \mu_3\mu_4).$$

For if (x_1, y_1), etc., are the coordinates of P_1, etc.,

$$(P_1P_2, P_3P_4)=\frac{P_1P_3 \,.\, P_2P_4}{P_1P_4 \,.\, P_2P_3}=\frac{(x_1-x_3)(x_2-x_4)}{(x_1-x_4)(x_2-x_3)}=(x_1x_2, x_3x_4),$$

and
$$x_1-x_3=-c\left\{\frac{1}{a+b\mu_1}-\frac{1}{a+b\mu_3}\right\}=\frac{bc(\mu_1-\mu_3)}{(a+b\mu_1)(a+b\mu_3)},$$

with similar equations.

Therefore $(x_1x_2, x_3x_4)=(\mu_1\mu_2, \mu_3\mu_4)$, and the result follows.

The ratio (P_1P_2, P_3P_4), which is the same for all transversals, is called *a cross-ratio of the pencil, and is denoted by* $O(P_1P_2, P_3P_4)$, where O is the vertex of the pencil.

If $O(P_1P_2, P_3P_4)=-1$, we say that *the pencil is harmonic*, and that OP_1, OP_2 and OP_3, OP_4 are pairs of *conjugate rays*.

(2) It follows that the cross-ratio of the pencil formed by the four lines OA, OB, OC, OD is given by

$$O(AB, CD)=\frac{\sin AOC \,.\, \sin BOD}{\sin AOD \,.\, \sin BOC}*,$$

where AOC is the least angle through which OA must be turned in order that it may coincide with OC (*H.A.*, V, 11): and so for the other angles.

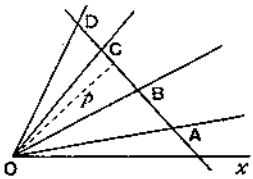


FIG. 4.

For denoting the angles xOA, xOB, xOC, xOD by α, β, γ, δ, we have

$$\mu_1-\mu_3=\tan\alpha-\tan\gamma=\frac{\sin(\alpha-\gamma)}{\cos\alpha\cos\gamma}=-\frac{\sin AOC}{\cos\alpha\cos\gamma},$$

with similar equations. Hence $O(AB, CD)$, which is equal to $(\mu_1\mu_2, \mu_3\mu_4)$, has the value stated above.

(3) *Or geometrically thus*: Let p be the length of the perpendicular from O to AD, then

$$AC \,.\, p=2\Delta AOC=OA \,.\, OC \sin AOC.$$

Using this and similar equations, we have

$$(AB, CD)=\frac{AC \,.\, BD}{BC \,.\, AD}=\frac{\sin AOC \,.\, \sin BOD}{\sin AOD \,.\, \sin BOC}.$$

This is the same for *all* transversals, and is called the *cross-ratio of the pencil, and is denoted by* $O(AB, CD)$.

* This is frequently taken as the definition of the cross-ratio of a pencil.

16. Homographic Ranges. (1) Let the variables x, x' (which may be complex) be connected by the homographic relation

$$pxx' + qx + rx' + s = 0. \quad \text{.....(A)}$$

Let the values of x, x' be represented by points X, X' on the same or on different axes.

If (a, a'), (b, b'), ... are pairs of corresponding values of x, x', the corresponding points being (A, A'), (B, B'), ... , then the ranges

$$(AB \ldots X \ldots), \quad (A'B' \ldots X' \ldots)$$

are said to be *homographic*. This is expressed by writing

$$(AB \ldots X \ldots) = (A'B' \ldots X') \text{ or simply } (X) = (X').$$

(2) It follows from Art. 12, (1), that *any four points of one range are equi-cross with the corresponding points of the other.*

(3) Conversely, *if a correspondence exists such that any four points A, B, C, X of one range and the corresponding points A', B', C', X' of another range are equi-cross, then the ranges are homographic.**

For we may regard X, X' as variable and the other points as fixed, then, since $(XA, BC) = (X'A', B'C')$, we have

$$\frac{x-b}{x-c} \cdot \frac{a-c}{a-b} = \frac{x'-b'}{x'-c'} \cdot \frac{a'-c'}{a'-b'}, \quad \text{.....(B)}$$

and this equation reduces to one of the same form as (A).

17. Vanishing Points. If $p \neq 0$, equation (A) can be written

$$\left(x + \frac{r}{p}\right)\left(x' + \frac{q}{p}\right) = \frac{qr}{p^2} - \frac{s}{p}, \quad \text{.....(D)}$$

that is to say,

$$IX \,.\, J'X' = (qr - ps)/p^2, \quad \text{.....(E)}$$

where I, J' are the points $x = -r/p$, $x' = -q/p$,

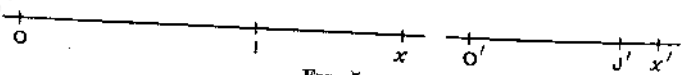


FIG. 5.

The points I, J' are called the *vanishing points*, and if ∞, ∞' are the points at infinity on the ranges, I corresponds to ∞' and J' to ∞.

18. Ranges on the Same Axis. (1) If two homographic ranges are on the same axis, two points F, G exist each of which corresponds to itself. These are the *self-corresponding* or *double points* of the ranges.

* In geometry, this statement is taken as the definition of homographic ranges.

The origin being the same for both ranges, F, G are given by

$$px^2+(q+r)x+s=0, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{F})$$

therefore $$OF+OG=-(q+r)/p=OI+OJ',$$

so that *FG and IJ' have the same mid-point,*

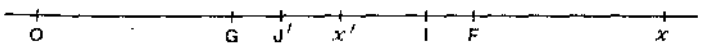


FIG. 6.

(2) If X, X' are corresponding points, since F corresponds to F and G to G, by equation (E),

$$IX\,.\,J'X'=IF\,.\,J'F=IG\,.\,J'G. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{G})$$

We also have such equations as

$$(FA, BC)=(FA', B'C'), \quad (XA, FG)=(X'A', FG). \quad \ldots\ldots\ldots\ldots(\mathbf{H})$$

Again, since $(XA, FG)=(X'A', FG)$, it follows that

$$(XX', FG)=(AA', FG)=\text{a constant}, \quad \ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{I})$$

and therefore

$$(XX', FG)=(I\infty', FG)=\frac{IF}{IG}=-\frac{pf+r}{pf+q}, \quad \ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{K})$$

where f is a root of equation (F).

19. Involution. (1) Suppose that two homographic ranges have the following property:

A pair of non-coincident corresponding points A, A' exists such that A may be supposed to belong to the first range and A' to the second, or A to the second and A' to the first.

We shall prove that *every pair of corresponding points (X, X') may be so regarded*, and we say that the ranges form an *involution.*

Let the homographic relation be $pxx'+qx+rx'+s=0$.

In this we may have $x=a$, $x'=a'$ and also $x=a'$, $x'=a$; therefore

$$paa'+qa+ra'+s=0, \quad paa'+qa'+ra+s=0;$$

hence $(q-r)(a-a')=0$; and thus $q=r$, for $a\neq a'$.

Hence the homographic relation is

$$pxx'+q(x+x')+s=0, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{A})$$

which is symmetrical with regard to x, x', and the result follows.

(2) Thus it follows from Art. 16, (2), that if (A, A'), (B, B'), ... (X, X')... are pairs of corresponding points in an involution, then

$$(AA'BB'\ldots XX'\ldots)=(A'AB'B\ldots X'X\ldots). \quad \ldots\ldots\ldots\ldots\ldots(\mathbf{B})$$

20. Centre and Double Points of an Involution.

(1) If $p \neq 0$, equation (A) of Art. 19 may be written

$$\left(x+\frac{q}{p}\right)\left(x'+\frac{q}{p}\right)=\frac{q^2}{p^2}-\frac{s}{p}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

The point $x=-\frac{q}{p}$ is called the *centre* of the involution, and if this point is taken as the origin O, the equation is of the form

$$xx'=k, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(D)}$$

where k is a constant.

(2) The *double points* or *foci* F, G are given by $x^2=k$, and if (A, A'), (B, B') ... are pairs of corresponding points,

$$OF^2=OG^2=OA \,.\, OA'=OB \,.\, OB'=\ldots=k. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(E)}$$

Therefore F, G *divide* AA', BB', ... *harmonically.*

(3) Distinct cases arise according as $k \gtrless 0$.

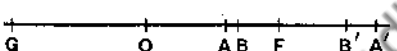


FIG. 7.

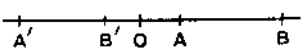


FIG. 8.

(i) *If* $k>0$, the foci are real and *one of the segments* AA', BB' *is entirely within the other.* The involution is said to be *positive* or *non-overlapping* (Fig. 7).

(ii) *If* $k<0$, the foci are imaginary, the segments AA', BB' overlap, and the involution is said to be *negative* or *overlapping* (Fig. 8).

(4) As special cases of equation (B),

$$(FG, AA')=(FG, A'A), \quad (FA, BA')=(FA', B'A). \quad \ldots\ldots\ldots\text{(F)}$$

21. Homographic Pencils. Let $y=\mu x$, $Y=\mu' X$ be the equations to two straight lines referred to different (or to the same) pairs of axes.

If μ, μ' have different values subject to the condition

$$p\mu\mu'+q\mu+r\mu'+s=0,$$

the lines $y=\mu x$, $Y=\mu' X$ are said to form *homographic pencils* in which these lines are corresponding rays.

Such pencils determine homographic ranges on any transversal. This follows from Art. 15.

If the homographic relation is $p\mu\mu'+q(\mu+\mu')+s=0$, the lines $y=\mu x$, $y=\mu' x$ form a *pencil in involution* (or simply an *involution*) in which these lines are corresponding rays.

Such a pencil determines a range in involution on any transversal.

22. Cross-ratios and a Four-point Figure. Let A, B, C, D be four points corresponding to the complex numbers z_1, z_2, z_3, z_4.

(i) *If one cross-ratio of z_1, z_2, z_3, z_4 is real, then all are real and A, B, C, D lie on a circle or they are collinear.*

(ii) *In the first case, if V is any point on the circle, then*

$$V(AD, BC) = (z_1z_4, z_2z_3).$$

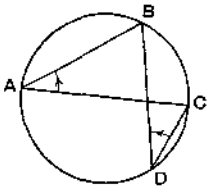


FIG. 9.

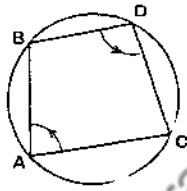


FIG. 10.

Let $$(z_1z_4, z_2z_3) = \frac{z_1 - z_2}{z_1 - z_3} \cdot \frac{z_4 - z_3}{z_4 - z_2} = k, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (\mathbf{A})$$

where k is real. By Art. 10, every cross-ratio of z_1, z_2, z_3, z_4 is real. Equating the amplitudes in (A), we have $\angle CAB + \angle BDC = 2m\pi + \text{am } k$, where m is an integer or zero. Now $\text{am } k = 0$ or π, according as $k \gtrless 0$; hence,

(i) *if* $k > 0$, $\angle CAB + \angle BDC = 0$, that is $\angle CAB = \angle CDB$, therefore the points are concyclic or collinear, and occur in one of the orders A, B, C, D or A, D, C, B (Fig. 9);

(ii) *if* $k > 0$, $\angle CAB + \angle BDC = \pi$ and A, B, C, D are concyclic or collinear, occurring in one of the orders A, B, D, C or A, C, D, B (Fig. 10).

Again, $$V(AD, BC) = \frac{\sin AVB}{\sin AVC} \cdot \frac{\sin DVC}{\sin DVB} = \pm \frac{AB}{AC} \cdot \frac{DC}{DB}, \quad \ldots\ldots\ldots\ldots (\mathbf{B})$$

where AB, etc., are the numerical measures of the lengths AB, etc. Also it is evident from the preceding that the sign is + or − according as $k \gtrless 0$.

Further, considering the moduli in (A),

$$\frac{AB}{AC} \cdot \frac{DC}{DB} = |k|,$$

and the last part of the theorem follows.

In particular, *if z_1, z_2, z_3, z_4 are harmonically related, the corresponding points lie on a circle or they are collinear, and in either case they form a harmonic system, as understood in modern geometry.**

* That is to say they subtend a harmonic pencil at any point on the circle.

23. Some Properties of a Four-point Figure. Let a, b, c A, B, C be the sides and angles of the triangle ABC and let D be an point in its plane. Take the positive direction of rotation as determine by a point which moves round the triangle from A to C to B.

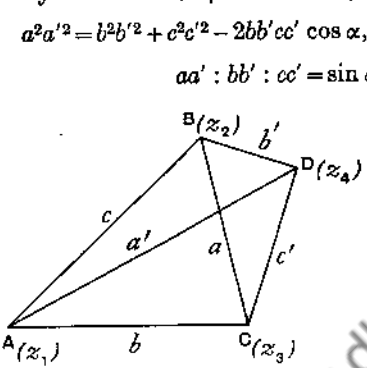
Let a', b', c' be the lengths of DA, DB, DC, and let A', B', C' be th angles BDC, CDA, ADB.

Then if $\alpha = A + A'$, $\beta = B + B'$, $\gamma = C + C'$, *we shall prove that*

$$a^2a'^2 = b^2b'^2 + c^2c'^2 - 2bb'cc' \cos\alpha, \text{ with two similar equations,} \quad \ldots\ldots(A$$

and

$$aa' : bb' : cc' = \sin\alpha : \sin\beta : \sin\gamma. \quad \ldots\ldots(B$$



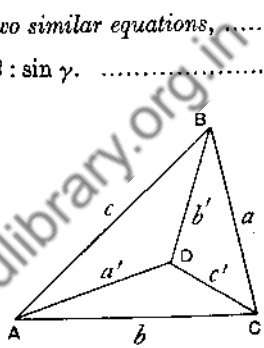


Fig. 11.

Proof. Let A, B, C, D be represented by the numbers z_1, z_2, z_3, z_4, an consider the identity

$$(z_2 - z_3)(z_1 - z_4) + (z_3 - z_1)(z_2 - z_4) + (z_1 - z_2)(z_3 - z_4) = 0. \quad \ldots\ldots($$

Let $\lambda, \mu, \nu, \lambda', \mu', \nu'$ be the angles, measured from 0 to 2π, which t directed lines BC, CA, AB, DA, DB, DC make with Ox, so that

$$z_3 - z_2 = a(\cos\lambda + \iota \sin\lambda), \text{ etc.}, \quad z_1 - z_4 = a'(\cos\lambda' + \iota \sin\lambda'), \text{ etc.};$$

then, from (C), we have

$$\Sigma aa'\{\cos(\lambda + \lambda') + \iota \sin(\lambda + \lambda')\} = 0,$$

and therefore, $\Sigma aa' \cos(\lambda + \lambda') = 0$, $\Sigma aa' \sin(\lambda + \lambda') = 0$.

It readily follows that

$$a^2a'^2 = b^2b'^2 + c^2c'^2 + 2bb'cc' \cos(\mu + \mu' - \nu - \nu') = 0, \quad \ldots\ldots($$

with two similar equations; also

$$\frac{aa'}{\sin(\mu + \mu' - \nu - \nu')} = \frac{bb'}{\sin(\nu + \nu' - \lambda - \lambda')} = \frac{cc'}{\sin(\lambda + \lambda' - \mu - \mu')}. \quad \ldots\ldots($$

Now A is the angle through which AC must be turned to lie along AI and thus, $A = \nu - (\pi + \mu)$, and simil. ly, $A' = \nu' - \mu'$;

hence, $$\mu + \mu' - \nu - \nu' = -(\pi + \alpha).$$

The equations (A) and (B) follow immediately from (D) and (E).

EXERCISE II

1. If the *distance between the points* (x_1, y_1), (x_2, y_2) is defined as the principal value of

$$\sqrt{\{(x_1-x_2)^2+(y_1-y_2)^2\}},$$

prove that the distance between any two points on the line $y=\iota x$ or on the line $y=-\iota x$ is zero.

2. If the tangent of the angle between the lines $y=mx+c$, $y=m'x+c'$ is defined by

$$\tan\theta=(m-m')/(1+mm'),$$

prove that if m or $m'=\pm\iota$, then $\tan\theta=\pm\iota$.

3. Show that the substitution

$$x=X\cos\alpha-Y\sin\alpha, \quad y=X\sin\alpha+Y\cos\alpha,$$

transforms the equations $y=\pm\iota x$ into $Y=\pm\iota X$.

That is to say, the equations $y=\pm\iota x$ are unaltered by turning the axes through an angle α.

4. If the equations to OA, OB, OC, OD are as under, verify the values given for $O(AB, CD)$:

(i) $$y=0, \quad x=0, \quad y=\mu x, \quad y=\mu' x,$$
$$O(AB, CD)=(0\infty, \mu\mu')=\mu/\mu'.$$

If α, β are linear functions of x, y, and the equations are

(ii) * $$\alpha=0, \quad \beta=0, \quad \alpha=\mu\beta, \quad \alpha=\mu'\beta,$$
$$O(AB, CD)=\mu/\mu'.$$

(iii) * $$\alpha-\mu_1\beta=0, \quad \alpha-\mu_2\beta=0, \quad \alpha-\mu_3\beta=0, \quad \alpha-\mu_4\beta=0,$$
$$O(AB, CD)=(\mu_1\mu_2, \mu_3\mu_4).$$

(iv) $$y=x\tan\alpha, \quad y=x\tan\alpha', \quad y=\iota x, \quad y=-\iota x,$$
$$O(AB, CD)=\cos 2(\alpha-\alpha')+\iota\sin 2(\alpha-\alpha').$$

[* Take $\alpha=0$, $\beta=0$ as axes.]

5. Prove that the lines $y=\pm\iota x$ are harmonic conjugates with regard to any two lines at right angles through O.

Also show that they form a pencil of constant cross-ratio with regard to any two lines through O which intersect at a given angle.

[This follows from the last example.]

6. If (AB, XY) is harmonic, then

(i) X, Y are inverse points for the circle on AB as diameter.

(ii) The circle on AB as diameter is cut orthogonally by any circle through X, Y.

(iii) If M, N are the mid-points of AB, XY,

$$AB^2+XY^2=4MN^2,$$

and if O is any point in AB,

$$2OM\,.\,ON=OA\,.\,OB+OX\,.\,OY.$$

7. Prove that $(PQ, AB)\,.\,(PQ, BC)=(PQ, AC)$.

8. If $(x-f)/(x-g)=k(x'-f)/(x'-g)$ where k is constant, the points x, x' describe homographic ranges of which f, g are self-corresponding points.

9. If the ranges $(abc \ldots x \ldots)$, $(a'b'c' \ldots x' \ldots)$ are homographic, the vanishing points I, J' are given by

$$\frac{x-b}{x-c}=\frac{a-b}{a-c}\cdot\frac{a'-c'}{a'-b'} \quad \text{and} \quad \frac{x'-b'}{x'-c'}=\frac{a'-b'}{a'-c'}\cdot\frac{a-c}{a-b}.$$

If the ranges are on the same axis, and the origin is the same for both, the self-corresponding points are given by

$$\frac{x-b}{x-c}\cdot\frac{x-c'}{x-b'}=\frac{a-b}{a-c}\cdot\frac{a'-c'}{a'-b'}.$$

[For the first equation put $x'=\infty$ in equation (B) of Art. 16. For the last part we have

$$(xa, bc)=(xa', b'c').]$$

10. If two homographic ranges have a common point O, the line joining corresponding points (x, x') passes through a fixed point V which is such that $OIVJ'$ is a parallelogram.

[The homographic relation is of the form $pxx'+qx+rx'=0$. Taking the axes of the ranges as OX, OY, the equation to xx' is

$$\frac{X}{x}+\frac{Y}{x'}=1 \quad \text{or} \quad p\left(\frac{X}{x}+\frac{Y}{x'}\right)+\frac{q}{x'}+\frac{r}{x}=0,$$

which passes through the point $(-r/p, -q/p)$.]

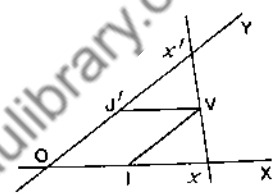


FIG. 12.

11. If $(0, a, b, x)$, $(0, a', b', x')$ are corresponding points on two homographic ranges, prove that

$$(ab'-a'b)xx'-a'b'(a-b)x+ab(a'-b')x'=0.$$

12. If two homographic pencils have a common ray $(\alpha=0)$, then corresponding rays intersect on a fixed line.

[Choose a pair of corresponding rays $\beta=0$, $\beta'=0$. Any other pair may be taken as $\alpha-\mu\beta=0$, $\alpha-\mu\beta'=0$, and these intersect on $\beta-\beta'=0$.]

13. If (A, A'), (B, B'), (X, X') are three pairs of points in involution, then

$$AB \,.\, XA' \,.\, X'B'=-A'B' \,.\, X'A \,.\, XB,$$

and conversely, if this relation holds, the pairs are in involution.

[For $(AX, BX')=(A'X', B'X).$]

14. If (A, A'), (B, B'), (C, C') are pairs of points in involution and L, M, N are the mid-points of AA', BB', CC', prove that

(i) $$AA'^2 \,.\, MN+BB'^2 \,.\, NL+CC'^2 \,.\, LM=-4MN \,.\, NL \,.\, LM.$$

(ii) $$\frac{LM}{LN}=\frac{AB \,.\, AB'}{AC \,.\, AC'}.$$

[Let O be the centre of the involution. Denoting OA, OL, ... by a, l, ..., we have $aa'=bb'=cc'=k$. Now prove that $AA'^2=4(l^2-k)$ and

$$2a(l-m)=a\{a+a'-(b+b')\}=(a-b)(a-b'), \text{ etc.}]$$

15. If (x, x') is any point-pair in the involution determined by the pairs (a, a'), (b, b'), the equation connecting x, x' is

$$xx'\{a+a'-(b+b')\}-(x+x')(aa'-bb')+aa'(b+b')-bb'(a+a')=0.$$

[We have $(ax, bx')=(a'x', b'x).$]

16. If (a, a'), (x, x') are point-pairs in an involution of which f, g are the foci, then

$$\frac{a-x}{a'-x}\cdot\frac{a-x'}{a'-x'}=-\frac{a-f}{a'-f}\cdot\frac{a-g}{a'-g}.$$

[We have $(xf, aa')=(x'f, a'a)=-(x'g, a'a)$, since $(fg, aa')=-1$.]

17. For the involution in which (β, γ) and (α, δ) are pairs of corresponding points, prove that

(i) The centre is the point $x=\dfrac{\beta\gamma-\alpha\delta}{\beta+\gamma-\alpha-\delta}$.

(ii) The foci are given by

$$x^2(\beta+\gamma-\alpha-\delta)-2x(\beta\gamma-\alpha\delta)+\beta\gamma(\alpha+\delta)-\alpha\delta(\beta+\gamma)=0.$$

(iii) If the centre is taken as origin, the involution is determined by $xx'=k^2$, where

$$k^2=\frac{(\beta-\alpha)(\beta-\delta)(\gamma-\alpha)(\gamma-\delta)}{(\beta+\gamma-\alpha-\delta)^2}.$$

[If h is the centre, then

$$(\beta-h)(\gamma-h)=(\alpha-h)(\delta-h)=k^2.$$

The equation in (ii) is given by $(x\beta, \alpha\gamma)=(x\gamma, \delta\beta)$.]

18. If (z_1z_3, z_2z_4) is harmonic and a is the mid-point of z_2z_4, prove that

(i) $\overline{az_1}\cdot\overline{az_3}=\overline{az_2}^2$ where $\overline{az_1}=\text{mod } az_1$, etc.

(ii) The line z_2z_4 bisects the angle z_1az_3.

19. In the quadrilateral $ABDC$, given that the sum of the opposite angles A and D is α and that $AB\,.\,CD=CA\,.\,BD$, prove that

$$\angle ABC-\angle ADC=\tfrac{1}{2}(\pi-\alpha) \quad \text{and} \quad AD\,.\,BC=2\sin\frac{\alpha}{2}\cdot AB\,.\,CD.$$

20. Given three points A, B, C corresponding to complex numbers z_1, z_2, z_3, it is required to find D corresponding to z_4 such that

$$(z_1z_4, z_2z_3)=\rho=r(\cos\alpha+i\sin\alpha),$$

where ρ is a given complex number. Prove the following construction.

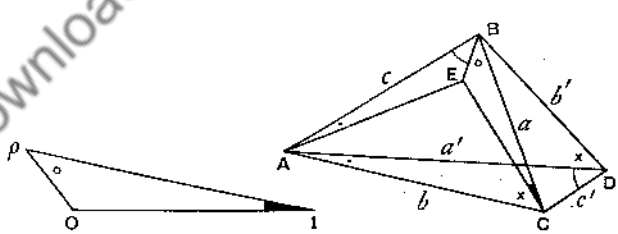


FIG. 13.

Mark the points 1, ρ, and make $\triangle BEC$ directly similar to $\triangle\rho O1$. Draw $\triangle ACD$ directly similar to $\triangle AEB$. Then D is the required point.

[Prove that the triangles ACE, ADB are similar; also that

$$\angle BEC=\angle CAB+\angle BDC \quad \text{and} \quad BE/CE=cc'/bb'.$$

Hence, if z_4 corresponds to D and $(z_1z_4, z_2z_3)=\rho'$, we have $|\rho'|=cc'/bb'=r$; and am $\rho'=2m\pi+\angle CAB+\angle BDC=2m\pi+\alpha$. Therefore $\rho'=\rho$.]

21. (i) Given three points A, B, C, it is required to find a point D such that A, B, C, D are equi-anharmonic.

(ii) Show that there are two positions (D_1, D_2) of D and no more; also that for each of these

$$DA : DB : DC = 1/a : 1/b : 1/c.$$

(iii) If $\triangle ABC$ is named so that $\angle A \leqslant 60°$, $\angle B < 120°$, then the angles which BC, CA, AB subtend at D_1 are

$$A+60°, \quad B+60°, \quad C+60° \quad \text{or} \quad 360°-(C+60°),$$

and the angles which they subtend at D_2 are

$$60°-A, \quad \pm(60°-B), \quad \pm(60°-C).$$

[That there are only two positions of D is due to the fact that if any cross-ratio of A, B, C, D is $-\omega$ or $-\omega^2$, so also is each of the others.

Let $\omega = \cos\frac{2\pi}{3} + \iota \sin\frac{2\pi}{3}$, then $\text{am}(-\omega) = 2\pi - \frac{\pi}{3}$, $\text{am}(-\omega^2) = \frac{\pi}{3}$; and if in Ex. 20 we take $\alpha = 2\pi - \frac{\pi}{3}$ or $\frac{\pi}{3}$, we have the following:

Construction. Draw the equilateral triangles BE_1C, BE_2C and make the triangles ACD_1, ACD_2 directly similar to AE_1B, AE_2B. Then D_1, D_2 are the required points. The rest follows from Art. 23.]

22. Let $u=0$, $u'=0$ be equations of the second degree in x, y with real coefficients. Let the conics represented by $u=0$, $u'=0$ meet in P, P', Q, Q'.

Prove that

(i) If one of these points (Q) is imaginary, then another (Q') is the conjugate imaginary point. (Art. 6 and *H.A.*, V, 14.)

(ii) Let A, B, C be the points of intersection of (PP', QQ'), $(PQ', P'Q)$, $(PQ, P'Q')$. Then A, B, C are all real unless two points of intersection (P, P') are real and two (Q, Q') are imaginary.

In the latter case A is real, B and C are conjugate imaginary points, so that the line BC is real. (Art. 6, Ex. 1.)

The triangle ABC is the diagonal point triangle of the quadrangle $PP'Q'Q$, *and is* self-conjugate *with regard to every conic through P, P', Q', Q.*

23. In the last example, if the equations are

$$u \equiv 2xy - y^2 + x - 2 = 0, \quad v \equiv x^2 - y = 0,$$

prove that the coordinates of A, B, C are

$$\left(\frac{1}{4}, -\frac{5}{4}\right), \quad \left(\frac{2 \pm \iota\sqrt{3}}{2}, \quad \frac{7 \pm \iota\sqrt{3}}{4}\right),$$

and that the equation of BC is $2x - 4y + 5 = 0$.

Verify that BC is the polar of A with regard to each of the conics.

24. Find the vertices of the common self-conjugate triangle of the conics whose equations are

$$x^2 - 2y^2 + 10y - 13 = 0, \quad 5x^2 - 8x + 6y - 7 = 0,$$

showing that the coordinates of these points are $(1, 1)$, $(2, 2)$, $(-2, \frac{1}{5}2)$.

CHAPTER II

THE QUADRATIC AND SYSTEMS OF QUADRATICS

1. Resultant of Two Quadratics. Let α, β and α', β' be the roots of the equations

$$u = ax^2 + 2bx + c = 0, \quad u' = a'x^2 + 2b'x + c' = 0$$

respectively. These equations have a common root if and only if

$$(\alpha - \alpha')(\alpha - \beta')(\beta - \alpha')(\beta - \beta') = 0.$$

Let $$R = a^2a'^2(\alpha - \alpha')(\alpha - \beta')(\beta - \alpha')(\beta - \beta'). \quad \text{.....(A)}$$

Then it is easy to see that R can be expressed in the following forms.

$$R = a'^2(a\alpha'^2 + 2b\alpha' + c)(a\beta'^2 + 2b\beta' + c) \quad \text{.....(B)}$$

$$= (ac' - a'c)^2 - 4(ab' - a'b)(bc' - b'c) \quad \text{.....(C)}$$

$$= (ac' + a'c - 2bb')^2 - 4(ac - b^2)(a'c' - b'^2). \quad \text{.....(D)}$$

Thus $R = 0$ *is a necessary and sufficient condition that the equations may have a common root.*

Moreover, R is a rational integral function of the coefficients, and is of the lowest degree possible that this may be the case.

On this account R is called the *resultant* of $u = 0$, $u' = 0$.

2. Theorem. *If $u = 0$, $u' = 0$ are quadratic equations with real coefficients, the resultant R is negative if, and only if, the roots (α, β), (α', β') of both equations are real and the intervals (α, β), (α', β') overlap.*

Proof. (i) *Let the roots of both equations be real.* We have

$$R = a^2a'^2(\alpha - \alpha')(\alpha - \beta')(\beta - \alpha')(\beta - \beta').$$

Now $(\alpha - \alpha')(\alpha - \beta')$ is negative if and only if α lies between α' and β'. Also $(\beta - \alpha')(\beta - \beta')$ is negative if and only if β lies between α' and β'.

Hence R is negative if and only if one and not both of the roots α, β lie between α' and β', i.e. when the intervals (α, β), (α', β') overlap.

(ii) *Let the roots of at least one of the equations, say those of the first, be imaginary. Then, taking the equations as in the last article, we have $b^2 < ac$. and, by equation* (C),

$$\frac{R}{a^2c^2} = \left(\frac{c'}{c} - \frac{a'}{a}\right)^2 - \frac{4b^2}{ac}\left(\frac{b'}{b} - \frac{a'}{a}\right)\left(\frac{c'}{c} - \frac{b'}{b}\right).$$

Hence, $$R > \left\{\left(\frac{b'}{b}-\frac{a'}{a}\right)+\left(\frac{c'}{c}-\frac{b'}{b}\right)\right\}^2 - 4\left(\frac{b'}{b}-\frac{a'}{a}\right)\left(\frac{c'}{c}-\frac{b'}{b}\right)$$
$$> \left\{\left(\frac{b'}{b}-\frac{a'}{a}\right)-\left(\frac{c'}{c}-\frac{b'}{b}\right)\right\}^2$$

Therefore R cannot be negative.

3. The Harmonic Relation. Let (α, β), (α', β') be the roots of

$$u \equiv ax^2 + 2bx + c = 0, \quad u' \equiv a'x^2 + 2b'x + c' = 0$$

respectively.

(1) *The condition that* $(\alpha\beta, \alpha'\beta')$ *may be harmonic is* $ac' + a'c - 2bb' = 0$.

For by Ch. I, 8, the condition is $2(\alpha\beta + \alpha'\beta') = (\alpha + \beta)(\alpha' + \beta')$,

giving $$\frac{2c}{a} + \frac{2c'}{a'} = 4\frac{b}{a}\cdot\frac{b'}{a'} \quad \text{or} \quad ac' + a'c = 2bb'.$$

When this is the case we say that *the quadratics are related harmonically.*

(2) *It is required to find a quadratic which is related harmonically to* $u = 0$ *and also to* $u' = 0$.

Let the required equation be $px^2 + 2qx + r = 0$; then by the preceding,

$$ar - 2bq + cp = 0 \quad \text{and} \quad a'r - 2b'q + c'p = 0. \quad \ldots\ldots\ldots\ldots\text{(A)}$$

Eliminating r, $-2q$, p from these equations, we have

$$J \equiv \begin{vmatrix} 1 & -x & x^2 \\ a & b & c \\ a' & b' & c' \end{vmatrix} = 0, \quad \ldots\ldots\ldots\ldots\text{(B)}$$

which may be written

$$J \equiv (ab')x^2 + (ac')x + (bc') = 0. \quad \ldots\ldots\ldots\ldots\text{(C)}$$

This is the required equation.

(3) *For all values of* λ, *the quadratic* $J = 0$ *is related harmonically to* $u - \lambda u' = 0$.

For by equations (A),

$$(a - \lambda a')r - 2(b - \lambda b')q + (c - \lambda c')p = 0.$$

4. The Function J is of great importance in the theory of quadratics.

(1) It may be written in the forms

$$J = \begin{vmatrix} 1 & -x & x^2 \\ a & b & c \\ a' & b' & c' \end{vmatrix} = \begin{vmatrix} ax+b & bx+c \\ a'x+b' & b'x+c' \end{vmatrix},$$

or $$J = (ab')x^2 + (ac')x + (bc').$$

The second form is derived from the first by adding x times the second column to the third and x times the first column to the second.

(2) *The roots of* $J=0$ *are real or imaginary according as the resultant* R *of* $u=0$, $u'=0$ *is positive or negative. Also if the roots are equal, then* u, u' *have a common factor.*

For $$R=(ac')^2-4(ab')(bc').$$

(3) If y is introduced so as to make u, u' homogeneous, and we write

$$u=ax^2+2bxy+cy^2, \quad u'=a'x^2+2b'xy+c'y^2,$$

the *Jacobian* of u, u' is defined as

$$\begin{vmatrix} \frac{\partial u}{\partial x} & \frac{\partial u}{\partial y} \\ \frac{\partial u'}{\partial x} & \frac{\partial u'}{\partial y} \end{vmatrix} = 4 \begin{vmatrix} ax+by & bx+cy \\ a'x+b'y & b'x+c'y \end{vmatrix} = 4J.$$

5. The Involution determined by Two Quadratics. Let (α, β), (α', β') be the roots of the quadratics $u=0$, $u'=0$, those of $J=0$ being x_1, x_2.

(1) *The points* x_1, x_2 *are the foci of the involution in which* (α, β), (α', β') *are pairs of corresponding points.*

For $J=0$ is harmonically related to $u=0$ and $u'=0$; and therefore $(x_1x_2, \alpha\beta)$ and $(x_1x_2, \alpha'\beta')$ are both harmonic.

(2) *If* ξ, ξ' *are the roots of* $u-\lambda u'=0$, *where* λ *has any value whatever, then* ξ, ξ' *are corresponding points in the involution.*

For $J=0$ is harmonically related to $u-\lambda u'=0$.

(3) *The character of the involution* depends on the value of R, the resultant of $u=0$ and $u'=0$.

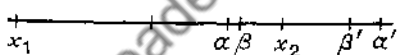


FIG. 14.

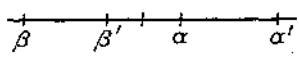


FIG. 15.

(i) *If* $R>0$ then x_1, x_2 are real, one of the intervals $(\alpha\beta)$, $(\alpha'\beta')$ is entirely within the other, and the involution is *non-overlapping* (Fig. 14).

(ii) *If* $R<0$, *then* x_1, x_2 *are imaginary and the involution is overlapping* (Fig. 15).

(iii) *If* $R=0$, then $x_1=x_2$ and the involution consists of pairs of points, one of which coincides with x_1, x_2, the other being anywhere on the axis.

6. Another Form of J. If the point x is a focus of the involution in which (α, β), (α', β') are pairs of corresponding points, we have

$$(x\alpha, \beta\alpha')=(x\beta, \alpha\beta'),$$

which reduces to $$(x-\alpha)(x-\alpha')(\beta-\beta')+(x-\beta)(x-\beta')(\alpha-\alpha')=0.$$

This equation has the same roots as $J=0$, and comparing the coefficients of x^2, we find that

$$2J = aa'\{(x-\alpha)(x-\alpha')(\beta-\beta')+(x-\beta)(x-\beta')(\alpha-\alpha')\}.$$

7. Theorem. *If λ_1, λ_2 are the values of λ given by*

$$\lambda^2(a'c'-b'^2)-\lambda(ac'+a'c-2bb')+ac-b^2=0, \quad \ldots\ldots\ldots\ldots\ldots\ldots(A)$$

and x_1, x_2 are the roots of $J=0$, then

$$u-\lambda_1 u' = (a-\lambda_1 a')(x-x_1)^2 \quad \textit{and} \quad u-\lambda_2 u' = (a-\lambda_2 a')(x-x_2)^2; \quad \ldots(B)$$

also

$$\lambda_1 = \frac{ax_1+b}{a'x_1+b} \quad \textit{and} \quad \lambda_2 = \frac{ax_2+b}{a'x_2+b'}. \quad \ldots\ldots\ldots\ldots\ldots\ldots(C)$$

For if ξ, ξ' are the roots of

$$u-\lambda u' = (a-\lambda a')x^2+2(b-\lambda b')x+c-\lambda c'=0, \quad \ldots\ldots\ldots\ldots\ldots\ldots(D)$$

then

$$u-\lambda u' = (a-\lambda a')(x-\xi)(x-\xi'), \quad \ldots\ldots\ldots\ldots\ldots\ldots(E)$$

and the condition that $\xi=\xi'$ is

$$(a-\lambda a')(c-\lambda c') = (b-\lambda b')^2,$$

which is the same equation as (A). If, then, this equation holds, ξ is a focus of the involution determined by $u=0$, $u'=0$, and therefore

$$\xi=\xi'=x_1 \quad \text{or} \quad x_2.$$

If λ_1, λ_2 are the corresponding values of λ, we have by (E)

$$u-\lambda_1 u' = (a-\lambda_1 a')(x-x_1)^2,$$

with a similar equation involving λ_2, x_2.

Also when $\lambda=\lambda_1$, each root of (D) is equal to x_1, therefore

$$x_1 = -\frac{b-\lambda_1 b'}{a-\lambda_1 a'}, \quad \text{giving} \quad \lambda_1 = \frac{ax_1+b}{a'x_1+b},$$

with a similar result when $\lambda=\lambda_2$.

NOTE. It follows that equation (A) is transformed into $J=0$ by the substitution

$$\lambda = (ax+b)/(a'x+b').$$

8. Theorem. *Constants A, B, A', B', x_1, x_2 can be found so that*

$$u \equiv ax^2+2bx+c \equiv A(x-x_1)^2+B(x-x_2)^2,$$
$$u' \equiv a'x^2+2b'x+c' \equiv A'(x-x_1)^2+B'(x-x_2)^2,$$

except when u, u' have a common factor.

If $u \not\equiv u'$, then u and u' are obtained in the required form from equations (B) of the last article, by eliminating u' and u in turn.

If u, u' have a common factor, then $x_1=x_2$, $\lambda_1=\lambda_2$, the equations (B) become identical, and u, u' cannot be so expressed.

Or ab initio thus—assuming the above identities, expand and equate coefficients, therefore

$$A+B=a. \quad \ldots\ldots\ldots(\mathbf{A}) \qquad A'+B'=a'. \quad \ldots\ldots\ldots(\mathbf{D})$$

$$Ax_1+Bx_2=-b. \quad \ldots\ldots(\mathbf{B}) \qquad A'x_1+B'x_2=-b'. \quad \ldots\ldots(\mathbf{E})$$

$$Ax_1^2+Bx_2^2=c. \quad \ldots\ldots\ldots(\mathbf{C}) \qquad A'x_1^2+B'x_2^2=c'. \quad \ldots\ldots\ldots(\mathbf{F})$$

Eliminating A, B from equations (A), (B), (C),

$$\begin{vmatrix} 1 & 1 & a \\ x_1 & x_2 & -b \\ x_1^2 & x_2^2 & c \end{vmatrix} = 0.$$

Expanding and dividing by x_1-x_2, we have, *except when* $x_1=x_2$,

$$ax_1x_2+b(x_1+x_2)+c=0. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{G})$$

Similarly, from (D), (E), (F),

$$a'x_1x_2+b'(x_1+x_2)+c'=0. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{H})$$

Eliminating x_2 from (G), (H),

$$\begin{vmatrix} ax_1+b & bx_1+c \\ a'x_1+b' & b'x_1+c' \end{vmatrix} = 0.$$

Therefore x_1 and, by symmetry, x_2 are the roots of

$$J \equiv \begin{vmatrix} ax+b & bx+c \\ a'x+b' & b'x+c' \end{vmatrix} = 0. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{I})$$

The values of A, B, A', B' can then be found from (A), (B), (D), (E).

The theorem may be stated thus:

Let $u \equiv ax^2+2bxy+cy^2, \quad u' \equiv a'x^2+2b'xy+c'y^2,$

then if u, u' *have no common factor, they may be expressed as follows:*

$$u \equiv AX^2+BY^2, \quad u' \equiv A'X^2+B'Y^2,$$

where X, Y *are the factors of* J *and* A, B, A', B' *are constants.*

This is called the *canonical form* of two quadratics.

Ex. 1. *Determine the constants so that*

$$5x^2+2x+11 \equiv A(x-a)^2+B(x-b)^2,$$
$$x^2-8x-2 \equiv A'(x-a)^2+B'(x-b)^2.$$

Here a, b are the roots of

$$J \equiv \begin{vmatrix} 5x+1, & x+11 \\ x-4, & -4x-2 \end{vmatrix} = 0,$$

giving $a=1$, $b=-2$. By equating coefficients

$$\left.\begin{matrix} A+B=5, \\ A+4B=11, \end{matrix}\right\} \therefore A=3, \ B=2; \qquad \left.\begin{matrix} A'+B'=1, \\ A'+4B'=-2, \end{matrix}\right\} \therefore A'=2, \ B'=-1.$$

Thus

$$5x^2+2x+11 \equiv 3(x-1)^2+2(x+2)^2,$$
$$x^2-8x-2 = 2(x-1)^2-(x+2)^2.$$

9. Linear Transformation of Quadratics. Consider the transformation of $u \equiv ax^2 + 2bxy + cy^2$ into $U \equiv AX^2 + 2BXY + CY^2$ by the substitution $x = lX + mY, \quad y = l'X + m'Y.$

(1) *It will be shown that* * $AC - B^2 = (lm' - l'm)^2(ac - b^2)$. .....(A)

Let α, β be the values of x/y for which $u = 0$, and let α_1, β_1 be the corresponding values of X/Y, so that

$$\alpha = \frac{l\alpha_1 + m}{l'\alpha_1 + m'} \quad \text{and} \quad \alpha_1 = \frac{-m + \alpha m'}{l - \alpha l'}, \quad \text{.....(B)}$$

with similar equations connecting β, β_1. Now

$$x - \alpha y = (l - \alpha l')X + (m - \alpha m')Y = (l - \alpha l')(X - \alpha_1 Y);$$

and similarly $x - \beta y = (l - \beta l')(X - \beta_1 Y)$. .....(C)

Also, since $u = a(x - \alpha y)(x - \beta y)$ and $U = A(X - \alpha_1 Y)(X - \beta_1 Y)$;

therefore $A = a(l - \alpha l')(l - \beta l')$. .....(D)

Again, $\alpha_1 - \beta_1 = \dfrac{-m + \alpha m'}{l - \alpha l'} - \dfrac{-m + \beta m'}{l - \beta l'} = \dfrac{(lm' - l'm)(\alpha - \beta)}{(l - \alpha l')(l - \beta l')}$, ...(E)

and therefore by (D), $A(\alpha_1 - \beta_1) = a(\alpha - \beta)(lm' - l'm)$.

Now $a^2(\alpha - \beta)^2 = 4(b^2 - ac)$ and $A^2(\alpha_1 - \beta_1)^2 = 4(B^2 - AC)$;

whence equation (A) follows.

(2) *Further, if, by the same substitution,* $u' \equiv a'x^2 + 2b'xy + c'y^2$ *is transformed into* $U' \equiv A'X^2 + 2B'XY + C'Y^2$, *we shall show that*

$$AC' + A'C - 2BB' = (lm' - l'm)^2(ac' + a'c - 2bb'). \quad \text{.....(F)}$$

Proof. For all values of k, we have

$$ax^2 + 2bxy + cy^2 + k(a'x^2 + 2b'xy + c'y^2)$$
$$\equiv AX^2 + 2BXY + CY^2 + k(A'X^2 + 2B'XY + C'Y^2).$$

If one side of this identity is a perfect square, so also is the other. Therefore the following equations in k are identical:

$$(a + ka')(c + kc') - (b + kb')^2 = 0,$$
$$(A + kA')(C + kC') - (B + kB')^2 = 0.$$

Comparing coefficients, we find that

$$\frac{AC' + A'C - 2BB'}{ac' + a'c - 2bb'} = \frac{AC - B^2}{ac - b^2} = (lm' - l'm)^2.$$

On account of these properties, the functions $ac - b^2$ and $ac' + a'c - 2bb'$ are called *invariants*.

* This can also be proved by a method similar to that of Art. 15 of this chapter.

It can be seen *a priori* that $ac-b^2$ is a factor of $AC-B^2$, and that the remaining factor is independent of a, b, c.

For if the first expression vanishes, so does the second, and A, B, C are of the first degree in a, b, c.

(3) *If* $J=(ab')x^2+(ac')xy+(bc')y^2$, $J'=(AB')X^2+(AC')XY+(BC')Y^2$,

then $$J'=(lm'-l'm)J. \quad \text{.....(G)}$$

For by Art. 6, $$2J=uu'\left\{\frac{\alpha-\alpha'}{(x-\alpha y)(x-\alpha' y)}+\frac{\beta-\beta'}{(x-\beta y)(x-\beta' y)}\right\}; \quad \text{.....(H)}$$

and by equations similar to (C), (D) of this article,

$$\frac{\alpha_1-\alpha_1'}{(X-\alpha_1 Y)(X-\alpha_1' Y)}=(lm'-l'm)\cdot\frac{\alpha-\alpha'}{(x-\alpha y)(x-\alpha' y)},$$

with a similar equation involving β, β'.

Since $u=U$ and $u'=U'$, the result follows at once.

On this account J is called a *covariant* of u, u'.

Ex. 1. *If* $$u=ax^2+2bxy+cy^2=AX^2+BY^2$$

and $$u'=a'x^2+2b'xy+c'y^2=A'X^2+B'Y^2$$

where $X=x-x_1y$, $Y=x-x_2y$, *prove that, if* R *is the resultant of* u, u',

$$\frac{AB}{ac-b^2}=\frac{AB'+A'B}{ac'+a'c-2bb'}=\frac{(ab'-a'b)^2}{R},$$

The determinant of transformation from X, Y to x, y is x_1-x_2; therefore,

$$ac-b^2=(x_1-x_2)^2AB,$$

and

$$ac'+a'c-2bb'=(x_1-x_2)^2(AB'+A'B).$$

Now x_1, x_2 are the roots of $(ab')x^2+(ac')x+(bc')=0$; therefore,

$$(ab')^2(x_1-x_2)^2=(ac')^2-4(ab')(bc')=R,$$

and the results follow immediately.

10. Homographic Transformation. Let $u\equiv ax^2+2bx+c$ be transformed into $U\equiv AX^2+2BX+C$ by the homographic substitution

$$x=(lX+m)/(l'X+m').$$

Then, multiplying by $(l'X+m')^2$ to remove fractions, it will be seen that the coefficients A, B, C are the same as in Art. 9; therefore,

$$AC-B^2=(lm'-l'm)^2(ac-b^2).$$

Moreover, if $u'\equiv a'x^2+2b'x+c'$ is transformed in the same way, then by Art. 9, (3), the equation

$$J\equiv(ab')x^2+(ac')x+(bc')=0$$

is transformed into

$$J\equiv(AB')X^2+(AC')X+(BC')=0.$$

11. Graph of $(ax^2+2bx+c)/(a'x^2+2b'x+c')$.

(1) Let (α, β), (α', β') be the roots of

$$u \equiv ax^2+2bx+c=0, \quad u' \equiv a'x^2+2b'x+c'=0.$$

Assume that a, a' are both positive. This involves no loss of generality. Let $y=u/u'$, then

$$y(a'x^2+2b'x+c')=ax^2+2bx+c;$$

$$\therefore \ (a'y-a)x^2+2(b'y-b)x+c'y-c=0;$$

$$\therefore \ x=\frac{-b'y+b\pm\sqrt{Q}}{a'y-a}, \quad \text{.........................(A)}$$

where
$$Q=(b'y-b)^2-(a'y-a)(c'y-c)$$
$$=(b'^2-a'c')y^2+(ac'+ca'-2bb')y+b^2-ac$$
$$=(b'^2-a'c')(y-y_1)(y-y_2), \quad \text{.........................(B)}$$

where y_1, y_2 are the roots of $Q=0$.

Therefore x is real if, and only if, $Q \geqslant 0$.

If R is the resultant of $u=0$, $u'=0$, then

$$R=(ac'+ca'-2bb')^2-(ac-b^2)(a'c'-b'^2),$$

and y_1, y_2 are real or imaginary according as $R \gtrless 0$. If y_1, y_2 are real, they are turning values of y, and the corresponding values x_1, x_2 of x are given by

$$x_1=\frac{-b'y_1+b}{a'y_1-a}, \quad x_2=\frac{-b'y_2+b}{a'y_2-a}. \quad \text{.....................(C)}$$

Now $R<0$ if, and only if, the roots of both $u=0$ and $u'=0$ are real and the intervals $(\alpha\beta')$, $(\alpha'\beta')$ overlap * (Art. 2); and we consider various cases which can arise.

First Case. If $R>0$, y_1 and y_2 are real, and the condition that $Q>0$ is as follows:

(i) *If* $b'^2>a'c'$, y cannot lie between y_1 and y_2. Hence if $y_1>y_2$, y_1 is a minimum, and y_2 a maximum value of y.

(ii) *If* $b'^2<a'c'$, y must lie between y_1 and y_2, and if $y_1>y_2$, y_1 is a maximum value of y.

(iii) *If* $b'^2=a'c'$, then u' is a perfect square, and one of the two y_1, y_2 is infinite.

Second Case. If $R<0$, the roots of $u=0$, $u'=0$ are real Art. 2, (ii), so that $b^2>ac$ and $b'^2>a'c'$. Also y_1, y_2 are imaginary. Hence Q is positive for all values of y, and y may have any real value.

* In this case the roots of $u=0$, $u'=0$ are said to *interlace*.

Third Case. If $R=0$, u and u' have a common factor, say $x-\alpha$, and then

$$y=\frac{a(x-\alpha)(x-\beta)}{a'(x-\alpha)(x-\beta')},$$

which is equivalent to $(x-\alpha)\{a'(x-\beta')y-a(x-\beta)\}=0$.

Therefore the graph consists of a *rectangular hyperbola, and the line* $x-\alpha=0$.

(2) Further information can be obtained by considering the value of $\frac{dy}{dx}$.

We have $\frac{dy}{dx}=2\{(ax+b)(a'x^2+2b'x+c')-(a'x+b')(ax^2+2bx+c)\}/u'^2$

$$=2\{(ax+b)(b'x+c')-(bx+c)(a'x+b')\}/u'^2$$
$$=2\{(ab')x^2+(ac')x+(bc')\}/u'^2$$
$$=2(ab')(x-x_1)(x-x_2)/u'^2, \quad \text{.....(D)}$$

where x_1, x_2 are the roots of $J\equiv(ab')x^2+(ac')x+(bc')=0$.

If x has either of these values, then

$$\frac{ax+b}{a'x+b'}=\frac{bx+c}{b'x+c'}=\frac{u}{u'}=y,$$

so that the corresponding values y_1, y_2 of y are given by

$$y_1=\frac{ax_1+b}{a'x_1+b'}, \quad y_2=\frac{ax_2+b}{a'x_2+b'}. \quad \text{.....(E)}$$

These values of y, if real and distinct, are turning values, and there can be no others.

It is easily seen that these results are in agreement with the preceding. For equations (C) and (E) are identical; also x_1, x_2 (and therefore y_1, y_2) are real or imaginary according as $(ac')^2-4(ab')(bc')\gtrless 0$, i.e. $R\gtrless 0$.

Considering various cases which can arise, we have the following.

First Case. If $R>0$, then x_1, x_2 are real. Let $x_1<x_2$.

(i) *If* $(ab')>0$, the signs of $\frac{dy}{dx}$ as x passes from $-\infty$ to ∞ are shown below:

x	$-\infty$		x_1		x_2		$+\infty$
$\frac{dy}{dx}$		$+$	0	$-$	0	$+$	

Therefore x_1 gives a maximum and x_2 a minimum value of y.

(ii) *If* $(ab')<0$, the signs are reversed, x_1 giving a minimum and x_2 a maximum value.

(iii) *If* $(ab')=0$, one of the two x_1, x_2 (say x_1) is infinite, and then by (E) we have $y_1=b/b'=a/a'$. In this case

$$\frac{a}{a_1}-y=\frac{(ac')}{a'(a'x^2+2b'x+c')}. \quad \text{.....(F)}$$

Second Case. *If* $R<0$, $\frac{dy}{dx}$ always has the same sign as (ab'), and y has no turning values.

Third Case. *If* $R=0$, then $x_1=x_2=-\frac{(ac')}{2(ab')}$. Also the equations $u=0$, $u'=0$ have a common root α, which is equal to $-\frac{(ac')}{2(ab')}$.

Thus $x_1=x_2=\alpha$; *and, corresponding to the value* x_1 *of* x, y *may have any value whatever*, which agrees with the third case of the last section.

In tracing the graph, it is to be noted that y is a continuous function of x, except for $x=\alpha'$, $x=\beta'$.

12. A Linear Transformation. The equation $y=u/u'$ may be reduced to a simpler form, thus: We have

$$\frac{a}{a'}-y=\frac{a}{a'}-\frac{u}{u'}=\frac{2(ab')x+(ac')}{a'(a'x^2+2b'x+c')}.$$

Hence if $(ab')\neq 0$, the substitution

$$X=2(ab')x+(ac'), \quad Y=a-a'y \quad \text{.....(G)}$$

reduces the equation to

$$Y=\frac{X}{A'X^2+2B'X+C'}, \quad \text{.....(H)}$$

where $A'X^2+2B'X+C'\equiv a'x^2+2b'x+c'$.

A comparison of coefficients shows that

$$A'=\frac{a'}{4(ab')^2}, \quad B'=\frac{2b'(ab')-a'(ac')}{4(ab')^2}, \quad \text{.....(I)}$$

and since the determinant of transformation from X to x is $2(ab')$,

$$a'c'-b'^2=4(ab')^2(A'C'-B'^2). \quad \text{.....(J)}$$

We have also

$$\frac{dY}{dX}=-\frac{A'X^2-C'}{u'^2}. \quad \text{.....(K)}$$

Hence the turning values of Y (which correspond to those of y) are given by

$$A'X^2-C'=0.$$

Points of Inflexion. (i) *If* $(ab')\neq 0$, these are given by $\frac{d^2Y}{dX^2}=0$, or by

$$2(A'X+B')(A'X^2-C')=A'X(A'X^2+2B'X+C'), \quad \text{.....(L)}$$

giving

$$X^3-3\frac{C'}{A'}X-2\frac{B'C'}{A'^2}=0. \quad \text{.....(M)}$$

This equation has one or three real roots according as

$$\left(\frac{2B'C'}{A'^2}\right)^2 - 4\left(\frac{C'}{A'}\right)^3 \lessgtr 0, \quad \text{i.e. according as} \quad B'^2 \lessgtr A'C'.$$

Therefore *the curve represented by* $y = u/u'$ *has one or three points of inflexion according as the roots of* $u' = 0$ *are real or imaginary.*

(ii) *If* $(ab') = 0$, we use equation (**F**). The points of inflection are given by

$$\frac{d^2y}{dx^2} = 0, \quad \text{or} \quad 4(a'x + b') - a'u' = 0, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{N})$$

giving

$$3a'^2x^2 + 6a'b'x + 4b'^2 - a'c' = 0. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{O})$$

The roots of this equation are real or imaginary according as

$$(3a'b')^2 \gtrless 3a'^2(4b'^2 - a'c'), \quad \text{i.e. according as} \quad b'^2 < a'c'.$$

Thus *there are two points of inflexion if the roots of* $u' = 0$ *are imaginary, otherwise no such point exists.*

(iii) Further, we shall show that in all cases *the points of inflexion lie on the straight line whose equation is*

$$2(ab')x + 4(a'c' - b'^2)y = ac' + 3a'c - 4bb'. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{P})$$

This may be deduced from the preceding, or directly as follows.

At a point of inflexion, we have

$$y(a'x^2 + 2b'x + c') = ax^2 + 2bx + c, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{Q})$$

$$\frac{dy}{dx}(a'x^2 + 2b'x + c') + 2y(a'x + b') = 2(ax + b), \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{R})$$

$$2\frac{dy}{dx}(a'x + b') + a'y = a, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{S})$$

where (**S**) is derived from (**R**) by differentiation and putting $\frac{d^2y}{dx^2} = 0$.

Multiplying equations (**Q**), (**R**), (**S**) by

$$3a', \quad -2(a'x + b'), \quad (a'x^2 + 2b'x + c'),$$

respectively, and adding, we obtain equation (**P**).

13. Examples.

Ex. 1. *Trace the curve represented by* $y = \dfrac{9x^2 - 12x}{9x^2 - 25}$.

Asymptotes. If $x \to \infty$, then $y = 1 - \dfrac{4}{3x}$ (nearly). If $3x - 5 \to 0$, then $y \to \infty$, and

$$3x - 5 = \frac{9x^2 - 12x}{3x + 5} \cdot \frac{1}{y} = \frac{9(\frac{5}{3})^2 - 12 \cdot \frac{5}{3}}{3 \cdot \frac{5}{3} + 5} \cdot \frac{1}{y} \text{ or } \frac{1}{2y} \text{ (nearly).}$$

Similarly, if $3x + 5 \to 0$, $y \to \infty$ and $3x + 5 = -\dfrac{9}{2y}$ (nearly).

Thus, the lines $y = 1$, $3x \pm 5 = 0$ are asymptotes, and the curve approaches them as in Fig. 16. The asymptote $y = 1$ meets the curve again where $x = 2\frac{1}{12}$.

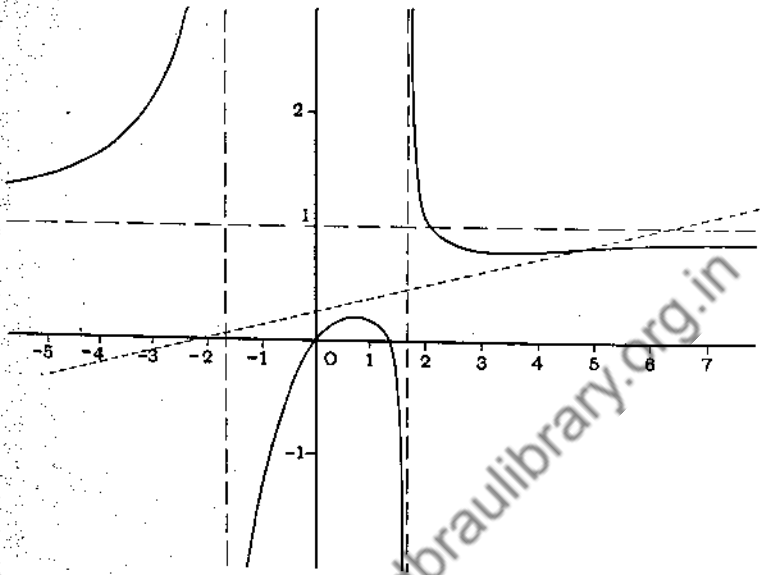


FIG. 16.

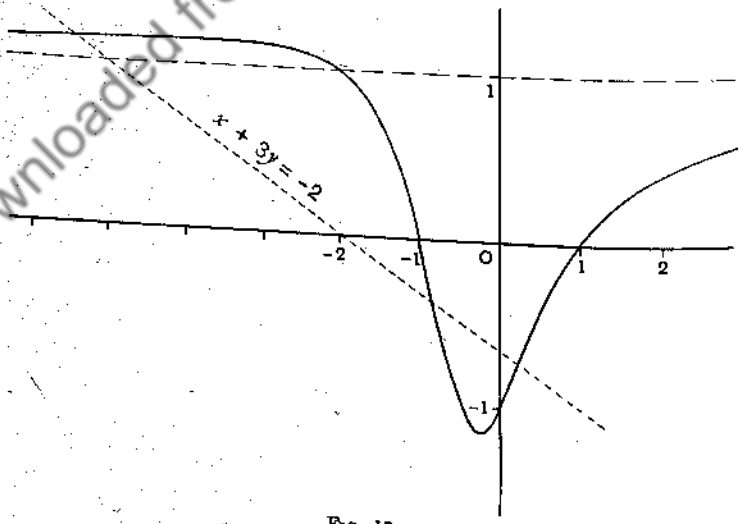


FIG. 17.

Solving for x, we have $(y-1)(3x)^2+4.(3x)-25y=0$; and therefore

$$3x=\frac{-2\pm\sqrt{\{4+25y(y-1)\}}}{y-1}.$$

Now $4+25y(y-1)=(5y-1)(5y-4)$, therefore no part of the curve lies between the lines $y=\frac{1}{5}$ and $y=\frac{4}{5}$. Turning values of y are $\frac{1}{5}$ and $\frac{4}{5}$. The corresponding values of x are $\frac{5}{6}$ and $\frac{10}{3}$.

There is one point of inflexion, which lies on the line $12x-100y+25=0$.

Ex. 2. $$y=\frac{x^2-1}{x^2+x+1}.$$

The roots of $u'=0$ are imaginary, and there are two turning values. Solving for x,

$$x=\frac{-y\pm\sqrt{4-3y^2}}{2(y-1)}.$$

The turning values are $y_1=\frac{2}{\sqrt{3}}=1{\cdot}15$, $y_2=-\frac{2}{\sqrt{3}}=-1{\cdot}15$; and the corresponding values of x are $x_1=-3{\cdot}73$, $x_2=-0{\cdot}27$. The curve lies between $y=y_1$ and $y=y_2$.

If $x\to\infty$, then $y=1-\frac{1}{x}$ (nearly). Thus the line $y=1$ is an asymptote, and it meets the curve again where $x=-2$. (Fig. 17.)

There are three points of inflexion lying on the line $x+3y+2=0$.

14. Quadratic in Two Variables. Let the quadratic in x, y be

$$u\equiv ax^2+2hxy+by^2+2gx+2fy+c,$$

and let $$\Delta\equiv\begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix}\equiv abc+2fgh-af^2-bg^2-ch^2.$$

Let A, B, ..., be the cofactors of a, b, ..., in Δ; so that

$$A=bc-f^2,\quad F=gh-af,\quad \text{etc.}$$

(1) *Forms of u.* We have

$$au=(ax+hy+g)^2+(ab-h^2)y^2+2(af-gh)y+(ca-g^2)$$
$$=(ax+hy+g)^2+Cy^2-2Fy+B. \quad\text{.....(A)}$$

Similarly, $$bu=(hx+by+f)^2+Cx^2-2Gx+A. \quad\text{.....(B)}$$

And since $BC-F^2=a\Delta$ and $CA-G^2=b\Delta$, we have

$$Cau=C(ax+hy+g)^2+(Cy-F)^2+a\Delta, \quad\text{.....(C)}$$

$$Cbu=C(hx+by+f)^2+(Cx-G)^2+b\Delta. \quad\text{.....(D)}$$

If $a=b=0$, $$hu=2(hx+f)(hy+g)+ch-2fg. \quad\text{.....(E)}$$

Hence *if* $\Delta=0$, *then* u *is the product of linear factors.* For, if a and b are not both zero, $Cy^2-2Fy+B$ and $Cx^2-2gx+A$ are squares; and from (**A**) or (**B**) it follows that au or bu is the sum or difference of two squares. If $a=b=0$, and $h\neq0$, then $\Delta=2fgh-ch^2$, and the truth of the statement follows from (**E**).

(2) *Forms of the equation* $u=0$. If $C\neq 0$, this may be written

$$C(ax+hy+g)^2+(Cy-F)^2+a\Delta=0 \quad (a\neq 0), \ldots\ldots\ldots\ldots\text{(F)}$$

$$C(hx+by+f)^2+(Cx-G)^2+b\Delta=0 \quad (b\neq 0). \ldots\ldots\ldots\ldots\text{(G)}$$

If $C=0$, the forms are

$$(ax+hy+g)^2-2Fy+B=0 \quad (a\neq 0), \ldots\ldots\ldots\ldots\text{(H)}$$

$$(hx+by+f)^2-2Gx+A=0 \quad (b\neq 0). \ldots\ldots\ldots\ldots\text{(I)}$$

If $a=0$, $b=0$ and $h\neq 0$, the equation may be written

$$2(hx+f)(hy+g)=2fg-ch. \ldots\ldots\ldots\ldots\text{(J)}$$

(3) *If* x, y *are variables connected by the equation*

$$u\equiv ax^2+2hxy+by^2+2gx+2fy+c=0,$$

then x *and* y *can be expressed in terms of a single parameter* t.

Let (x', y') be any solution of $u=0$, so that (x', y') is any point on the curve represented by $u=0$, and let

$$x=X+x', \quad y=Y+y'.$$

Substituting these values for x and y in $u=0$, the equation becomes

$$aX^2+2hXY+bY^2+2g'X+2f'Y=0, \ldots\ldots\ldots\ldots\text{(K)}$$

where $$f'=hx'+by'+f, \quad g'=ax'+hy'+g.$$

Now let $$t=Y/X,$$

then from (K), $$X(a+2ht+bt^2)+2g'+2f't=0; \ldots\ldots\ldots\ldots\text{(L)}$$

whence we find that $$x-x'=\frac{y-y'}{t}=-\frac{2(g'+f't)}{a+2ht+bt^2}. \ldots\ldots\ldots\ldots\text{(M)}$$

When the factors of $ax^2+2hxy+by^2$ are real, another useful method is that of *H.A.*, III, 10, Ex. 2.

Ex. 1. *If*

$$u\equiv ax^2+2hxy+by^2+2gx+2fy+c=0$$

and

$$\xi=ax+hy+g, \quad \eta=hx+by+f, \quad \zeta=gx+fy+c,$$

prove that

$$\text{(i) } \frac{dy}{dx}=-\frac{\xi}{\eta}, \quad \text{(ii) } \frac{d^2y}{dx^2}=\frac{\Delta}{\eta^3}.$$

Since $$aG+hF+gC=0, \quad hG+bF+fC=0, \text{ and } gG+fF+cC=\Delta,$$

$$G\xi+F\eta+C\zeta=x(aG+hF+gC)+y(hG+bF+fC)+(gG+fF+cC)=\Delta. \ldots\ldots\text{(N)}$$

Then, (i) from the equation $u=0$, by differentiation, $u_1=2(\xi+\eta y_1)=0$; hence,

$$y_1=-\xi/\eta.$$

(ii) Differentiating again, $$y_2=(\xi\eta_1-\eta\xi_1)/\eta^2.$$

Also $$\xi_1=a+hy_1=(a\eta-h\xi)/\eta, \text{ and } \eta_1=h+by_1=(h\eta-b\xi)/\eta;$$ and we have

$$\eta^3y_2=\xi(h\eta-b\xi)+\eta(h\xi-a\eta)=-\xi(Cx-G)-\eta(Cy-F)=G\xi+F\eta+C\zeta;$$

hence, from (N),

$$y_2=\Delta/\eta^3.$$

15. Linear and Homographic Transformation. Consider a homogeneous quadratic function u of x, y, z, and let

$$u \equiv ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy.$$

Suppose that u is transformed into u' by the linear substitution

$$x = l_1X + m_1Y + n_1Z, \quad y = l_2X + m_2Y + n_2Z, \quad z = l_3X + m_3Y + n_3Z,$$

where $$u' \equiv a'X^2 + b'Y^2 + c'Z^2 + 2f'YZ + 2g'ZX + 2h'XY\ ;$$

then if $$\Delta = \begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix} \text{ and } \Delta' = \begin{vmatrix} a' & h' & g' \\ h' & b' & f' \\ g' & f' & c' \end{vmatrix},$$

it will be shown that $$\Delta' = (l_1m_2n_3)^2\Delta.$$

Proof. Substituting the above values of x, y, z in u and equating the coefficients of X^2, YZ in the identity $u \equiv u'$, we have

$$a' = al_1^2 + bl_2^2 + cl_3^2 + 2fl_2l_3 + 2gl_3l_1 + 2hl_1l_2,$$

$$f' = am_1n_1 + bm_2n_2 + cm_3n_3 + f(m_2n_3 + m_3n_2) + g(m_3n_1 + m_1n_3) + h(m_1n_2 + m_2n_1),$$

with similar values for the other coefficients.

Now let $\lambda_1 = al_1 + hl_2 + gl_3$, $\lambda_2 = hl_1 + bl_2 + fl_3$, $\lambda_3 = gl_1 + fl_2 + cl_3$;

and let (μ_1, μ_2, μ_3), (ν_1, ν_2, ν_3) be similar functions of the m's and n's respectively, then $$a' = l_1\lambda_1 + l_2\lambda_2 + l_3\lambda_3,$$

$$f' = m_1\nu_1 + m_2\nu_2 + m_3\nu_3 = n_1\mu_1 + n_2\mu_2 + n_3\mu_3,$$

with similar values for the other coefficients.

Hence, by the rule for multiplication of determinants,

$$\Delta' = \begin{vmatrix} \lambda_1 & \lambda_2 & \lambda_3 \\ \mu_1 & \mu_2 & \mu_3 \\ \nu_1 & \nu_2 & \nu_3 \end{vmatrix} \times \begin{vmatrix} l_1 & l_2 & l_3 \\ m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{vmatrix} = \begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix} \times \begin{vmatrix} l_1 & l_2 & l_3 \\ m_1 & m_2 & m_3 \\ n_1 & n_2 & n_3 \end{vmatrix}^2$$

The function $(l_1m_2n_3)$ is called the *determinant* of transformation, and on account of the property just proved Δ is said to be an *invariant* of u.

For the non-homogeneous function

$$u \equiv ax^2 + 2hxy + by^2 + 2gx + 2fy + c,$$

the corresponding *homographic* substitution is

$$x = \frac{l_1X + m_1Y + n_1}{l_3X + m_3Y + n_3}, \quad y = \frac{l_2X + m_2Y + n_2}{l_3X + m_3Y + n_3}.$$

Suppose that these values are substituted for x, y, and that we multiply by $(l_3X + m_3Y + n_3)^2$ to remove fractions.

Denoting the result by u', it will be seen that the coefficients $a', b', \ldots$ are the same as before, so that the result just proved continues to hold.

EXERCISE III

In this exercise (α, β), (α', β') *are the roots of*

$u \equiv ax^2+2bx+c=0$, $u' \equiv a'x^2+2b'x+c'=0$, *where* a, a' *are positive.*

Also $\Delta = ac-b^2$, $\Delta' = a'c'-b'^2$, $K = ac'+a'c-2bb'$.

Other letters, as J, x_1, x_2, λ_1, λ_2, *have the same meaning as in the text.*

1. Determine the constants so that

$$x^2-4x-8 = A(x-a)^2+B(x-b)^2, \quad x^2-2x-5 = A'(x-a)^2+B'(x-b)^2.$$

2. If $\alpha=\beta$, prove that $x-\alpha$ is a factor of J.

3. If $u=ax^2+2bx+c$, $u'=a'(x-\alpha')^2$, then $u = A(x-x_1)^2+B(x-\alpha')^2$,

where $$x_1 = -\frac{b\alpha'+c}{a\alpha'+b}, \quad A = \frac{(a\alpha'+b)^2}{a\alpha'^2+2b\alpha'+c}, \quad B = \frac{ac-b^2}{a\alpha'^2+2b\alpha'+c}.$$

4. Referring to Art. 7, show that

(i) $(b'^2-a'c')(a-\lambda_1 a')(a-\lambda_2 a') = (ab'-a'b)^2$.

(ii) If $b'^2<a'c'$ and $b^2<ac$, then λ_1 and λ_2 are both positive.

(iii) If $b'^2<a'c'$ and $b^2>ac$, λ_1 is positive, $(\lambda_1>\lambda_2)$ and λ_2 negative.

[(ii) a, a', c, c' are positive and $(ac'+a'c)^2>4aca'c'>4b^2b'^2$.]

5. Draw the curve represented by $y=\dfrac{(x-2)(x-3)}{(x-1)(x-4)}$.

[The interval (2, 3) is within (1, 4); but $a/a'=b/b'$, so that one turning value is at ∞; also

$$y = 1+\frac{2}{x^2-5x+4}, \quad \frac{dy}{dx} = -\frac{2(2x-5)}{x^2-5x+4}.$$

Hence, $x=2{\cdot}5$ gives a turning value. There is no real point of inflexion.]

6. Draw the curve represented by $y=\dfrac{(x-1)(x-3)}{(x-2)(x-4)}$.

[The intervals (1, 3), (2, 4) overlap, $\therefore$ y has no turning values. Also $\dfrac{dy}{dx}$ is always negative for $(ab')<0$. There is one point of inflexion lying on the line $2x+4y=7$.]

7. If $\rho=(\alpha\beta, \alpha'\beta')$ where (α, β), (α', β') are the roots of $u=0$, $u'=0$, prove that

$$\left(\frac{\rho+1}{\rho-1}\right)^2 = \frac{(ac'+a'c-2bb')^2}{4(ac-b^2)(a'c'-b'^2)}.$$

8. Prove that

$$J^2 = -(\Delta' u^2 - Kuu' + \Delta u'^2)$$
$$= (b'^2-a'c')(u-\lambda_1 u')(u-\lambda_2 u').$$

Hence show that if $b'^2<a'c'$, then $u-\lambda_1 u'$ is negative and $u-\lambda_2 u'$ is positive for all values of x except x_1 and x_2.

$$[2J^2 = \begin{vmatrix} 1 & -x & x^2 \\ a & b & c \\ a' & b' & c' \end{vmatrix} \cdot \begin{vmatrix} x^2 & 2x & 1 \\ c & -2b & a \\ c' & -2b' & a' \end{vmatrix} = \begin{vmatrix} 0 & u & u' \\ u & 2\Delta & K \\ u' & K & 2\Delta' \end{vmatrix}.]$$

9. Prove that $$xJ=\begin{vmatrix} u & bx+c \\ u' & b'x+c' \end{vmatrix}.$$

Hence show that if $J(\alpha)$, $J(\beta)$ denote the results of substituting α, β for x in J and $u'(\alpha)$, $u'(\beta)$ have similar meanings, then

$$\frac{J(\alpha)}{J(\beta)}=-\frac{u'(\alpha)}{u'(\beta)}.$$

10. Prove that

(i) $\dfrac{(x_1-\alpha)(x_1-\alpha')}{(x_1-\beta)(x_1-\beta')}=\dfrac{(x_2-\alpha)(x_2-\alpha')}{(x_2-\beta)(x_2-\beta')}$; (ii) $\dfrac{(x_1-\alpha)(x_2-\alpha)}{(x_1-\beta)(x_2-\beta)}=-\dfrac{(\alpha'-\alpha)(\beta'-\alpha)}{(\alpha'-\beta)(\beta'-\beta)}$.

[For (i), $(x_1x_2,\ \alpha\beta')=(x_1x_2,\ \beta\alpha')$. For (ii), $(x_1\alpha',\ \alpha\beta)=(x_1\beta',\ \beta\alpha)=-(x_2\beta',\ \beta\alpha)$.]

11. If the homographic relation $axx'+bx+cx'+d=0$ is transformed into

$$AXX'+BX+CX'+D=0$$

by the substitutions $x=(lX+m)/(l'X+m')$, $x'=(lX'+m)/(l'X'+m')$, prove that

(i) $B-C=(lm'-l'm)(b-c)$.

(ii) $(B+C)^2-4AD=(lm'-l'm)^2\{(b+c)^2-4ad\}$.

(iii) $\dfrac{BC-AD}{(B-C)^2}=\dfrac{bc-ad}{(b-c)^2}$.

[(i) Follows by direct substitution. (ii) If $x=x'$, then $X=X'$, and $ax^2+(b+c)x+d=0$ is transformed into $AX^2+(B+C)X+D=0$.]

12. If $$u=ax^2+2bx+c=A(x-x_1)^2+B(x-x_2)^2,$$

$$u'=a'x^2+2b'x+c'=A'(x-x_1)^2+B'(x-x_2)^2,$$

$axx'+b(x+x')+c=0$, and $X=(x-x_1)/(x-x_2)$, $X'=(x'-x_1)/(x'-x_2)$,

prove that (i) $AXX'+B=0$, (ii) $\dfrac{A'X^2+B'}{AX^2+B}+\dfrac{A'X'^2+B'}{AX'^2+B}=\dfrac{AB'+A'B}{AB}$.

[By direct substitution; or thus: $(x_1x_2,\ \alpha\beta)$ and $(xx',\ \alpha\beta)$ are harmonic, therefore, as in Ex. 10, (ii),

$$\frac{x-x_1}{x-x_2}\cdot\frac{x'-x_1}{x'-x_2}=-\frac{\alpha-x_1}{\alpha-x_2}\cdot\frac{\beta-x_1}{\beta-x_2}=-\frac{ax_1^2+2bx_1+c}{ax_2^2+2bx_2+c}=-\frac{B(x_1-x_2)^2}{A(x_2-x_1)^2}.$$

13. If $axx'+b(x+x')+c=0$, prove that

$$\frac{a'x^2+2b'x+c'}{ax^2+2bx+c}+\frac{a'x'^2+2b'x'+c'}{ax'^2+2bx'+c}=\frac{ac'+a'c-2bb'}{ac-b^2}.$$

[From the preceding, or thus: the left-hand side is equal to

$$\frac{1}{x-x'}\left\{\frac{a'x^2+2b'x+c'}{ax+b}-\frac{a'x'^2+2b'x'+c'}{ax'+b}\right\},\ \text{etc.}]$$

14. If $$u\equiv ax^2+2hxy+by^2+2gx+2fy+c=0,$$

and x, y are expressed in terms of a parameter t, as in Art. 14, (3), prove that

$$\frac{dx}{dt}=\frac{2\eta}{a+2ht+bt^2},\ \text{where}\quad \eta=hx+by+f.$$

[Use (L) of Art. 14, (3).]

15. If $b'^2<a'c'$ and $y=\sqrt{\dfrac{u}{u'}}$, then

$$\int\frac{px+q}{u'\sqrt{u}}\,dx=\frac{1}{\sqrt{(a'c'-b'^2)}}\left\{A\int\frac{dy}{\sqrt{(\lambda_1-y^2)}}+B\int\frac{dy}{\sqrt{(y^2-\lambda_2)}}\right\},$$

where A, B are constants and λ_1, λ_2 are as in Art. 7.* Verify the following proof.

Let $(mx+n)^2=\lambda_1u'-u=(\lambda_1-y^2)u'$, $(m'x+n')^2=u-\lambda_2u'=(y^2-\lambda_2)u'$.

Then we have $J=\sqrt{a'c'-b'^2}\,.\,(mx+n)(m'x+n')$. Also $\dfrac{1}{y}\dfrac{dy}{dx}=\dfrac{J}{uu'}$. ∴

Find constants A, B so that $px+q\equiv B(mx+n)+A(m'x+n')$; then,

$$\int\frac{px+q}{u'\sqrt{u}}\,dx=\int\frac{(px+q)\sqrt{u'}}{J}\,dy=\frac{1}{\sqrt{a'c'-b'^2}}\int\left(\frac{A\sqrt{u'}}{mx+n}+\frac{B\sqrt{u'}}{m'x+n'}\right)dy$$

$$=\frac{1}{\sqrt{a'c'-b'^2}}\left\{A\int\frac{dy}{\sqrt{\lambda_1-y^2}}+B\int\frac{dy}{\sqrt{y^2-\lambda_2}}\,dy\right\}.$$

Three Quadratics

In Exx. 16-25 $u_1=a_1x^2+2b_1x+c_1$, $u_2=a_2x^2+2b_2x+c_2$, $u_3=a_3x^2+2b_3x+c_3$, J_1 *is the* J *of* u_2, u_3. *Also* $\Delta_1=a_1c_1-b_1^2$, $2K_1=a_2c_3+a_3c_2-2b_2b_3$, *with similar meanings for* J_2, Δ_2, $2K_2$, *etc.*

16. Prove the following identical relations.

(i) $u_1(a_2b_3)+u_2(a_3b_1)+u_3(a_1b_2)\equiv(a_1b_2c_3)$.

(ii) $$\begin{vmatrix} 1 & -x & x^2 & 0 \\ a_1 & b_1 & c_1 & u_1 \\ a_2 & b_2 & c_2 & u_2 \\ a_3 & b_3 & c_3 & u_3 \end{vmatrix}\equiv 0,$$

and therefore $u_1J_1+u_2J_2+u_3J_3\equiv 0$.

17. The condition that $u_1=0$, $u_2=0$, $u_3=0$ determine three pairs of points in involution is $(a_1b_2c_3)=0$.

We say that *three quadratics are* mutually harmonic *when every two of them are harmonically related.*

18. If for infinitely many values of x, y, z,

$$a_1yz+b_1(y+z)+c_1=0,\quad a_2zx+b_2(z+x)+c_2=0,\quad a_3xy+b_3(x+y)+c_3=0,$$

prove that in general K_1, K_2, K_3 are all zero, and therefore $u_1=0$, $u_2=0$, $u_3=0$ are mutually harmonic.

[Eliminate y, z. The resulting quadratic in x must vanish identically, and the coefficient of x is $b_2K_3+b_3K_2-b_1K_1$. This and similar expressions must vanish.]

19. By multiplying the arrays on the left, prove the identity on the right,

$$\left\|\begin{matrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \\ 1 & -x & x^2 \end{matrix}\right\|,\quad \left\|\begin{matrix} c_1 & -2b_1 & a_1 \\ c_2 & -2b_2 & a_2 \\ c_3 & -2b_3 & a_3 \\ x^2 & 2x & 1 \end{matrix}\right\|,\quad \begin{vmatrix} \Delta_1 & K_3 & K_2 & u_1 \\ K_3 & \Delta_2 & K_1 & u_2 \\ K_2 & K_1 & \Delta_3 & u_3 \\ u_1 & u_2 & u_3 & 0 \end{vmatrix}=0;$$

and therefore $u_1^2(\Delta_2\Delta_3-K_1^2)+\ldots+\ldots+2u_2u_3(K_2K_3-\Delta_1K_1)+\ldots+\ldots=0$.

* From Greenhill's *Calculus*.

20. (i) If the three quadratics $u_1=0$, $u_2=0$, $u_3=0$, are mutually harmonic, then

$$\frac{u_1^2}{\Delta_1}+\frac{u_2^2}{\Delta_2}+\frac{u_3^2}{\Delta_3}\equiv 0.$$

(ii) Conversely, if u_1, u_2, u_3 are connected by an identical relation of the form

$$pu_1^2+qu_2^2+ru_3^2\equiv 0,$$

the three quadratics are mutually harmonic.

[These follow at once from Ex. 19.]

21. If $u_1=a_1x^2+2b_1xy+c_1y^2$, $u_2=a_2x^2+2b_2xy+c_2y^2$, $u_3=a_3x^2+2b_3xy+c_3y^2$, and these are transformed into $U_1=A_1X^2+2B_1XY+C_1Y^2$, etc., by the substitution

$$x=lX+mY, \quad y=l'X+m'Y,$$

then $$(A_1B_2C_3)=(lm')^3(a_1b_2c_3).$$

[For $(A_2B_3)X^2+(A_2C_3)XY+(B_2C_3)Y^2=(lm')\{(a_2b_3)x^2+(a_2c_3)xy+(b_2c_3)y^2\}$;

$$\therefore\ A_1(B_2C_3)+C_1(A_2B_3)-2B_1\cdot\tfrac{1}{2}(A_2C_3)$$
$$=(lm')^3[a_1(b_2c_3)+c_1(a_2b_3)-2b_1\cdot\tfrac{1}{2}(a_2c_3)].]$$

22. Show that $(ax^2+bx+c)/(cx^2+bx+a)$ is capable of all real values if $b^2>(a+c)^2$.

There will be two values between which it cannot lie if $4ac<b^2<(a+c)^2$, and two values between which it must lie if $b^2<4ac$.

23. If $r^2=x^2+y^2$ where x, y are connected by

$$ax^2+2hxy+by^2=1, \quad \text{.....(A)}$$

prove that the maximum and minimum values of r are given by

$$\left(a-\frac{1}{r^2}\right)\left(b-\frac{1}{r^2}\right)=h^2.$$

[This gives the lengths of the semi-axes of the conic represented by (A).

Let $r^2=\dfrac{1}{t}$, $z=\dfrac{x}{y}$, then $t=\dfrac{az^2+2hz+b}{z^2+1}$.]

24. If $r^2=x^2+y^2+z^2$ where x, y, z are connected by $ax^2+by^2+cz^2=1$ and $lx+my+nz=0$, prove that the maximum and minimum values of r are given by

$$\frac{l^2}{a-\frac{1}{r^2}}+\frac{m^2}{b-\frac{1}{r^2}}+\frac{n^2}{c-\frac{1}{r^2}}=0.$$

25. Prove that the conics

$$ax^2+2hxy+by^2=1, \quad a'x^2+2h'xy+b'y^2=1$$

have a common pair of conjugate diameters, and that the equation to these lines is

$$(ah'-a'h)x^2+(ab'-a'b)xy+(hb'-h'b)y^2=0.$$

[The equations to the conics can be put in the form

$$AX^2+BY^2=1, \quad A'X^2+B'Y^2=1.]$$

CHAPTER III

DOUBLE SERIES

1. Double Series. An array of terms such as the following is called a *double series*.

$$\begin{aligned} &a_{11}+a_{12}+a_{13}+\dots \\ &+a_{21}+a_{22}+a_{23}+\dots \\ &+a_{31}+a_{32}+a_{33}+\dots \\ &+\dots\dots\dots\dots\dots \end{aligned}$$

The array is supposed to extend to infinity on the right and below. The nth term of the mth row is denoted by a_{mn} and the series by Σa_{mn}.

Suppose a rectangle to be drawn so as to contain just the first n terms of the first m rows, and let the sum of the terms in the rectangle be denoted by s_{mn}. If $m=n$, the rectangle becomes a square, and the sum of the terms in the square is denoted by σ_n, so that $s_{nn}=\sigma_n$.

2. Definition of Convergence of a Double Series. If there is a fixed number s such that

$$|s_{mn}-s|<\epsilon, \text{ provided only that } m>\mu \text{ and } n>\mu,$$

where ϵ is any positive number however small, and μ is any positive number however great, then Σa_{mn} is said to be *convergent*, s is called its *sum*, and we shall write $\Sigma a_{mn}=s$.

It is important to observe that m and n are supposed to tend to infinity *independently, in any way whatever.*

3. *If Σa_{mn} and Σb_{mn} are convergent double series with sums s and t respectively, then $\Sigma(a_{mn}+b_{mn})$ and $\Sigma(a_{mn}-b_{mn})$ are convergent, and their sums are $s+t$, $s-t$ respectively.*

For let s_{mn}, t_{mn} be the sums of the first n terms of the first m rows of Σa_{mn}, Σb_{mn} respectively: then for sufficiently large values of m, n,

$$|s_{mn}-s|<\tfrac{1}{2}\epsilon \quad \text{and} \quad |t_{mn}-t|<\tfrac{1}{2}\epsilon,$$

therefore

$$|(s_{mn}\pm t_{mn})-(s\pm t)|<\epsilon;$$

and the result follows from the definition in Art. 2.

4. We shall now consider processes of summation where a restriction is imposed on the way in which m and n tend to infinity.

(1) *Sum by squares.* The terms of Σa_{mn} can be arranged to form the single series

$$a_{11}+(a_{21}+a_{22}+a_{12})+(a_{31}+a_{32}+a_{33}+a_{23}+a_{13})+\dots, \quad \dots\dots\dots(\mathbf{A})$$

in which the nth term is the sum of the terms of the double series between the $(n-1)$th and the nth squares, drawn as in Fig. 18.

The sum of the first n terms of the series is σ_n, the sum of the terms in the nth square.

If $\sigma_n \to \sigma$, then (A) converges to the sum σ, which is called the *sum by squares* of Σa_{mn}.

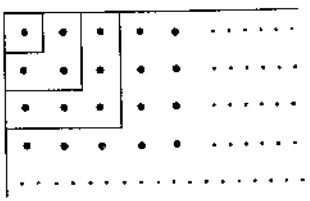


Fig. 18.

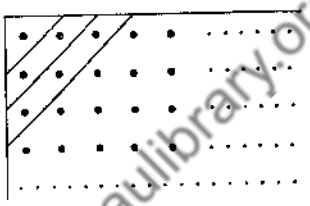


Fig. 19.

(2) *Sum by diagonals.* The terms of Σa_{mn} can be arranged to form the single series

$$a_{11}+(a_{21}+a_{12})+(a_{31}+a_{22}+a_{13})+\dots, \quad \dots\dots\dots\dots\dots(\mathbf{B})$$

where the nth term is the sum of the terms between the $(n-1)$th and the nth 'diagonal,' drawn as in Fig. 19.

The sum to n terms of the series (B) is the sum of the terms cut off by the nth diagonal. Denote this by d_n; then if $d_n \to d$, the series (B) converges to d, which is called the *sum by diagonals of* Σa_{mn}.

(3) *Sum by rows.* Suppose that the series formed by the terms in the first, second, third, ... rows of Σa_{mn} converge to the sums $r_1, r_2, r_3, \dots$ respectively.

Suppose also that the series $r_1+r_2+r_3+\dots$ converges to a sum r. Then r is called the *sum by rows* of Σa_{mn}. Thus $r_m = \Sigma_{n=1}^{\infty} a_{mn}$, and

$$\text{sum by rows} = \Sigma_{m=1}^{m=\infty} r_m = \Sigma_{m=1}^{m=\infty} \Sigma_{n=1}^{n=\infty} a_{mn} = \lim_{m\to\infty} \lim_{n\to\infty} s_{mn}.$$

(4) *Sum by columns.* Suppose that the series formed by the terms in the first, second, third ... columns of Σa_{mn} converge to the sums $c_1, c_2, c_3, \dots$ and that the series $c_1+c_2+c_3+\dots$ converges to a sum c. Then c is called the sum by columns of Σa_{mn}, and

$$\text{sum by columns} = \Sigma_{n=1}^{n=\infty} c_n = \Sigma_{n=1}^{n=\infty} \Sigma_{m=1}^{m=\infty} a_{mn} = \lim_{n\to\infty} \lim_{m\to\infty} s_{mn}.$$

On account of the restriction put upon the way in which m, n are to tend to infinity in (1)-(4), the sums so obtained (if such sums exist) may be different from one another.

Ex. 1. *Consider the double series in the margin, where* $a_{mn}=+1$ *or* -1 *according as* $n=m+1$ *or* $m-1$ *and* $a_{mn}=0$ *for every other* n.

Here sum by squares $=0$, sum by diagonals $=0$,
sum by rows $=+1$, sum by columns $=-1$.

$$\begin{array}{l} 0+1+0+0+0+\dots \\ -1+0+1+0+0+\dots \\ +0-1+0+1+0+\dots \\ +0+0-1+0+1+\dots \\ +\dots\dots\dots\dots \end{array}$$

Ex. 2. *Consider the summation by rows and columns of the double series*

$$\begin{array}{l} 1+\ x\ +\ x^2/\lfloor 2+\ x^3/\lfloor 3+\dots, \\ +1+(2x)+(2x)^2/\lfloor 2+(2x)^3/\lfloor 3+\dots, \\ +1+(3x)+(3x)^2/\lfloor 2+(3x)^3/\lfloor 3+\dots, \\ +\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \end{array}$$

Sum by rows $=e^x+e^{2x}+e^{3x}+\dots=e^x/(1-e^x)$, if $e^x<1$, i.e. if $x<0$.

The terms of the first column form a divergent series, and summation by columns is impossible.

5. A Double Limit. The summation by rows or columns is an instance of a 'double limit.' Here s_{mn} is a function of two independent variables m, n. In such a case it is important to notice that *the operation of proceeding to a limit with each of the variables is not necessarily commutative.*

For example, if $s_{mn}=\dfrac{m}{m+n}$, then $\lim\limits_{m\to\infty} s_{mn}=1$, $\lim\limits_{n\to\infty} s_{mn}=0$;

therefore $\lim\limits_{n\to\infty}\lim\limits_{m\to\infty} s_{mn}=1$ and $\lim\limits_{m\to\infty}\lim\limits_{n\to\infty} s_{mn}=0$.

Double Series of Positive Terms

6. *If* Σa_{mn} *is a double series of positive terms which has a sum* s *by squares, then the series is convergent and its sum is* s.

For all values of m and n, s_{mn} lies between σ_m and σ_n unless $m=n$, and then $s_{mn}=\sigma_n$.

Let m and n tend to infinity independently in any way; then by hypothesis $\sigma_m\to s$ and $\sigma_n\to s$. Therefore $|s_{mn}-s|<\epsilon$ for sufficiently large values of m and n. Hence Σa_{mn} is convergent and its sum is s.

7. *If* Σa_{mn} *is a convergent double series of positive terms, then any single series formed by some or all of the terms of* Σa_{mn} *is convergent.*

Let s be the sum of Σa_{mn}, and let Σu_n be the single series: then since every u is an a,

$$u_1+u_2+\dots+u_n\leqslant s.$$

Therefore Σu_n converges to a sum $\leqslant s$.

8. *No derangement of the terms of a convergent double series Σa_{mn} of positive terms affects its convergence or alters its sum s.*

Using Art. 6, this follows from the corresponding property of single series.

For, summing by squares, Σa_{mn} is transformed into the single series

$$a_{11}+(a_{21}+a_{22}+a_{12})+(a_{31}+a_{32}+a_{33}+a_{23}+a_{13})+\dots \quad \dots\dots\dots\dots(\mathrm{A})$$

This series converges to s. Also, if the brackets are removed and the terms rearranged in any way, the resulting series also converges to s.

Hence the new double series is convergent and its sum is s.

9. *If Σa_{mn} and Σb_{mn} are series of positive terms such that Σb_{mn} is convergent and every term in $\Sigma a_{mn} \leqslant$ the corresponding term in Σb_{mn}, then Σa_{mn} is convergent.*

If we transform each of the series into single series, as in summing by squares, and remove brackets, the theorem follows from Art. 6 and the corresponding property of single series.

10. *If Σa_{mn} is a double series of positive terms which has a sum s by squares, then it has a sum s by diagonals and conversely.*

To sum Σa_{mn} by squares, we transform it into the single series

$$a_{11}+(a_{21}+a_{22}+a_{12})+(a_{31}+a_{32}+a_{33}+a_{23}+a_{13})+\dots \quad \dots\dots\dots\dots(\mathrm{A})$$

To sum it by diagonals, we transform it into the single series

$$a_{11}+(a_{21}+a_{12})+(a_{31}+a_{22}+a_{13})+\dots \quad \dots\dots\dots\dots\dots\dots(\mathrm{B})$$

If the brackets are removed, the series (A) and (B) only differ in the order of the terms.

Also all the terms are positive: hence if either of the series converges to a sum s, so does the other.

11. *If Σa_{mn} is a double series of positive terms which has a sum s by squares, then it has a sum s by rows and conversely.*

(1) Suppose that Σa_{mn} has a sum s by squares, so that $\sigma_n \to s$.

By Art. 6, Σa_{mn} is convergent, therefore by Art. 7 the series formed by the terms in any row converges to a sum $\leqslant s$. That is to say, $\lim_{n\to\infty} s_{mn}$ exists and is $\leqslant s$.

Again, because Σa_{mn} is convergent, for sufficiently large values of m and n, $s - s_{mn} < \epsilon$. Also $s_{mn} \leqslant \lim_{n\to\infty} s_{mn}$, therefore

$$s-\epsilon < \lim_{n\to\infty} s_{mn} \leqslant s \quad \text{for} \quad m > \mu.$$

Hence $\lim_{m\to\infty} \lim_{n\to\infty} s_{mn} = s$, that is to say, Σa_{mn} has a sum s by rows.

(2) Suppose that Σa_{mn} has a sum s by rows, so that

$$\lim_{m\to\infty}\lim_{n\to\infty} s_{mn} = s.$$

Then $$\sigma_m \leqslant \lim_{n\to\infty} s_{mn} \leqslant s.$$

Therefore $\sigma_m \to$ a limit s' as $m\to\infty$, and by (1) it follows that $s' = s$.

12. *In Theorem* 11, *we can replace* '*rows*' *by* '*columns*,' the proof being precisely similar.

13. *Thus if a double series of positive terms can be summed in any one of the four ways described in* (4), *then it can be summed in the three other ways. In every case the sum is the same and is the sum of the series, which is convergent.*

Absolutely Convergent Double Series

14. The double series Σa_{mn} is said to be *absolutely convergent* if $\Sigma|a_{mn}|$ is convergent.

15. *If Σa_{mn} is an absolutely convergent double series, then it is convergent.*

For $a_{mn}+|a_{mn}| = 0$ or $2a_{mn}$, therefore $\Sigma(a_{mn}+|a_{mn}|)$ is convergent, for its terms are $\geqslant 0$ and are $\leqslant$ the corresponding terms of $\Sigma 2|a_{mn}|$, which is convergent.

And by Art. 3, since $\Sigma|a_{mn}|$ is convergent, so is Σa_{mn}.

16. *If Σa_{mn} is an absolutely convergent double series, it can be summed by squares, diagonals, rows or columns. In every case the sum is the same, and this sum is the sum of the series.*

For let $\Sigma|a_{mn}| = s$ and $\Sigma\{(a_{mn}+|a_{mn}|\} = s'$, then by Art. 3,

$$\Sigma\{(a_{mn}+|a_{mn}|) - |a_{mn}|\} = s' - s,$$

that is, $\Sigma a_{mn} = s' - s$.

This is true if Σ denotes a summation by rectangles, squares, diagonals, rows or columns, s and s' being the same in every case, which proves the theorem.

17. *If Σa_{mn} is an absolutely convergent double series, then any single series formed by some or all of the terms of Σa_{mn} is absolutely convergent.*

This follows from Art. 7, for $\Sigma|a_{mn}|$ is convergent.

18. *No derangement of the terms of an absolutely convergent double series Σa_{mn} affects its convergence or alters its sum s.*

For Σa_{mn} can be summed by squares and so transformed into the single series $a_{11}+(a_{21}+a_{22}+a_{12})+(a_{31}+a_{32}+a_{33}+a_{23}+a_{13})+\dots$.

This series converges to a sum s. Also, if the brackets are removed, the series is absolutely convergent and its sum is unaltered by rearranging the terms: whence the result.

19. *The double series* Σa_{mn} *is absolutely convergent if, for all values of* m *and* n, $|a_{mn}| \leqslant b_{mn}$, *where* Σb_{mn} *is a convergent double series of positive terms.* This follows from Art. 9.

Ex. 1. *Prove that if* $|q|<1$,

$$\frac{q}{1+q}+\frac{q^3}{1+q^3}+\frac{q^5}{1+q^5}+\ldots=\frac{q}{1-q^2}-\frac{q^2}{1-q^4}+\frac{q^3}{1-q^6}-\ldots. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

Consider the double series

$$\left.\begin{aligned} q/(1+q) &= q-q^2+q^3-q^4+\ldots \\ q^3/(1+q^3) &= q^3-q^6+q^9-q^{12}+\ldots \\ q^5/(1+q^5) &= q^5-q^{10}+q^{15}-q^{20}+\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

The sum by rows is the left-hand side of (A) and the sum by columns is the right-hand side. These sums will exist and will be equal if the double series is absolutely convergent.

In (B), replace q by q', where $q'=|q|$ and change every $-$ sign to $+$. Thus we get the double series

$$\left.\begin{aligned} &q'+q'^2+q'^3+q'^4+\ldots \\ &q'^3+q'^6+q'^9+q'^{12}+\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

For this series, sum by rows $=\dfrac{q'}{1-q'}+\dfrac{q'^3}{1-q'^3}+\dfrac{q'^5}{1-q'^5}+\ldots. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(D)}$

If $q'<1$, then (D) is convergent (by d'Alembert's Test); hence (C) is convergent, (B) is absolutely convergent, and the result follows.

Ex. 2.* **Montfort's transformation.** *If* $u_1, u_2, \ldots$ *are all positive and* $\Sigma u_n x^n$ *is convergent for* $|x|<1$, *show that for sufficiently small values of* x

$$\Sigma_1^\infty u_n x^n = u_1\left(\frac{x}{1-x}\right)+\Delta u_1\left(\frac{x}{1-x}\right)^2+\Delta^2 u_1\left(\frac{x}{1-x}\right)^3+\ldots.$$

Prove also that this certainly holds if $-1<x<\frac{1}{3}$.

Let $y=\dfrac{x}{1-x}$ so that $x=\dfrac{y}{1+y}$ and

$$\Sigma_1^\infty u_n x^n = u_1\left(\frac{y}{1+y}\right)+u_2\left(\frac{y}{1+y}\right)^2+\ldots. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

Consider the double series

$$\left.\begin{aligned} &u_1y-u_1y^2+u_1y^3-\ldots+(-1)^{n-1}u_1y^n+\ldots \\ &\quad +u_2y^2-2u_2y^3-\ldots+(-1)^{n-2}C_1^{n-1}u_2y^n+\ldots \\ &\quad\quad +u_3y^3-\ldots+(-1)^{n-3}C_2^{n-1}u_3y^n+\ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}\right\}, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

where the rows are the expansions of the successive terms of (A).

* This transformation is sometimes useful for changing a series into one which converges more rapidly.

If $|x|<1$ and $|y|<1$, the sum by rows of this double series is $\Sigma_1^\infty u_n x^n$.

Next let $y'=|y|$, and consider the double series

$$\left.\begin{array}{r} u_1y'+u_1y'^2+\ u_1y'^3+\dots \\ +u_2y'^2+2u_2y'^3+\dots \\ +\ u_3y'^3+\dots \\ \dots\dots\dots\dots\dots\dots \end{array}\right\}, \quad \dots\dots\dots\dots(C)$$

which is obtained from (B) by changing every $-$ into $+$ and putting y' for y.

If $\dfrac{y'}{1-y'}<1$, so that $y'<\frac{1}{2}$, this double series is convergent, for its sum by rows is the sum of the convergent series $\Sigma u_n\left(\dfrac{y'}{1-y'}\right)^n$. Hence if $y'<\frac{1}{2}$, i.e. if $-1<x<\frac{1}{3}$, the series (B) is absolutely convergent and its sum by columns is $\Sigma_1^\infty u_n x^n$.

Also the sum of the terms in the nth column

$$=(-1)^{n-1}y^n(u_1-C_1^{n-1}u_2+C_2^{n-1}u_3-\dots+(-1)^{n-1}u_n)$$
$$=(-1)^{n-1}y^n(1-C_1^{n-1}E+C_2^{n-1}E^2-\dots+(-1)^{n-1}E^n)u_1$$
$$=y^n(E-1)^{n-1}u_1=\Delta^{n-1}u_1\,.\,y^n.$$

20. Complex Double Series.

Let $z_{mn}=x_{mn}+\iota y_{mn}$, and suppose that Σx_{mn} and Σy_{mn} are convergent, their sums being s and t respectively, then we say that Σz_{mn} is *convergent* and that its sum is $s+\iota t$.

Further, we say that Σz_{mn} is *absolutely convergent* when $\Sigma|z_{mn}|$ is convergent. In this case, *Σx_{mn} and Σy_{mn} are absolutely convergent;* for

$$|x_{mn}|\leqslant|z_{mn}| \quad \text{and} \quad |y_{mn}|\leqslant|z_{mn}|.$$

It follows that Theorems 15-19 are true for complex as for real absolutely convergent double series.

21. Substitution of a Power Series for y in $\Sigma u_n y^n$.

(1) Theorem. *If the series*

$$z=u_0+u_1y+u_2y^2+\dots, \quad y=v_0+v_1x+v_2x^2+\dots,$$

are absolutely convergent when $|y|<b$ *and* $|x|<a$, $\dots\dots\dots\dots$(A)

and, if in addition, $y_1=|v_0|+|v_1x|+|v_2x^2|+\dots<b$, $\dots\dots\dots\dots$(B)

then z can be expressed as a convergent power series in x.

Proof. If $|x|<a$, we can use the rule for the multiplication of series to express $y^2, y^3, \dots$ as power series in x. In this way we can express z in the form of the double series

$$\left.\begin{array}{lllll} u_0 & +0 & +0 & & +\dots \\ +u_1v_0 & +u_1v_1x & +u_1v_2x^2 & & +\dots \\ +u_2v_0^2 & +2u_2v_0v_1x & +u_2(v_1^2+2v_0v_2)x^2 & & +\dots \\ +\dots\dots & & & & \end{array}\right\}, \quad \dots\dots\dots\dots(C)$$

in which the rth row consists of the terms in the expansion of $u_r y^r$. This double series has a sum z by rows.

Again, let accents indicate absolute values or moduli, so that

$$u_r' = |u_r|, \quad v_r' = |v_r|, \quad x' = |x|,$$

and consider the double series

$$\left.\begin{array}{llll} u_0' & +0 & +0 & +\ldots \\ +u_1'v_0' & +u_1'v_1'x' & +u_1'v_2'x'^2 & +\ldots \\ +u_2'v_0'^2 & +2u_2'v_0'v_1'x' & +u_2'(v_1'^2+2v_0'v_2')x'^2 & +\ldots \\ +\ldots & & & \end{array}\right\}, \quad \ldots\ldots\ldots\ldots(\mathrm{D})$$

obtained by accenting all the letters in (C).

If $y_1<b$, we can sum (D) by rows, the sum being that of $\Sigma u_n' y_n^n$. Therefore (D) is convergent and (C) is absolutely convergent. Hence (C) has a sum z by columns, that is to say, z can be expressed as a convergent power series in x.

(2) The conditions of the last theorem being satisfied, *it is required to find a range of values of x for which the transformation is possible.*

Choose any positive number $k<a$; then $\Sigma v_n' k^n$ is convergent and consequently $v_n' k^n \to 0$. Therefore we can find g so that $v_n' k^n \leqslant g$ for every n.

Hence if $x'<k$, we have

$$v_n' x'^n = v_n' k^n \left(\frac{x'}{k}\right)^n \leqslant g\left(\frac{x'}{k}\right)^n.$$

Consequently

$$y_1 = v_0' + v_1'x' + v_2'x'^2 + \ldots \leqslant v_0' + g\frac{x'}{k}\left\{1+\frac{x'}{k}+\left(\frac{x'}{k}\right)^2+\ldots\right\}.$$

Hence $y_1 \leqslant v_0' + \dfrac{gx'}{k-x'} < b$, provided that

$$x'(g+b-v_0') < k(b-v_0'),$$

where it is to be observed that $b-v_0'>0$.

Hence the transformation is possible for every x in the interval $(-h, h)$, where $$h = k(b-v_0')/(g+b-v_0').$$

(3) *Particular cases.* If $v_0=0$, the transformation is possible if

$$|x| < kb/(g+b).$$

Again, if $\Sigma u_n y^n$ is absolutely convergent *for all values of y*, b may be as great as we like and we can put $h=k$.

Now k is any positive number $<a$, hence the transformation is possible if $|x|<a$.

22. Sum of the r-th Powers of the Roots of an Equation.

Theorem. *If s_r is the sum of the r-th powers of the roots of*

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0,$$

then s_r/r is the coefficient of x^r in the expansion of

$$-\log(1 + p_1 x + p_2 x^2 + \ldots + p_n x^n)$$

in ascending powers of x.

Proof. If $\alpha_1, \alpha_2, \ldots \alpha_n$ are the roots, we have

$$\begin{aligned}\log(1 + p_1 x + p_2 x^2 + \ldots) &= \log(1 - \alpha_1 x)(1 - \alpha_2 x) \ldots \\ &= \log(1 - \alpha_1 x) + \log(1 - \alpha_2 x) + \ldots \\ &= -\left(s_1 x + s_2 \frac{x^2}{2} + \ldots + s_r \frac{x^r}{r} + \ldots\right). \quad \ldots\ldots\ldots(\mathrm{A})\end{aligned}$$

Also $$\log(1 + p_1 x + p_2 x^2 + \ldots)$$

$$= (p_1 x + p_2 x^2 + \ldots) - \tfrac{1}{2}(p_1 x + p_2 x^2 + \ldots)^2 + \ldots \quad \ldots\ldots\ldots(\mathrm{B})$$

Consider the series

$$(p_1' x' + p_2' x'^2 + \ldots \div) + \tfrac{1}{2}(p_1' x' + p_2' x'^2 + \ldots)^2 + \ldots, \quad \ldots\ldots\ldots(\mathrm{C})$$

where $p_1' = |p_1|$, $p_2' = |p_2|$, ..., $x' = |x|$. We can find a positive number h such that

$$p_1' h + p_2' h^2 + \ldots + p_n' h^n < 1.$$

Hence if $|x| < h$, the series (C) is convergent, and consequently the series obtained by expanding the terms of (B) is absolutely convergent.

Hence the series (B) may be expressed as a power series in x which must be identical with the series (A). Equating the coefficient of x^r we have the result in question.

Ex. 1. *If $\alpha + \beta = p$ and $\alpha\beta = q$, prove that*

$$\alpha^n + \beta^n = p^n - \frac{n}{\lfloor 1}p^{n-2}q + \frac{n(n-3)}{\lfloor 2}p^{n-4}q^2 - \frac{n(n-4)(n-5)}{\lfloor 3}p^{n-6}q^3 + \ldots,$$

the general term being

$$(-1)^r \frac{n(n-r-1)(n-r-2)\ldots(n-2r+1)}{\lfloor r}p^{n-2r}q^r,$$

and the last term $(-1)^{\frac{n-1}{2}} npq^{\frac{n-1}{2}}$ *or* $2(-q)^{\frac{n}{2}}$, *according as n is odd or even.*

We have $(1-\alpha x)(1-\beta x) = 1 - px + qx^2$, therefore $(\alpha^n + \beta^n)/n$ is equal to the coefficient of x^n in

$$x(p - qx) + \frac{1}{2}x^2(p - qx)^2 + \ldots \frac{1}{n}x^n(p - qx)^n + \ldots.$$

23. Quotient of Two Power Series.

If $f(x) = u_0 + u_1 x + u_2 x^2 + \ldots$ and $\phi(x) = v_0 + v_1 x + v_2 x^2 + \ldots$ where $v_0 \neq 0$ and both series are absolutely convergent for, say, $|x| < a$, then, for sufficiently small values of x, $f(x)/\phi(x)$ can be expressed as a convergent power series in x.

Let $y = v_1 x + v_2 x^2 + \dots$, then we have

$$\frac{1}{\phi(x)} = \frac{1}{v_0 + y} = \frac{1}{v_0}\left\{1 - \frac{y}{v_0} + \left(\frac{y}{v_0}\right)^2 - \dots\right\}. \quad \dots\dots\dots\dots\dots\text{(A)}$$

Since $v_0 + v_1 x + v_2 x^2 + \dots$ is absolutely convergent, for sufficiently small values of x, say for $|x| < h$,

$$y_1 = v_1' x' + v_2' x'^2 + \dots < v_0',$$

where accents indicate absolute values. For such values of x,

$$|y| \leqslant y_1 < |v_0|.$$

Therefore the series in (A) is absolutely convergent; and, by Art. 21, $1/\phi(x)$ can be expressed as an absolutely convergent power series in x.

Since the series for $f(x)$ is absolutely convergent for $|x| < a$, the product $f(x) \cdot 1/\phi(x)$ can be expressed as such a series if $|x| < h < a$.

24. Reversion of Power Series.

Suppose that

$$y = a_1 x + a_2 x^2 + a_3 x^3 + \dots,$$

the series being absolutely convergent for $|x| < a$.

A very important question arises: *Can x be expressed as a convergent power series in y?*

Let us assume that $x = b_0 + b_1 y + b_2 y^2 + \dots$,

the series being convergent for some value of y other than zero. Then for sufficiently small values of x, $\Sigma b_n y^n$ can be arranged as a convergent power series in x and

$$x = b_0 + b_1 a_1 x + (b_1 a_2 + b_2 a_1^2) x^2 + (b_1 a_3 + 2 b_2 a_1 a_2 + b_3 a_1^3) x^3 + \dots;$$

and, equating coefficients (*H.A.*, XX, 20), we see that $b_0, b_1, b_2, \dots$ are determined in succession from the equations

$$b = 0, \quad b_1 a_1 = 1, \quad b_1 a_2 + b_2 a_1^2 = 0, \dots.$$

Thus $$x = \frac{1}{a_1} y - \frac{a_2}{a_1^3} y^2 + \frac{1}{a_1^5}(2a_2^2 - a_1 a_3) y^3 + \dots.$$

If it can be proved that this series is convergent for some value of y other than zero, then this equality holds for sufficiently small values of x, and gives an answer to the question.

25. Bernoulli's Numbers.

We define the numbers $B_1, B_2, B_3, \dots$ as in *H.A.*, VIII, 8, (5); so that

$B_1 = \frac{1}{2}$; $B_3, B_5, \dots$ are all zero; and $B_2, -B_4, B_6, -B_8, \dots$

are what are commonly known as *Bernoulli's Numbers*.

We then have the following important theorem.

Theorem. *For sufficiently small values of* x,

$$\frac{x}{1-e^{-x}} = 1 + B_1 x + B_2 \frac{x^2}{\lfloor 2} + \ldots + B_r \frac{x^r}{\lfloor r} + \ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots (\mathbf{A})$$

Let $z = x/(1-e^{-x})$; then if $x \neq 0$ we have

$$z = \frac{1}{1-y} \quad \text{where} \quad y = \frac{x}{\lfloor 2} - \frac{x^2}{\lfloor 3} + \frac{x^3}{\lfloor 4} - \ldots .$$

If a positive number h exists such that

$$\frac{h}{\lfloor 2} + \frac{h^2}{\lfloor 3} + \frac{h^3}{\lfloor 4} + \ldots < 1, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (\mathbf{B})$$

and if $|x| < h$, then z can be expressed as an absolutely convergent power series in x (Art. 22).

The condition (B) is the same as

$$\frac{1}{h}(e^h - 1 - h) < 1, \quad \text{that is} \quad e^h - 1 - 2h < 0.$$

By drawing the graphs of $y = e^x$ and $y = 1 + 2x$, it is evident that the last inequality holds for small values of h. In fact, by *H.A.*, Exercise XLIX, 20, it is true if $h = 1{\cdot}260$.* We may therefore assume that, if $|x| < 1{\cdot}26$,

$$\frac{x}{1-e^{-x}} = 1 + b_1 x + b_2 \frac{x^2}{\lfloor 2} + \ldots + b_r \frac{x^r}{\lfloor r} + \ldots ,$$

and therefore $$x = \left(1 + b_1 x + b_2 \frac{x^2}{\lfloor 2} + \ldots\right)\left(x - \frac{x^2}{\lfloor 2} + \frac{x^3}{\lfloor 3} - \ldots\right).$$

Multiplying these series (which are absolutely convergent) and equating the coefficients of x^{r+1},

$$\frac{b_r}{\lfloor r}\frac{1}{\lfloor 1} - \frac{b_{r-1}}{\lfloor r-1}\frac{1}{\lfloor 2} + \frac{b_{r-2}}{\lfloor r-2}\frac{1}{\lfloor 3} - \ldots + (-1)^r \frac{1}{\lfloor r+1} = 0,$$

and therefore $$C_1^{r+1} b_r - C_2^{r+1} b_{r-1} + C_3^{r+1} b_{r-2} - \ldots + (-1)^r = 0. \quad \ldots\ldots\ldots\ldots (\mathbf{C})$$

If we change $b_1, b_2, b_3, \ldots$ into $B_1, B_2, B_3, \ldots$, we obtain equation (E) of *H.A.*, VIII, 8, (5), which determines the values of $B_1, B_2, B_3, \ldots$ in succession. Hence $b_r = B_r$ for every r; which concludes the proof.

It is convenient to use the *symbolic notation* of *H.A.*, VIII, 8, (5); thus equation (A) may be written

$$\frac{x}{1-e^{-x}} = e^{Bx}, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (\mathbf{A})$$

where B_m *is to be written for* B^m *after expansion.*

* It can be shown that the series (A) is convergent if $|x| < 2\pi$. See Bromwich, *Theory of Infinite Series*, p. 234.

Ex. 1. *Use equation* (A) *to show that* $B_3, B_5, B_7, \ldots$ *are all zero.*

We have $$\frac{x}{1-e^{-x}}-\frac{1}{2}x=\frac{-x}{1-e^{x}}-\frac{1}{2}(-x) \quad \text{and} \quad B_1=\frac{1}{2}.$$

Hence $\dfrac{x}{1-e^{-x}}-B_1x$ is an *even* function of x, so that no odd power of x can occur in its expansion; that is, B_3, B_5, etc., are all zero.

Ex. 2. *Show that* $$\frac{x}{e^x-1}=e^{Bx}-x. \qquad \text{(D)}$$

As in Ex. 1, $\dfrac{x}{e^x-1}=\dfrac{x}{1-e^{-x}}-x$, which gives the result.

In what follows, it is supposed that x has values for which the series in (A) *is convergent.*

(i) *Linear relations connecting terms of the sequence* $B_1, B_2, B_3 \ldots$. If k is any real number,

$$e^{kx}\cdot\frac{x}{1-e^{-x}}=\left(1+kx+k^2\frac{x^2}{\lfloor 2}+\ldots\right)\left(1+B_1x+B_2\frac{x^2}{\lfloor 2}+\ldots\right)$$
$$=1+(k+B_1)x+(k^2+2kB_1+B_2)\frac{x^2}{\lfloor 2}+\ldots,$$

a result which may be written symbolically, $\quad e^{kx}\cdot e^{Bx}=e^{(k+B)x}. \qquad$ (E)

Using this equation in connection with various identities, we can find a large number of relations connecting the B's.

Ex. 3. *Show that* $$(B+k)^m-(B+k-1)^m=mk^{m-1}. \qquad \text{(F)}$$

Take the identity $$\frac{1}{t(1-t)}-\frac{1}{1-t}=\frac{1}{t}.$$

Multiply by x/t^{k-1}, and put $t=e^{-x}$. Therefore

$$e^{kx}\cdot\frac{x}{1-e^{-x}}-e^{(k-1)x}\cdot\frac{x}{1-e^{-x}}=xe^{kx},$$

that is, $$e^{(k+B)x}-e^{(k-1+B)x}=xe^{kx};$$

and equating coefficients of x^m, we have

$$\frac{(k+B)^m}{\lfloor m}-\frac{(k-1+B)^m}{\lfloor m}=\frac{k^{m-1}}{\lfloor m-1},$$

which gives equation (F). In particular, when $k=1, 0$ in succession,

$$(B+1)^m-B^m=m, \quad B^m-(B-1)^m=0. \qquad \text{(G)}$$

Ex. 4. *Prove that* $$(2B+k)^m+(2B+k-1)^m-2(B+k)^m=0. \qquad \text{(H)}$$

Take the identity $$\frac{1}{1-t^2}+\frac{t}{1-t^2}-\frac{1}{1-t}=0.$$

Multiply by $2x/t^k$ and put $t=e^{-x}$. Therefore

$$e^{kx}\cdot\frac{2x}{1-e^{-2x}}+e^{(k-1)x}\cdot\frac{2x}{1-e^{-2x}}-2e^{kx}\cdot\frac{x}{1-e^{-x}}=0,$$

that is $$e^{(k+2B)x}+e^{(k-1+2B)x}-2e^{(k+B)x}=0.$$

Equating coefficients of x^m, we have equation (H). In particular, when $k=0, 1$,

$$(2B)^m+(2B-1)^m-2B^m=0, \quad (2B+1)^m+(2B)^m-2(B+1)^m=0. \qquad \text{(I)}$$

26. Bernoulli's Theorem. *If* $S_r = 1^r + 2^r + 3^r + \ldots + n^r$ *where* r *is a positive integer, then*

$$(r+1)S_r = n^{r+1} + B_1 C_1^{r+1} n^r + B_2 C_2^{r+1} n^{r-1} + \ldots + B_r C_r^{r+1} n, \quad \ldots\ldots\ldots\ldots\text{(J)}$$

an equation which may be written symbolically as

$$(r+1)S_r = (n+B)^{r+1} - B^{r+1}. \quad \ldots\ldots\ldots\ldots\text{(J)}$$

This has been proved in *H.A.*, VIII, 8, (7). The usual proof is as follows.

Since $e^x + e^{2x} + e^{3x} + \ldots + e^{nx} = n + S_1 x + S_2 \frac{x^2}{\lfloor 2} + \ldots + S_r \frac{x^r}{\lfloor r} + \ldots$, we have

$$n + S_1 x + S_2 \frac{x^2}{\lfloor 2} + \ldots = \frac{e^{nx}-1}{1-e^{-x}} = \frac{e^{nx}}{x} \cdot \frac{x}{1-e^{-x}} - \frac{1}{x} \cdot \frac{x}{1-e^{-x}}. \quad \ldots\ldots\ldots\ldots\text{(K)}$$

Hence by equations (**A**) and (**E**),

$$n + S_1 x + S_2 \frac{x^2}{\lfloor 2} + \ldots = \frac{1}{x} e^{(n+B)x} - \frac{1}{x} e^{Bx},$$

and equating the coefficients of x^r,

$$\frac{S_r}{\lfloor r} = \frac{(n+B)^{r+1}}{\lfloor r+1} - \frac{B^{r+1}}{\lfloor r+1},$$

which gives equation (J).

NOTE. Since $S_0 = n$, equation (K) may be written symbolically as

$$e^{Sx} = (e^{nx}-1)/(1-e^{-x}), \quad \ldots\ldots\ldots\ldots\text{(K)}$$

where, after expansion, indices of powers of S are to be changed into suffixes.

27. Expansions of x cosech x, x coth x, tanh x.

It is to be remembered that $B_1 = \frac{1}{2}$; $B_3, B_5, \ldots$ are all zero, and $B_2, -B_4, B_6, -B_8, \ldots$ are Bernoulli's numbers. Also the series denoted by e^{Bx} is convergent if $|x| < 2\pi$. (See Art. 25, Note.)

From the identity $\frac{1}{1/t - t} = \frac{1}{1-t} - \frac{1}{1-t^2}$, it follows that

$$x \cdot \frac{2}{e^x - e^{-x}} = 2 \cdot \frac{x}{1-e^{-x}} - \frac{2x}{1-e^{-2x}},$$

therefore

$$x \operatorname{cosech} x = 2e^{Bx} - e^{2Bx}, \quad \ldots\ldots\ldots\ldots\text{(L)}$$

where $|2x| < 2\pi$, that is $|x| < \pi$. On expansion this gives

$$x \operatorname{cosec} x = 1 - 2(2-1)B_2 \frac{x^2}{\lfloor 2} - 2(2^3-1)B_4 \frac{x^4}{\lfloor 4} - \ldots$$

$$- 2(2^{2r-1}-1)B_{2r} \frac{x^{2r}}{\lfloor 2r} - \ldots, \quad \ldots\ldots\ldots\ldots\text{(L)}$$

where $|x| < \pi$.

Again, $$x\cdot\frac{e^x+e^{-x}}{e^x-e^{-x}}+x=\frac{2xe^x}{e^x-e^{-x}}=\frac{2x}{1-e^{-2x}},$$

therefore $$x\coth x=e^{2Bx}-x, \quad \text{.....(M)}$$

that is, $$x\coth x=1+2^2B_2\frac{x^2}{\lfloor 2}+\ldots+2^{2r}B_{2r}\frac{x^{2r}}{\lfloor 2r}+\ldots, \quad \text{.....(M)}$$

where $|x|<\pi$. This equation may also be written symbolically

$$x\coth x=\cosh 2Bx. \quad \text{.....(M)}$$

Finally, using the identity $\frac{1}{1+t}=\frac{2}{1-t^2}-\frac{1}{1-t}$, we have

$$x\cdot\frac{e^x-e^{-x}}{e^x+e^{-x}}+x=\frac{2x}{1+e^{-2x}}=\frac{4x}{1-e^{-4x}}-\frac{2x}{1-e^{-2x}}.$$

Therefore $$x\tanh x=e^{4Bx}-e^{2Bx}-x. \quad \text{.....(N)}$$

Expanding and dividing by x, which is not to be zero,

$$\tanh x=2^2(2^2-1)B_2\frac{x}{\lfloor 2}+2^4(2^4-1)B_4\frac{x^3}{\lfloor 4}+\ldots$$
$$+2^{2r}(2^{2r}-1)B_{2r}\frac{x^{2r-1}}{\lfloor 2r}+\ldots, \quad \text{.....(N)}$$

where $|4x|<2\pi$, that is $|x|<\frac{\pi}{2}$.

28. Expansions of x cosec x, x cot x and tan x. Since

$$\operatorname{cosec} x=\iota\operatorname{cosech}\iota x, \quad \cot x=\iota\coth\iota x \quad \text{and} \quad \tan x=\frac{1}{\iota}\tanh\iota x,$$

these expansions may be obtained by putting ιx for x in (L), (M), (N), and since $|\iota x|=|x|$, we have

$$x\operatorname{cosec} x=1+2(2-1)B_2\frac{x^2}{\lfloor 2}-2(2^3-1)B_4\frac{x^4}{\lfloor 4}+\ldots$$
$$+(-1)^{r-1}.2(2^{2r-1}-1)B_{2r}\frac{x^{2r}}{\lfloor 2r}+\ldots, \quad \text{.....(O)}$$

when $|x|<\pi$.

$$x\cot x=1-2^2B_2\frac{x^2}{\lfloor 2}+2^4B_4\frac{x^4}{\lfloor 4}-\ldots+(-1)^r2^{2r}B_{2r}\frac{x^{2r}}{\lfloor 2r}+\ldots, \quad \text{.....(P)}$$

when $|x|<\pi$,

$$\tan x=2^2(2^2-1)B_2\frac{x}{\lfloor 2}-2^4(2^4-1)B_4\frac{x^3}{\lfloor 4}+\ldots$$
$$+(-1)^{r-1}2^{2r}(2^{2r-1}-1)B_{2r}\frac{x^{2r-1}}{\lfloor 2r}+\ldots, \quad \text{.....(Q)}$$

when $|x|<\frac{\pi}{2}$.

Substituting the values of $B_2, B_4, \dots$, these formulae give

$$\frac{x}{\sin x} = 1 + \frac{1}{6}x^2 + \frac{7}{360}x^4 + \frac{31}{15120}x^6 + \dots \quad (-\pi < x < \pi),$$

$$x \cot x = 1 - \frac{1}{3}x^2 - \frac{1}{45}x^4 - \frac{2}{945}x^6 - \dots \quad (-\pi < x < \pi),$$

$$\tan x = x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \frac{17}{315}x^7 + \dots \quad \left(-\frac{\pi}{2} < x < \frac{\pi}{2}\right).$$

Euler used the last two series to calculate values of $\tan x$ and $\cot x$ to twenty places of decimals.

29. Formal Use of the Operators E and Δ in Infinite Series. Many interesting results can be obtained by a purely formal reckoning in which the symbols E and Δ are supposed to obey the laws of algebra and the question of convergence of any infinite series which may occur is disregarded.

Of course, results so obtained cannot be accepted without further investigation. It is often easy to give an independent proof.

As an example, we give Cayley's method of obtaining the theorem proved in *H.A.*, XXIII, 4, Ex. 4.

Ex. 1. *If*

$$\frac{t}{e^t - 1} = 1 - B_1 t + B_2 \frac{t^2}{\lfloor 2} - B_3 \frac{t^3}{\lfloor 3} + \dots$$

so that $(-1)^{n-1}B_{2n}$ *is the n-th number of Bernoulli, then*

$$(-1)^r B_r = \left(1 - \frac{\Delta}{2} + \frac{\Delta^2}{3} - \frac{\Delta^3}{4} + \dots\right) 0^r.$$

Cayley's Method. We have

$$e^{t \cdot 0} = 1 + t \cdot \frac{0}{\lfloor 1} + t^2 \cdot \frac{0^2}{\lfloor 2} + \dots \quad \text{and} \quad e^t - 1 = e^{t \cdot 1} - e^{t \cdot 0} = \Delta e^{t \cdot 0},$$

so that

$$e^t = (1 + \Delta) e^{t \cdot 0} \quad \text{and} \quad t = \log(1 + \Delta) e^{t \cdot 0}.$$

Therefore

$$\frac{t}{e^t - 1} = \frac{\log(1 + \Delta)}{\Delta} e^{t \cdot 0}$$

and

$$1 - B_1 t + B_2 \frac{t^2}{\lfloor 2} - \dots = \left(1 - \frac{\Delta}{2} + \frac{\Delta^2}{3} - \dots\right)\left(1 + t \cdot \frac{0}{\lfloor 1} + t^2 \cdot \frac{0^2}{\lfloor 2} + \dots\right),$$

and the result is obtained by equating the coefficients of t^r.

EXERCISE IV

1. If by expanding the terms of

$$1+(2x-x^2)+(2x-x^2)^2+\dots \qquad \text{(A)}$$

we form the double series

$$\left.\begin{array}{l} 1+0 \quad +0 \quad +0 \;+\dots \\ +\;2x-x^2 \quad +0 \quad +0 \;+\dots \\ +\,4x^2-\;4x^3+x^4 \;+0 \;+\dots \\ +\,8x^3-12x^4+6x^5-x^6+\dots \\ +\dots\dots\dots\dots\dots\dots \end{array}\right\}, \qquad \text{(B)}$$

where any row is the expansion of the corresponding term of (A), for what values of x is summation possible (i) by rows, (ii) by columns, (iii) by diagonals.

Verify that all of these ways are possible if the series

$$1+2x-x^2+4x^2-4x^3+x^4+\dots, \qquad \text{(C)}$$

obtained by expanding (A), is absolutely convergent.

2. Prove that the double series

$$\begin{array}{rl} \Sigma x^m y^n = & 1+x \;\;+x^2 \;\;+x^3 \;\;+\dots \\ & +\;y+xy\;+x^2y\;+x^3y\;+\dots \\ & +y^2+xy^2+x^2y^2+x^3y^2+\dots \\ & +\dots\dots\dots\dots\dots \end{array}$$

is absolutely convergent if $|x|<1$ and $|y|<1$, and find the sum.

3. If for every m, n, $|a_{mn}|\leq k$ where k is a positive fixed number, prove that the double series $\Sigma a_{mn}x^m y^n$ is absolutely convergent, provided that $|x|<1$ and $|y|<1$.

[For if $|x|=x'$ and $|y|=y'$, by the last example $\Sigma x'^m y'^n$ is convergent. Now use Art. 9.]

4. If $|x|<1$, prove that

$$\frac{x}{1-x}+\frac{x^2}{1-x^2}+\frac{x^3}{1-x^3}+\dots=x\cdot\frac{1+x}{1-x}+x^4\,\frac{1+x^2}{1-x^2}+x^9\,\frac{1+x^3}{1-x^3}+x^{16}\cdot\frac{1+x^4}{1-x^4}+\dots.$$

[Prove that each side is equal to $\Sigma_{m=1}^{m=\infty}\Sigma_{n=1}^{n=\infty}x^{mn}$.]

5. If $|x|<1$, prove that

$$\frac{x}{1-x}+\frac{x^2}{1-x^2}+\frac{x^3}{1-x^3}+\dots=x+d_2x^2+d_3x^3+\dots+d_nx^n+\dots,$$

where d_n is the number of divisors of n (including n and 1).

[The double series

$$\begin{array}{l} x+x^2+x^3+\dots \\ +x^2+x^4+x^6+\dots \\ +x^3+x^6+x^9+\dots \\ +\dots\dots\dots\dots \end{array}$$

is absolutely convergent, and its sum is the sum of the series on the left. Let p be any divisor of n and let $n=pq$. If $p\neq q$, the term x^n occurs in both the rows $x^p+x^{2p}+\dots$ and $x^q+x^{2q}+\dots$. But if $p=q$, these rows are identical. Hence the number of times which x^n occurs in the double series is d_n.]

6. If m, n have independently the values 0, 1, 2, ..., find conditions for the absolute convergence of the double series

$$\Sigma \frac{\lfloor m+n}{\lfloor m \lfloor n} x^m y^n;$$

and under these conditions find the sum of the series.

7. If $|q|<1$, prove that

(i) $$\frac{1}{1+q}+\frac{q}{1+q^3}+\frac{q^2}{1+q^5}+\ldots=\frac{1}{1-q}-\frac{q}{1-q^3}+\frac{q^2}{1-q^5}+\ldots,$$

(ii) $$\frac{q}{(1-q)^2}+\frac{q^2}{(1-q^2)^2}+\frac{q^3}{(1-q^3)^2}+\ldots=\frac{q}{1-q}+\frac{2q^2}{1-q^2}+\frac{3q^3}{1-q^3}+\ldots,$$

(iii) $$\frac{q(1+q^2)}{(1-q^2)^2}+\frac{q^3(1+q^6)}{(1-q^6)^2}+\frac{q^5(1+q^{10})}{(1-q^{10})^2}+\ldots=\frac{q}{1-q^2}+\frac{3q^3}{1-q^6}+\frac{5q^5}{1-q^{10}}+\ldots.$$

[These are 'q series' of Elliptic Functions.]

8. Prove that

$$\frac{1}{x}+\frac{1}{x(x+1)}+\frac{1}{x(x+1)(x+2)}+\ldots=e\left\{\frac{1}{x}-\frac{1}{\lfloor 1}\frac{1}{x+1}+\frac{1}{\lfloor 2}\frac{1}{x+2}-\ldots\right\}.$$

[Use the identity

$$\frac{1}{x(x+1)\ldots(x+n)}=\frac{1}{\lfloor n}\left\{\frac{1}{x}-C_1^n\cdot\frac{1}{x+1}+C_2^n\cdot\frac{1}{x+2}-\ldots+(-1)^nC_n^n\frac{1}{x+n}\right\}$$

to arrange the left-hand side as a double series. Prove that the double series is absolutely convergent. The right-hand side is the sum by columns.]

NOTE. This may have been discovered by a formal reckoning such as the following. Denoting the left-hand side by L and the right-hand side by R,

$$L=\left(1-\Delta+\frac{\Delta^2}{\lfloor 2}-\ldots\right)\frac{1}{x}=(e^{-\Delta})\frac{1}{x}=(e^{1-E})\frac{1}{x}$$

and

$$(e^{1-E})\frac{1}{x}=e\cdot(e^{-E})\frac{1}{x}=e\left(1-E+\frac{E^2}{\lfloor 2}-\ldots\right)\frac{1}{x}=R.$$

9. If $y>0$, show that

(i) $$\frac{1}{y+2}+\frac{1\cdot 2}{(y+2)(y+3)}+\frac{1\cdot 2\cdot 3}{(y+2)(y+3)(y+4)}+\ldots \text{ to } \infty=\frac{1}{y}.$$

(ii) $$\frac{1}{y(y+1)}+\frac{1}{y(y+1)(y+2)}+\frac{1\cdot 2}{y(y+1)(y+2)(y+3)}+\ldots \text{ to } \infty=\frac{1}{y^2}.$$

(iii) Hence show that if $x>0$,

$$\frac{1}{x^2}+\frac{1}{(x+1)^2}+\frac{1}{(x+2)^2}+\ldots=\frac{1}{x}+\frac{1}{2}\cdot\frac{1}{x(x+1)}+\frac{\lfloor 2}{3}\cdot\frac{1}{x(x+1)(x+2)}+\ldots.$$

[Convert the left-hand side into a double series by putting $y=x$, $x+1$, $x+2$, ..., in (ii). Explain why the double series is convergent, and that its sum by columns is the right-hand side.]

(iv) Hence find to five places of decimals the value of $\frac{1}{10^2}+\frac{1}{11^2}+\frac{1}{12^2}+\ldots$.

10. The double series $\Sigma(-1)^{m+n}\cdot\frac{1}{mn}$ converges to the sum $(\log 2)^2$ by rows, columns and diagonals.

[See *H.A.*, XX, 24, Ex. 1.]

11. If $0<p<\frac{1}{2}$, the double series $\Sigma(-1)^{m+n}\frac{1}{m^p n^p}$ converges by rows and columns to

$$\left(1-\frac{1}{2^p}+\frac{1}{3^p}-\dots\right)^2,$$

but it has no definite sum by diagonals.

12. Use the transformation of Art. 19, Ex. 2, to show that

$$\Sigma_{n=1}^{\infty} n^3x^n=\frac{x}{1-x}+7\left(\frac{x}{1-x}\right)^2+12\left(\frac{x}{1-x}\right)^3+6\left(\frac{x}{1-x}\right)^4.$$

13. If $\Sigma(-1)^{n-1}u_n$ is convergent, show that

$$u_1-u_2+u_3-\dots=\frac{1}{2}u_1-\frac{1}{2^2}\Delta u_1+\frac{1}{2^3}\Delta^2u_1-\dots.$$

[In Ex. 2, Art. 19, put $x=-1$, and use Abel's theorem.]

14. Given that $\frac{\pi}{4}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\dots$, prove that

$$\frac{\pi}{2}=1+\frac{1}{3}+\frac{1\cdot2}{3\cdot5}+\frac{1\cdot2\cdot3}{3\cdot5\cdot7}+\dots.$$

[Use the last example.]

15. Show that the sum of the series $(a+b)^m+(a+2b)^m+\dots(a+nb)^m$ may be written in the form

$$[(a+nb+Bb)^{m+1}-(a+Bb)^{m+1}]/(m+1)b,$$

where, after expansion, the indices of powers of B are to be replaced by suffixes, and the numerical value of B_s is given by the expansion $x/(1-e^{-x})=\Sigma\frac{B_sx^s}{\lfloor s}$.

16. If $S_r=1^r+2^r+\dots+n^r$ and $N=2n+1$, show that S_{r-1} can be expressed as a polynomial in N by the formula

$$2^r\,.\,r\,.\,S_{r-1}=2(N+B)^r-(N+2B)^r-(2B)^r,$$

where, after expansion, indices of powers of B are to be changed into suffixes. Verify this when $r=3$.

[If $f(x)=n+S_1x+S_2\frac{x^2}{\lfloor 2}$, by equation (**K**) of Art. 26,

$$f(x)=\frac{e^{\frac{1}{2}(N-1)x}-1}{1-e^{-x}}=\frac{e^{\frac{1}{2}Nx}}{\frac{x}{e^2}-e^{-\frac{x}{2}}}-\frac{1}{1-e^{-x}};$$

$$\therefore\ xf(x)=e^{\frac{Nx}{2}}(2e^{\frac{1}{2}Bx}-e^{Bx})-e^{Bx}$$
$$=2e^{\frac{1}{2}(N+B)x}-e^{(\frac{1}{2}N+B)x}-e^{Bx}.$$

Putting $2x$ for x and equating coefficients of x^r, the result follows at once.]

17. If x has any value, the series

$$1+\frac{m+1}{2m+1}\cdot\frac{x}{\underline{|1}}+\frac{(m+1)(m+2)}{(2m+1)(2m+2)}\cdot\frac{x^2}{\underline{|2}}+\cdots$$

is convergent. Denoting the sum by S, prove that $\lim_{m\to\infty} S=e^{x/2}$.

[**Let** $\mu=1/m$ and $y=x/2$, then

$$S=1+\frac{1+\mu}{1+\mu/2}\cdot\frac{y}{\underline{|1}}+\frac{(1+\mu)(1+2\mu)}{(1+\mu/2)(1+2\mu/2)}\cdot\frac{y^2}{\underline{|2}}+\cdots.$$

Write this in the form

$$S=1+(1+a_1\mu+a_2\mu^2+\ldots)\frac{y}{\underline{|1}}+(1+b_1\mu+b_2\mu^2+\ldots)\frac{y^2}{\underline{|2}}+\ldots,$$

and arrange as a double series

$$\begin{aligned}&1+\quad\frac{y}{\underline{|1}}+\frac{y^2}{\underline{|2}}\quad+\cdots\\&+0+\mu a\cdot\frac{y}{\underline{|1}}+\mu b\cdot\frac{y^2}{\underline{|2}}+\cdots\\&+\cdots\cdots\cdots\cdots\cdots\cdots.\end{aligned}$$

Do the same things for the series

$$S'=1+\frac{1+\mu}{1-\mu/2}\cdot\frac{y'}{\underline{|1}}+\frac{(1+\mu)(1+2\mu)}{(1-\mu/2)(1-2\mu/2)}\cdot\frac{y'^2}{\underline{|2}}+\ldots,$$

where $y'=|y|$ and prove that S' is convergent. It follows that the double series for S is absolutely convergent, and may be summed by rows. Therefore

$$S=r_0+r_1\mu+r_2\mu^2+\ldots,$$

where $r_0=e^y$ and r_1, r_2, ... are convergent series. Hence $\lim_{\mu\to 0} S=e^y$.]

CHAPTER IV

UNIFORM CONVERGENCE

1. Series whose Terms are Functions of a Variable x. Such a series will be written in the form

$$u_1(x)+u_2(x)+\ldots+u_n(x)+\ldots .$$

The sum to n terms will be denoted by $s_n(x)$, the sum to infinity (if it exists) by $s(x)$, and the remainder after n terms by $R_n(x)$.

Suppose that the series converges for all values of x in a certain interval.

Further, suppose that the terms of the series are all continuous functions of x in the interval.

The question arises as to whether $s(x)$ is necessarily continuous.

For any given value of n, $s_n(x)$ is continuous, for it is the sum of n continuous functions. But $s(x)$ is not the sum of a definite number of terms of the series. Therefore we are not justified in assuming that $s(x)$ is continuous. Consider the following instance.

Let
$$s_n(x)=\frac{nx}{nx+1}.$$

Here $s_n(x)$ is continuous in the interval $0\leqslant x<a$ where a is a positive number; also, *if x is not zero*, $s(x)=\lim\ s_n(x)=1$, as $n\to\infty$, but *if x is zero*, $s(x)=0$ for $s_n(x)=0$ for all values of n. Therefore $s(x)$ is discontinuous at $x=0$. It is useful to illustrate this graphically.

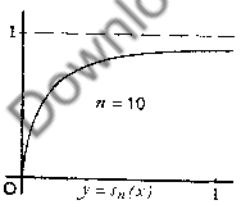


FIG. 20.

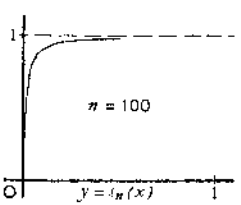


FIG. 21.

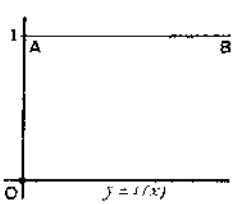


FIG. 22.

In Figs. 20, 21 the graph of $y=s_n(x)=nx/(nx+1)$ is shown for $n=10$ and $n=100$. It will be seen that as x tends to zero, y (although continuous) decreases very rapidly from a value nearly equal to 1 to zero. The graph of $y=s(x)=\lim nx/(nx+1)$ consists of the point O and the line AB, omitting the point A itself (Fig. 22).

The discontinuity arises from the fact that $s_n(x)$ is a function of two independent variables n and x.

In such cases it frequently happens that the operations of proceeding to the limit with each of the variables is not commutative. In this instance,

$$\lim_{x\to 0}\lim_{n\to\infty} s_n(x)=\lim_{n\to 0} 1=1, \text{ but } \lim_{n\to\infty}\lim_{x\to 0} s_n(x)=\lim_{n\to\infty} 0=0.$$

Ex. 1. *With regard to the series*

$$\frac{x}{x+1}+\frac{x}{(x+1)(2x+1)}+\frac{x}{(2x+1)(3x+1)}+\cdots,$$

although every term is a continuous function of x in the interval $0\leqslant x<a$, the series converges to a sum which is not continuous throughout the interval.

For $s_n(x)=nx/(nx+1)$; hence $s(x)$ is discontinuous at $x=0$.

Ex. 2. *If $R_n(x)$ is the remainder after n terms of the series in Ex.* 1, *and $x>0$ find the least value of n for which $R_n(x)<\epsilon$.*

We have

$$R_n(x)=s(x)-s_n(x)=1-\frac{nx}{nx+1}=\frac{1}{nx+1};$$

$$\therefore\ R_n(x)<\epsilon \quad \text{if} \quad nx+1>\frac{1}{\epsilon} \quad \text{or if} \quad n>\frac{1}{x}\left(\frac{1}{\epsilon}-1\right).$$

The required value of n is therefore the integer next greater than

$$\frac{1}{x}\left(\frac{1}{\epsilon}-1\right).$$

The value of n found in this example *depends on* x, and tends to ∞ as $x\to 0$. On this account, when x is small, the series is said to converge *infinitely slowly*.

2. Definition of Uniform Convergence. What has been said in Art. 1 leads to the following definitions:

(1) If for every value of x in a given interval

$$\lim_{n\to\infty} s_n(x)=s(x),$$

and if at every point of the interval a number m *independent of* x can be found so that

$$|\, s(x)-s_n(x)\,|<\epsilon \quad \text{for} \quad n\geqslant m,$$

where ϵ is any positive number, however small, *the function $s_n(x)$ is said to converge uniformly* in the interval to the limit $s(x)$.

(2) If the series $\Sigma u_n(x)$ converges for every value of x in a given interval, and if at every point of the interval a number m *independent of* x can be found so that

$$|\, R_n(x)\,|=|\, u_{n+1}(x)+u_{n+2}(x)+\ldots \text{ to } \infty\,|<\epsilon \text{ for } n\geqslant m,$$

the series is said to converge uniformly in the interval.

Ex. 1. *With regard to the geometric series* $1+x+x^2+\dots$,

(i) *The series converges uniformly in any interval which lies entirely within* $(-1, 1)$.

(ii) *Near the points* $x=\pm 1$, *the convergence is infinitely slow, and in an interval containing either of these points the convergence is not uniform.*

(i) Let $-a<x<a$ where a is any positive number less than unity. Let $|x|=x'$, so that $x'<a$, then

$$\begin{aligned} |R_n(x)| &= |x^n+x^{n+1}+\dots \text{ to } \infty| \\ &\leqslant x'^n+x'^{n+1}+\dots \text{ to } \infty \\ &< a^n+a^{n+1}+\dots \text{ to } \infty ; \end{aligned}$$

that is,
$$|R_n(x)|<a^n/(1-a).$$

Hence $R_n(x)<\epsilon$ if $a^n<(1-a)\epsilon$, that is, if $n\log a<\log(\epsilon-a\epsilon)$.
Since both sides of this inequality are negative, it is equivalent to

$$n>\frac{\log(\epsilon-a\epsilon)}{\log a}.$$

If then we take m to be the integer next greater than $\log(\epsilon-a\epsilon)/\log a$, we have

$$R_n(x)<\epsilon \quad \text{for} \quad n\geqslant m.$$

Since m is independent of x, the series converges uniformly in the interval.

(ii) *Let* $-1<x<1$. In this case we cannot choose a so that $x'<a<1$. As in the preceding, we have $|R_n(x)|\geqslant x'^n/(1-x')$; and, if m is the integer next greater than $\log(\epsilon-x'\epsilon)/\log x'$, then $|R_n(x)|<\epsilon$ for $n\geqslant m$.
Thus the series converges, but infinitely slowly, near $x=\pm 1$; for as $x'\to 1$, $\log x'\to 0$ and $m\to\infty$. And since m is not independent of x, the convergence is not uniform in the interval $(-1\leqslant x\leqslant 1)$.

3. Weierstrass's Test. *If* Σv_n *is a convergent series of positive terms and if, for all values of* n *and for all values of* x *in a certain interval*

$$|u_n(x)|\leqslant v_n,$$

then the series $\Sigma u_n(x)$ *converges absolutely and uniformly in the interval.*

Proof. Because $|u_n(x)|\leqslant v_n$ and Σv_n is convergent, $\Sigma|u_n(x)|$ is convergent, and therefore $\Sigma u_n(x)$ is absolutely convergent.

Let $R_n(x)$ and R_n' be the remainders after n terms of $\Sigma u_n(x)$ and Σv_n respectively. Then

$$|R_n(x)| = |u_{n+1}(x)+u_{n+2}(x)+\dots|;$$

and hence $R_n(x)\leqslant |u_{n+1}(x)|+|u_{n+2}(x)|+\dots\leqslant v_{n+1}+v_{n+2}+\dots\leqslant R_n'$.

Because Σv_n is convergent we can choose m so that $R_n'<\epsilon$ for $n\geqslant m$, therefore

$$R_n(x)<\epsilon \quad \text{for} \quad n\geqslant m.$$

Now m is independent of x, therefore $\Sigma u_n(x)$ converges uniformly.

Ex. 1. *The series* $\sin x + \frac{1}{2^2}\sin 2x + \frac{1}{3^2}\sin 3x + \ldots$ *converges absolutely and uniformly for all values of* x.

For $\left|\frac{1}{n^2}\sin nx\right| \leqslant \frac{1}{n^2}$ and $\Sigma\frac{1}{n^2}$ is convergent.

4. A Fundamental Theorem on Continuity. *If, at every point* x *in a given interval, the series* $\Sigma u_n(x)$ *converges uniformly to a sum* $s(x)$ *and if all the terms of the series are continuous functions of* x *at every point in the interval, so also is the sum* $s(x)$.

Proof. Let $s_n(x)$ and $R_n(x)$ denote the sum to n terms and the remainder after n terms of the series, so that

$$s(x) = s_n(x) + R_n(x).$$

Because the series converges uniformly, we can find m *independent of* x and x' so that $|R_m(x)| < \frac{1}{3}\epsilon$, and $|R_m(x')| < \frac{1}{3}\epsilon$,

where x and x' are any points in the interval.

Again, $s_m(x)$ is a continuous function of x, for it is the sum of a *fixed* number of terms each of which is continuous.

We can therefore choose η so that

$$|s_m(x) - s_m(x')| < \tfrac{1}{3}\epsilon \quad \text{if} \quad |x - x'| < \eta.$$

From these inequalities it follows that

$$|R_m(x) - R_m(x') + s_m(x) - s_m(x')| < \epsilon.$$

Therefore $|s(x) - s(x')| < \epsilon$ if $|x - x'| < \eta$.

That is to say, $s(x)$ is a continuous function of x.

5. Real Power Series. *The series* $\Sigma a_n x^n$ *converges absolutely and uniformly in any interval* $(-k, k)$ *which lies entirely within the interval of convergence* $(-R, R)$, *and its sum* $s(x)$ *is a continuous function of* x.

Proof. Choose h so that $k < h < R$. Then $\Sigma|a_n|h^n$ is convergent and, for every x in the interval $(-k, k)$,

$$|a_n x^n| < |a_n| . h^n.$$

Hence, by Weierstrass's test, $\Sigma a_n x^n$ converges uniformly and by Art. 4, $s(x)$ is a continuous function of x.

In considering the question whether $s(x)$ is continuous at either or both of the end points $x = \pm R$ of the interval, we require the following theorem.

6. Abel's Theorem. *If* Σa_n *converges (though not absolutely) and* $0 < x < 1$, *then* $\lim_{x \to 1} (a_0 + a_1 x + a_2 x^2 + \ldots \text{ to } \infty) = a_0 + a_1 + a_2 + \ldots \text{ to } \infty$.

We have to show that $\lim_{x\to 1}\{(1-x)a_1+(1-x^2)a_2+\ldots \text{ to } \infty\}=0.$

Let t_n be the sum to n terms of the last series, so that

$$t_n=(1-x^n)a_n+(1-x^{n-1})a_{n-1}+\ldots+(1-x)a_1.$$

Since Σa_n is convergent, we can find fixed numbers h, l such that, for all values of n,

$$l<a_n+a_{n-1}+\ldots+a_1<h.$$

Also the sequence

$$1-x^n,\quad 1-x^{n-1},\ \ldots\ 1-x,$$

is a decreasing sequence of positive terms, for $0<x<1$.

Therefore, by Abel's inequality (*H.A.*, XX, 10),

$$(1-x^n)l<t_n<(1-x^n)h.$$

Now, x is independent of n; and, as $x\to 1$, we shall have after a certain stage,

$$1-x<k/n^2,$$

where k is any positive constant, no matter how great n may be. Consequently

$$0<1-x^n<1-(1-k/n^2)^n.$$

Also $$\lim_{n\to\infty}(1-k/n^2)^n=\lim_{n\to\infty}e^{-k/n}=e^0=1.$$

Therefore $t_n\to 0$, which proves the theorem.

7. *If $\Sigma a_n x^n$ converges at an end point of its interval of convergence $(-R, R)$, then this point belongs to the interval of continuity of its sum $s(x)$.*

For $$a_0+a_1R\left(\frac{x}{R}\right)+a_2R^2\left(\frac{x}{R}\right)^2+\ldots=s(x).$$

Suppose that the series converges to the sum s_1 at $x=R$, so that

$$a_0+a_1R+a_2R^2+\ldots=s_1.$$

Then by Abel's theorem, $\lim_{x\to R}s(x)=s_1$, showing that the point $x=R$ belongs to the interval of continuity.

Similarly the point $x=-R$ belongs to this interval if $\Sigma a_n x^n$ converges when $x=-R$.

For example, $$\log(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\ldots \text{ if } |x|<1.$$

Also the series is convergent when $x=1$, hence

$$1-\tfrac{1}{2}+\tfrac{1}{3}-\tfrac{1}{4}+\ldots=\lim_{x\to 1}\log(1+x)=\log 2.$$

8. Multiplication of Series. The theorem of *H.A.*, XX, 24, follows easily from Abel's theorem. We have to show that *if*

$$d_n = u_0v_n + u_1v_{n-1} + u_2v_{n-2} + \ldots + u_nv_0$$

and the series Σu_n, Σv_n, Σd_n *converge (though not absolutely), then*

$$(u_0+u_1+u_2+\ldots)(v_0+v_1+v_2+\ldots) = d_0+d_1+d_2+\ldots .$$

Proof. The series Σu_nx^n, Σv_nx^n converge absolutely in the interval $(-1<x<1)$, for they converge when $x=1$. Hence at all points in this interval, by *H.A.*, XX, 22,

$$(u_0+u_1x+u_2x^2+\ldots)(v_0+v_1x+v_2x^2+\ldots) = d_0+d_1x+d_2x^2+\ldots ;$$

and, by Abel's theorem, since Σu_n, Σv_n, Σd_n are convergent,

$$\lim_{x\to 1}(u_0+u_1x+u_2x^2+\ldots) = u_0+u_1+u_2+\ldots .$$

Similar equations hold for Σv_n and Σd_n, and therefore

$$(u_0+u_1+u_2+\ldots)(v_0+v_1+v_2+\ldots) = d_0+d_1+d_2+\ldots .$$

9. Differentiation of Power Series.

(1) *The sum* $s(x)$ *of the infinite series*

$$a_0+a_1x+a_2x^2+\ldots+a_nx^n+\ldots$$

has a derivative $s'(x)$ *at every point within the interval* $(-R, R)$ *of convergence of the series and* $s'(x) = a_1+2a_2x+\ldots+na_nx^{n-1}+\ldots$.

If $x+h$ is within the interval $(-R, R)$,

$$s(x+h) = a_0+a_1(x+h)+a_2(x+h)^2+\ldots . \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

Transform the last series into the double series

$$\left.\begin{array}{llll} a_0 & +0 & +0 & \ldots \\ +a_1x & +a_1h & +0 & \ldots \\ +a_2x^2 & +2a_2xh & +a_2h^2 & \ldots \\ + & \ldots\ldots\ldots & & \end{array}\right\} . \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

Let accented letters denote absolute values, and consider the double series

$$\left.\begin{array}{llll} a_0' & +0 & +0 & \ldots \\ +a_1'x' & +a_1'h' & +0 & \ldots \\ +a_2'x'^2 & +2a_2'x'h' & +a_2'h'^2 & \ldots \\ + & \ldots\ldots\ldots & & \end{array}\right\} . \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

Summing the series (C) by rows, we obtain

$$a_0'+a_1'(x'+h')+a_2'(x'+h')^2+\ldots .$$

This series converges if $x'+h'<R$.

Hence (C) is convergent and (B) is absolutely convergent if

$$|x|+|h|<R. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(D)}$$

With this condition, every column of (B) converges absolutely, and the sum by columns of the double series is $s(x+h)$. Thus

$$s(x+h)=s(x)+hs_1(x)+h^2s_2(x)+\dots, \quad \text{.................(E)}$$

where
$$s_1(x)=a_1 \quad +2a_2x \quad +3a_3x^2 \quad +\dots,$$
$$s_2(x)=a_2 \quad +3a_3x \quad +6a_4x^2 \quad +\dots,$$
$$\dots\dots\dots\dots\dots\dots\dots$$

Hence
$$\frac{s(x+h)-s(x)}{h}=s_1(x)+hs_2(x)+h^2s_3(x)+\dots.$$

The sum of the last series is continuous in the interval $(-R, R)$, and the sum tends to $s_1(x)$ as $h\to 0$, therefore

$$\lim_{h\to 0}\frac{s(x+h)-s(x)}{h}=s_1(x), \text{ that is to say, } s'(x)=s_1(x).$$

Ex. 1. *Show that the series*

$$u_0+u_1x+u_2x^2+\dots+u_nx^n+\dots \quad \text{..............................(A)}$$

and
$$u_1+2u_2x+3u_3x^2+\dots+nu_{n-1}x^{n-1}+\dots \quad \text{.......................(B)}$$

have the same interval of convergence.

It has just been shown that if (A) is absolutely convergent, so is (B).

Again, $|u_nx^{n-1}|\leqslant n|u_nx^{n-1}|$, hence, if (B) is absolutely convergent, so is (A). This proves the statement in question.

10. Higher Derivatives. Applying the theorem of Art. 9 to the equation

$$s'(x)=a_1+2a_2x+3a_3x^2+\dots,$$

we infer the existence of the second derivative $s''(x)$ of $s(x)$, and that

$$s''(x)=1\,.\,2a_2+2\,.\,3a_3x+3\,.\,4a_4x^2+\dots.$$

Continuing in this way, it is seen that the rth derivative $s^{(r)}(x)$ exists, and that

$$s^{(r)}(x)=\lfloor r\, a_r+\frac{\lfloor r+1}{\lfloor 1}a_{r+1}x+\frac{\lfloor r+2}{\lfloor 2}a_{r+2}x^2+\dots$$
$$=\lfloor r\,(a_r+C_1^{r+1}a_{r+1}x+C_2^{r+2}a_{r+2}x^2+\dots).$$

Note that *all these series are absolutely convergent in the interval* $(-R, R)$.

11. A particular case of Taylor's Theorem. *If at any point in the interval* $(-R, R)$ *the function* $s(x)$ *can be expanded in a convergent series of positive integral powers of* x, *then*

$$s(x+h)=s(x)+\frac{h}{\lfloor 1}s'(x)+\frac{h^2}{\lfloor 2}s''(x)+\dots+\frac{h^r}{\lfloor r}s^{(r)}(x)+\dots,$$

provided that
$$|x|+|h|<R.$$

For by equation (E) of Art. 9,

$$s(x+h)=s(x)+hs_1(x)+\ldots+h^r s_r(x)+\ldots,$$

where $s_r(x)$ is the coefficient of h^r in the expansion of

$$a_0+a_1(x+h)+\ldots+a_r(x+h)^r+\ldots;$$

$$\therefore\ s_r(x)=a_r+C_1^{r+1}a_{r+1}x+C_2^{r+2}a_{r+2}x^2+\ldots=\frac{s^{(r)}(x)}{\lfloor r};$$

and the theorem follows as stated.

12. Integration of Power Series. *If at any point of the interval* $(-R, R)$

$$s(x)=a_0+a_1x+a_2x^2+\ldots+a_nx^n+\ldots,$$

then, within the same interval,

$$\int s(x)\,dx=a_0x+\frac{1}{2}a_1x^2+\frac{1}{3}a_2x^3+\ldots+\frac{1}{n+1}a_nx^{n+1}+\ldots+C,$$

where C *is independent of* x.

For the series $a_0x+\frac{1}{2}a_1x^2+\frac{1}{3}a_2x^3+\ldots$ converges absolutely at any point in the interval; hence, denoting its sum by y, we have

$$\frac{dy}{dx}=a_0+a_1x+a_2x^2+\ldots=s(x),$$

and the result follows from Art. 9.

Ex. 1. **Gregory's Series.** *Using* $\tan^{-1}y$ *to denote the angle whose tangent is* y *and which lies between* $-\pi/2$ *and* $\pi/2$ *or* $=\pi/2$, *prove that*

$$\tan^{-1}y=y-\frac{y^3}{3}+\frac{y^5}{5}-\frac{y^7}{7}+\ldots \quad \textit{when} \quad -1<y\leqslant 1. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

Let $x=\tan^{-1}y$, then $y=\tan x$ and $\dfrac{dy}{dx}=\sec^2 x=1+y^2$;

$$\therefore\ \frac{dx}{dy}=\frac{1}{1+y^2}=1-y^2+y^4-\ldots \quad \text{if} \quad -1<y<1.$$

Hence, by integration, $\tan^{-1}y=x=y-\dfrac{y^3}{3}+\dfrac{y^5}{5}-\ldots$ if $-1<y<1$.

Also the series is convergent when $y=1$, and therefore, by Abel's theorem, the equation holds when $y=1$, so that

$$\frac{\pi}{4}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\ldots. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

NOTE. For the evaluation of π, the series (B) converges too slowly. Computers have applied equation (A) to such equalities as

$$\frac{\pi}{4}=\tan^{-1}\frac{1}{2}+\tan^{-1}\frac{1}{5}+\tan^{-1}\frac{1}{8}, \quad \text{(Dase)}$$

$$\frac{\pi}{4}=4\tan^{-1}\frac{1}{5}-\tan^{-1}\frac{1}{70}+\tan^{-1}\frac{1}{99}; \quad \text{(Rutherford)}$$

obtaining the value of π to 200 and 440 places respectively.

For further information see *Encyc. Brit.*, article on 'Circle.'

13. Values of $S_n = \frac{1}{1^n} + \frac{1}{2^n} + \frac{1}{3^n} + \ldots$ to ∞, for $n = 2, 3, 4$, etc.

It is proved in treatises on trigonometry that, if $|\theta| < \pi$,

$$\sin\theta = \theta\left(1 - \frac{\theta^2}{\pi^2}\right)\left(1 - \frac{\theta^2}{2\pi^2}\right)\ldots\left(1 - \frac{\theta^2}{r^2\pi^2}\right)\ldots.$$

Taking logarithms, we find that

$$\log\theta - \log\sin\theta = \Sigma_{r=1}^\infty \log\left(1 - \frac{\theta^2}{r^2\pi^2}\right)$$

$$= \Sigma_{r=1}^\infty \left[\frac{\theta^2}{r^2\pi^2} + \frac{1}{2}\frac{\theta^4}{r^4\pi^4} + \frac{1}{3}\frac{\theta^6}{r^6\pi^6} + \ldots\right].$$

This double series converges when summed by rows; hence, since it is a series of positive terms, it converges to the same sum when summed by columns. Therefore it follows that

$$\log\theta - \log\sin\theta = \frac{\theta^2}{\pi^2}S_2 + \frac{1}{2}\frac{\theta^4}{\pi^4}S_4 + \frac{1}{3}\frac{\theta^6}{\pi^6}S_6 + \ldots; \quad \ldots\ldots\ldots\ldots(A)$$

and thus, $S_{2n}/n\pi^{2n}$ is equal to the coefficient of θ^{2n} in the expansion of

$$-\log\left(1 - \frac{\theta^2}{\lfloor 3} + \frac{\theta^4}{\lfloor 5} - \ldots\right).$$

The values of S_2, S_4, S_6, ..., can be found in terms of Bernoulli's numbers in the following manner. From equation (A), by differentiation,

$$\theta\cot\theta = 1 - 2\left[\frac{\theta^2}{\pi^2}S_2 + \frac{\theta^4}{\pi^4}S_4 + \ldots + \frac{\theta^{2n}}{\pi^{2n}}S_{2n} + \ldots\right];$$

and, by Art. 28 of the preceding chapter,

$$\theta\cot\theta = 1 - 2^2B_2\frac{\theta^2}{\lfloor 2} + 2^4B_4\frac{\theta^4}{\lfloor 4} - \ldots + (-1)^n 2^{2n}B_{2n}\frac{\theta^{2n}}{\lfloor 2n} + \ldots;$$

hence, by equating coefficients, we find that

$$S_{2n} = \frac{(-1)^{n-1}2^{2n-1}}{\lfloor 2n}\cdot B_{2n}\pi^{2n}.$$

No corresponding formula exists for the values of S_3, S_5, S_7, etc.; the first few of these, according to Legendre, are given in the table below.

S_3	= 1·202	056	903	16	S_5	= 1·036	927	755	14
S_7	= 1·008	349	277	38	S_9	= 1·002	008	392	83
S_{11}	= 1·000	494	188	60	S_{13}	= 1·000	122	713	35
S_{15}	= 1·000	030	588	24	S_{17}	= 1·000	007	637	20

14. Euler's Constant. *If* $u_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} - \log n$, *then*

(i) *as* $n \to \infty$, $u_n \to$ *a constant* γ, *known as Euler's constant.**

(ii) $\gamma = \log_e 2 - 2\left\{\frac{1}{3 \cdot 2^3} S_3 + \frac{1}{5 \cdot 2^5} S_5 + \frac{1}{7 \cdot 2^7} S_7 + \ldots\right\}$.

The identity, $\frac{3}{1} \cdot \frac{5}{3} \cdot \frac{7}{5} \cdots \frac{2n+1}{2n-1} \cdot \frac{1}{2n+1} = 1$, may be written in the form

$$\left(\frac{1+\frac{1}{2}}{1-\frac{1}{2}}\right) \cdot \left(\frac{1+\frac{1}{4}}{1-\frac{1}{4}}\right) \cdot \left(\frac{1+\frac{1}{6}}{1-\frac{1}{6}}\right) \cdots \left(\frac{1+\frac{1}{2n}}{1-\frac{1}{2n}}\right) = 2n+1.$$

Taking logarithms of each side, and observing that, as n tends to infinity, $\log(2n+1) - \log 2n$ tends to zero, we have on expansion

$$2\sum_{r=1}^{r=n}\left\{\frac{1}{2r} + \frac{1}{3}\left(\frac{1}{2r}\right)^3 + \frac{1}{5}\left(\frac{1}{2r}\right)^5 + \ldots\right\} - \log 2n \to 0;$$

that is,

$$u_n + 2T \to \log 2,$$

where

$$T = \sum_{r=1}^{r=n}\left\{\frac{1}{3 \cdot 2^3}\frac{1}{r^3} + \frac{1}{5} \cdot \frac{1}{2^5}\frac{1}{r^5} + \ldots\right\},$$

Now, T is an infinite double series, which, when summed by columns, is

$$\frac{1}{3 \cdot 2^3} S_3 + \frac{1}{5 \cdot 2^5} S_5 + \frac{1}{7 \cdot 2^7} S_7 + \ldots,$$

and this is obviously convergent; hence, since all the terms of T are positive, it converges to the same limit when summed by rows.

Therefore

$$u_n \to \gamma = \log_e 2 - 2T.$$

Ex. 1. *Calculate the value of* γ *to ten decimal places.*

Observing that

$$\log 3 = \log(1+\tfrac{1}{2})/(1-\tfrac{1}{2}) = 1 + 2\left\{\frac{1}{3} \cdot \frac{1}{2^3} + \frac{1}{5} \cdot \frac{1}{2^5} + \frac{1}{7} \cdot \frac{1}{2^7} + \ldots\right\},$$

and writing S_r' for $(S_r - 1)$, we have

$$\gamma = 1 + \log 2 - \log 3 - 2\left\{\frac{1}{3 \cdot 2^3} S_3' + \frac{1}{5 \cdot 2^5} S_5' + \ldots \text{ to } \infty\right\}.$$

The numbers, S_3', S_5', ..., when multiplied by the appropriate fraction, decrease very rapidly, and using the values of S_{2r+1}, given in Art. 13, we have

$$1 + \log 2 = 1{\cdot}693\ 147\ 180\ 56, \qquad \log 3 = 1{\cdot}098\ 612\ 288\ 67,$$

and

$$S_3'/(3 \cdot 2^3) = 0{\cdot}008\ 419\ 073\ 63, \qquad S_5'/(5 \cdot 2^5) = 0{\cdot}000\ 230\ 798\ 47,$$

$$S_7'/(7 \cdot 2^7) = 0{\cdot}000\ 009\ 318\ 38, \qquad S_9'/(9 \cdot 2^9) = 0{\cdot}000\ 000\ 435\ 85,$$

and so on; from which it will be found that, to ten decimal places,

$$\gamma = 0{\cdot}577\ 215\ 664\ 9.$$

* Another proof of (i) is given in *H.A.*, XIX, 9.

15. Complex Series. The notion of uniform convergence is extended to complex sequences and series as follows. In the definitions of Art. 2, replace x by the complex variable z and for 'interval' read 'area in the z-plane.' Thus for the series $\Sigma u_n(z)$, whose terms are functions of the complex variable z (*H.A.*, XVII, 29), we have the following definition.

If the series $\Sigma u_n(z)$ converges for every value of z which is represented by a point in a given area A, and if at every point z in A a number m independent of z can be found so that

$$| R_n(z) | = | u_{n+1}(z) + u_{n+2}(z) + \dots \text{ to } \infty | < \epsilon \text{ for } n \geqslant m,$$

the series is said to converge uniformly in the area.

With the alterations mentioned above, Weierstrass's test for uniform convergence (Art. 3) and the theorem on continuity in Art. 4 hold for complex series. The theorem on continuity is as follows.

If, at every point z in a given area, the series $\Sigma u_n(z)$ converges uniformly to a sum $s(z)$, and if all the terms of the series are continuous functions of z at every point in the area, so also is the sum $s(z)$.

16. Complex Power Series. (1) *The series $\Sigma a_n z^n$ converges absolutely and uniformly in any area A of the z-plane which is entirely within its circle of convergence and the sum $s(z)$ is a continuous function of z in this area.*

For, let z be any point in A and let R be the radius of convergence. Choose h so that $|z| < h < R$. Then $\Sigma | a_n | h^n$ is convergent and $|a_n z^n| < | a_n | h^n$. Therefore, by Weierstrass's test, $\Sigma a_n z^n$ is absolutely and uniformly convergent. Hence $\Sigma a_n z^n$ converges absolutely and uniformly in the region A and $s(z)$ is a continuous function of z.

The question as to whether *the region of continuity of $s(z)$ extends right up to and includes points on the circle of convergence* is considered below.

(2) *Let z_0 be a point on the circle of convergence of $\Sigma a_n z^n$ at which the series is convergent, and suppose that z approaches z_0 by moving along the radius Oz_0, then* $\lim s(z) = s(z_0)$.

Let $a_n = a_n' (\cos\alpha + \iota \sin\alpha)$,

and $z = r(\cos\theta + \iota \sin\theta)$,

then $z_0 = R(\cos\theta + \iota \sin\theta)$

and $a_n z^n = a_n' r^n \{\cos(n\theta + \alpha) + \iota \sin(n\theta + \alpha)\}$

$$= u_n \left(\frac{r}{R}\right)^n + \iota v_n \left(\frac{r}{R}\right)^n,$$

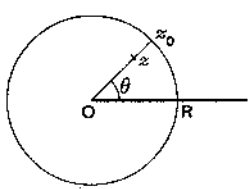


FIG. 23.

where $u_n = R^n a_n' \cos(n\theta + \alpha)$ and $v_n = R^n a_n' \sin(n\theta + \alpha)$.

Now, if $r/R=1$, $\Sigma a_n z^n$ is convergent by hypothesis; therefore the real series Σu_n, Σv_n are convergent, and by Abel's theorem,

$$\lim_{r\to R} \Sigma_0^\infty u_n\left(\frac{r}{R}\right)^n = \Sigma_0^\infty u_n \quad \text{and} \quad \lim_{r\to R} \Sigma_0^\infty v_n\left(\frac{r}{R}\right)^n = \Sigma_0^\infty v_n ;$$

therefore $$\lim_{z\to z_0} s(z) = \Sigma_0^\infty u_n + \iota\Sigma_0^\infty v_n = s(z_0).$$

(3) *If z approaches z_0 from within the circle of convergence in such a way that its path cuts the circle at a finite angle,* then*

$$\lim s(z) = s(z_0).$$

Through z draw a circle with centre O to cut the radius Oz_0 at z_1.

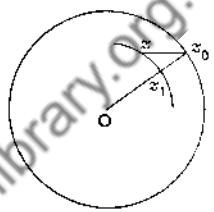


FIG. 24.

Because $s(z)$ is continuous at all points inside the circle of convergence, we can choose η_1 so that

$$|s(z)-s(z_1)| < \tfrac{1}{2}\epsilon \quad \text{if} \quad |z-z_1| < \eta_1 ;$$

and on account of Theorem (2) we can choose η_2 so that $|s(z_1)-s(z_0)| < \tfrac{1}{2}\epsilon$ if $|z_1-z_0| < \eta_2$.

Now when z is near z_0, both $|z-z_1|$ and $|z_1-z_0|$ are less than $|z-z_0|$. (This is evident geometrically.)

If the smaller of η_1 and η_2 is denoted by η, both of the above inequalities hold if $|z-z_0|<\eta$. Hence by addition,

$$|s(z)-s(z_0)| < \epsilon \quad \text{if} \quad |z-z_0| < \eta,$$

therefore $$\lim s(z) = s(z_0).$$

(4) *Any point z_0 on the circle of convergence of $\Sigma a_n z^n$, at which the series converges, belongs to the region of continuity of its sum $s(z)$.*

This follows from (2) and (3), it being understood that *points near z_0 on the circumference of the circle* do not necessarily belong to the region.

17. Binomial Theorem, n rational, z complex. *If n is rational and $|z|<1$, the sum of the series*

$$1 + nz + \frac{n(n-1)}{\lfloor 2}z^2 + \ldots + \frac{n(n-1)\ldots(n-r+1)}{\lfloor r}z^r + \ldots ,$$

is the principal value of $(1+z)^n$. This is also true, if $|z|=1$, in two cases:

(i) if $n>0$; (ii) if $-1<n<0$ and $z\neq -1$.

First suppose that $|z|<1$.

Let $z = r(\cos\theta + \iota\sin\theta)$ and $u = 1+z = \rho(\cos\phi + \iota\sin\phi)$.

* This is to exclude cases in which z, as it approaches z_0, ultimately moves along the circumference, so passing through points at which the series is not necessarily convergent.

The point z is within the circle $(0, 1)$ and the point u is within the circle $(1, 1)$, so that

$$-\tfrac{1}{2}\pi < \phi < \tfrac{1}{2}\pi.$$

Thus ϕ is the angle between $-\tfrac{1}{2}\pi$ and $\tfrac{1}{2}\pi$ such that

$$\tan\phi = \frac{r\sin\theta}{r+1\cos\theta}.$$

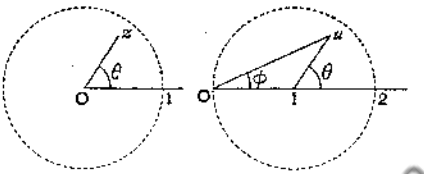


FIG. 25.

Also $\rho = (1 + 2r\cos\theta + r^2)^{\frac{1}{2}}$.

Let
$$f(n) = 1 + nz + \frac{n(n-1)}{\lfloor 2}z^2 + \dots .$$

Because $|z| < 1$, the series is absolutely convergent and, as in *H.A.*, XXI, 3, for all values of m and n,

$$f(m) \cdot f(n) = f(m+n). \qquad \text{(A)}$$

(i) *Let* $n = p/q$, where p, q are positive integers, prime to one another.

Then
$$\left\{f\left(\frac{p}{q}\right)\right\}^q = f(p) = (1+z)^p.$$

Hence $f\left(\frac{p}{q}\right)$ is a qth root of $(1+z)^p$, so that

$$f\left(\frac{p}{q}\right) = \rho^{\frac{p}{q}}\left(\cos\frac{p\phi + 2k\pi}{q} + \iota\sin\frac{p\phi + 2k\pi}{q}\right),$$

where $\rho^{\frac{p}{q}}$ is the real positive qth root of ρ^p, and k is one of the numbers $0, 1, 2, \dots q-1$.

That k has the same value for all values of z follows from the fact that the sum of the series denoted by $f\left(\frac{p}{q}\right)$ is a continuous function of z. To find this value let $\theta = 0$; then $\phi = 0$ and $f\left(\frac{p}{q}\right) = \cos\frac{2k\pi}{q} + \iota\sin\frac{2k\pi}{q}$. But in this case $f\left(\frac{p}{q}\right)$ is real and positive; thus $k = 0$. Hence, if $|z| < 1$,

$$f\left(\frac{p}{q}\right) = \rho^{\frac{p}{q}}\left(\cos\frac{p\phi}{q} + \iota\sin\frac{p\phi}{q}\right) = \text{the principal value of } (1+z)^{\frac{p}{q}}.$$

(ii) *Let* $n = -\frac{p}{q}$. From equation (A), we have $f\left(-\frac{p}{q}\right) \cdot f\left(\frac{p}{q}\right) = f(0) = 1$; therefore

$$f\left(-\frac{p}{q}\right) = \rho^{-\frac{p}{q}}\left(\cos\frac{p\phi}{q} - \iota\sin\frac{p\phi}{q}\right) = \rho^{-\frac{p}{q}}\left\{\cos\left(-\frac{p\phi}{q}\right) + \iota\sin\left(-\frac{p\phi}{q}\right)\right\},$$

which is the principal value of $(1+z)^{-\frac{p}{q}}$.

In considering the case when $|z|=1$, we note that

(i) The sum $f(n)$ of the series is a continuous function of z at all points within the circle of convergence. Also any point on the circle at which the series converges belongs to the region of continuity (Art. 16).

(ii) The series converges at all points on the circle, if $n>0$; and at all points on the circle except the point $z=-1$, if $-1<n<0$ (*H.A.*, XX, 21).

(iii) The principal value of $(1+z)^n$ is continuous for all values of z.

Hence the result is that stated above.

Ex. 1. *If* $z=\cos\theta+\iota\sin\theta$ *where* $-\pi<\theta<\pi$, *then*

$$1+nz+\frac{n(n-1)}{\lfloor 2}z^2+\ldots=(2\cos\tfrac{1}{2}\theta)^n(\cos\tfrac{1}{2}n\theta+\iota\sin\tfrac{1}{2}n\theta).$$

For the series is convergent, $\phi=\frac{1}{2}\theta$ and $\rho=2\cos\frac{\theta}{2}$.

18. A Property of the Binomial Series. *If* $|z|<1$ *and* n *is any number, the series*

$$f(n)=1+nz+\frac{n(n-1)}{\lfloor 2}z^2+\ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathrm{A})$$

can be arranged as an absolutely convergent power series in n. *Consequently its sum* $f(n)$ *is a continuous function of* n.

Proof. Transform the series (A) into the double series

$$\left.\begin{array}{lllll} 1, & 0, & 0, & 0, & \ldots \\ 0, & nz, & 0, & 0, & \ldots \\ 0, & -\frac{1}{2}nz^2, & \frac{1}{2}n^2z^2, & 0, & \ldots \\ 0, & \frac{1}{3}nz^3, & -\frac{1}{2}n^2z^3, & \frac{1}{6}n^3z^3, & \ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \end{array}\right\}, \quad \ldots\ldots\ldots\ldots\ldots\ldots(\mathrm{B})$$

the mth row containing the terms in the expansion of the mth term of (A).

Now let $z'=|z|$, $n'=|n|$, and consider the double series

$$\left.\begin{array}{lllll} 1, & 0, & 0, & 0, & \ldots \\ 0, & n'z', & 0, & 0, & \ldots \\ 0, & \frac{1}{2}n'z'^2, & \frac{1}{2}n'^2z'^2, & 0, & \ldots \\ 0, & \frac{1}{3}n'z'^3, & \frac{1}{2}n'^2z'^3, & \frac{1}{6}n'^3z'^3, & \ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \end{array}\right\}. \quad \ldots\ldots\ldots\ldots\ldots\ldots(\mathrm{C})$$

Summing by rows, we obtain the series

$$1+n'z'+\frac{n'(n'+1)}{\lfloor 2}z'^2+\ldots,$$

which is convergent if $z'<1$.

Hence (**C**) is convergent and (**B**) absolutely convergent, so that the sum of (**B**) by rows is equal to its sum by columns. Therefore

$$f(n) = 1 + c_1 n + c_2 n^2 + \dots, \qquad \text{(D)}$$

where

$$c_1 = z - \tfrac{1}{2}z^2 + \tfrac{1}{3}z^3 - \dots,$$
$$c_2 = \tfrac{1}{2}z^2 - \tfrac{1}{3}(\tfrac{1}{1}+\tfrac{1}{2})z^3 + \tfrac{1}{4}(\tfrac{1}{1}+\tfrac{1}{2}+\tfrac{1}{3})z^4 - \dots,$$
$$\dots\dots\dots\dots\dots\dots$$

and the series (**D**) is absolutely convergent for all values of n. Therefore $f(n)$ is a continuous function of n.

19. Binomial Theorem (*continued*). If x is real and > -1, the principal value of $(1+x)^n$ is the real positive value of $(1+x)^n$, which is equal to $e^{n\log(1+x)}$.

This is a continuous function of n; so also is $f(n)$. Hence we can extend Euler's proof, given in *H.A.*, XXI, 3, to the case of a *real index*.

20. Logarithmic Series. If $-1<x<1$, for all real values of n,

$$1 + nx + \frac{n(n-1)}{\lfloor 2}x^2 + \dots$$
$$= \text{the principal value of } (1+x)^n$$
$$= e^{n\log(1+x)}$$
$$= 1 + n\log(1+x) + \frac{1}{\lfloor 2}\{n\log(1+x)\}^2 + \dots.$$

By Art. 18, we can arrange the first series in the form

$$1 + c_1 n + c_2 n^2 + \dots,$$

and, equating coefficients, we find that

$$\log(1+x) = x - \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 - \dots$$
$$\tfrac{1}{2}\{\log(1+x)\}^2 = \tfrac{1}{2}x^2 - \tfrac{1}{3}(\tfrac{1}{1}+\tfrac{1}{2})x^3 + \tfrac{1}{4}(\tfrac{1}{1}+\tfrac{1}{2}+\tfrac{1}{3})x^4 - \dots$$
$$+ (-1)^n\frac{1}{n}\left(\tfrac{1}{1}+\tfrac{1}{2}+\dots+\frac{1}{n-1}\right)x^n + \dots,$$

and so on.

These series converge when $x=1$, therefore, by Abel's theorem, the results hold when $x=1$.

EXERCISE V

1. If a is any positive number less than unity, prove that the function x^n converges uniformly to zero as a limit in the interval $(0, a)$.
[Show that $x^n < \epsilon$ if $n > \log\epsilon/\log a$.]

2. Show that the function x^n converges to zero in the interval $0 \leqslant x < 1$, but that as $x \to 1$ the convergence is infinitely slow.

3. If $s(x)=\lim_{n\to\infty} x^n$ where $0\leqslant x\leqslant 1$, show that $s(x)$ is discontinuous at the point $x=1$.

4. Illustrate Exx. 1·3 by drawing the graph of $y=x^n$ from $x=0$ to $x=1$ for the values 2, 4, 50 of n. (Fig. 26.)

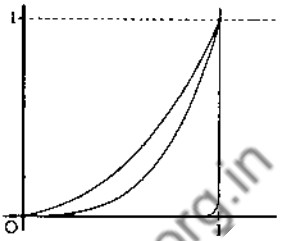


Fig. 26.

5. If $$y=s_n(x)=\frac{nx}{n^2x^2+1},$$

prove that (i) the function $s_n(x)$ converges to zero in any interval (a, b).

(ii) If the interval does not include zero, the convergence is uniform, but if zero is included, then $x=0$ is a point of non-uniform convergence.

(iii) For a given value of n, the maximum value of y is $\frac{1}{2}$ and the corresponding value of x is $1/n$.

(iv) Draw the graph of $y=s_n(x)$ for $n=2$, 4, 10 and $x>0$. Prove by graphical considerations that the convergence is not uniform at $x=0$.

[(i), (ii) Prove that $|s_n(x)|<\epsilon$ if

$$n>\frac{1}{2\epsilon|x|}(1+\sqrt{1-4\epsilon^2}).$$

Hence show that if x is in the interval (a, b), *which does not include zero*, $s_n(x)<\epsilon$ for $n\geqslant m$, where m is the integer next greater than

$$\frac{1}{2\epsilon k}(1+\sqrt{1-4\epsilon^2}),$$

k being the smaller of $|a|$, $|b|$. Now complete the explanations in (i) and (ii).]

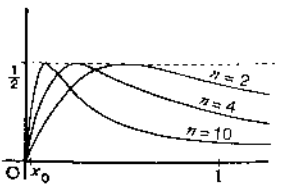


Fig. 27.

(v) Take any value x_0 of x, however small. From (iii) it appears that as $n\to\infty$, the peak of the curve $y=s_n(x)$ moves to the left of the ordinate through x_0. Hence it is impossible to find m so that $|s_n(x)|<\epsilon$ for $n\geqslant m$ and for every x in the interval (O, x_0).

Therefore $x=0$ is a point of non-uniform convergence.

6. If $$y=s_n(x)=\frac{nx(1-x)}{n^2x^2+(1-x)^2},$$

(i) prove that $s_n(x)$ converges to zero in the interval $0\leqslant x\leqslant 1$.

(ii) Show that $|s_n(x)|<\epsilon$ if $n>\frac{1}{2\epsilon}\cdot\left|\frac{x}{1-x}\right|\cdot(1+\sqrt{1-4\epsilon^2})$.

(iii) If $a\leqslant x\leqslant 1$, where a is any positive number less than unity, show that

$$|s_n(x)|<\epsilon \text{ if } n>\frac{1}{2\epsilon}\cdot\frac{1-a}{a}(1+\sqrt{1-4\epsilon^2}),$$

and that the convergence is uniform in the interval.

(iv) Explain why, in an interval including zero, $x=0$ is a point of non-uniform convergence.

Illustrate this by drawing the graph of $y=s_n(x)$ *for* $n=2, 4, 10$ *and* $0 \leqslant x \leqslant 1$, *and by considering the shape of the graph for large values of* n. *In doing this, prove the following :*

(v) For a given value of n, the maximum value of y is $\frac{1}{2}$ and the corresponding value of x is $1/(n+1)$.

(vi) Prove that $\lim_{n\to\infty} \frac{y}{x}=n$ and

$$\lim_{n\to\infty} \frac{y}{x-1}=-\frac{1}{n};$$

hence show that the curve cuts the x-axis at angles $\tan^{-1} n$, $-\tan^{-1} 1/n$ at the points $x=0$, $x=1$.

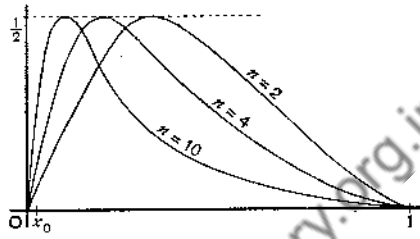


FIG. 28.

(vii) However small x_0 may be, we can find n so that part of the graph of $y=s_n(x)$ very nearly coincides with the segment $x_0 1$ of the x-axis, but the curve has a peak of height $\frac{1}{2}$ to the left of the ordinate through x_0.

7. Prove that if $\dfrac{1}{1+px+qx^2}=1+a_1x+a_2x^2+a_3x^3+\dots$, then

$$1+a_1x+2a_2x^2+3a_3x^3+\dots=\frac{1+px+p^2x^2+2pqx^3+q^2x^4}{(1+px+qx^2)^2}.$$

8. If $y=\left(\dfrac{1+x}{1-x}\right)^n=a_0+a_1x+a_2x^2+\dots+a_rx^r+\dots$, show that

(i) $(1-x^2)\dfrac{dy}{dx}=2ny$; (ii) $(r+1)a_{r+1}-2na_r-(r-1)a_{r-1}=0$.

9. Assume that $\sin x=a_0+a_1x+a_2x^2+\dots$, and, by differentiating twice, prove that

$$\sin x=x-\frac{x^3}{\lfloor 3}+\frac{x^5}{\lfloor 5}-\dots, \quad \cos x=1-\frac{x^2}{\lfloor 2}+\frac{x^4}{\lfloor 4}-\dots.$$

10. Using $\sin^{-1} y$ to denote that angle whose sine is y, which lies either

between $-\pi/2$ and $\pi/2$, or is equal to $\pi/2$,

show that, if $-1<y\leqslant 1$, then

$$\sin^{-1} y=y+\frac{1}{2}\cdot\frac{y^3}{3}+\frac{1\cdot 3}{2\cdot 4}\cdot\frac{y^5}{5}+\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6}\cdot\frac{y^7}{7}+\dots.$$

[If $y=\sin x$, then $\dfrac{dy}{dx}=\cos x=\sqrt{(1-y^2)}$, therefore

$$\frac{dx}{dy}=(1-y^2)^{-\frac{1}{2}}=1+\frac{1}{2}y^2+\frac{1\cdot 3}{2\cdot 4}y^4+\dots \text{ if } -1<y<1.$$

Proceed by integration, and use Abel's theorem.]

11. Prove the exponential theorem as follows.

Let $E(x)=1+x+\frac{x^2}{\lfloor 2}+\dots$, and show that (i) $E(x).E(y)=E(x+y)$.

(ii) If x is a positive integer, $E(x)=\{E(1)\}^x=e^x$.

(iii) If p, q are positive integers, $E\left(\frac{p}{q}\right)=e^{\frac{p}{q}}$.

(iv) If x is a positive rational, $E(-x)=\frac{1}{E(x)}=e^{-x}$.

(v) Consider the case of an irrational index.

12. If $-1<x<1$, show that

(i) $\cos\theta+2x\cos 2\theta+3x^2\cos 3\theta+\dots=\frac{\cos\theta-2x+x^2\cos\theta}{(1-2x\cos\theta+x^2)^2}$.

(ii) $\sin\theta+2x\sin 2\theta+3x^2\sin 3\theta+\dots=\frac{(1-x^2)\sin\theta}{(1-2x\cos\theta+x^2)^2}$.

[Denote the sums by C and S respectively, then if $z=\cos\theta+\iota\sin\theta$ we have

$$C+\iota S=z+2xz^2+3x^2z^3+\dots=z(1-xz)^{-2}.$$

Equate real and imaginary parts.]

13. If $-\pi<\theta<\pi$, show that for all values of n,

$$1+n\cos\theta+\frac{n(n-1)}{\lfloor 2}\cos 2\theta+\frac{n(n-1)(n-2)}{\lfloor 3}\cos 3\theta+\dots=(2\cos\tfrac{1}{2}\theta)^n\cos\tfrac{1}{2}n\theta,$$

$$n\sin\theta+\frac{n(n-1)}{\lfloor 2}\sin 2\theta+\frac{n(n-1)(n-2)}{\lfloor 3}\sin 3\theta+\dots=(2\cos\tfrac{1}{2}\theta)^n\sin\tfrac{1}{2}n\theta.$$

[Proceed as in Ex. 12.]

14. If R_n is the remainder after n terms in

$$S_3=\frac{1}{1^3}+\frac{1}{2^3}+\frac{1}{3^3}+\dots$$

then $$\frac{1}{2}\,\frac{1}{(n+1)(n+2)}<R_n<\frac{1}{2}\,\frac{1}{(n-1)n}.$$

Hence show that $S_3=\Sigma_{r=1}^{r=100}\frac{1}{r^3}+\frac{1}{2.100.99}-\epsilon$,

where $\epsilon<2.10^{-6}$.

15. Show that

$$S_3\left(1-\frac{1}{2^3}\right)\left(1-\frac{1}{3^3}\right)\left(1-\frac{1}{5^3}\right)\left(1-\frac{1}{7^3}\right)=1+\frac{1}{11^3}+\frac{1}{13^3}+\dots+\frac{1}{r^3}+\dots,$$

where all values of r prime to 2, 3, 5, and 7 occur.

[Multiplication of S_3 by $\left(1-\frac{1}{2^3}\right)$ removes all multiples of 2, etc. Similarly for S_5, S_7, and so on.]

16. Show that $$S_3=\Sigma_{r=1}^{r=n}\frac{1}{r^3}+\frac{1}{4(n-3)(n-2)(n-1)^n}-\epsilon_n,$$

where $$\epsilon_n<4/(n-3)(n-2)(n-1)n(n+1).$$

CHAPTER V

THE COMPLEX VARIABLE

1. Variation of mod z. If $z=x+iy$, where x and y are real variables, independent of one another, we say that z varies continuously when x and y vary continuously. If z varies continuously from a value z_0 to a value z_1, the point z passes from the point z_0 to the point z_1 along a continuous curve.

During this variation $|z|$ varies continuously but, as will be seen in Art. 2, the variation of $\operatorname{am} z$ is not necessarily continuous.

When the point z arrives at z_1, $|z|$ has the same value, whatever path z describes, but the value acquired by $\operatorname{am} z$ depends on the particular path pursued.

2. Variation of am z. We require the following rule, which assigns a precise meaning to $\operatorname{am} z$ throughout any variation of z.

Let z_0 be the initial value of z, and let $\angle XOz=\theta$ and $\angle XOz_0=\theta_0$. Let z describe a continuous curve which does not pass through O, then θ varies continuously. Choose any particular value of $\operatorname{am} z_0$; for instance, let

$$\operatorname{am} z_0=2k\pi+\theta_0,$$

where k is a fixed integer or zero, then $\operatorname{am} z$ is defined by $\operatorname{am} z=2k\pi+\theta$.

Thus in Fig. 29 if $\operatorname{am} z_0=\theta_0$ and z moves from z_0 to z_1 along the path A, $\operatorname{am} z_1=\theta_0+\phi$, where $\phi=\angle z_0Oz_1$.

But if z describes the path B, moving once round O,

$$\operatorname{am} z_1=\theta_0+\phi+2\pi.$$

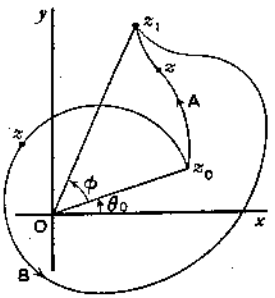


FIG. 29.

Defined thus, *am z is one-valued and varies continuously as z describes a continuous curve which does not pass through O.*

If the point O is on the z-path, the value of $\operatorname{am} z$ undergoes a sudden change equal to π or $-\pi$ as z passes through O. Thus *am z is not continuous at O.*

If ϕ is the increment of $\operatorname{am} z$ when z moves from z_0 to z_1, then $-\phi$ is the increment when z moves back along the same path from z_1 to z_0.

3. Description of a Closed Curve. If z describes a closed curve and returns to its original position, the value of $\operatorname{am} z$ is unaltered provided that O *is outside the curve.*

But if the curve is such that z moves m times round O, always in the positive sense, $\operatorname{am} z$ *is increased by* $2m\pi$.

Theorem. *Suppose that an area, bounded by a curve S, is divided into a number of smaller areas bounded by curves $A, B, C, \ldots$. Then the increment in $\operatorname{am} z$ when z describes the curve S is equal to the sum of the increments in $\operatorname{am} z$ when z describes the curves $A, B, C, \ldots$, all the curves being described in the same sense and none of them passing through O.*

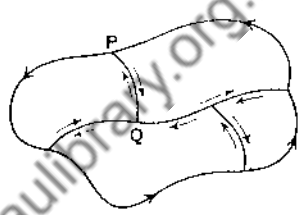


FIG. 30.

For if z describes $A, B, C, \ldots$ each once, all in the same sense, it will describe S once and each dividing line such as PQ twice, namely once from P to Q and once from Q to P. The total change in $\operatorname{am} z$ due to the passage of z along the dividing lines is therefore zero, and the increment is the same as when z describes the curve S.

4. Conformal Representation. In representing graphically the variation of a function Z of the complex variable z (*H.A.*, XVII, 29), it is often convenient to represent z and Z by points *in different planes*.

If Z is a one-valued function of z and the point z moves along some curve in the z-plane, then the point Z will describe a corresponding curve in the Z-plane.

Ex. 1. *If $Z=z^2$, find the path described by the point Z in the following cases; when z describes* (i) *the circle with centre O and radius c,* (ii) *the line $x=c$.*

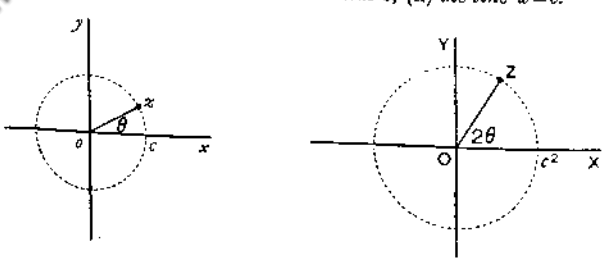


FIG. 31.

(i) We have $Z=r(\cos\theta+\iota\sin\theta)$, $Z=r^2(\cos 2\theta+\iota\sin 2\theta)$.

If then $r=c$ and θ varies from 0 to 2π, the point z describes the complete circle $(0, c)$, and the point Z describes the circle $(0, c^2)$ *twice*. (Fig. 31.)

(ii) Let $X+\iota Y=Z=z^2=(x+\iota y)^2$, then $X=x^2-y^2$, $Y=2xy$.

If z moves so that $x=c$, we have $X=c^2-y^2$, $Y=2cy$; and eliminating y, we have $X=c^2-\frac{Y^2}{4c^2}$, which is the equation to the Z-path.

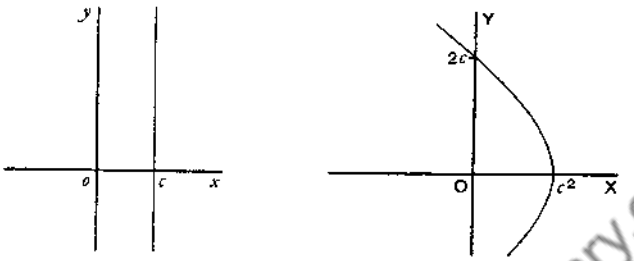


FIG. 32.

This equation represents a parabola, focus at O, axis parallel to OX. (Fig. 32.)

5. Variation of $z^{\frac{1}{n}}$. As a typical instance consider the equation $Z^3=z$, where $Z=R(\cos\phi+\iota\sin\phi)$, $z=r(\cos\theta+\iota\sin\theta)$.

We have $R^3(\cos 3\phi+\iota\sin 3\phi)=r(\cos\theta+\iota\sin\theta)$, $R=r^{\frac{1}{3}}$, $\phi=\theta/3$, where $r^{\frac{1}{3}}$ denotes the arithmetical cube root of r.

Let z, starting from the point p where $\theta=-\pi$ describe the circle (o, r) *three times* in the positive sense: then Z describes the circle (O, R) *once.*

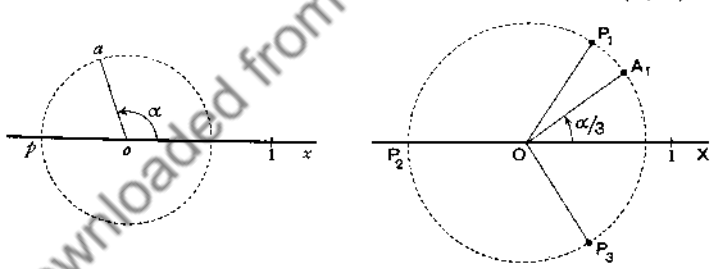


FIG. 33.

During the first description of the z-circle, θ varies from $-\pi$ to π, ϕ varies from $-\pi/3$ to $\pi/3$ and Z describes the arc P_3P_1. During the second and the third descriptions of the z-circle, Z describes the arcs P_1P_2 and P_2P_3 respectively.

Let a be any particular value of z of modulus r and amplitude α, the point a being on the z-circle.

Mark the points A_1, A_2, A_3 which correspond to z as it passes through a after one and after two revolutions round o. These points are on the Z-circle, and their amplitudes are $\alpha/3$, $(\alpha+2\pi)/3$, $(\alpha+4\pi)/3$.

The numbers A_1, A_2, A_3 are the three values of $a^{\frac{1}{3}}$, and of these A_1 is the principal value. Thus the equation $Z^3=z$ determines Z as a *three-valued function* of z: these values are called *branches* of the function.

If $z=r(\cos\theta+\iota\sin\theta$ where $-\pi<\theta\leqslant\pi$, we may denote the branches of the function $Z=z^{\frac{1}{3}}$ by Z_1, Z_2, Z_3, where

$$Z_1=r^{\frac{1}{3}}(\cos\theta/3+\iota\sin\theta/3),$$
$$Z_2=r^{\frac{1}{3}}\{\cos(2\pi+\theta)/3+\iota\sin(2\pi+\theta)/3\},$$
$$Z_3=r^{\frac{1}{3}}\{\cos(4\pi+\theta)/3+\iota\sin(4\pi+\theta)/3\}.$$

Of these, Z_1 is called the *principal branch*.

Now suppose that z, starting from a, describes a continuous curve. Mark the points A_1, A_2, A_3 corresponding to the values of $a^{\frac{1}{3}}$, A_1 being the principal value.

FIG. 34.

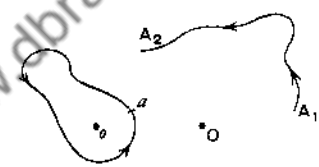


FIG. 35.

The point Z will describe a continuous curve starting at A_1, and

(i) If the z-path does not contain o, Z will return to A_1 as in Fig. 34.

(ii) If the z-path winds round o *once* (Fig. 35), Z will not return to A_1, but will finally assume the position A_2.

Moreover, if the z-path continues through a, we shall have

$$Z=r^{\frac{1}{3}}\{\cos(2\pi+\theta)/3+\iota\sin(2\pi+\theta)/3\}\quad(-\pi<\theta\leqslant\pi),$$

so that Z_1 passes continuously into Z_2.

A similar argument leads to the following conclusions.

If n is a positive integer, the equation $Z^n=z$ determines Z as an n-valued function of z.

If $z=r(\cos\theta+\iota\sin\theta)$ where $-\pi<\theta\leqslant\pi$, the n values or branches of the function are Z_1, Z_2, ... Z_n, where

$$Z_m=r^{\frac{1}{n}}\left\{\cos\frac{1}{n}(\overline{m-1}\,.\,2\pi+\theta)+\iota\sin\frac{1}{n}(\overline{m-1}\,.\,2\pi+\theta)\right\}.$$

Each of the functions $z_1, z_2, \ldots, z_n$ *is a continuous one-valued function of* z.

Further, if the z*-path winds round the origin, each of these functions passes continuously into the next, excepting that the last passes continuously into the first.*

6. Variation of $z^{\frac{p}{q}}$. Let p, q be positive integers prime to one another. Consider the equation $Z^q = z^p$, where

$$Z = R(\cos\phi + \iota\sin\phi), \quad z = r(\cos\theta + \iota\sin\theta).$$

Then
$$R^q(\cos q\phi + \iota\sin q\phi) = r^p(\cos p\theta + \iota\sin p\theta);$$

$$\therefore\ R = r^{\frac{p}{q}}, \quad \phi = \frac{p}{q}\theta,$$

where $r^{\frac{p}{q}}$ is the arithmetical qth root of r^p.

Hence if z describes the circle (o, r) q times, Z will describe the circle (O, R) p times.

By an argument similar to that in Art. 5 we conclude that *if* p, q *are positive integers, prime to one another, the equation* $Z^q = z^p$ determines Z *as a* q*-valued function of* z.

If $z = r(\cos\theta + \iota\sin\theta)$ *where* $-\pi < \theta \leqslant \pi$, *the* q *values or branches of the function are* $Z_1, Z_2, \ldots Z_q$ *where*

$$Z_m = r^{\frac{p}{q}}\left\{\cos\frac{1}{q}(\overline{m-1}\,.\,2\pi + p\theta) + \iota\sin\frac{1}{q}(\overline{m-1}\,.\,2\pi + p\theta)\right\},$$

with conclusions similar to those in Art. 5 *regarding the continuity of* Z_1, $Z_2, \ldots, Z_q$.

7. Variation of a Polynomial. Let $Z = a_0 + a_1z + a_2z^2 + \ldots + a_nz^n$; then Z is a continuous function of z, and, if the point z describes a closed path, so does the point Z.

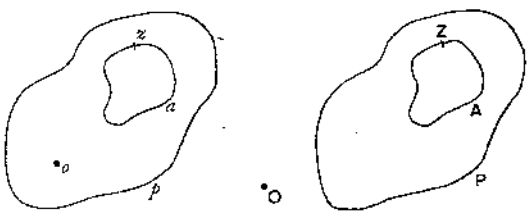


FIG. 36.

Variation of the Amplitude. Let z describe the closed path p, so that Z describes the closed path P. Such a path is called a *contour*.

(1) *If the path p of z neither contains nor passes through a value of z for which $Z=0$, the total variation of am Z is zero.*

For let z_0 be any point within p, and let Z_0 correspond to z_0. Then by hypothesis, Z_0 is not zero, and because Z is continuous for all values of z, we can find η so that

$$|Z-Z_0|<|Z_0|, \quad \text{provided that} \quad |z-z_0|<\eta,$$

which is the same as saying that

the length $Z_0Z <$ the length OZ_0, if the length $z_0z<\eta$.

FIG. 37.

Draw a circle with centre z_0 and radius η.

It follows that *if z describes a closed path a within this circle, Z will describe a closed path A which neither contains nor passes through the point O, and consequently the variation of am Z for this path is zero.*

Moreover, the area bounded by P can be divided into areas bounded by curves $A, B, \ldots$, each of which possesses the property just described.

Also the variation in am Z when Z describes the path P is the sum of the variations for the paths $A, B, \ldots$.

Hence the variation in am Z for the path P is zero.

(2) *If the z-path p contains m roots of $Z=0$, a k-multiple root being counted as equivalent to k distinct roots, then the variation in am Z is $2m\pi$.*

Let $z_1, z_2, \ldots z_m$ be the roots of $Z=0$ enclosed by p, then $Z=(z-z_1)(z-z_2)\ldots(z-z_m).\phi(z)$, where $\phi(z)$ vanishes for no value of z within the curve p. Now am Z is equal to

$$\text{am}\,(z-z_1)+\text{am}\,(z-z_2)+\ldots+\text{am}\,(z-z_m)+\text{am}\,\phi(z);$$

and, by (1) the variation of am $\phi(z)$ is zero.

Also, as the point z_1 is within p, the increment of am $(z-z_1)$ is the angle turned through by the line zz_1 in a complete revolution, namely 2π.

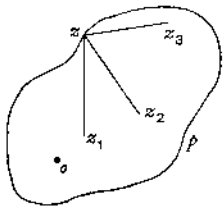


FIG. 38.

Similarly the increment of each of the other amplitudes is 2π, and therefore the increment of am Z is $2m\pi$.

If one of the roots as z_1 is a k-multiple root, instead of the factor $z-z$, we have $(z-z_1)^k$. Now am $(z-z_1)^k = k$ am $(z-z_1)$, whence it follows that such a root counts as equivalent to k distinct roots.

Hence the total variation of am Z is $2m\pi$.

(3) Conversely, we infer * that *if z describes a closed path p which does not pass through a root of $Z=0$, then the number of roots enclosed by p is equal to the increment of am Z divided by 2π, a k-multiple root being counted as k distinct roots.*

8. An Equation of the n-th Degree has n Roots. We are now able to infer the truth of this theorem. Let

$$Z = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n = z^n \phi(z),$$

where

$$\phi(z) = \frac{a_0}{z^n} + \frac{a_1}{z^{n-1}} + \ldots + a_n.$$

Choose a positive number M, and find m so that

$$|Z| > M, \quad \text{provided that} \quad |z| \geqslant m.$$

Let z describe a circle with centre o and radius m. No root of $Z=0$ exists outside or on the circle, and $\phi(z)$ vanishes at no point within it.

Hence the number of roots of $Z=0$ is equal to the increment of am Z divided by 2π. Now

$$\text{am } Z = \text{am } z^n + \text{am } \phi(z) = n \,.\, \text{am } z + \text{am } \phi(z);$$

also the increment of am $\phi(z)$ is zero, and that of am z is 2π, therefore the number of roots $= n \,.\, 2\pi/2\pi = n$.

9. Derivatives. Let z be any point in the z-plane and z' a neighbouring point. If, as z' approaches z and becomes indefinitely near to it, the ratio

$$\{f(z') - f(z)\}/(z'-z)$$

tends to the same limit, *no matter what may be the path*, this limit is called the derivative of $f(z)$ and is denoted by $f'(z)$.

Thus $f'(z) = \lim \{f(z+h) - f(z)\}/h$ where $h \to 0$ in any way whatever, if there is such a limit.

* If the student is not satisfied with this argument, he is referred to Hardy's *Pure Mathematics*, fourth edition, p. 439.

When $f'(z)$ exists, it can be found by the same rules as in the case of a real variable. For example, if $f(z)=a_0+a_1z+a_2z^2+\ldots+a_nz^n$, then

$$f'(z)=a_1+2a_2z+3a_3z^2+\ldots+na_nz^{n-1}.$$

10. Theorem. *If Z is a function of z which has a derivative at the point z_0 and z approaches z_0 by either of the paths a, b, then the corresponding Z-paths A, B intersect at the same angle as a, b.*

Let z_1, z_2 moving along the paths a, b respectively tend to z_0 as a limiting position, and let Z_0, Z_1, Z_2 correspond to z_0, z_1, z_2. Because Z has a derivative at z_0, the expressions

$$\frac{Z_1-Z_0}{z_1-z_0} \quad \text{and} \quad \frac{Z_2-Z_0}{z_2-z_0}$$

tend to the same definite limit, namely this derivative. Therefore the triangles $z_0z_1z_2$, $Z_0Z_1Z_2$ tend to become directly similar (*H.A.*, Ex. IX, 14) and the angles $z_1z_0z_2$, $Z_1Z_0Z_2$ tend to equality.

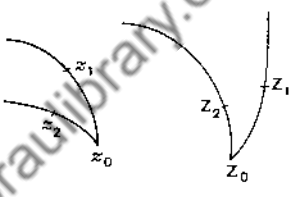


FIG. 39.

Hence, in the limit, the angle between the tangents to the Z-paths is equal to that between the tangents to the z-paths.

It thus appears that *if $f(z)$ has a derivative* the relation $Z=f(z)$ establishes the similarity of parts of corresponding figures *which are in the neighbourhood* of corresponding points.

For two similar figures the *magnification* of one relative to the other is the ratio of any two corresponding lengths.

If z, Z and $z+\delta z$, $Z+\delta Z$ are pairs of corresponding points, we define *the magnification* m of the Z-plane relative to the z-plane at the points z, Z by

$$m=\lim\frac{|\delta Z|}{|\delta z|}=\lim\left|\frac{\delta Z}{\delta z}\right|=\left|\frac{dZ}{dz}\right|.$$

Thus in general m depends on z and the relation does not necessarily involve the similarity of *finite* parts of corresponding figures.

11. Theorems on Infinite Series.

(1) The sum $s(z)$ of the infinite series $a_0+a_1z+a^2z^2+\ldots$ has a derivative $s'(z)$ at every point within its circle of convergence and

$$s'(z)=a_1+2a_2x+3a_3x^2+\ldots.$$

The proof is the same as in Ch. IV, Art. 9, if we replace x by z, for 'interval $(-R, R)$' read 'circle of convergence,' and let accented letters denote moduli.

(2) **Extension of Taylor's Theorem.** Let $s(z)$ be the sum of the series $\Sigma a_n z^n$, and let z be any point within the circle (O, R). Draw a circle with centre z to touch (O, R) internally. Then if $z+h$ is any point within the smaller circle,

$$s(z+h)=s(z)+hs'(z)+\frac{h^2}{\lfloor 2}s''(z)+\ldots+\frac{h^r}{\lfloor r}s^{(r)}(z)+\ldots .$$

For $|z|+|h|<R$, and the proof is the same as that in Ch. IV, Art. 11, if we write z for x.

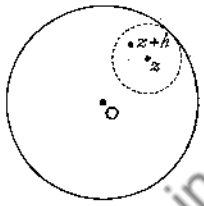


FIG. 40.

EXERCISE VI

1. If $Z^2=z$, trace the Z-path corresponding to the z-path in Fig. 41, explaining why Z acquires two different values as z passes through a. What are these values?

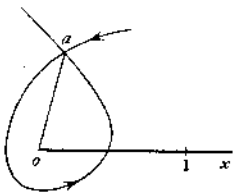


FIG. 41.

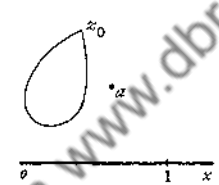


FIG. 42.

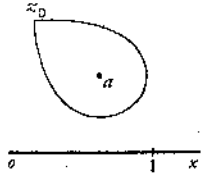


FIG. 43.

2. If $Z=\sqrt{z-a}$, trace the Z-paths corresponding to the z-paths in Figs. 42, 43.

3. Consider the function $Z=\sqrt{(z-a_1)(z-a_2)}$. Show that if z describes a closed curve which does not contain either of the points a_1, a_2, then Z returns to its initial value. In other words, the function Z is one-valued in any part of the plane which contains neither a_1 nor a_2.

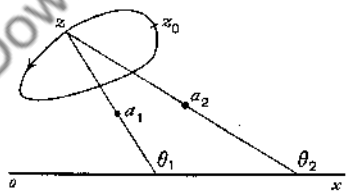


FIG. 44.

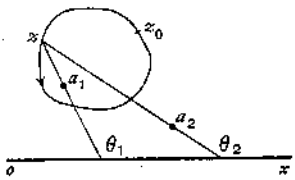


FIG. 45.

[Let $z-a_1=r_1(\cos\theta_1+\iota\sin\theta_1)$, $z-a_2=r_2(\cos\theta_2+\iota\sin\theta_2)$;

then $Z=r_1^{\frac{1}{2}}r_2^{\frac{1}{2}}\{\cos\frac{1}{2}(\theta_1+\theta_2)+\iota\sin\frac{1}{2}(\theta_1+\theta_2)\}$,

and in the circumstances of the question, θ_1, θ_2 return to their original values.]

4. Referring to Ex. 3 and Fig. 45, if z starts from z_0 and describes a closed curve containing a_1, what is the value of z when it returns to z_0?

Take $$z_0 - a_1 = \rho_1(\cos\alpha_1 + \iota \sin\alpha_1),$$
$$z_0 - a_2 = \rho_2(\cos\alpha_2 + \iota \sin\alpha_2).$$

5. If $Z = z^2$ and z varies so that (i) $x = c$, (ii) $y = d$, find the corresponding Z-paths.

Explain why these cut at right angles, and verify by ordinary Cartesian geometry.

[The equations to the Z-paths are

$$X = c^2 - \frac{Y^2}{4c^2} \quad \text{and} \quad X = \frac{Y^2}{4d^2} - d^2. \quad \text{(Art. 4, Ex. 1, (ii).)}$$

These are confocal parabolas with their axes along the x-axis: they therefore cut orthogonally.]

6. For the following transformations explain by ordinary geometrical considerations why two z-paths cut at the same angle as the corresponding Z-paths.

(i) $Z = z + a$; (ii) $Z = tz$ (t real);

(iii) $Z = az + b$; (iv) $Z = \frac{1}{z}$. (*H.A.*, IX. 2.)

Some knowledge of the Differential Calculus is assumed in the following.

7. If $X + \iota Y = Z = f(z) = f(x + \iota y)$ and $f'(z)$ exists, prove that

$$\text{(i)} \quad \frac{\partial X}{\partial x} = \frac{\partial Y}{\partial y}, \quad \frac{\partial X}{\partial y} = -\frac{\partial Y}{\partial x};$$

$$\text{(ii)} \quad \frac{\partial^2 X}{\partial x^2} + \frac{\partial^2 X}{\partial y^2} = 0, \quad \frac{\partial^2 Y}{\partial x^2} + \frac{\partial^2 Y}{\partial y^2} = 0.$$

[(i) For
$$\frac{\partial Z}{\partial x} = \frac{dZ}{dz} \cdot \frac{\partial z}{\partial x} = f'(z),$$
$$\frac{\partial Z}{\partial y} = \frac{dZ}{dz} \cdot \frac{\partial z}{\partial y} = \iota f'(z).$$

Hence, writing $X + \iota Y$ for Z, we have

$$\iota\left(\frac{\partial X}{\partial x} + \iota \frac{\partial Y}{\partial x}\right) = \frac{\partial X}{\partial y} + \iota \frac{\partial Y}{\partial y},$$

and the results follow by equating real and imaginary parts.]

8. If Z has a derivative, then neither X nor Y can be chosen arbitrarily.

[For by Ex. 7, (ii), both X and Y satisfy the differential equation

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0.]$$

9. If m is the magnification at the corresponding points Z, z, then

$$m^2 = \left(\frac{\partial X}{\partial x}\right)^2 + \left(\frac{\partial Y}{\partial x}\right)^2 = \left(\frac{\partial X}{\partial y}\right)^2 + \left(\frac{\partial Y}{\partial y}\right)^2 = \frac{\partial X}{\partial x}\frac{\partial Y}{\partial y} - \frac{\partial X}{\partial y}\frac{\partial Y}{\partial x}.$$

[For
$$m = \left|\frac{dZ}{dz}\right| = \left|\frac{\partial Z}{\partial x}\right| = \left|\frac{\partial X}{\partial x} + \iota \frac{\partial Y}{\partial x}\right|, \quad \text{etc.}]$$

10. If Z has a derivative and $Z=X+\iota Y$, the curves

$$X=\text{constant}, \quad Y=\text{constant}$$

cut at right angles.

[For by Ex. 7, (i), $\dfrac{\partial X}{\partial x}\dfrac{\partial Y}{\partial x}+\dfrac{\partial X}{\partial y}\dfrac{\partial Y}{\partial y}=0.$]

11. If $Z=u+v(\cos\alpha+\iota\sin\alpha)$ where α is a real constant and u, v are functions of x, y such that Z has a derivative, then the curves $u=\text{constant}$, $v=\text{constant}$ cut at the angle α.

[If the curves cut at an angle θ, we have

$$\tan\theta\left(\frac{\partial u}{\partial x}\frac{\partial v}{\partial x}+\frac{\partial u}{\partial y}\frac{\partial v}{\partial y}\right)=\frac{\partial u}{\partial x}\frac{\partial v}{\partial y}-\frac{\partial u}{\partial y}\frac{\partial v}{\partial x}.$$

Also by Ex. 7, (i),

$$\frac{\partial u}{\partial x}+\frac{\partial v}{\partial x}\cos\alpha=\frac{\partial v}{\partial y}\sin\alpha \quad \text{and} \quad \frac{\partial u}{\partial y}+\frac{\partial v}{\partial y}\cos\alpha=-\frac{\partial v}{\partial x}\sin\alpha.]$$

12. If $Z=c/z$ where c is constant and $Z=X+\iota Y$, $z=x+\iota y$, prove that

$$Y/y=-c/(x^2+y^2).$$

Hence show that the magnification at the corresponding points Z, z is Y/y.

[For $m=\left|\dfrac{dZ}{dz}\right|=\left|\dfrac{c}{z^2}\right|$ and $|z^2|=|z|^2=x^2+y^2.$]

13. For the substitution $Z=(az+b)/(a'z+b')$, prove that the magnification at the corresponding points Z, z is V/v where

$$z+\frac{b'}{a'}=u+\iota v, \quad Z-\frac{a}{a'}=U+\iota V.$$

[This follows from Ex. 12, for the substitution can be written

$$\left(z+\frac{b'}{a'}\right)\left(Z-\frac{a}{a'}\right)=-\frac{ab'-a'b}{a'^2},$$

and the paths described by $z+\dfrac{b'}{a'}$ and $Z-\dfrac{a}{a'}$ are obtained from the z- and the Z-paths by *translations*.

14. For the substitution $\dfrac{1}{Z}=\dfrac{1}{z}+c$, where c is a real constant, prove that

$$\frac{x}{X-c(X^2+Y^2)}=\frac{y}{Y}=\frac{1}{(1-cX)^2+c^2Y^2},$$

where $Z=X+\iota Y$ and $z=x+\iota y$.

15. The substitution $Z=az+b$, where a, b are constants, changes any figure in the z-plane into a similar figure in the Z-plane, the magnification being $|a|$.

Also, if a is real and the axes in the two planes are parallel, corresponding figures are similarly situated.

CHAPTER VI

EXPONENTIAL AND LOGARITHMIC FUNCTIONS

1. The Exponential Function, denoted by $E(z)$ or $\exp z$, is defined by

$$E(z) = 1 + z + \frac{z^2}{\lfloor 2} + \frac{z^3}{\lfloor 3} + \cdots,$$

the series being convergent for all values of z.

It has been shown (*H.A.*, XIX, 11) that, if $z = x + \iota y$ where x and y are real,

$$E(z) = e^x (\cos y + \iota \sin y),$$

so that $E(z + 2\iota k\pi) = E(z)$ and consequently $E(z)$ is periodic, and its period is $2\iota\pi$. We shall now consider graphically the variation of two complex numbers u and z connected by the equation $u = e^z$.

2. The Relation $u = e^z = e^x(\cos y + \iota \sin y)$. Corresponding to any point z we have the point u, whose polar coordinates are (e^x, y).

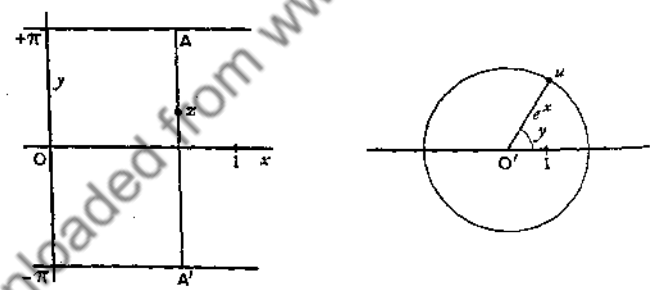


FIG. 46.

In the z-plane draw the lines $y = \pm\pi$, and let any line parallel to the y-axis cut them in A, A'. Let z describe the segment $A'A$, then x remains constant and y varies from $-\pi$ to π. Therefore the point u describes the circle with centre O' and radius e^x. If we suppose x to vary from $-\infty$ to $+\infty$, the corresponding positions of AA' fill the strip of the z-plane between the parallels $y = \pm\pi$, and the corresponding circles fill the whole of the u-plane.

We say that *the strip of the z-plane corresponds to the whole of the u-plane*, meaning *that a one-to-one correspondence exists between the points of one and the points of the other.*

Now, let the z-plane be divided into strips by the parallels, $y=(2k+1)\pi$, where k is zero or any integer. Because the value of u is unaltered by adding $2k\pi$ to y, therefore *each strip of the z-plane corresponds to the whole of the u-plane* in the sense described above.

Thus the equation $u=e^z$, which determines u as a *one-valued* function of z, also determines z as an *infinitely many-valued* function of u.

Let $u=\rho(\cos\phi+\iota\sin\phi)$.

Then, for any particular value of u, the corresponding values of z (marked $\ldots z_{-1}, z_0, z_1, \ldots$ in Fig. 47) are given by $z=x+\iota y$ where

$$x=\log\rho, \quad y=\phi+2k\pi,$$

and k is zero or any integer.

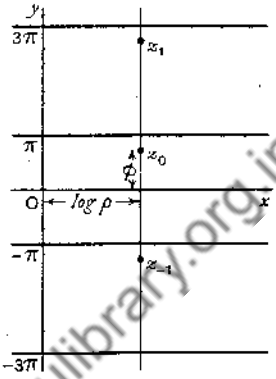


FIG. 47.

3. The Logarithmic Function. (1) The values of z corresponding to any particular value of u for which

$$u=\rho(\cos\phi+\iota\sin\phi)=e^z \quad \text{where} \quad -\pi<\phi\leqslant\pi$$

are called *logarithms of* u, and any one of them is denoted by *Log u*.

From the last article it will be seen that

$$\text{Log}\, u=\log\rho+\iota\phi+2k\iota\pi, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

where k is zero or any integer.

(2) **The principal value of Log u** is defined as the value for which $k=0$, and is denoted by $\log u$, thus

$$\log u=\log\rho+\iota\phi \quad (-\pi<\phi\leqslant\pi), \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

and

$$\text{Log}\, u=\log u+2k\iota\pi. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

In Fig. 47 the points $\ldots z_{-1}, z_0, z_1 \ldots$ represent the values of Log u, and z_0 corresponds to $\log u$. The following special cases should be noticed.

For a real positive number x we have $\phi=0$, $\rho=x$.

The principal value of Log x is $\log x$, and

$$\text{Log}\, x=\log x+2k\iota\pi. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(D)}$$

For a real negative number $(-x)$ we have

$$-x=x(\cos\pi+\iota\sin\pi);$$

hence the principal value of Log $(-x)$ is $\log x+\iota\pi$, and

$$\text{Log}\,(-x)=\log x+\iota(2k+1)\pi. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(E}$$

(3) **Logarithm of a Product.** It follows at once that

$$\operatorname{Log} u_1u_2 = \operatorname{Log} u_1 + \operatorname{Log} u_2 + 2\iota k\pi, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(F)}$$

where k is zero or any integer.

For if $u_1 = E(z_1)$, $u_2 = E(z_2)$, then $u_1u_2 = E(z_1 + z_2)$, and by definition,

$$\operatorname{Log} u_1 = z_1 + 2\iota k_1\pi, \quad \operatorname{Log} u_2 = z_2 + 2\iota k_2\pi,$$

and

$$\operatorname{Log} u_1u_2 = z_1 + z_2 + 2\iota k_3\pi,$$

where k_1, k_2, k_3 are integers or zero, whence the result follows.

It should be noticed that the equation,

$$\operatorname{Log} u_1u_2 = \operatorname{Log} u_1 + \operatorname{Log} u_2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(G)}$$

is true in the sense that *every value of one side is one of the values of the other side.*

(4) **Logarithm of a Quotient.** In the same way

$$\operatorname{Log}\frac{u_1}{u_2} = \operatorname{Log} u_1 - \operatorname{Log} u_2 + 2\iota k\pi. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(H)}$$

Ex. 1. *The logarithms having their principal values, prove that*

$$\log u_1u_2 = \log u_1 + \log u_2 + 2\iota k\pi;$$

and k is zero if, only if, $-\pi < \phi_1 + \phi_2 \leqslant \pi$, where ϕ_1, ϕ_2 are the amplitudes of u_1, u_2.

For

$$\log u_1 + \log u_2 = \log \rho_1 + \log \rho_2 + \iota(\phi_1 + \phi_2).$$

This is a value of $\log u_1u_2$ by equation (G), but it is not the principal value unless the given condition holds.

4. General Meaning of a^z. (1) If x is real and a real and positive,

$$a^x = e^{x\log a} = E(x\log a).$$

In accordance with this we have the following definition: *For all values of a and z, real or complex, the meaning of a^z is defined by*

$$a^z = E(z\operatorname{Log} a),$$

where Log a has any of its values. The principal value of a^z is defined as

$$E(z\log a).$$

(2) Let

$$a = a'(\cos\alpha + \iota\sin\alpha), \quad z = x + \iota y;$$

then

$$z\operatorname{Log} a = (x + \iota y)\{\log a' + \iota(\alpha + 2k\pi)\} = A + \iota B,$$

where

$$A = x\log a' - y(\alpha + 2k\pi), \quad B = y\log a' + x(\alpha + 2k\pi);$$

and hence

$$a^z = E(A + \iota B) = e^A(\cos B + \iota\sin B).$$

Thus in general, *a^z has infinitely many values and no two of them are equal.* The proof is given in Ex. 4 below.

Ex. 1. *Use the general value of a^z to find the n-th root of unity.*

Here $a=1,\quad z=1/n;$ hence $a'=1,\quad \alpha=0,\quad x=1/n,\quad y=0;$

therefore $A=0,\quad B=\dfrac{2\pi k}{u},$ and thus $1^{\frac{1}{n}}=\cos\dfrac{2k\pi}{n}+\iota\sin\dfrac{2k\pi}{n}.$

Ex. 2. *Find the values of ι^ι, showing that they are all real.*

Here $a=\iota=\cos\dfrac{\pi}{2}+\iota\sin\dfrac{\pi}{2};$ thus $a'=1,\quad \alpha=\dfrac{\pi}{2};$ also $x=0,\quad y=1,$

hence $A=-\left(\dfrac{\pi}{2}+2k\pi\right),\quad B=0;$ and we have $\iota^\iota=e^{-\left(\frac{\pi}{2}+2k\pi\right)}.$

Ex. 3. *Show that $(-1)^{\sqrt{2}}$ has no real value, and find its principal value.*

We have $-1=\cos\pi+\iota\sin\pi;$ and $a'=1,\quad \alpha=\pi,$ also $x=\sqrt{2},\quad y=0;$

thus $A=0,\quad B=\sqrt{2}(2k+1)\pi;$ and $(-1)^{\sqrt{2}}=\cos\sqrt{2}(2k+1)\pi+\iota\sin\sqrt{2}(2k+1)\pi.$

It follows that no value of $(-1)^{\sqrt{2}}$ is real, and putting $k=0$ we have

$$\text{principal value}=\cos\sqrt{2}\pi+\iota\sin\sqrt{2}\pi.$$

Ex. 4. *Show that no two values of a^z are equal unless z is real and rational.*

We have $$a^z=e^A(\cos B+\iota\sin B),$$

where A, B have the values given above.

Suppose that a^z has equal values for the values k_1, k_2 of k, then

(i) The two values of e^A are equal, therefore $y=0$ and z is real.

(ii) The values of B must differ by $2k\pi$ where k is an integer or zero. The values of B are $x(\alpha+2k_1\pi)$ and $x(\alpha+2k_2\pi);$ hence $2k_1x\pi-2k_2x\pi=2k\pi.$

Therefore x is equal to the ratio of two integers or zero, and is therefore rational. Hence z is real and rational.

5. Binomial Theorem. We can now state this theorem in a more general form as follows.

If n is real and z complex, the sum of the series

$$1+nz+\frac{n(n-1)}{\lfloor 2}z^2+\ldots$$

is the principal value of $(1+z)^n$, for all values of z which make the series convergent.

This has been proved in Ch. IV, Art. 17, for rational values of n. Now the principal value of $(1+z)^n$ is $E\{n\log(1+z)\}$. This is a continuous function of n, and so is the sum of the series. Hence the theorem is true for all real values of n.

NOTE. It can be shown that *the theorem is true for all complex values of n.* For a proof, see Hardy's *Pure Mathematics*, p. 405.

6. The Logarithmic Series. *At any point within or on the circle* $|z|=1$ *excepting the point* $z=-1$,

$$\log(1+z)=z-\tfrac{1}{2}z^2+\tfrac{1}{3}z^3-\dots .$$

Proof. (i) *If* $|z|<1$ and n is real,

$$1+nz+\frac{n(n-1)}{\underline{|2}}z^2+\dots \quad\text{.......(A)}$$

$$=\text{the principal value of } (1+z)^n$$

$$=E\{n\log(1+z)\}$$

$$=1+n\log(1+z)+\frac{1}{\underline{|2}}\{n\log(1+z)\}^2+\dots \quad\text{.......(B)}$$

In Ch. IV, Art. 16, it has been shown that the series (A) can be arranged as a power series in n without altering its sum. Denote this series by

$$1+c_1n+c_2n^2+\dots \quad\text{.......(C)}$$

Then since (B) and (C) have the same sum for all real values of n, we may equate coefficients, hence if $|z|<1$,

$$\log(1+z)=c_1=z-\tfrac{1}{2}z^2+\tfrac{1}{3}z^3-\dots .$$

(ii) Denote the sum of the series $z-\frac{1}{2}z^2+\frac{1}{3}z^3-\dots$ by $s(z)$. The region of continuity of $s(z)$ includes every point on the circle of convergence $|z|=1$ at which the series is convergent.

Also the series converges at all points on the circle, excepting the point $z=-1$.

Therefore at all such points, the sum of the series is $\log(1+z)$.

NOTE. The logarithm defined by the series $z-\frac{1}{2}z^2+\frac{1}{3}z^3-\dots$ is

$$\log\rho+\iota\phi,$$

where $$1+z=\rho(\cos\phi+\iota\sin\phi) \quad\text{and}\quad -\frac{\pi}{2}<\phi<\frac{\pi}{2}.$$

For at any point within or on the circle $|z|=1$, excepting the point $z=-1$, we have $-\frac{\pi}{2}<\phi<\frac{\pi}{2}$.

7. Trigonometrical Series. In the formula

$$\log(1+z)=z-\tfrac{1}{2}z^2+\tfrac{1}{3}z^3-\dots$$

put $z=r(\cos\theta+\iota\sin\theta)$ where $-\pi<\theta<\pi$. Then, as in the last article,

$$\log(1+z)=\log\rho+\iota\phi,$$

where $\rho=\sqrt{(1+2r\cos\theta+r^2)}$, $\tan\phi=\dfrac{r\sin\theta}{1+r\cos\theta}$, and $-\pi/2<\phi<\pi/2$; therefore we have

$$\log\rho+\iota\phi=r(\cos\theta+\iota\sin\theta)-\tfrac{1}{2}r^2(\cos 2\theta+\iota\sin 2\theta)+\dots .$$

Equating real and imaginary parts, we find that

$$r\cos\theta-\tfrac{1}{2}r^2\cos 2\theta+\tfrac{1}{3}r^3\cos 3\theta-\ldots=\tfrac{1}{2}\log(1+2r\cos\theta+r^2), \quad \ldots\ldots(\mathrm{A})$$

$$r\sin\theta-\tfrac{1}{2}r^2\sin 2\theta+\tfrac{1}{3}r^3\sin 3\theta-\ldots=\tan^{-1}\frac{r\sin\theta}{1+r\cos\theta}, \quad \ldots\ldots\ldots(\mathrm{B})$$

the function on the right having its principal value, which lies between $-\pi 2$ and $\pi/2$.

It has been assumed that $0\leqslant r\leqslant 1$ and $-\pi<\theta<\pi$. When $r=1$, we have

$$\cos\theta-\tfrac{1}{2}\cos 2\theta+\tfrac{1}{3}\cos 3\theta-\ldots=\log\left(2\cos\frac{\theta}{2}\right), \quad \ldots\ldots\ldots\ldots(\mathrm{C})$$

$$\sin\theta-\tfrac{1}{2}\sin 2\theta+\tfrac{1}{3}\sin 3\theta-\ldots=\tfrac{1}{2}\theta. \quad \ldots\ldots\ldots\ldots\ldots\ldots(\mathrm{D})$$

Gregory's Series (see page 66, Ex. 1) is a particular case of the series given by equation (B); for, putting $\theta=\pi/2$, we have

$$r-\tfrac{1}{3}r^3+\tfrac{1}{5}r^5-\tfrac{1}{7}r^7+\ldots=\tan^{-1}r. \quad \ldots\ldots\ldots\ldots\ldots\ldots(\mathrm{E})$$

This has been proved for $0\leqslant r\leqslant 1$; it therefore holds for $-1\leqslant r\leqslant 0$. Hence it is true if $|r|\leqslant 1$. When $r=1$, we have

$$1-\tfrac{1}{3}+\tfrac{1}{5}-\tfrac{1}{7}+\ldots=\frac{\pi}{4}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathrm{F})$$

EXERCISE VII

1. Prove that $\log\dfrac{u_1}{u_2}=\log u_1-\log u_2$, provided that

$$-\pi<\mathrm{am}\,u_1-\mathrm{am}\,u_2<\pi.$$

2. Show that $1^\iota=e^{2k\pi}$, where k is an integer.

3. Explain the fallacy in the following argument: We have $e^{2m\pi}=e^{2n\pi}$, where m, n are integers. Raising each side to the power ι, it follows that

$$e^{-2m\pi}=e^{-2n\pi}.$$

4. Prove that the values of $(1+\iota)^\iota$ are

$$e^{-(\frac{1}{4}+2k)\pi}\{\cos(\tfrac{1}{2}\log 2)+\iota\sin(\tfrac{1}{2}\log 2)\}.$$

5. The general value of e^z is $E(z)\,.\,(\cos 2k\pi z+\iota\sin 2k\pi z)$.

6. The principal value of $(\cos\alpha+\iota\sin\alpha)^{x+\iota y}$ is

$$\cos(x+\iota y)\alpha+\iota\sin(x+\iota y)\alpha,$$

which may be regarded as an extension of De Moivre's theorem.

7. Consider the equations

(i) $\dfrac{1}{a^z}=a^{-z}$, (ii) $a^{z_1}\,.\,a^{z_2}=a^{z_1+z_2}$, (iii) $(ab)^z=a^zb^z$.

Prove that for (i) and (iii) every value of one side is a value of the other side, but that this is not the case for (ii).

Also prove that (i) and (ii) are true for the principal values, but this is not always the case for (iii).

8. Draw a graph of the equation

$$y = \sin x - \tfrac{1}{2}\sin 2x + \tfrac{1}{3}\sin 3x - \dots,$$

showing that it consists of segments of parallel straight lines, and is discontinuous where $x = (2k+1)\pi$, k being an integer or zero.

9. At all points within or on the circle $|z| = 1$, excepting the point $z = 1$, prove that

$$\log(1-z) = -z - \frac{z^2}{2} - \frac{z^3}{3} - \dots.$$

10. The logarithm defined by the series in Ex. 9 is

$$\log \rho + \iota\phi,$$

where $1 - z = \rho(\cos\phi + \iota\sin\phi)$ and $-\frac{\pi}{2} < \phi < \frac{\pi}{2}$.

11. Prove that at all points within or on the circle $|z| = 1$, excepting the points $z = \pm 1$,

$$\log\frac{1+z}{1-z} = 2(z + \tfrac{1}{3}z^3 + \tfrac{1}{5}z^5 + \dots).$$

[Let $1 + z = \rho(\cos\phi + \iota\sin\phi)$, $1 - z = \rho'(\cos\phi' + \iota\sin\phi')$.

Then $\log\frac{1+z}{1-z} = \log(1+z) - \log(1-z)$, provided that $-\pi < \phi - \phi' < \pi$. But this is the case, for under the given conditions ϕ and ϕ' lie between $-\pi/2$ and $\pi/2$, etc.]

12. Show that at all points on the positive side of the y-axis, and at all points on this axis except $z = \pm 1$,

$$\log z = 2\left\{\frac{z-1}{z+1} + \frac{1}{3}\left(\frac{z-1}{z+1}\right)^3 + \dots\right\}.$$

[Let $t = (z-1)/(z+1)$. Denote the points 1, -1, z by A, A', P. If $|t| = 1$, then $|z-1| = |z+1|$, i.e. $AP = A'P$.

Hence if t is on the circle $|z+1| = 1$, z is on the y-axis. If $|t| < 1$, we have $AP < A'P$, and z is to the right of the y-axis. Now use Ex. 11.]

13. Show that if the point z is on, or to the right of, the parallel to the y-axis through the point $z = -\frac{1}{2}$, the series

$$\frac{z}{1+z} + \frac{1}{2}\left(\frac{z}{1+z}\right)^2 + \frac{1}{3}\left(\frac{z}{1+z}\right)^3 + \dots$$

converges to the sum $\log(1+z)$.

CHAPTER VII

ELIMINATION

1. Resultant. Suppose that we have k homogeneous equations in k variables or k equations, not all homogeneous, in $k-1$ variables. In the first case a solution of the system is $(0, 0, \ldots)$, every variable being zero. *This is excluded from further consideration.*

In general, it is possible to find an equation free from the variables. Any process leading to such a result is called *elimination*, and any equation so obtained is a *necessary* condition that the given equations may have a common solution. Suppose that $R=0$ is a *necessary and sufficient* condition that the system may have a solution. Further, suppose that R is a rational integral function of the coefficients of the lowest degree possible. Then R (or R multiplied by some numerical constant) is called the *resultant* or the *eliminant* of the system. The case of two quadratics has been considered in Ch. II, 1, 2.

2. Method of Symmetric Functions. Consider the pair

$$f(x)\equiv a_0x^m+a_1x^{m-1}+\ldots+a_m=0,\quad \phi(x)=b_0x^n+b_1x^{n-1}+\ldots+b_n=0,$$

of which the roots are $(\alpha_1, \alpha_2, \ldots \alpha_m)$, $(\beta_1, \beta_2, \ldots \beta_n)$ respectively.

A common solution exists if and only if one of the quantities $\phi(\alpha_1)$, $\phi(\alpha_2)$, $\ldots$ $\phi(\alpha_m)$ is zero, that is if $\phi(\alpha_1)\,.\,\phi(\alpha_2)\ldots\phi(\alpha_m)=0$.

The left-hand side is a symmetric function of $\alpha_1, \alpha_2, \ldots \alpha_m$ of order n. If it is multiplied by $a_0{}^n$ it becomes a rational integral function of the coefficients. We therefore define the resultant R of $f(x)=0$, $\phi(x)=0$ by

$$R=a_0{}^n\phi(\alpha_1)\phi(\alpha_2)\ldots\phi(\alpha_m). \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(A)$$

Again, we have $\phi(x)\equiv b_0(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n)$;

and therefore $\phi(\alpha_1)=b_0(\alpha_1-\beta_1)(\alpha_1-\beta_2)\ldots(\alpha_1-\beta_n)$.

Hence if $\Pi(\alpha-\beta)$ denotes the product of the mn factors of the form $\alpha_r-\beta_s$, then

$$R=a_0{}^nb_0{}^m\Pi(\alpha-\beta). \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(B)$$

Therefore also $R=(-1)^{mn}a_0{}^nb_0{}^m\Pi(\beta-\alpha)$,

and consequently $R=(-1)^{mn}b_0{}^mf(\beta_1)f(\beta_2)\ldots f(\beta_n)$. $\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(C)$

For the pair of equations in two variables, x and y,

$$u = a_0x^m + a_1x^{m-1}y + \ldots + a_my^m = a_0(x-\alpha_1y)(x-\alpha_2y)\ldots = 0,$$

$$v = b_0x^n + b_1x^{n-1}y + \ldots + b_ny^n = b_0(x-\beta_1y)(x-\beta_2y)\ldots = 0,$$

the resultant R is defined as above, and $R=0$ is the necessary and sufficient condition that $u=0$, $v=0$ may have a common solution other than (0, 0).

3. Order and Weight of R. Looking at the forms (C) and (A) of Art. 2, it will be seen that *R is a homogeneous function of the coefficients of each equation.*

Moreover, *R is of order $m+n$ in the coefficients, those of $f(x)$ occurring to the degree n and those of $\phi(x)$ to the degree m.*

We shall now prove that *the sum of the suffixes in any term of R is equal to mn.* This is generally expressed by saying that *R is of weight mn.*

Let $\alpha_1, \alpha_2, \ldots, \beta_1, \beta_2, \ldots$ be multiplied by λ. The effect of this is

$$\text{to change} \quad a_1, b_1 \quad \text{into} \quad \lambda a_1, \lambda b_1,$$

$$\text{to change} \quad a_2, b_2 \quad \text{into} \quad \lambda^2 a_2, \lambda^2 b_2,$$

and so on.

Thus any term in R is multiplied by λ^w, where w is the sum of the suffixes. But looking at the form (B), we see that R is multiplied by λ^{mn}, therefore $w=mn$.

4. Second Method of Elimination. We consider the process usually employed in elementary algebra. It is illustrated below with reference to two cubic equations, and it will be found that *if it is applied to equations of higher degree than the second, irrelevant factors are introduced.*

(1) *Resultant of two cubic equations.* Consider the equations

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0 \quad \text{and} \quad b_0x^3 + b_1x^2 + b_2x + b_3 = 0 \ldots\ldots\ldots\ldots\text{(A)}$$

Multiply these by b_0, a_0 respectively and subtract; also multiply by b_3, a_3, subtract and divide by x; then we have

$$(a_0b_1)x^2 + (a_0b_2)x + (a_0b_3) = 0 \quad \text{and} \quad (a_0b_3)x^2 + (a_1b_3)x + (a_2b_3) = 0 \ldots\ldots\text{(B)}$$

Whence, eliminating x, we have $S=0$, where S is

$$\{(a_0b_1)(a_2b_3) - (a_0b_3)^2\}^2 - \{(a_0b_1)(a_1b_3) - (a_0b_2)(a_0b_3)\}\{(a_0b_2)(a_2b_3) - (a_0b_3)(a_1b_2)\}.$$

This is of order 8 and weight 12, whereas the resultant R is of order 6 and weight 9. Hence $S=QR$, where $Q = h(a_1b_2) + k(a_0b_3)$, h and k being numerical constants.

Now the part of S which does not contain (a_0b_3) explicitly is equal to

$$(a_0b_1)(a_2b_3)\{(a_0b_1)(a_2b_3)-(a_1b_3)(a_0b_2)\}=-(a_0b_1)(a_1b_2)(a_2b_3)(a_0b_3),$$

for $$(a_0b_1)(a_2b_3)+(a_0b_2)(a_3b_1)+(a_0b_3)(a_1b_2)=0.$$

Hence S is divisible by (a_0b_3), and the quotient R is given by

$$R=(a_0b_3)^3+(a_0b_1)(a_1b_3)^2+(a_0b_2)^2(a_2b_3)$$
$$-2(a_0b_1)(a_0b_3)(a_2b_3)-(a_0b_1)(a_1b_2)(a_2b_3)-(a_0b_2)(a_0b_3)(a_1b_3).$$

NOTE. If $(a_0b_3)=0$, equations (B) have the common solution $-(a_0b_2)/(a_0b_1)$.

5. Equations in Two or More Variables. (1) Consider the pair

$$\left.\begin{aligned} u\equiv ax^2+2hxy+by^2+2gx+2fy+c &=0\\ u'\equiv a'x^2+2h'xy+b'y^2+2g'x+2f'y+c' &=0\end{aligned}\right\} \quad \text{.....(A)}$$

First method. Write the equations in the form

$$ax^2+2vx+w=0, \quad a'x^2+2v'x+w'=0, \quad \text{.....(B)}$$

where $v=hy+g$, $w=by^2+2fy+c$ and v', w' have similar values. Therefore

$$2(av')x+(aw')=0, \quad (aw')x+2(vw')=0, \quad \text{.....(C)}$$

and $$(aw')^2-4(av')(vw')=0. \quad \text{.....(D)}$$

This is a biquadratic in y, and if y_1 is a root, the corresponding value x_1 of x is obtained by putting $y=y_1$ in either of the equations (C).

Second method. The solution may be made to depend on a cubic equation. The function $u+\lambda u'$ is the product of linear functions of x and y if

$$\begin{vmatrix} a+\lambda a', & h+\lambda h', & g+\lambda g' \\ h+\lambda h', & b+\lambda b', & f+\lambda f' \\ g+\lambda g', & f+\lambda f', & c+\lambda c' \end{vmatrix}=0. \quad \text{.....(E)}$$

Let λ_1 be a root of this cubic and let

$$u+\lambda_1 u'=(lx+my+n)(l'x+m'y+n'),$$

then the given equations are equivalent to the two pairs

$$u=0, \quad lx+my+n=0; \quad u=0, \quad l'x+m'y+n'=0.$$

(2) *Two equations in x, y of the m-th and n-th degrees respectively have mn solutions.* For suppose that the equations, arranged in powers of x, are

$$u_0x^m+u_1x^{m-1}+u_2x^{m-2}+\ldots+u_m=0, \quad \text{.....(A)}$$
$$v_0x^n+v_1x^{n-1}+v_2x^{n-2}+\ldots+v_n=0,$$

where u_r, v_r are polynomials in y of degree r. If x is eliminated from the equations, the resultant R is of weight mn, and hence is of degree mn in y.

Let y_1 be one of the mn values of y given by $R=0$: then if $y=y_1$, equations (A) are satisfied by the same value (x_1) of x. Therefore (x_1, y_1) is a solution of equations (A), and the equations have mn solutions.

(3) *If* (x_1, y_1), (x_2, y_2), ... *are the solutions of equations* (A), *any symmetric function of the form* $\Sigma x_1^h y_1^k$ *can be expressed in terms of the coefficients.*

Illustration. Suppose it is required to find $\Sigma x_1^2 y_1$. Let $t = \lambda x + \mu y$, and eliminate x, y between this equation and equations (A), thus obtaining an equation of degree mn in t. The roots of this are

$$t_1 = \lambda x_1 + \mu y_1, \quad t_2 = \lambda x_2 + \mu y_2, \quad \text{etc.}$$

If, then, we find the value of Σt_1^3, the coefficient of $\lambda^2\mu$ in this is the value of $3\Sigma x_1^2 y_1$.

(4) It can also be proved that *three equations in* x, y, z *of degrees* m, n, p *have* mnp *solutions.* Moreover, any symmetric function of the form $\Sigma x_1^h y_1^k z_1^l$ can be expressed in terms of the coefficients by taking $t = \lambda x + \mu y + \nu z$, and proceeding as above.

6. Resultants expressed as Determinants.

(1) *Sylvester's method.* To eliminate x from equations (A) of Art. 5, (2),

multiply the equation of the mth degree by $x^{n-1}, x^{n-2}, \ldots x, 1$;

multiply the equation of the nth degree by $x^{m-1}, x^{m-2}, \ldots x, 1$;

we thus have $m+n$ equations from which we can eliminate $x^{m+n-1}, x^{m+n-2}, \ldots x$, regarded as independent variables.

Ex. 1. *Eliminate* x *from* $a_0x^2 + a_1x + a_2 = 0, \quad b_0x^2 + b_1x + b_2 = 0.$

Multiplying each by x, 1 we have

$$\begin{aligned} a_0x^3 + a_1x^2 + a_2x &= 0, \\ a_0x^2 + a_1x + a_2 &= 0, \\ b_0x^3 + b_1x^2 + b_2x &= 0, \\ b_0x^2 + b_1x + b_2 &= 0. \end{aligned}$$

Eliminating x^3, x^2, x, regarded as independent variables, we have

$$S = \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix} = 0.$$

The expression S is of order 4 and weight 4, so that it contains no extraneous factor. In fact, since the term $a_0^2b_2^2$ occurs, we have $S = R$.

(2) *Bézout's method.* We can express the resultant of two equations of the nth degree as a symmetrical determinant of the nth order in the following way. Take, for example, the equations

$$\begin{aligned} f(x) &\equiv a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0, \\ \phi(x) &\equiv b_0x^4 + b_1x^3 + b_2x^2 + b_3x + b_4 = 0; \end{aligned}$$

then we have the following four equations,

$$a_0(b_1x^3+b_2x^2+b_3x+b_4)=b_0(a_1x^3+a_2x^2+a_3x+a_4),$$
$$(a_0x+a_1)(b_2x^2+b_3x+b_4)=(b_0x+b_1)(a_2x^2+a_3x+a_4),$$
$$(a_0x^2+a_1x+a_2)(b_3x+b_4)=(b_0x^2+b_1x+b_2)(a_3x+a_4),$$
$$(a_0x^3+a_1x^2+a_2x+a_3)b_4=(b_0x^3+b_1x^2+b_2x+b_3)a_4.$$

Expanding these, we have four equations from which we can eliminate x^3, x^2, x, regarded as independent quantities. The result is

$$S\equiv\begin{vmatrix} (a_0b_1) & (a_0b_2) & (a_0b_3) & (a_0b_4) \\ (a_0b_2) & (a_0b_3)+(a_1b_2) & (a_0b_4)+(a_1b_3) & (a_1b_4) \\ (a_0b_3) & (a_0b_4)+(a_1b_3) & (a_1b_4)+(a_2b_3) & (a_2b_4) \\ (a_0b_4) & (a_1b_4) & (a_2b_4) & (a_3b_4) \end{vmatrix}=0.$$

Further, we can show that $S=R$, for if α_1, α_2, ... are the roots of $f(x)=0$, then

$$R=a_0^4\phi(\alpha_1)\phi(\alpha_2)\phi(\alpha_3)\phi(\alpha_4).$$

Now both R and S are of order $4+4$ and of weight 4×4, therefore $S=kR$ where k is a *numerical* factor. Looking at the second diagonal of S, we see that the term $(a_0b_4)^4$ occurs in the expansion. This term also occurs in R, therefore $S=R$.

The method may be applied to two equations of different degrees as in the example below.

Ex. 2. *Use Bézout's method to eliminate x from*

$$f(x)=a_0x^2+a_1x+a_2=0,$$
$$\phi(x)=b_0x^3+b_1x^2+b_2x+b_3=0,$$

showing that the result is

$$S\equiv\begin{vmatrix} (a_0b_1) & (a_0b_2) & a_0b_3 \\ (a_0b_2) & a_0b_3+(a_1b_2) & a_1b_3 \\ a_0 & a_1 & a_2 \end{vmatrix}=0.$$

Also show that if α_1, α_2 are the roots of $f(x)=0$, then

$$S=-a_0^3\phi(\alpha_1)\phi(\alpha_2).$$

Multiplying the first equation by x and proceeding as in the text,

$$a_0(b_1x^2+b_2x+b_3)=b_0(a_1x^2+a_2x),$$
$$(a_0x+a_1)(b_2x+b_3)=(b_0x+b_1)a_2x,$$

which may be written

$$(a_0b_1)x^2+(a_0b_2)x+a_0b_3=0,$$
$$(a_0b_2)x^2+\{a_0b_3+(a_1b_2)\}x+a_1b_3=0.$$

Taking these with the first equation and eliminating x^2, x as independent quantities, we have the first result.

Again, if $R=a_0^3\phi(\alpha_1)\phi(\alpha_2)$, it will be seen that both R and S are of order $3+2$ and of weight 2×3, thus $S=kR$ where k is a numerical factor.

Now the term $a_0^2b_3^3$ occurs in the second diagonal of S, and since S is of the third order, $-a_0^3b_3^2$ occurs in the expansion. Also $a_0^3b_3$ occurs in R, therefore $S=-R$.

7. Discriminant of a Binary Quantic. (1) Let $\alpha_1, \alpha_2, \dots \alpha_n$ be the roots of

$$f(x) \equiv (a_0, a_1, a_2, \dots a_n \between x, 1)^n,$$

and let R be the resultant of $f(x)=0$ and $f'(x)=0$, so that

$$R = a_0^{n-1} f'(\alpha_1) f'(\alpha_2) \dots f'(\alpha_n).$$

Now $f(x) = a_0(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)\dots$; therefore we have

$$f'(x) = a_0(x-\alpha_2)(x-\alpha_3)\dots + a_0(x-\alpha_1)(x-\alpha_3)\dots + \dots,$$

and
$$f'(\alpha_1) = a_0(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\dots(\alpha_1-\alpha_n),$$

with similar values for $f'(\alpha_2)$, etc. Hence it follows that

$$R = (-1)^{\frac{1}{2}n(n-1)} a_0^{2n-1} \Pi(\alpha_r - \alpha_s)^2. \quad \dots\dots\dots\text{(A)}$$

(2) *The* discriminant Δ *of* $f(x)$ *is defined as the resultant of*

$$\phi(x) \equiv (a_0, a_1 \dots a_{n-1} \between x, 1)^{n-1} = 0 \quad \textit{and} \quad \psi(x) \equiv (a_1, a_2, \dots a_n \between x, 1)^{n-1} = 0,$$

and it will be proved that $a_0^{2(n-1)} \Pi(\alpha_r - \alpha_s)^2 = (-1)^{\frac{1}{2}n(n-1)} n^n \Delta$. ....(B)

We have the equalities $f(x) \equiv x\phi(x) + \psi(x)$, $f'(x) \equiv n\phi(x)$.

Hence, if $\beta_1, \beta_2, \dots \beta_{n-1}$ are the roots of $\phi(x)=0$, which is the same as $f'(x)=0$, then

$$\Delta = a_0^{n-1}\psi(\beta_1)\psi(\beta_2)\dots = a_0^{n-1} f(\beta_1) f(\beta_2) \dots .$$

Now, by Art. 2, (C), $R = (-1)^{n(n-1)}(na_0)^n f(\beta_1) f(\beta_2) \dots$ . ...(C)

$$\therefore\ R = n^n a_0 \Delta, \quad \dots\dots\dots\text{(D)}$$

and equation (B) follows from (A).

Thus defined, Δ *is the simplest rational integral function of the coefficients whose vanishing is the condition that* $f(x)=0$ *has two equal roots.*

For the quadratic $ax^2+2bx+c$, equation (B) gives

$$\Delta = -\tfrac{1}{4}a^2(\alpha-\beta)^2 = ac - b^2.$$

For the cubic and quartic the definition gives the values of Δ as stated in *H.A.*, XII, 2, 10.

Ex. 1. *For the equation* $x^n + ax + b = 0$, *prove that the product of the squares of the differences of the roots is* $(-1)^{\frac{1}{2}n(n+1)}\{(-n)^n b^{n-1} - (n-1)^{n-1}a^n\}$.

Here Δ is the resultant of

$$\phi(x) \equiv x^{n-1} + \frac{a}{n} = 0 \quad \text{and} \quad \psi(x) \equiv \frac{n-1}{n}ax + b = 0.$$

$$\therefore\ \Delta = (-1)^{n-1}\left(\frac{n-1}{n}a\right)^{n-1}\left\{\left(-\frac{nb}{(n-1)a}\right)^{n-1} + \frac{a}{n}\right\}$$

$$= b^{n-1} + \left(\frac{a}{n}\right)^n (1-n)^{n-1};$$

$$\therefore\ \Pi(\alpha_r - \alpha_s)^2 = (-1)^{\frac{1}{2}n(n-1)}\{n^n b^{n-1} + a^n(1-n)^{n-1}\},$$

and the last expression is equal to the one in question.

EXERCISE VIII

1. Prove that (i) the resultant of $ax^n+by^n=0$ and $a'x^n+b'y^n=0$ is
$$(ab'-a'b)^n.$$

(ii) The resultant of $ax^3+3cx=0$ and $3cx^2+e=0$ is $e(ae-9c^2)^2$.

2. Prove that the squares of the differences of a root of $x^2+bx+c=0$ and a root of $x^2+bx+d=0$ are the roots of
$$x^2+\{2(c+d)-b^2\}x+(c-d)^2=0.$$

3. If $u\equiv ax^2+2bx+c$, $u'=a'x^2+2b'x+c'$, $J\equiv(ab')x^2+(ac')x+(bc')$, R is the resultant of $u=0$, $u'=0$ and R' that of $u=0$, $J=0$, prove that
$$R'=(ac-b^2)R.$$

[If $A=(bc')$, $B=(ca')$, $C=(ab')$, then
$$R'=(cC-aA)^2+2(bA+cB)(aB+2bC).$$
Subtract $(aA+bB+cC)^2$, which is zero.]

4. The result of eliminating x from $ax^2+bx+c=0$ and $x^3=1$ is
$$a^3+b^3+c^3-3abc=0.$$

Obtain this result by the method of symmetric functions. Also as follows: Multiply the first equation by 1, x, x^2. Put $x^3=1$ and eliminate x, x^2 as independent variables.

5. The result of eliminating x from $ax^3+bx^2+cx+d=0$ and $x^4=1$ is
$$\begin{vmatrix} a & b & c & d \\ b & c & d & a \\ c & d & a & b \\ d & a & b & c \end{vmatrix}=0.$$

[Use the second method of Ex. 4.]

6. If $u=0$, $u'=0$ be two equations of the second degree in x, y with real coefficients, show that

(i) if $(p+\iota p', q+\iota q')$ is a solution, so also is $(p-\iota p', q-\iota q')$, where p, p', q, q' are real;

(ii) if the three values of λ given by equation (E) of Art. 5 are all real, then the four solutions of the given equations are all real or all imaginary.

7. Solve the equations $2xy-y^2+x-2=0$, $x^2-y=0$.

8. Solve the equations $x^2-2y^2+10y-13=0$, $5x^2-8x+6y-7=0$.

9. If (x_1y_1), (x_2y_2), (x_3y_3) are the solutions of $y^2=4x$, $xy=y+2$, prove that
$$\Sigma x_1=2,\ \Sigma y_1=0,\ \Sigma x_1y_1=6,\ \Sigma x_1^2y_2y_3=12,\ \Sigma y_1^2x_2x_3=12.$$

10. If $(\alpha_1, \beta_1, \gamma_1)$, $(\alpha_2, \beta_2, \gamma_2)$, ..., are the solutions of the equations
$$x=y+y^2,\quad y=z+z^2,\quad z=x+x^2,$$
prove that $\alpha_1+\alpha_2+\ldots=-4$, $\alpha_1\beta_1+\alpha_2\beta_2+\ldots=2$, the summation being extended to all the solutions.

11. Prove that the equations

$$\frac{a}{a'}x-\frac{b}{b'}y+\frac{a'}{x}+\frac{b'}{y}=0,$$
$$\frac{b}{b'}y-\frac{c}{c'}z+\frac{b'}{y}+\frac{c'}{z}=0,$$
$$\frac{c}{c'}z-\frac{a}{a'}x+\frac{c'}{z}+\frac{a'}{x}=0,$$

are inconsistent unless $a+b+c=0$.

12. Given that $$\frac{ayz}{(y-z)^2}=\frac{bzx}{(z-x)^2}=\frac{cxy}{(x-y)^2},$$

prove that each of these is equal to

$$abc\div(a^2+b^2+c^2-2bc-2ca-2ab).$$

13. Show that the equations $x^2-yz=a$, $y^2-zx=b$, $z^2-xy=c$, are equivalent to

$$(a+b+c)(x+y+z)=k,$$
$$(a+\omega^2b+\omega c)(x+\omega y+\omega^2z)=k,$$
$$(a+\omega b+\omega^2c)(x+\omega^2y+\omega z)=k,$$

where $$k=\pm\sqrt{(a^3+b^3+c^3-3abc)},$$

where ω is an imaginary cube root of unity. Hence show that if $k=0$ the equations are inconsistent unless a, b, c are all zero.

14. If a, b, c are real and $a+b+c>0$, prove that the equations

$$x^2+2yz=a,\quad y^2+2zx=b,\quad z^2+2xy=c$$

have four real and four imaginary solutions. Find the real solutions if $a=-3$, $b=5$, $c=2$.

15. Prove that in general the equations

$$\frac{l_1x+m_1y+n_1}{x}=\frac{l_2x+m_2y+n_2}{y}=l_3x+m_3y+n_3$$

have three solutions.

[Denote each member of the equations by k, then k is given by

$$\begin{vmatrix} l_1-k & m_1 & n_1 \\ l_2 & m_2-k & n_2 \\ l_3 & m_3 & n_3-k \end{vmatrix}=0.$$

16. Solve the equations $$\frac{x+y}{x}=\frac{2x-3y+5}{y}=x-y+2.$$

17. Show that the equations $$\frac{x+y}{x}=\frac{2x-y+6}{y}=3x-2y+4$$

have a single real solution and find it.

18. If the equations

$$(x+1)(y-1)=(y+1)(z-1)=(z+1)(x-1)=\lambda-1$$

and

$$x+y+z=3a$$

are consistent, then $(\lambda+3)(\lambda-a^2)=0$. Also find all the solutions if $a=-\frac{10}{9}$.

19. Eliminate x from $x^5=1$, $y=x-x^4$, showing that the result is
$$y(y^4+5y^3+5)=0.$$

20. Eliminate x from $x^7=1$, $y=x+x^6$, showing that the result is
$$(y-2)(y^3+y^2-4y+1)=0.$$

21. Use Bézout's method to eliminate x from the equations
$$a_0x^3+a_1x^2+a_2x+a_3=0, \quad b_0x^3+b_1x^2+b_2x+b_3=0,$$
showing that the result is
$$\begin{vmatrix} (a_0b_1) & (a_0b_2) & (a_0b_3) \\ (a_0b_2) & (a_0b_3)+(a_1b_2) & (a_1b_3) \\ (a_0b_3) & (a_1b_3) & (a_2b_3) \end{vmatrix}=0.$$

22. Eliminate x from $x^3+px^2+qx+r=0$, $x^2-xy+1=0$, showing that the result is $ry^3+(pr+q)y^2+(pq+qr+p-3r)y+(1-q)^2+(p-r)^2=0$.

If α, β, γ are the roots of the first equation, what are those of the last? Verify by the use of symmetric functions.

23. Eliminate x from $ax^5+bx+c=0$, $cx^5+bx^4+a=0$, showing that the result is $(b^2+c^2-a^2)(a^2-ab-c^2)+b^2c^2=0$.

[If α is a common root, so is α^{-1}. We may therefore write
$$ax^5+bx+c=(ax^3+px^2+qx+c)(x^2+kx+1).]$$

24. The condition that ax^7+bx^3+c and cx^7+bx^4+a may have a common quadratic factor is $(a^2+ab-c^2)(a^2-ab-c^2)^2=b^2c^2(a^2-c^2)$.

25. Eliminate x, y, z from
$$bx^2-2fx+c=0, \quad cy^2-2gy+a=0, \quad az^2-2hz+b=0, \quad xyz=1,$$
showing that the result is $abc+2fgh-af^2-bg^2-ch^2=0$.

26. Rationalise the equation
$$(x+\sqrt{x^2-bc})(y+\sqrt{y^2-ca})(z+\sqrt{z^2-ab})=abc,$$
showing that the result is
$$2xyz-ax^2-by^2-cz^2+abc=0.$$
[This follows from the last example.]

27. If (x_1, y_1), (x_2, y_2), (x_3, y_3) are the solutions of $x^3+y^3=a^3$, $lx+my=1$, prove that $x_1y_1+x_2y_2+x_3y_3=-9l^4m^4/(l^3-m^3)^2$.

28. If $a\neq0$ and x, y, z satisfy the equations
$$axy+bx+cy+d=0,$$
$$ayz+by+cz+d=0,$$
$$azx+bz+cx+d=0,$$
prove that $a(b^2+c^2-bc-ad)(ax^2+(b+c)x+d)=0$.

Hence show that if the equations are satisfied by values of x, y, z which are not all equal, then $b^2+c^2=bc+ad$; and, if this condition is satisfied, there are infinitely many solutions.

NOTE. Except for equal values of the variables, the equations in Exx. 28, 31 are inconsistent unless a certain relation holds among the coefficients. If this relation holds, the equations are not independent. Such systems are called *poristic*.

29. Having given the equations

$$y^2+z^2+ayz=z^2+x^2+azx=x^2+y^2+axy,$$

prove that if x, y, z are all different, then

$$a=1 \quad \text{and} \quad x+y+z=0.$$

30. Having given the equations

$$yz+\frac{1}{yz}+ax+\frac{b}{x}=zx+\frac{1}{zx}+ay+\frac{b}{y}=xy+\frac{1}{xy}+az+\frac{b}{z},$$

where x, y, z are all unequal, prove that $ab=1$, and that each member of the equations is zero.

31. If x, y, z are all unequal and

$$axy+h\left(\frac{x}{y}+\frac{y}{x}\right)+\frac{b}{xy}+g(x+y)+f\left(\frac{1}{x}+\frac{1}{y}\right)+c=0,$$

together with two equations obtained from this by the cyclic substitution (xyz), prove that

$$h^2-ab-ch+fg=0.$$

32. With regard to the equations *

$$\frac{ax+hy+gz}{x}=\frac{hx+by+fz}{y}=\frac{gx+fy+cz}{z}.$$

Let $\quad \Delta=\begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix}, \quad \phi(k)=\begin{vmatrix} a-k & h & g \\ h & b-k & f \\ g & f & c-k \end{vmatrix},$

and let $A, B, \ldots$ be the cofactors of $a, b, \ldots$ in Δ.

(i) Prove that the solutions of the equations are given by

$$(F+kf)x=(G+kg)y=(H+kh)z,$$

where k is a root of $\phi(k)=0$.

(ii) Show also that

$$\frac{x^2}{\frac{\partial\phi}{\partial a}}=\frac{y^2}{\frac{\partial\phi}{\partial b}}=\frac{z^2}{\frac{\partial\phi}{\partial c}}=-\frac{x^2+y^2+z^2}{\frac{\partial\phi}{\partial k}},$$

and that

$$yz(Gh-Hg)+zx(Hf-Fh)+xy(Fg-Gf)=0.$$

(iii) If (x_1, y_1, z_1), etc., are solutions corresponding to the roots k_1, k_2, k_3 of $\phi(k)=0$, then

$$(F+k_1f)(F+k_2f)(F+k_3f)=-(Hf-Fh)(Fg-Gf)$$

and

$$x_1x_2+y_1y_2+z_1z_2=0.$$

(iv) If $k_1=k_2$, then for the value k_1 of k the values of $x:y:z$ are indeterminate.

* The numbers x, y, z are proportional to the direction cosines of the axes of the quadric $ax^2+by^2+cz^2+2fyz+2gzx+2hxy=1$.

CHAPTER VIII

PROBABILITY

(*Continued from* H.A., *XXXII*)

1. Probability of Causes. (1) Suppose that an event has happened and that it must have arisen from one of a certain number of causes $C_1, C_2, \ldots$. *What is the probability that a specified cause, C_1, actually led to the event?*

This question is said to be one of *inverse probability*.

Ex. 1. *Each of three bags A, B, C contains white and black balls, the numbers of which are as follows:*

	A	B	C
white - -	a_1	a_2	a_3
black - -	b_1	b_2	b_3

A bag is chosen at random, a ball is drawn from it and is found to be white.

It is required to find the probabilities Q_1, Q_2, Q_3 that the ball came from A, B, C, respectively.

If the numbers of the balls are altered as below, the probabilities in question remain unchanged:

	A	B	C
white - -	a_1x	a_2y	a_3z
black - -	b_1x	b_2y	b_3z

when x, y, z are any numbers whatever. Choose these so that

$$x(a_1+b_1)=y(a_2+b_2)=z(a_3+b_3). \qquad \text{(A)}$$

The three bags now contain the same number of balls, therefore any one of the $(a_1x+a_2y+a_3z)$ white balls is as likely to be drawn as another.

If the ball which was drawn came from A, then it belonged to the group a_1x of white balls, and so for the other possibilities.

Therefore $\qquad Q_1 : Q_2 : Q_3 = a_1x : a_2y : a_3z = p_1 : p_2 : p_3,$

where $\qquad p_1 = a_1/(a_1+b_1), \quad p_2 = a_2/(a_2+b_2), \quad p_3 = a_3/(a_3+b_3);$

for, from (**A**), we have

$$x = k/(a_1+b_1), \quad y = k/(a_2+b_2), \quad z = k/(a_3+b_3),$$

and therefore $\qquad a_1x : a_2y : a_3z = a_1/(a_1+b_1) : a_2/(a_2+b_2) : a_3/(a_3+b_3).$

Now a white ball *is* drawn, therefore

$$Q_1+Q_2+Q_3=1 \quad \text{and} \quad Q_1 = p_1/(p_1+p_2+p_3),$$

with similar values for Q_2, Q_3.

It is to be noticed that p_1 *is the probability that the event will occur on the supposition that the ball comes from A, and so for* p_2, p_3.

Ex. 2. The same as the preceding, except that there are m_1 bags such as A containing a_1 white and b_1 black balls, m_2 such as B, and m_3 such as C, as in Ex. 1. Also Q_1, Q_2, Q_3 are the chances that the ball came from an A, B, C bag respectively.

Alter the numbers of the balls as in the preceding. Then any one of the

$$m_1a_1x + m_2a_2y + m_3a_3z$$

white balls is as likely to be drawn as another, and Q_1 is the chance that it comes from one of the m_1 groups of a_1x balls, so also for Q_2, Q_3, therefore

$$Q_1 : Q_2 : Q_3 = m_1a_1x : m_2a_2y : m_3a_3z = m_1p_1 : m_2p_2 : m_3p_3,$$

and as before,
$$Q_1 + Q_2 + Q_3 = 1,$$

therefore
$$Q_1 = m_1p_1/(m_1p_1 + m_2p_2 + m_3p_3),$$

with similar values for Q_2, Q_3.

NOTE. If P_1 is the chance estimated *before* the event that an A bag will be chosen and P_2, P_3 have similar meanings, we have

$$P_1 : P_2 : P_3 = m_1 : m_2 : m_3;$$

therefore
$$Q_1 : Q_2 : Q_3 = P_1p_1 : P_2p_2 : P_3p_3$$

and
$$Q_1 = P_1p_1/(P_1p_1 + P_2p_2 + P_3p_3), \quad \text{etc.}$$

Observe that P_1p_1 is the chance that a white ball is drawn, and that from an A bag.

(2) A General Statement. Suppose that an event has occurred which must have been due to one of the causes, C_1, C_2, ... C_n.

Let P_r be the probability of the existence of the cause C_r, estimated *before* the event took place.

Let p_r be the probability of the event on the assumption that the cause C_r exists.

Then the probability Q_r of the existence of the cause C_r, estimated after *the event has occurred, is given by*

$$Q_r = P_rp_r/(P_1p_1 + P_2p_2 + \dots P_np_n).$$

For an argument similar to that in the last two examples shows that

$$Q_1 : Q_2 : Q_3 : \dots = P_1p_1 : P_2p_2 : P_3p_3 : \dots,$$

and since the event *has* happened,

$$Q_1 + Q_2 + \dots + Q_n = 1,$$

whence the result follows.

NOTE. It is usual to call P_1, P_2, ... P_n the *a priori* probabilities of the existence of the causes and Q_1, Q_2, ... Q_n the *a posteriori* probabilities.

The product P_rp_r is the *antecedent probability* that the event will occur, and that from the rth cause.

The argument depends on the assumption (1) that Q_1, Q_2, ... *are proportional to* P_1p_1, P_2p_2, ..., which is justified in (1).

In particular, if an event is due to one of *two causes*, the odds in favour of its having occurred from the first cause are as $P_1p_1 : P_2p_2$.

The way in which these principles are applied to determine the *Probability of Future Events* is illustrated in Exx. 4 and 6.

Ex. 3. *A bag contains* 5 *balls, and of these it is equally likely that* 0, 1, 2, 3, 4, 5 *are white. A ball is drawn and is found to be white. What is the chance that this is the only white ball?*

There are 6 possible hypotheses; the number of white balls may be 0, 1, 2, 3, 4, 5. Denoting these possibilities by $C_0, C_1, \dots C_5$, and using a notation similar to the above, we have $P_0 = P_1 = \dots = P_5 = \frac{1}{6}$; and $p_0 = 0, \quad p_1 = \frac{1}{5}, \quad p_2 = \frac{2}{5}, \dots, \quad p_5 = \frac{5}{5}$;

$$\therefore \quad P_0p_0 + P_1p_1 + \dots + P_5p_5 = \frac{1}{6} \cdot \frac{1+2+3+4+5}{5} = \frac{1}{2};$$

$$\therefore \text{ the required chance} = Q_1 = P_1p_1 \div \tfrac{1}{2} = \tfrac{1}{15}.$$

Ex. 4. *If in the last example the ball which was drawn is replaced, what is the chance that a second drawing will give a white ball?*

$$Q_0p_0 + Q_1p_1 + \dots + Q_5p_5 = \tfrac{2}{6}(p_0^2 + p_1^2 + \dots + p_5^2) = \frac{2}{6 \cdot 5^2}(1^2 + 2^2 + 3^2 + 4^2 + 5^2).$$

Hence the required chance $= \tfrac{11}{15}$.

Ex. 5. *A pack of cards is counted, face downwards, and it is found that one card is missing. Two cards are drawn and are found to be spades. What are the odds against the missing card being a spade?*

The 'event' is that two spades are drawn. There are two possible hypotheses:

(C_1) The missing card is a spade.

(C_2) The missing card is not a spade.

The *a priori* probabilities P_1, P_2 of C_1, C_2 are $P_1 = \frac{1}{4}, \quad P_2 = \frac{3}{4}$.

The chances p_1, p_2 of the event under the hypotheses C_1, C_2 are

$$p_1 = \tfrac{12}{51} \cdot \tfrac{11}{50}, \quad p_2 = \tfrac{13}{51} \cdot \tfrac{12}{50}.$$

The odds against the missing card being a spade are as

$$P_2p_2 : P_1p_1 = \tfrac{3}{4} \cdot \tfrac{13}{51} \cdot \tfrac{12}{50} : \tfrac{1}{4} \cdot \tfrac{12}{51} \cdot \tfrac{11}{50} = 39 : 11.$$

Ex. 6. *A bag contains m balls which are either white or black, all possible numbers being equally likely. If p white and q black balls have been drawn in $p+q$ successive trials without replacement, the chance that another drawing will give a white ball is*

$$(p+1)/(p+q+2).$$

The possible hypotheses, all equally likely, are that the number of white balls are

$$m-q, \quad m-q-1, \quad \dots \quad m-q-r+1, \quad \dots \quad p.$$

Denote these by $C_1, C_2, \dots C_r, \dots C_{m-q-p+1}$.

If $p_1, p_2, \dots$ are the antecedent probabilities of the event under these hypotheses, we have

$$p_r = C_p^{m-q-r+1} \cdot C_q^{q+r-1} / C_{p+q}^m = A u_r v_r,$$

where

$$u_r = r(r+1)(r+2) \dots (r+q-1),$$

$$v_r = (n-r)(n-r+1)(n-r+2) \dots (n-r+p-1),$$

$$n = m-q-p+2,$$

and A is independent of r.

If $Q_1, Q_2, \dots$ are the *a posteriori* probabilities of $C_1, C_2, \dots$, then $Q_r = u_rv_r/S$,

where $$S = \Sigma_{r=1}^{r=n-1} u_rv_r = \frac{\lfloor p \rfloor q}{\lfloor p+q+1}} \cdot \frac{\lfloor m+1}{\lfloor n-2}} \quad \text{(by } H.A.\text{, Ch. XXI, 10, Ex. 1.)}$$

If p_r' is the chance that, with hypothesis C_r, another drawing gives a white ball,

$$p_r' = \frac{m-q-p-r+1}{m-q-p} = \frac{n-1-r}{m-q-p};$$

thus $p_{n-1}' = 0$, and the chance that another drawing gives a white ball is

$\Sigma_{r=1}^{r=n-2} Q_r p_r' = S'/(m-q-p)S$, where $S' = \Sigma_{r=1}^{r=n-2} u_r (n-1-r)(n-r)\ldots(n-r+p)$.

Thus S' can be obtained from S by writing $n-1$ for n and p for $p-1$; and hence

$$S' = \frac{\lfloor p+q+2}{\lfloor p+1 \rfloor q} \cdot \frac{\lfloor m+1}{\lfloor n-3} \quad \text{and} \quad \frac{S'}{S} = \frac{(p+1)(n-2)}{p+q+2}; \quad \text{the chance} = (p+1)/(p+q+2).$$

2. Value of Testimony. The theory of probability has been used to estimate the value of the testimony of witnesses. Such an application is open to adverse criticism. It rests on two assumptions which can hardly be justified, namely: (i) that to each witness there pertains a constant p (his *credibility*), which measures the average frequency with which he speaks the truth; (ii) that the statements of witnesses are independent of one another in the sense required in the theory of probability.

If we are prepared to make these assumptions, the procedure is as follows.

Ex. 1. *If p is the probability that a statement made by A is true and p' has a similar meaning for B, what are the odds in favour of the truth of a statement which A and B concur in making?*

The 'event' is the agreement of A and B in making a certain statement. The possibilities are: (i) the statement is true; (ii) it is false.

If it is true, the chance that they both say it is true is pp'.

If it is false, the chance that they both say it is true is $(1-p)(1-p')$.

Thus the *antecedent probabilities* of the event on the hypotheses (i), (ii) are

$$pp' \quad \text{and} \quad (1-p)(1-p'),$$

and the odds in favour of the truth of the statement are as $pp' : (1-p)(1-p')$.

Ex. 2. *A bag contains n balls, one of which is white. The probabilities that A and B speak the truth are p, p' respectively. A ball is drawn from the bag, and A and B both assert that it is white. What are the odds in favour of its being white?*

The 'event' is the agreement of A and B in making a statement. The possibilities are (i) it is true, (ii) it is false.

The *a priori* probabilities P_1, P_2, of (i), (ii) are $P_1 = 1/n$, $P_2 = (n-1)/n$.

If p_1, p_2 are the chances of the event under (i) and (ii), we have $p_1 = pp'$.

In the case of (ii), $(n-1)$ balls remain in the bag, and one of these is white. The chance that A should choose this ball and wrongly assert that it was drawn from the bag is $(1-p)/(n-1)$. The chance that B should do the same thing is $(1-p')/(n-1)$; hence

$$p_2 = (1-p)(1-p')/(n-1)^2,$$

and the odds in favour of a white ball having been drawn are as

$$P_1 p_1 : P_2 p_2 = \frac{1}{n} pp' : \frac{n-1}{n} \cdot (1-p)(1-p') \cdot \frac{1}{(n-1)^2}$$

$$= (n-1)pp' : (1-p)(1-p').$$

3. Duration of Play. (1) *A and B engage in a series of games which cannot be drawn, and p, q are their respective chances of winning a single game. At the start, A has £m, B has £n, and the loser in any game is to give £1 to his opponent. It is required to find each person's chance of winning all the other's money.*

Suppose that after a certain number of games A has £x, and that *then* his chance of winning all of B's money is u_x. In the next game A must win or lose £1, and the respective chances of these happenings are p and q.

In the first case A's chance of winning all of B's money is u_{x+1}, and in the second case it is u_{x-1}, therefore

$$u_x = pu_{x+1} + qu_{x-1}. \quad \text{.....(A)}$$

(1) *If* $p \neq q$, the solution is given by $u_x = A\alpha^x + B\beta^x$, where α, β are the roots of $py^2 - y + q = 0$. Since $p+q=1$, the roots are 1, q/p. Hence the solution is given by

$$u_x = A + B\left(\frac{q}{p}\right)^x.$$

Now A's chance is zero when he has no money, and unity when he has £$(m+n)$; hence

$$u_0 = A + B = 0 \quad \text{and} \quad u_{m+n} = A + B\left(\frac{q}{p}\right)^{m+n} = 1,$$

whence we find that $u_x = (p^{m+n} - p^{m+n-x}q^x)/(p^{m+n} - q^{m+n})$.

At the beginning of the contest the chances which A and B respectively have each of winning all of the other's money are u_m and u_n, and these are given by

$$u_m = \frac{p^n(p^m - q^m)}{p^{m+n} - q^{m+n}}, \quad u_n = \frac{q^m(p^n - q^n)}{p^{m+n} - q^{m+n}}.$$

(2) *If A and B are equally skilled*, then $p = q = \frac{1}{2}$, and equation (A) becomes

$$u_{x+1} - 2u_x + u_{x-1} = 0 \quad \text{or} \quad u_{x+1} - u_x = u_x - u_{x-1},$$

showing that u_0, u_1, u_2, ... is an arithmetic progression, and since $u_0 = 0$ and $u_{m+n} = 1$, we have

$$u_m = m/(m+n) \quad \text{and} \quad u_n = n/(m+n).$$

It follows that $u_m + u_n = 1$ (a fact which is not evident *a priori*). Whence we conclude that after a certain number of games, one of the two A, B will have won all of the other's money. Also their respective chances of doing this are in the ratio of their respective capitals.

This may be taken as justifying a remark made by Whitworth, when he says, 'To the community gambling is disadvantageous because its tendency is opposed to the equable distribution of wealth, ... making the rich richer and the poor poorer.'

4. 'Runs of Luck.' Let p be the chance in favour of an event at a single trial and q the chance against it.

(1) *It is required to find the chance that in n trials the event may happen on k successive occasions bounded by failures. Such a happening is called a* run of k.

Denoting the required probability by u_n, we shall prove that

$$u_{n+1} = u_n + (1 - u_{n-k})qp^k. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

For if there is a run of k in $(n+1)$ trials, then either

(i) the run occurs in the first n trials, the chance of which is u_n; or

(ii) the run is completed at the $(n+1)$th trial. In order that this may be the case, the successes (s) and the failures (f) must be distributed as under:

No. of trial happening	$1.2\ldots.n-k$	$n-k+1$	$n-k+2, \ldots n, n+1$
	no run of k	f	$s \quad \ldots \quad s, \quad s$

The chance that there is no run of k in the first $n-k$ trials is $1-u_{n-k}$, the chance that the $(n-k+1)$th trial fails and that the following k trials succeed is qp^k. Hence the chance that (ii) happens is $(1-u_{n-k})qp^k$.

Also the happenings (i) and (ii) are mutually exclusive;

$$\therefore \quad u_{n+1} = u_n + (1 - u_{n-k})qp^k.$$

(2) *If v_n is the chance that in n trials there is no run of k, then*

$$v_n = \textit{coefficient of } x^n \textit{ in the expansion of } \frac{1 - p^k x^k}{1 - x + qp^k x^{k+1}}.$$

For $v_n = 1 - u_n$, hence by the preceding,

$$v_{n+1} - v_n + qp^k v_{n-k} = 0; \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

$$\therefore \quad v_n = \text{coefficient of } x^n \text{ in the expansion of } \frac{\phi(x)}{1 - x + qp^k x^{k+1}},$$

where $\phi(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k$, and $a_0, a_1, \ldots a_k$ are independent of x. (See *H.A.*, XXII, 4.)

To find the constants, we observe that

$$u_1 = u_2 = \ldots = u_{k-1} = 0, \quad \therefore \quad v_1 = v_2 = \ldots = v_{k-1} = 1.$$

Also
$$u_k = p^k \quad \text{and} \quad u_{k+1} = p^k + qp^k;$$

$$\therefore \quad v_k = 1 - p^k \quad \text{and} \quad v_{k+1} - v_k + qp^k = 0.$$

Taking v_0 as defined by (B) when $n = k$, we have $v_{k+1} - v_k + qp^k v_0 = 0$, so that $v_0 = 1$. Hence, for sufficiently small values of x,

$$1 + x + x^2 + \ldots + x^{k-1} + (1 - p^k)x^k + \ldots = \frac{\phi(x)}{1 - x + qp^k x^{k+1}};$$

hence, by multiplication and equating coefficients, we find that $a_0 = 1$, and $a_k = -1 + v_k = -p^k$, every other a being zero.

Therefore $$\phi(x) = 1 - p^k x^k.$$

In the special case in which $k = 2$, we can proceed more simply thus:

Ex. 1. *If p is the chance of success and q that of failure at a single trial, the chance v_n that in n trials there are no two consecutive successes is given by*

$$v_{n+1} = qv_n + pqv_{n-1} \quad \textit{and} \quad v_0 = v_1 = 1.$$

For suppose that there are no two consecutive successes in $n+1$ trials; the chance of this is v_{n+1}, and

(i) If the last trial fails, success must not occur twice running in the first n trials.

(ii) If the last trial succeeds, the nth trial must fail, and two consecutive successes must not occur in the first $n-1$ trials.

The chances of (i) and (ii) are respectively qv_n and pqv_{n-1}; hence, $$v_{n+1} = qv_n + pqv_{n-1}.$$

Also we have $v_1 = 1$, $v_2 = 1 - p^2$, $pqv_0 = v_2 - qv_1$, and $v_0 = 1$.

5. Expectation. (1) Suppose that a person (A) has a ticket in a lottery which gives him a chance p of a prize of £a.

If the lottery were held N times, where N is a large number, we may expect him to get the prize about pN times, receiving £pNa. Thus we may say that *on an average* he receives £pa for a single lottery, and this is called his *expectation*.

Next suppose that A's ticket gives him a chance p_1 of receiving £a_1, a chance p_2 of receiving £a_2, and so on.

If the lottery were held N times, where N is large, we may expect him to receive £a_1 on about p_1N occasions, £a_2 on about p_2N occasions, and so on. Altogether he may be expected to get about £$N(p_1a_1 + p_2a_2 + \ldots)$.

Thus we may say that *on an average* he gets £$(p_1a_1 + p_2a_2 + \ldots)$ for a single lottery. This sum is the sum of the expectations arising from his chances of securing the separate sums, and is called his *expectation*.

Definitions. The *average value* of a quantity P, subject to risk, is the average value which P assumes in the long run. This value is also called the *expected value* of P or the *expectation* with regard to P.

If a quantity P can assume the values $P_1, P_2, P_3, \ldots$ and the chances that it has these values are respectively $p_1, p_2, p_3, \ldots$, the *average* or the *expected* value of P is $p_1P_1 + p_2P_2 + p_3P_3 + \ldots$.

This is merely a generalisation of what has been said in the case of a lottery.

It should be observed that every p denotes the chance that P has the corresponding value, so that *events need not be independent.*

Ex. 1. A man's *expectation of life* is usually taken to mean the average number of years which men of his age survive.

If p_r is the chance that he will survive r years, dying before the end of the next year, his expectation of life is roughly $p_1 \cdot 1 + p_2 \cdot 2 + p_3 \cdot 3 + \ldots$. A closer estimate is given below in Art. 6, Ex. 1.

Ex. 2. *A person draws* 2 *balls from a bag containing* 3 *white and* 5 *black balls. If he is to receive* 10*s. for every white ball which he draws and* 1*s. for every black ball, what is his expectation?*

The number of ways in which 2 balls can be drawn is $C_2^8 = 28$.

Of these the number of ways in which

2 white balls can be drawn is $C_2^3 = 3$,
1 white and 1 black ball can be drawn is $3 \cdot 5 = 15$,
2 black balls can be drawn is $C_2^5 = 10$.

Hence his chances of receiving 20s., 11s. and 2s. are respectively 3/28, 15/28, 10/28;

$$\therefore \text{ expectation} = \left(\tfrac{3}{28} \cdot 20 + \tfrac{15}{28} \cdot 11 + \tfrac{10}{28} \cdot 2\right) = 8\text{s. } 9\text{d.}$$

(2) *If f_r is the chance that an event fails in the first r trials and s is the number of trials in which on an average a single success is obtained, then*

$$s = 1 + f_1 + f_2 + f_3 + \ldots, \qquad \text{(A)}$$

where the series terminates or is assumed to be convergent.

For suppose that the first $(r-1)$ trials have failed, and that *then* u_r is the chance that the rth trial succeeds.

The chance that success occurs at the rth trial and not before is $f_{r-1}u_r$.

Hence, as in § (1),

$$s = u_1 \cdot 1 + f_1 u_2 \cdot 2 + f_2 u_3 \cdot 3 + \ldots. \qquad \text{(B)}$$

Assuming that s has a finite value, this series must terminate or converge. Also we have $f_1 = 1 - u_1$, $f_2 = f_1(1-u_2)$, ... $f_r = f_{r-1}(1-u_r)$, ...; for failure occurs in r trials if it occurs in the first $(r-1)$ trials and also at the rth trial; hence,

$$u_1 = 1 - f_1, \quad f_1 u_2 = f_1 - f_2, \ldots f_{r-1}u_r = f_{r-1} - f_r, \ldots;$$

therefore,

$$s = (1 - f_1) + 2(f_1 - f_2) + 3(f_2 - f_3) + \ldots$$
$$= 1 + f_1 + f_2 + f_3 + \ldots.$$

NOTE. (i) If success is certain at the rth trial, then $f_r = 0$. Consequently $f_{r+1}, f_{r+2}, \ldots$ are zero and the series terminates. (ii) If u_r does not tend to zero as $r \to \infty$, then f_r/f_{r-1} is less than unity by a finite number and therefore the series (A) is convergent. In this case the series (B) is also convergent, for its sum to r terms $\leqslant$ that of the series (A).

Ex. 3. *If p, q are the chances of success and failure at any trial, then, as in* § (1), $s = 1/p$. *Deduce this from the preceding.*

We have $f_r = q^r$, therefore

$$s = 1 + q + q^2 + \ldots \text{ to } \infty = 1/(1-q) = 1/p.$$

(3) *If p, q are the respective chances of the success and failure of an event at a single trial, then the average number of trials required to obtain a run of k successes is* $(p^{-k}-1)/q$.

Let s be the number of trials in question, and let v_n be the chance that in n trials there is no run of k successes. By Art. 4, (2), we have

$$1+v_1x+v_2x^2+\ldots=\frac{1-p^kx^k}{1-x+qp^kx^{k+1}}, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

and

$$s=1+v_1+v_2+\ldots. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

Putting $x=1$ in (A), it follows that

$$s=(1-p^k)/qp^k=(p^{-k}-1)/q.$$

Ex. 4. A coin is tossed until a run of 4 heads occurs. Find the average number of throws.

Required number $=\{(\frac{1}{2})^{-4}-1\}/\frac{1}{2}=2(2^4-1)=30$.

(4) *If at any trial, an event may turn out in one of the ways denoted by $A_1, A_2, \ldots$, and if on an average A_1 happens once in s_1 trials and A_2 happens once in s_2 trials, then the average number (σ) of trials in which one of the two A_1, A_2 happens is given by* $1/\sigma=1/s_1+1/s_2$.

For on an average, A_1 happens once in s_1 trials;

hence, A_1 happens s_2 times in s_1s_2 trials.

Similarly A_2 happens s_1 times in s_1s_2 trials;

therefore *one of the two* A_1, A_2 happens s_1+s_2 times in s_1s_2 trials;

$$\therefore \sigma=\frac{s_1s_2}{s_1+s_2} \quad \text{and} \quad \frac{1}{\sigma}=\frac{1}{s_1}+\frac{1}{s_2}.$$

6. Life Contingencies. In the business of life insurance, the necessary calculations are based on

(i) statistics regarding the average duration of life. These are to be found in 'Mortality' or 'Life' Tables;

(ii) careful estimates as to the interest likely to be yielded by investments.

(1) **Explanation of the tables on p. 116.** Of 100,000 persons of age 5, the number who reach the age x is denoted by l_x, and p_x is the probability that a person of age x and of the type referred to in the tables will live a year.

We also take q_x to represent the chance that such a person dies within the year, so that

$$p_x=l_{x+1}/l_x \quad \text{and} \quad q_x=(l_x-l_{x+1})/l_x.$$

The chances that a person of age x dies in the first, second, third, ... years are

$$\frac{l_x - l_{x+1}}{l_x}, \quad \frac{l_{x+1} - l_{x+2}}{l_x}, \quad \frac{l_{x+2} - l_{x+3}}{l_x}, \ldots .$$

For, taking the third year as an instance, out of l_x persons, $(l_{x+2} - l_{x+3})$ die during this year.

A man's *expectation of life* is usually taken to mean the average number of years which men of his age survive. This can be calculated as follows:

Ex. 1. *Find the expectation of life* (E_x) *of a person of age* x.

Suppose the deaths in any year to be *uniformly* distributed through the year, then if he is to die in the first year, his expectation of life is $\frac{1}{2}$ a year, if he dies in the second year it is $1\frac{1}{2}$ years, and so on, therefore

$$E_x = \frac{l_x - l_{x+1}}{l_x} \cdot \frac{1}{2} + \frac{l_{x+1} - l_{x+2}}{l_x} \cdot \frac{3}{2} + \frac{l_{x+2} - l_{x+3}}{l_x} \cdot \frac{5}{2} + \ldots$$

$$= \tfrac{1}{2} + (l_{x+1} + l_{x+2} + l_{x+3} + \ldots)/l_x,$$

where the series continues until the l's become zero.

Ex. 2. *Find the chance* (P) *that a person* A *of age* x *lives longer than one* B *of age* y.

If this event happens, then either

(i) A dies in a year subsequent to B,

(ii) or else A, B die in the same year, B dying first.

It is easy to see that the chance of (i) is

$$\frac{l_y - l_{y+1}}{l_y} \cdot \frac{l_{x+1}}{l_x} + \frac{l_{y+1} - l_{y+2}}{l_y} \cdot \frac{l_{x+2}}{l_x} + \ldots .$$

With regard to (ii), if A, B die in the same year and deaths are uniformly distributed through the year, the chance that B dies first is $\frac{1}{2}$. Hence the chance of (ii) is

$$\frac{1}{2}\left\{\frac{l_y - l_{y+1}}{l_y} \cdot \frac{l_x - l_{x+1}}{l_x} + \frac{l_{y+1} - l_{y+2}}{l_y} \cdot \frac{l_{x+1} - l_{x+2}}{l_x} + \ldots\right\}.$$

The required chance P is the sum of the two expressions just found; therefore

$$P = \{(l_y - l_{y+1})(l_x + l_{x+1}) + (l_{y+1} - l_{y+2})(l_{x+1} + l_{x+2}) + \ldots\}/2l_x l_y$$

$$= \tfrac{1}{2} + \{(l_{x+1}l_y - l_x l_{y+1}) + (l_{x+2}l_{y+1} - l_{x+1}l_{y+2}) \ldots\}/2l_x l_y$$

$$= \tfrac{1}{2} + \{l_{x+1}(l_y - l_{y+2}) + l_{x+2}(l_{y+1} - l_{y+3}) + \ldots - l_x l_{y+1}\}/2l_x l_y.$$

7. Annuities. If an insurance company agrees to make a yearly payment of 1 monetary unit to a person A of age x, the first payment to be made one year after the agreement, the next at the end of the second year, and so on, as long as A lives, we say that A secures an *annuity of* 1 (on his life).

The *value* or the *cost* of such an annuity is the sum of the present values of A's expectations under the agreement, and is denoted by a_x.

Taking an appropriate rate per cent. r and writing

$$v=\left(1+\frac{r}{100}\right)^{-1},$$

the present value of £M due n years hence is £Mv^n.

Now A's expectations are the sums of

$$l_{x+1}/l_x, \quad l_{x+2}/l_x, \quad l_{x+3}/l_x, \ \dots,$$

due one, two, three, ... years hence. Therefore

$$a_x=(vl_{x+1}+v^2l_{x+2}+v^3l_{x+3}+\dots)/l_x.$$

In actual practice, a '*commutation column*' is formed, giving values of D_x, where

$$D_x=v^xl_x,$$

so that we have

$$a_x=(D_{x+1}+D_{x+2}+D_{x+3}+\dots)/D_x.$$

The function a_x is very important, and its values are to be found in *Tables of Annuities*.

8. Life Insurance. The ordinary contract is as follows: A person A agrees to make certain payments (called *premiums*) to an insurance company at stated intervals, the company agreeing to pay a certain sum to his heirs at some specified time after his death.

Ex. 1. *What annual premium (P_x) should a person of age x pay in order that his heirs may receive* 1 *monetary unit at the end of the year in which he dies, the first premium to be paid at once, and the others at the end of the first, second, ... years, until he dies?*

At the time of the agreement the present value of the company's expectation arising from paymont of the premium is

$$P_x+P_x(vl_{x+1}+v^2l_{x+2}+\dots)/l_x=P_x(D_x+D_{x+1}+D_{x+2}+\dots)/D_x.$$

Also the present value of the expectation of the heirs is

$$\{v(l_x-l_{x+1})+v^2(l_{x+1}-l_{x+2})+\dots\}/l_x=(C_x+C_{x+1}+C_{x+2}+\dots)/D_x,$$

where for different values of x

$$C_x=v^{x+1}(l_x-l_{x+1}).$$

These expectations are supposed to be equal, therefore

$$P_x=\frac{C_x+C_{x+1}+C_{x+2}+\dots}{D_x+D_{x+1}+D_{x+2}+\dots}.$$

In practice a 'commutation' column is formed giving the values of C_x.

Ex. 2. *Prove that* $P_x=v-a_x/(1+a_x)$.

From the preceding it easily follows that the company's expectation $=P_x(1+a_x)$, and that of the heirs $=v+(v-1)a_x$;

$$\therefore \ P_x(1+a_x)=v(1+a_x)-a_x.$$

Thus P_x *can be calculated from the table of annuities.*

LIFE TABLES* (see Art. 6)

(Based on experience of all Government Annuities exclusive of the first year after purchase.)

MALES

Age. x	l_x	p_x	Age. x	l_x	p_x
5	100000	·99820	20	96600	·99664
6	99820	·99820	21	96275	·99651
7	99640	·99820	22	95939	·99638
8	99461	·99820	23	95592	·99625
9	99282	·99820	24	95234	·99612
10	99103	·99820	25	94864	·99600
11	98925	·99801	26	94485	·99587
12	98728	·99783	27	94095	·99574
13	98514	·99766	28	93694	·99560
14	98283	·99750	29	93282	·99546
15	98037	·99724	30	92858	·99531
16	97776	·99719	31	92422	·99516
17	97501	·99705	32	91975	·99500
18	97213	·99691	33	91515	·99484
19	96913	·99677	34	91043	·99467

FEMALES

Age. x	l_x	p_x	Age. x	l_x	p_x
5	100000	·99825	20	97144	·99745
6	99825	·99825	21	96896	·99731
7	99650	·99825	22	96635	·99717
8	99476	·99825	23	96362	·99702
9	99302	·99825	24	96075	·99686
10	99128	·99825	25	95773	·99670
11	98955	·99822	26	95457	·99653
12	98779	·99818	27	95126	·99635
13	98599	·99813	28	94779	·99617
14	98415	·99806	29	94416	·99599
15	98224	·99799	30	94037	·99580
16	98027	·99790	31	93642	·99560
17	97821	·99780	32	93230	·99540
18	97606	·99769	33	92801	·99520
19	97381	·99757	34	92356	·99499

* Part of tables published in a Report by the Government Actuary and the Actuary to the National Debt Commissioners in 1924.

EXERCISE IX

1. A bag contains 3 balls, and it is equally likely that 1, 2 or all of them are white. A ball is drawn and found to be white.

(i) What is the chance that this is the only white ball?

(ii) What is the chance that another drawing will give a white ball?

2. The same question as the last, except that each ball is as likely as not to be white.

[Here P_0, P_1, P_2, P_3 are the terms in the expansion of $(\frac{1}{2}+\frac{1}{2})^3$.]

3. A bag contains 5 balls, and it is not known how many of these are white. Two balls are drawn and are found to be white. What is the chance that all are white?

4. A bag contains 20 dice, one of which has every face marked six, all the rest being correctly marked. A die is drawn from the bag, it is thrown three times and always turns up six. What are the odds in favour of this being the false die?

$$[P_1=\frac{1}{20},\quad P_2=\frac{19}{20},\quad p_1=1,\quad p_2=\frac{1}{6^3}.]$$

5. A bag contains five dice, two of which are marked 1, 2, 3, 4, 6, 6, the others being correctly marked. Two dice are drawn from the bag, they are thrown, and both turn up six. What is the chance that they are both correctly marked?

[If C_1, C_2, C_3 denote the hypotheses both incorrect, one incorrect, both correct,

$$P_1=\tfrac{1}{10},\quad P_2=\tfrac{6}{10},\quad P_3=\tfrac{3}{10},$$
$$p_1=\tfrac{1}{6},\quad p_2=\tfrac{1}{18},\quad p_3=\tfrac{1}{36};$$
$$\therefore\ \Sigma Pp=\tfrac{11}{180},\quad Q_2=\tfrac{6}{360}\div\tfrac{11}{180}=\tfrac{3}{11}.]$$

6. A speaks the truth three times out of four, and B four times out of five. They agree in asserting that from a bag containing ten balls, all of different colours, a white ball has been drawn. Find the probability that this is true.

7. The chances that A, B, C speak the truth are respectively p, p', p''. What are the odds in favour of an event actually having happened which

(i) all three assert to have happened?

(ii) A, B assert to have happened and C denies?

[(i) $pp'p'':(1-p)(1-p')(1-p'')$.

(ii) $pp'(1-p''):(1-p)(1-p')p''$.]

8. The probability of a statement made by n witnesses of respective credibilities $p_1, p_2, \dots p_n$ is

$$p_1p_2\dots p_n/\{p_1p_2\dots p_n+(1-p_1)(1-p_2)\dots(1-p_n)\}.$$

Prove that this increases with n, provided that every $p>\frac{1}{2}$.

9. Each of x witnesses speaks the truth nine times out of ten. They all assert that an event has happened of which the *a priori* probability is $\alpha(<\frac{1}{2})$.

Prove that if

$$x\geqslant\log_9^r(1/\alpha-1)/\log 9,$$

it is at least an even chance that the event actually occurred.

10. How many witnesses to a hand at whist consisting entirely of trumps make it at least an even chance that this actually occurred, assuming that the credibility of each witness is $\frac{9}{10}$ and that the *a priori* probability of the event is $63 \cdot 10^{-13}$?

11. A bag contains n balls, and of these it is equally likely that 0, 1, 2, ... n are white. If balls are drawn from the bag and are not replaced, prove that

(i) the chance that the first r drawings give white balls is $1/(r+1)$;

(ii) if this event has happened, the chance that the next drawing gives a white ball is $(r+1)/(r+2)$.

12. A and B play draughts, and in each game the odds are $k:1$ in favour of the one who has the first move. They agree that the winner of each game shall have the first move in the next.

(i) If u_n denotes A's chance of winning the nth game, prove that

$$(k+1)u_{n+1}=(k-1)u_n+1.$$

(ii) Hence show that

$$u_n=\frac{1}{2}\pm\frac{1}{2}\left(\frac{k-1}{k+1}\right)^n,$$

according as A has, or has not, the first move in the first game.

(iii) If they bet £1 on each game, show that the advantage of having the first move in the first game is $£(k-1)$.

13. A bag contains a white and b black balls, and balls are drawn one by one until a white ball comes out. A bets B at each drawing x to y that a black ball is drawn. Prove that at the outset A's expectation is

$$by/(a+1)-x.$$

14. A bag contains a shillings and b sovereigns. If a person is to draw coins from the bag one by one until he draws a sovereign, prove that his expectation is

$$\{20+a/(b+1)\} \text{ shillings.}$$

15. Out of a total of m white and m black balls, m balls are selected at random and are put in a bag and the remaining m balls are put in another bag. If a ball is drawn from each bag, show that the chance that the two balls are of the same colour is $(m-1)/(2m-1)$.

[Show that the required chance is equal to

$$\Sigma_{r=1}^{r=m-1}\frac{(C_r^m)^2}{C_m^{2m}}\cdot\frac{2r(m-r)}{m^2}.]$$

16. If a die with p faces is thrown n times, show that the chance that f specified faces turn up is

$$\frac{1}{p^n}\{p^n-f(p-1)^n+\frac{f(f-1)}{\lfloor 2}(p-2)^n-\ldots\}.$$

17. If a coin is tossed five times, show that the chance of three consecutive heads is $\frac{1}{8}$.

[Chance that this does not occur is

$$\text{coefficient of } x^5 \text{ in } \frac{1-\frac{1}{8}x^3}{1-x+\frac{1}{16}x^4}.]$$

18. If a coin is tossed n times, the chance (v_n) that head never turns up twice running is given by

$$v_n = \frac{1}{2^{n+3}\sqrt{5}}\{(1+\sqrt{5})^{n+2} - (1-\sqrt{5})^{n+2}\}$$

$$= \frac{n+2}{2^{n+3}}\{1 + \frac{(n+1)n}{1\,.\,2\,.\,3}\cdot 5 + \ldots\}.$$

19. A and B play a series of games of which on an average A wins two out of three. Prove that on an average

(i) they must play $7\frac{1}{8}$ games before A wins 3 consecutive games;

(ii) they must play 39 before B wins 3 consecutive games;

(iii) they must play $5\frac{32}{43}$ games before one or the other wins 3 consecutive games.

[*Solution.* $s = \frac{(\frac{3}{2})^3 - 1}{\frac{1}{3}}$, $s' = \frac{3^3 - 1}{\frac{2}{3}}$, $\frac{1}{\sigma} = \frac{1}{s} + \frac{1}{s'}$. Art. 5, (3).]

20. Cards are dealt from a pack until the ace of spades turns up. Prove that, on an average, the number of cards dealt is $26\frac{1}{2}$.

[The number $= 1 + \frac{51}{52} + \frac{50}{52} + \frac{49}{52} + \ldots$ to 52 terms.]

21. A die is thrown until every face has turned up at least once. Prove that on an average the number of throws is 14·7.

[The average number is $1 + f_1 + f_2 + \ldots$ to ∞, where

$$f_n = C_1^6(\tfrac{5}{6})^n - C_2^6(\tfrac{4}{6})^n + C_3^6(\tfrac{3}{6})^n - C_4^6(\tfrac{2}{6})^n + C_5^6(\tfrac{1}{6})^n.]$$

22. If n cards are dealt from a pack and $u_{n,\,r}$ denotes the chance that exactly r spades turn up, prove that

(i) $u_{n,\,r} = C_r^n C_{13-r}^{52-n}/C_{13}^{52}$;

(ii) $u_{n,\,r} + u_{n,\,r+1} + u_{n,\,r+2} + \ldots$ to 40 terms $= \frac{53}{14}$;

(iii) if f_n denotes the chance that when n cards are dealt, r spades do not turn up, show that

$$f_n = u_{n,\,0} + u_{n,\,1} + u_{n,\,2} + \ldots + u_{n,\,r-1};$$

(iv) hence show that if cards are dealt from a pack until r spades turn up, on an average the number of cards dealt is $\frac{53}{14}r$.

[Sum the series $1 + f_1 + f_2 + \ldots$ by columns.]

23. (i) If n cards are dealt from a pack, find the chance that (i) no spade occurs (*a*) no spade or heart occurs; (*b*) no spade, heart or diamond occurs.

(ii) If these probabilities are denoted by u_n, v_n, w_n respectively and f_n is the chance that one or other of the four suits is not represented, prove that

$$f_n = 4u_n - 6v_n + 4w_n.$$

(iii) Cards are dealt from a pack until at least one card of every suit turns up. Prove that on an average the number of cards dealt is $7\frac{419}{630}$.

[The average number is $1 + f_1 + f_2 + f_3 + \ldots$, where f_n has the same meaning as in the last question.]

[*Solution.*

$$u_1 + u_2 + \ldots = \tfrac{39}{14},$$
$$v_1 + v_2 + \ldots = \tfrac{26}{27},$$
$$w_1 + w_2 + \ldots = \tfrac{13}{40},$$
$$s = 1 + 4\cdot\tfrac{39}{14} - 6\cdot\tfrac{26}{27} + 4\cdot\tfrac{13}{40} = 7\tfrac{419}{630}.]$$

ANNUITIES

24. '*Deferred temporary annuity.*' The symbol ${}_{n|t}a_x$ denotes the cost of an annuity of 1 issued to a person of age x, the annuity to commence to run n years hence (i.e. the first payment is $(n+1)$ years hence) and to continue for t years, if the annuitant lives so long. Prove that

$${}_{n|t}a_x=(a_{x+n}D_{x+n}-a_{x+n+t}D_{x+n+t})/D_x.$$

25. '*Temporary annuity.*' The symbol ${}_{|t}a_x$ denotes the value of an annuity as in Ex. 24, except that it is to commence to run at once. Prove that

$${}_{|t}a_x=a_x-a_{x+t}D_{x+t}/D_x.$$

(This is a '*temporary*' annuity.)

26. '*Deferred annuity.*' The symbol ${}_{n|}a_x$ denotes the value of an annuity as described in Ex. 24, except that it is to run until the death of the annuitant. Prove that

$${}_{n|}a_x=a_{x+n}D_{x+n}/D_x.$$

27. *Annuity on the joint lives of two persons.* The ages of A, B are x, y respectively, and a_{xy} denotes the value of an annuity to begin at once and to continue so long as both A and B are alive.

Prove that

$$a_{xy}=(vl_{x+1}l_{y+1}+v^2l_{x+2}l_{y+2}+\dots)/l_xl_y.$$

(*Tables exist giving values of* a_{xy}.)

28. The symbol $a_{\overline{yx}}$ denotes the value of an annuity as in Ex. 27, except that it is to cease only when both A and B are dead. Prove that

$$a_{\overline{m,n}}=\sum_{r=1}^{r=\infty}v^r\left\{\frac{l_{x+r}}{l_x}+\frac{l_{y+r}}{l_y}-\frac{l_{x+r}l_{y+r}}{l_xl_y}\right\}$$
$$=a_x+a_y-a_{x,y}.$$

CHAPTER IX

CONTINUED FRACTIONS (1)

This chapter and the following Exercise occur in H.A. *as Ch. XXXIII and Ex. LVI; they are reprinted here for convenience.*

EXPRESSION OF A QUADRATIC SURD AS A SIMPLE CONTINUED FRACTION

1. Surds of the Form $(\pm\sqrt{N}\pm b_1)/r_1$. From *H.A.*, Ch. XXIV, 33, it follows that *any simple recurring continued fraction is equal to a quadratic surd.* In other words, its value is of the form $\pm(\sqrt{N}\pm b_1)/r_1$, where N, b_1, r_1 are positive integers, except that b_1 may be zero, and N is not a perfect square.

We shall prove that conversely *any positive number of the form*

$$\pm(\sqrt{N}\pm b_1)/r_1$$

can be expressed as a simple recurring continued fraction.

In considering this theorem, it is to be observed that:

(i) *There is no loss of generality in assuming that $N-b_1^2$ is divisible by r_1.*

For $(\sqrt{N}\pm b_1)/r_1=(\sqrt{Nr_1^2}\pm b_1r_1)/r_1^2$ and $Nr_1^2-(b_1r_1)^2$ is divisible by r_1^2, hence $(\sqrt{N}\pm b_1)/r_1$ can always be replaced by an expression of the same form for which the above condition holds.

(ii) We need only consider surds which are greater than unity.

For if $N-b_1^2=\pm r_1r_2$, where r_2 is a positive integer, then

$$\frac{\sqrt{N}\pm b_1}{r_1}=1\div\frac{\sqrt{N}\mp b_1}{r_2}.$$

It follows that every positive quadratic surd or its reciprocal is of one of four types considered in the next article.

2. Types of Quadratic Surds. In every case it is assumed that

(i) *The surd in question is greater than unity.*

(ii) *$N-b_1^2$ is divisible by r_1.*

(A) *The type $(\sqrt{N}+b_1)/r_1$ where $b_1^2<N$.* This will be called the *normal* type, and is of special importance in the theory: it includes the forms $\sqrt{A/B}$ and $\sqrt{N}$.

To express $(\sqrt{N}+b_1)/r_1$ *as a simple continued fraction,* we form the equations

$$\frac{\sqrt{N}+b_1}{r_1}=a_1+\frac{\sqrt{N}-b_2}{r_1}=a_1+\frac{r_2}{\sqrt{N}+b_2}, \quad \text{.....(A)}$$

where a_1 is the integral part of $(\sqrt{N}+b_1)/r_1$ and

$$b_2=a_1r_1-b_1, \quad r_1r_2=N-b_2^2. \quad \text{.....(B)}$$

We shall first show that b_2, r_2 *are positive integers.*

Since a_1 is the integral part of $(\sqrt{N}+b_1)/r_1$,

$$a_1r_1<\sqrt{N}+b_1<a_1r_1+r_1, \quad \text{.....(C)}$$

and therefore

$$b_2<\sqrt{N}<b_2+r_1. \quad \text{.....(D)}$$

If we suppose that $b_2\leqslant 0$, it follows that $\sqrt{N}<r_1$, but $b_1<\sqrt{N}$, therefore $b_1<r_1$ and consequently $b_1<a_1r_1$. This is contrary to the supposition that $b_2\leqslant 0$. Hence b_2 is positive, and it is obviously an integer.

Again, b_2 is a positive number less than $\sqrt{N}$, therefore $N-b_2^2>0$, and consequently r_2 is positive. Further, we have

$$N-b_2^2=N-(a_1r_1-b_1)^2=N-b_1^2-r_1(a_1^2r_1-2a_1b_1),$$

and since $N-b_1^2$ is divisible by r_1, so also is $N-b_2^2$. Hence r_2 is a positive integer. Continuing the process, we form the equations

$$\frac{\sqrt{N}+b_n}{r_n}=a_n+\frac{\sqrt{N}-b_{n+1}}{r_n}=a_n+\frac{r_{n+1}}{\sqrt{N}+b_{n+1}}, \quad \text{.....(E)}$$

for $n=2, 3, \ldots$ where a_n is an integer such that

$$a_n<(\sqrt{N}+b_n)/r_n<a_n+1, \quad \text{.....(F)}$$

and

$$b_{n+1}=a_nr_n-b_n, \quad r_nr_{n+1}=N-b_{n+1}^2, \quad \text{.....(G)}$$

leading to

$$\frac{\sqrt{N}+b_1}{r_1}=a_1+\frac{1}{a_2+}\ \ldots\ \frac{1}{a_n+}\ \ldots \quad \text{.....(H)}$$

By steps similar to the above, we can show that *every a, b, r is a positive integer.* For taking $n=2$, by the preceding $(\sqrt{N}+b_2)/r_2>1$, therefore a_2 is a positive integer. Also $N-b_2^2$ is divisible by r_2. Reasoning as before, it will be seen that b_3 and r_3 are positive integers, and so for $n=3, 4, 5, \ldots$.

Finally, *the fraction is periodic,* for the *n*th complete quotient is

$$(\sqrt{N}+b_n)/r_n,$$

and for every n, $b_n<\sqrt{N}$, therefore $r_n=(b_n+b_{n+1})/a_n<2\sqrt{N}$.

Hence the fraction $(\sqrt{N}+b_n)/r_n$ cannot have more than $2N$ distinct values, and one of the complete quotients must occur again. From this stage, all the succeeding a's recur and in the same order: the same is true for the b's and r's. Thus *the continued fraction is periodic.*

It will now be shown that in the process of expressing a positive quadratic surd of any other type as a simple continued fraction, *a stage must occur at which the complete quotient is a surd of normal type. Whence it will follow that in every case the continued fraction is periodic.*

(B) *The type* $(\sqrt{N}-b_1)/r_1$ *where* $b_1^2<N$. Here the second complete quotient is a surd of normal type.

For instance, $$\frac{\sqrt{57}-7}{2}=1\Big/\frac{2}{\sqrt{57}-7}=1\Big/\frac{\sqrt{57}+7}{4}=\underset{*}{\frac{1}{3+}}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{1+}\,\underset{*}{\frac{1}{7}}$$

and $$\frac{\sqrt{57}-3}{2}=2+\frac{\sqrt{57}-7}{2}=2+1\Big/\frac{\sqrt{57}+7}{4}.$$

(C) *The form* $(b_1+\sqrt{N})/r_1$ *where* $b_1^2>N$. We form the equations

$$\frac{b_1+\sqrt{N}}{r_1}=a_1+\frac{b_2+\sqrt{N}}{r_1}=a_1+\frac{r_2}{b_2-\sqrt{N}},$$

$$\frac{b_2-\sqrt{N}}{r_2}=a_2+\frac{b_3-\sqrt{N}}{r_2}=a_2+\frac{r_3}{b_3+\sqrt{N}},\quad \text{etc.},$$

where $a_1, a_2, \ldots$ are the integral parts of the fractions on the left and, for every n,

$$b_{n+1}=b_n-a_nr_n,\quad r_nr_{n+1}=b_{n+1}^2-N.$$

As in (A), every r is an integer and every b is an integer or zero, and by hypothesis $b_1>\sqrt{N}$.

Suppose that $b_1, b_2, \ldots b_n$ are all greater than $\sqrt{N}$; then $r_1, r_2, \ldots r_n$ are all positive, and $b_1, b_2, \ldots b_{n+1}$ is a decreasing sequence of integers. Hence a stage must occur at which

$$b_n>\sqrt{N}>b_{n+1}.$$

This being so, *n cannot be even*; for in that case we should have

$$b_n-\sqrt{N}>a_nr_n,$$

and therefore $b_{n+1}>\sqrt{N}$.

Hence *n is odd*, and $b_n+\sqrt{N}>a_nr_n$. Consequently $\sqrt{N}+b_{n+1}>0$; and since also $\sqrt{N}-b_{n+1}>0$, it follows that $N-b_{n+1}^2>0$, and therefore r_{n+1} is negative.

Now $(n+1)$ being even, the $(n+1)$th complete quotient may be written

$$(\sqrt{N}-b_{n+1})/(-r_{n+1});$$

and since $b_{n+1}^2<N$, this or the next quotient is a surd of normal type according as $b_{n+1}\lesseqgtr 0$.

(D) *The type* $(b_1-\sqrt{N})/r_1$ *where* $b_1^2>N$. Here the second complete quotient is a surd of type (C).

3. Theorem. *Let the surd* $(\sqrt{N}+b)/r$ *be expressed as a simple recurring fraction, then* (i) *if* $b<\sqrt{N}<b+r$, *the fraction has no acyclic part;* (ii) *if* $\sqrt{N}>b+r$, *it has an acyclic part consisting of a single quotient;* (iii) *if* $b>\sqrt{N}$, *it has an acyclic part of one or more quotients.*

For if $x=(\sqrt{N}+b)/r$, then $(rx-b)^2=N$ and the second root of this quadratic is $(-\sqrt{N}+b)/r$; hence, from Chap. XXIV, 33, it follows that (i) *if* $-1<(-\sqrt{N}+b)/r<0$, the fraction has no acyclic part and these conditions are equivalent to $b<\sqrt{N}<b+r$; (ii) *if* $(-\sqrt{N}+b)/r<-1$, that is, if $\sqrt{N}>b+r$, the acyclic part consists of a single quotient; and (iii) *if* $(-\sqrt{N}+b)/r>0$, that is, if $b>\sqrt{N}$, the acyclic part contains one or more quotients.

In particular, *if* $A>B$, *the simple continued fraction equivalent to* $\sqrt{A/B}$ *has a single non-recurring quotient.*

4. Method of Reckoning. In practice we replace the written work involving surds by an easy mental process, as in the next example.

Ex. 1. *Express* $(\sqrt{37}+8)/9$ *as a simple continued fraction.*

Here a_1 = integral part of the surd = 1, also $b_1=8$, $r_1=9$. The various quantities are now found in succession from the equations

$$b_n=a_{n-1}r_{n-1}-b_{n-1}, \quad r_n=(N-b_n^2)/r_{n-1}, \quad a_n=\text{integral part of } (\sqrt{N}+b_n)/r_n,$$

giving the table:

n	1	2	3	4	5	6
b	8	1	3	4	5	3
r	9	4	7	3	4	7
a	1	1	1	3	2	1

The reckoning, if continued, is a repetition of the part between the dotted lines, and

$$\frac{\sqrt{37}+8}{9}=1+\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{3+}\,\frac{1}{2+}\,\cdots.$$

* *

NOTE. The third complete quotient, $(\sqrt{37}+3)/7$, marks the beginning of the recurring period, for $3<\sqrt{37}<3+7$. It will be shown in the last article of this chapter that, *from this stage, the above reckoning can be replaced by a* G.C.M. *process.*

5. $\sqrt{A/B}$ as a Continued Fraction.

(1) It is supposed that A, B are positive integers and that $A>B$. We have $\sqrt{\frac{A}{B}}=\frac{\sqrt{AB}}{B}=\frac{\sqrt{N}+b_1}{r_1}$, where $N=AB$, $b_1=0$, $r_1=B$. The surd is therefore of the type discussed in Art. 3, and it is expressed as a simple continued fraction by constructing equations of the type

$$\frac{\sqrt{N}+b_n}{r_n}=a_n+\frac{\sqrt{N}-b_{n+1}}{r_n}=a_n+\frac{r_{n+1}}{\sqrt{N}+b_{n+1}}, \text{ for values of } n=1, 2, 3, \ldots;$$

where a_n is an integer such that $a_n < (\sqrt{N}+b_n)/r_n < a_n+1$,
and
$$b_{n+1}=a_n r_n - b_n, \quad r_n r_{n+1}=N-b_{n+1}^2,$$
leading to
$$\sqrt{\frac{A}{B}}=\frac{\sqrt{N}}{r_1}=a_1+\frac{1}{a_2+}\cdots\frac{1}{a_n+}\cdots.$$

As in Art. 2, every a, b and r is a positive integer and the continued fraction is periodic. Also, it has been shown in Art. 3 that a_1 is the only non-recurring quotient.

(2) **The following inequalities** are required. Every complete quotient is greater than 1, therefore $\sqrt{N}+b_n > r_n$. .....(A)

Also $r_{n-1}=(N-b_n^2)/r_n=(\sqrt{N}-b_n)(\sqrt{N}+b_n)/r_n > \sqrt{N}-b_n$, therefore
$$\sqrt{N} < b_n + r_{n-1}. \quad .....(B)$$

Again, if $n>1$, the continued fraction equivalent to $(\sqrt{N}+b_n)/r_n$ has no acyclic part, therefore, as in Art. 3, $b_n < \sqrt{N} < b_n + r_n$ $(n \geqslant 2)$.....(C)

For any suffix m, $b_m < \sqrt{N}$, hence from (B) and (C),
$$b_m - b_n < r_{n-1} \quad \text{and} \quad b_m - b_n < r_n \quad (n \geqslant 2). \quad .....(D)$$

(3) **The Cycle of Quotients.** Let c be the number of elements in the cycle, then
$$\frac{\sqrt{N}}{r_1}-a_1=\frac{1}{a_2+}\frac{1}{a_3+}\cdots\underset{*}{\frac{1}{a_{c+1}+}}.$$

Now $\sqrt{N}/r_1 - a_1$ is a root of $r_1^2(x+a_1)^2=N$, the other root of this equation being $-\sqrt{N}/r_1 - a_1$. Therefore by *H.A.*, Ch. XXIV, 31,
$$\frac{\sqrt{N}}{r_1}+a_1=a_{c+1}+\frac{1}{a_c+}\frac{1}{a_{c-1}+}\cdots\underset{*}{\frac{1}{a_2+}}.$$

Hence $a_{c+1}+\dfrac{1}{a_c+}\cdots\dfrac{1}{a_2+}\underset{*}{\dfrac{1}{a_{c+1}+}}\cdots = 2a_1+\dfrac{1}{a_2+}\cdots\dfrac{1}{a_{c+1}+}\dfrac{1}{a_2+}\cdots,$

and therefore $a_{c+1}=2a_1$, $a_c=a_2$, $a_{c-1}=a_3$, etc.

Summary. It has been shown that $\sqrt{A/B}$ can be expressed as a simple recurring fraction in which (i) *there is a single non-recurring element*, a_1; (ii) *the last partial quotient of the cycle is* $2a_1$; (iii) *for the rest of the cycle, the partial quotients equidistant from the beginning and end are equal.*

All this may be expressed by writing
$$\sqrt{\frac{A}{B}}=\frac{\sqrt{N}}{r_1}=a_1+\frac{1}{a_2+}\underset{*}{\frac{1}{a_3+}}\cdots\frac{1}{a_3+}\frac{1}{a_2+}\frac{1}{2a_1+}\cdots;$$

and we shall call the sequence, $a_2, a_3, \ldots a_3, a_2$, the *reciprocal part* of the cycle of quotients.

(4) **The b and r Cycles.** Let c be the number of elements in the cycle, so that

$$\frac{\sqrt{N}}{r_1} = a_1 + \frac{1}{\underset{*}{a_2 +}} \cdots \frac{1}{\underset{*}{a_{c+1}}}.$$

The recurrence is due to the fact that the second complete quotient appears again as the $(c+2)$th. From this stage all the complete quotients recur in the same order; hence, $(\sqrt{N}+b_{c+m})/r_{c+m} = (\sqrt{N}+b_m)/r_m$, and therefore $b_{c+m}=b_m$ and $r_{c+m}=r_m$ for $m \geqslant 2$.

Remembering that $a_{c+1}=2a_1$, $a_{c-m}=a_{2+m}$ for $m=0, 1, 2, \ldots$, we have

$$r_{c+1}=(N-b_{c+2}^2)/r_{c+2}=(N-b_2{}^2)/r_2=r_1,\ r_c=(N-b_{c+1}^2)/r_{c+1}=(N-b_2{}^2)/r_1=r_2,$$
$$b_{c+1}=a_{c+1}r_{c+1}-b_{c+2}=2a_1r_1-b_2=b_2,\ \ b_c=a_cr_c-b_{c+1}=a_2r_2-b_2=b_3,$$

and so on.

Hence, (i) *the cycle of b's is* $b_2, b_3, \ldots b_{c+1}$ *and is reciprocal, i.e.* $b_{c+1}=b_2$, $b_c=b_3$, *etc.*; (ii) *the cycle of r's is* $r_1, r_2, \ldots r_c$, *and is reciprocal after the first term, i.e.* $r_c=r_2$, $r_{c-1}=r_3$, *etc.*

The character of the recurrence and the reciprocity of the three sequences is exhibited below, where the recurring periods are enclosed in brackets.

$$\begin{array}{cccccc}
1 & 2 & 3 & c & c+1 & c+2, \\
b_1 & [b_2 & b_3 \ldots & b_3 & b_2] & b_2, \\
[r_1 & r_2 & r_3 \ldots & r_2] & r_1 & r_2, \\
a_1 & [a_2 & a_3 \ldots & a_2 & 2a_1] & a_2.
\end{array}$$

It should be noticed that the a and b cycles correspond, and the *reciprocal* parts of the a and r cycles correspond.

(5) **Calculation of the Quotients.** In finding the values of b_n, r_n, a_n, *if we can tell when the middle of the b cycle has been reached*, no further calculation is necessary. This matter is settled by the following theorem.

If b_m, r_m, a_m *are respectively equal to* b_{n+1}, r_n, a_n, *then* b_m *and* b_{n+1} *are equidistant from the ends of the b cycle.*

For
$$r_{n+1}=(N-b_{n+1}^2)/r_n=(N-b_m{}^2)/r_m=r_{m-1}.$$

Also
$$a_{m-1}r_{m-1}=b_{m-1}+b_m \quad \text{and} \quad a_{n+1}r_{n+1}=b_{n+2}+b_{n+1}.$$

Subtracting and using the hypothesis, we find that

$$a_{m-1}-a_{n+1}=(b_{m-1}-b_{n+2})/r_{m-1}. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

Now by the inequalities in (2), (D), both $(b_{m-1}-b_{n+2})/r_{n+1}$ and $(b_{n+2}-b_{m-1})/r_{m-1}$ are less than unity. Therefore the right-hand side of (A) is numerically less than unity, and consequently $a_{m-1}=a_{n+1}$ and $b_{m-1}=b_{n+2}$.

We can show by a similar argument that b_{m-2}, r_{m-2}, a_{m-2} are respectively equal to b_{n+3}, r_{n+2}, a_{n+2}, and so on.

Putting $m=n$ and $m=n+1$ in succession, we have the following :

(i) *If two consecutive b's, namely b_m and b_{m+1}, are equal, then r_m and a_m are the mid-terms of the reciprocal parts of the r and a cycles. In this case c is even.*

(ii) *If $r_n=r_{n+1}$ and $a_n=a_{n+1}$ (so that two consecutive r's are equal and likewise the corresponding a's), then r_n, r_{n+1} and a_n, a_{n+1} are the mid-terms of the reciprocal parts of the r and a cycles, and b_{n+1} is the mid-term of the b cycle. In this case c is odd.*

Ex. 1. *Express $\sqrt{\frac{17}{11}}$ and $\sqrt{61}$ as simple continued fractions.*

(i) $\sqrt{\frac{17}{11}}=\frac{\sqrt{187}}{11}$. Hence $N=187$, $r_1=11$, $a_1=1$, and proceeding as in Art. 4, we construct the following table by a mental process :

b	0	[11	13	11	11			
r	[11	6	3	22				
a	1	[4	8	1	8	4	2].	

Because $b_4=b_5=11$, therefore a_4 is the mid-term of the reciprocal part of the a cycle. This cycle can therefore be completed, for its last term is $2a_1=2$, thus

$$\sqrt{\frac{17}{11}}=1+\frac{1}{\underset{*}{4}+}\,\frac{1}{8+}\,\frac{1}{1+}\,\frac{1}{8+}\,\frac{1}{4+}\,\frac{1}{\underset{*}{2}}.$$

(ii) For $\sqrt{61}$ we have $r_1=1$, $a_1=7$ and the b, r, a, table is

b	0	[7	5	7	5	4	6				
r	[1	12	3	4	9	5	5				
a	7	[1	4	3	1	2	2	1	3	4	1	14].

Seeing that $a_6=a_7$ and $r_6=r_7$, we conclude that a_6, a_7 are the mid-terms of the reciprocal part of the a cycle. Also the last quotient of the cycle is 14.

Therefore $$\sqrt{61}=7+\frac{1}{\underset{*}{1}+}\,\frac{1}{4+}\,\frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{2+}\,\frac{1}{1+}\,\frac{1}{3+}\,\frac{1}{4+}\,\frac{1}{1+}\,\frac{1}{\underset{*}{14}}.$$

(6) **Relations connecting the p's and q's.** Suppose that

$$\sqrt{\frac{A}{B}}=\frac{\sqrt{N}}{r_1}=a_1+\frac{1}{a_2+}\cdots\frac{1}{a_n+}\cdots,$$

where $N=AB$, $r_1=B$; and let p_r/q_r be the rth convergent, then

$$\frac{\sqrt{N}}{r_1}=a_1+\frac{1}{a_2+}\cdots\frac{1}{a_n+}\frac{1}{z}, \quad \text{where} \quad z=\frac{\sqrt{N}+b_{n+1}}{r_{n+1}};$$

therefore $$\frac{\sqrt{N}}{r_1}=\frac{zp_n+p_{n-1}}{zq_n+q_{n-1}}=\frac{(\sqrt{N}+b_{n+1})p_n+r_{n+1}p_{n-1}}{(\sqrt{N}+b_{n+1})q_n+r_{n+1}q_{n-1}}$$

and

$$\sqrt{N}(\sqrt{N}q_n+b_{n+1}q_n+r_{n+1}q_{n-1})=r_1(\sqrt{N}p_n+b_{n+1}p_n+r_{n+1}p_{n-1}).$$

Equating rational and irrational parts,

$$Nq_n=r_1(b_{n+1}p_n+r_{n+1}p_{n-1}), \qquad r_1p_n=b_{n+1}q_n+r_{n+1}q_{n-1}.$$

Solving for b_{n+1} and r_{n+1} and putting $N=AB$ and $r_1=B$, we find that

$$Aq_nq_{n-1}-Bp_np_{n-1}=(-1)^nb_{n+1}, \quad \text{.....(A)}$$

$$Bp_n^2-Aq_n^2 \quad =(-1)^nr_{n+1}. \quad \text{.....(B)}$$

(7) **Integral Solutions of $Bx^2-Ay^2=M$.** If for some value of n it happens that $(-1)^nr_{n+1}=M$, then, by equation (B), (p_n, q_n) is a solution of $Bx^2-Ay^2=M$.

Ex. 1. *Find two positive integral solutions of* $11x^2-17y^2=3$.

Expressing $\sqrt{\frac{17}{11}}$ as a continued fraction (§ (5), Ex. 1), we find that $r_3=r_1=3$. Also $p_2/q_2=5/4$, $p_4/q_4=46/37$, and therefore (5, 4), (46, 37) are solutions.

6. $\sqrt{N}$ as a Continued Fraction. (1) Here $r_1=1$ and all the conclusions of the last article hold. Additional theorems are the following.

(i) *In the cycle of r's, one member and only one is equal to* 1, *namely* r_1.

For suppose that $r_m=1$, then, remembering that $b_2=a_1$ and using the equations

$$a_mr_m=b_m+b_{m+1}, \quad r_mr_{m+1}=N-b_{m+1}^2,$$

we have $a_m=$integral part of $(\sqrt{N}+b_m)/r_m=a_1+b_m=b_2+b_m$.

Also $a_m=b_m+b_{m+1}$, therefore $b_{m+1}=b_2$ and

$$r_{m+1}=N-b_{m+1}^2=N-b_2^2=r_1r_2=r_2.$$

Therefore $(\sqrt{N}+b_{m+1})/r_{m+1}=(\sqrt{N}+b_2)/r_2$, and $r_m=1$ marks the beginning of a new cycle of r's.

(ii) *If* $r_n\geqslant 2$, *then* $a_n\leqslant b_n$. For in this case $n>1$ and $\sqrt{N}<b_n+r_n$, so that

$$a_n<(\sqrt{N}+b_n)/r_n<(2b_n+r_n)/r_n<b_n+1\leqslant b_n.$$

(iii) *If* $r_n=2$, *the number* (c) *of elements in the cycle belonging to* $\sqrt{N}$ *is even. Also* a_n *is the mid-term of the reciprocal part of the 'a' cycle, and* $a_n=a_1$ *or* a_1-1.

For a_1 is the integral part of $\sqrt{N}$ and $\sqrt{N}>b_n$, therefore $a_1\geqslant b_n$. Also a_n is the integral part of $(a_1+b_n)/r_n$, and so if $r_n=2$ we have

$$a_n>(a_1+b_n)/2-1>b_n-1\geqslant b_n.$$

But by the preceding, $a_n\leqslant b_n$, therefore $a_n=b_n$. Also $2a_n=b_n+b_{n+1}$, therefore $b_n=b_{n+1}$.

Hence by § (5), (i), c is even and a_n is the mid-term of the reciprocal part of the a cycle. Finally a_n is the integral part of $(a_1+a_n)/2$, so that $a_n=(a_1+a_n)/2$ or $(a_1+a_n-1)/2$, and therefore $a_n=a_1$ or a_1-1.

(2) Equations (A) and (B) at the top of the page become

$$Nq_nq_{n-1}-p_np_{n-1}=(-1)^nb_{n+1}, \quad \text{.....(A)}$$

$$p_n^2-Nq_n^2 \quad =(-1)^nr_{n+1}. \quad \text{.....(B)}$$

(3) **Integral Solutions of $x^2 - Ny^2 = M$.** If, for some value of n, it is found that $(-1)^n r_{n+1} = M$, then (p_n, q_n) is a solution of $x^2 - Ny^2 = M$.

In particular, if c is the number of elements in the cycle belonging to $\sqrt{N}$, the necessary and sufficient condition that r_{n+1} may be equal to 1 is that $n = tc$ where $t = 1, 2, 3, \dots$; hence, it follows that

(i) *for the equation* $x^2 - Ny^2 = 1$, solutions are (p_{tc}, q_{tc}) when c is even and (p_{2tc}, q_{2tc}) when c is odd;

(ii) *for the equation* $x^2 - Ny^2 = -1$, solutions are $(p_{(2t-1)c}, q_{(2t-1)c})$ when c is odd; the method giving no solution when c is even.

Ex. 1. *Find a positive integral solution of* $x^2 - 13y^2 = -1$.

We find that $\sqrt{13} = 3 + \overset{*}{\frac{1}{1+}}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{1+}\,\overset{*}{\frac{1}{6}}$,

so that $c = 5$. Also $p_5 = 18$, $q_5 = 5$ and $(18, 5)$ is a solution.

(4) **Calculation of Convergents.** The following formulae are useful in this connection. If we multiply equations (**A**), (**B**) firstly by q_n and q_{n-1}, and secondly by p_n and p_{n-1}, we obtain by addition

$$p_n = r_{n+1}q_{n-1} + b_{n+1}q_n \quad \text{and} \quad Nq_n = r_{n+1}p_{n-1} + b_{n+1}p_n. \quad \dots\dots\dots(\mathbf{C})$$

Again, changing n into $n-1$ in equation (**B**) and using equation (**A**), we find that $p_{n-1} = r_n q_n - b_{n+1}q_{n-1}$ and $Nq_{n-1} = r_n p_n - b_{n+1}p_{n-1}$. ....(**D**)

In general, the p's are considerably larger than the q's, and to find p_n/q_n we need only calculate the q's and then use the first of equations (**C**).

(5) **The Convergent p_c/q_c.** (i) *If* $m + n = c$, *where c is the number of elements in the cycle belonging to* $\sqrt{N}$, *then*

$$p_c = p_m q_{n+1} + p_{m-1}q_n \quad \text{and} \quad q_c = q_m q_{n+1} + q_{m-1}q_n. \quad \dots\dots\dots\dots(\mathbf{E})$$

For $$\frac{p_c}{q_c} = a_1 + \frac{1}{a_2+} \cdots \frac{1}{a_m+}\,\frac{1}{f},$$

where $$f = a_{m+1} + \frac{1}{a_{m+2}+} \cdots \frac{1}{a_c} = a_{n+1} + \frac{1}{a_n+}\,\frac{1}{a_{n-1}+} \cdots \frac{1}{a_2} = \frac{q_{n+1}}{q_n};$$

therefore $$\frac{p_c}{q_c} = \frac{fp_m + p_{m-1}}{fq_m + q_{m-1}} = \frac{p_m q_{n+1} + p_{m-1}q_n}{q_m q_{n+1} + q_{m-1}q_n}.$$

If X is the numerator and Y the denominator of the last fraction,

$$Xq_m - Yp_m = (-1)^{m-1}q_n \quad \text{and} \quad Xq_{m-1} - Yp_{m-1} = (-1)^m q_{n+1}.$$

Hence any common factor of X and Y is a factor of q_n and of q_{n+1}, and since these numbers are prime to one another, so also are X and Y. Thus the fractions p_c/q_c and X/Y are in their lowest terms, and therefore $p_c = X$ and $q_c = Y$, which are the results in question.

(ii) In particular, *if c is odd and* $n=\frac{1}{2}(c-1)$,

$$p_c=p_nq_n+p_{n+1}q_{n+1} \quad \text{and} \quad q_c=q_n^2+q_{n+1}^2. \quad \ldots\ldots\ldots\ldots\ldots\text{(F)}$$

If c is even and $n=\frac{1}{2}c$,

$$p_c=p_nq_{n+1}+p_{n-1}q_n \quad \text{and} \quad q_c=q_n(q_{n+1}+q_{n-1}). \quad \ldots\ldots\ldots\ldots\text{(G)}$$

(iii) *If* $m+n=c$, *then*

$$p_n+\sqrt{N}q_n=(-1)^m(p_m-\sqrt{N}q_m)(p_c+\sqrt{N}q_c), \quad \ldots\ldots\ldots\ldots\text{(H)}$$

which is equivalent to the two equations

$$p_mp_c-Nq_mq_c=(-1)^mp_n, \quad p_mq_c-q_mp_c=(-1)^mq_n. \quad \ldots\ldots\ldots\ldots\text{(I)}$$

For using equations (E), $p_mq_c-q_mp_c=(p_mq_{m-1}-q_mp_{m-1})q_n=(-1)^mq_n$.

Also we have the identity

$$(p_mp_c-Nq_mq_c)^2-N(p_mq_c-q_mp_c)^2=(p_m^2-Nq_m^2)(p_c^2-Nq_c^2).$$

Now $\quad p_m^2-Nq_m^2=(-1)^mr_{m+1}, \quad p_n^2-Nq_n^2=(-1)^nr_{n+1}$;

and, since $m+n=c$, we have $r_{m+1}=r_{n+1}$; and therefore

$$p_n^2-Nq_n^2=(-1)^c(p_m^2-Nq_m^2)=(p_m^2-Nq_m^2)(p_c^2-Nq_c^2).$$

Hence $\quad (p_mp_c-Nq_mq_c)^2=p_n^2.$

It remains to consider the sign of $p_mp_c-Nq_mq_c$.

The convergent p_m/q_m precedes p_c/q_c. First suppose that c is even. If m is even, $\sqrt{N}<p_c/q_c<p_m/q_m$ and $p_mp_c>Nq_mq_c$. If m is odd, it follows from *H.A.*, XXIV, 25, that $p_mp_c<Nq_mq_c$. The same results follow in a similar way when c is odd, and thus $p_mp_c-Nq_mq_c=(-1)^mp_n$.

It should be noticed that *these results hold if c is replaced by tc.*

(iv) *If N is a prime and c is even and* $n=\frac{1}{2}c$, *then*

$$p_c+\sqrt{N}q_c=\tfrac{1}{2}(p_n+\sqrt{N}q_n)^2, \quad \ldots\ldots\ldots\ldots\ldots\text{(J)}$$

which is equivalent to $\quad p_c=\frac{1}{2}(p_n^2+Nq_n^2) \quad$ *and* $\quad q_c=p_nq_n$.

Also $p_n^2-Nq_n^2=(-1)^n.2$, *and the mid-term of the reciprocal part of the a cycle is* a_1 or a_1-1.

For by equations (I), $p_np_c-Nq_nq_c=(-1)^np_n$ and $p_nq_c-q_np_c=(-1)^nq_n$, therefore

$$p_c/q_c=(p_n^2+Nq_n^2)/2p_nq_n \quad \ldots\ldots\ldots\ldots\ldots\text{(K)}$$

and $\quad \left(\dfrac{p_n^2-Nq_n^2}{2p_nq_n}\right)^2=\left(\dfrac{p_c}{q_c}\right)^2-N=\dfrac{1}{q_c^2}; \quad$ hence $\quad \dfrac{(p_n^2-Nq_n^2)}{p_nq_n}=(-1)^n\dfrac{2}{q_c},$

the sign being determined by the fact that $p_n\gtrless\sqrt{N}q_n$, according as n is even or odd. Since N is a prime and p_n is prime to q_n, the last fraction is in its lowest terms. Hence $p_n^2-Nq_n^2=(-1)^n.2$ or $(-1)^n$, and the latter alternative is impossible.

Therefore $p_n^2 - Nq_n^2 = (-1)^n \cdot 2$ and $q_c = p_n q_n$.

Hence, $r_{n+1} = 2$; and the rest follows by § (1), (iii), p. 128.

NOTE. *When N is not a prime, p_c and q_c may be found by using equation* (K) *and noting that p_c/q_c is in its lowest terms.*

Thus we find that $$\sqrt{21} = 4 + \underset{*}{\frac{1}{1+}}\frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{1+}\underset{*}{\frac{1}{8}},$$

so that for $\sqrt{21}$, $c=6$, $p_3=9$, $q_3=2$, and

$$\frac{p_6}{q_6} = \frac{81+21.4}{2.9.2} = \frac{55}{12}, \quad \text{and therefore} \quad p_6 = 55, \quad q_6 = 12.$$

(6) **The Convergent p_{n+tc}/q_{n+tc}.** (i) *If p_n/q_n is the n-th convergent of*

$$\sqrt{N} = a_1 + \frac{1}{a_2+} \cdots \frac{1}{2a_1+} \frac{1}{a_2+} \cdots$$

and c is the number of quotients in the cycle, then

$$p_{n+tc} = p_n p_{tc} + N q_n q_{tc} \quad \textit{and} \quad q_{n+tc} = p_n q_{tc} + q_n p_{tc}. \quad \ldots\ldots\ldots\ldots\text{(L)}$$

For the $(tc+1)$th quotient is $2a_1$ and the corresponding complete quotient is $a_1 + \sqrt{N}$, therefore

$$\sqrt{N} = \frac{(a_1+\sqrt{N})p_{tc} + p_{tc-1}}{(a_1+\sqrt{N})q_{tc} + q_{tc-1}}.$$

Removing fractions and equating rational and irrational parts, we have

$$a_1 p_{tc} + p_{tc-1} = N q_{tc} \quad \text{and} \quad a_1 q_{tc} + q_{tc-1} = p_{tc}. \quad \ldots\ldots\ldots\ldots\text{(M)}$$

Again,

$$\frac{p_{n+tc}}{q_{n+tc}} = a_1 + \frac{1}{a_2+} \cdots \frac{1}{2a_1+} \frac{1}{a_2+} \cdots \frac{1}{a_n} = a_1 + \frac{1}{a_2+} \cdots \frac{1}{a_1 + p_n/q_n},$$

the last quotient being the $(tc+1)$th. From this, by means of equations (I),

$$\frac{p_{n+tc}}{q_{n+tc}} = \frac{(a_1 + p_n/q_n)p_{tc} + p_{tc-1}}{(a_1 + p_n/q_n)q_{tc} + q_{tc-1}} = \frac{p_n p_{tc} + N q_n q_{tc}}{p_n q_{tc} + q_n p_{tc}}.$$

If X is the numerator and Y the denominator of the last fraction,

$$p_{tc}X - Nq_{tc}Y = p_n(p_{tc}^2 - Nq_{tc}^2) \quad \text{and} \quad p_{tc}Y - q_{tc}X = q_n(p_{tc}^2 - Nq_{tc}^2).$$

Now $p_{tc}^2 - Nq_{tc}^2 = \pm 1$, by (5), (iii), therefore any common factor of X and Y divides p_n and q_n, which are prime to one another. Hence X/Y is in its lowest terms: so also is p_{n+tc}/q_{n+tc}. Therefore $p_{n+tc} = X$, $q_{n+tc} = Y$, which are the equations in question.

As a special case we have

$$p_{(s+t)c} = p_{sc}p_{tc} + Nq_{sc}q_{tc} \quad \text{and} \quad q_{(s+t)c} = p_{sc}q_{tc} + q_{sc}p_{tc}; \quad \ldots\ldots\ldots\text{(N)}$$

in particular, $$p_{2tc} = p_{tc}^2 + Nq_{tc}^2 \quad \text{and} \quad q_{2tc} = 2p_{tc}q_{tc}. \quad \ldots\ldots\ldots\ldots\text{(O)}$$

(ii) Since $\sqrt{N}$ is irrational, equations (L) are *equivalent* to the single relation

$$p_{n+tc}+\sqrt{N}q_{n+tc}=(p_n+\sqrt{N}q_n)(p_{tc}+\sqrt{N}q_{tc}).$$

Putting $t=1$ and $n=c,\ 2c,\ 3c,\ \ldots$ in succession, we find that

$$p_{2c}+\sqrt{N}q_{2c}=(p_c+\sqrt{N}q_c)^2,\quad p_{3c}+\sqrt{N}q_{3c}=(p_c+\sqrt{N}q_c)^3\ \ldots,$$

and generally, for every positive t, $p_{tc}+\sqrt{N}q_{tc}=(p_c+\sqrt{N}q_c)^t$; .....(P)

and therefore $p_{n+tc}+\sqrt{N}q_{n+tc}=(p_n+\sqrt{N}q_n)(p_c+\sqrt{N}q_c)^t$. .....(Q)

Ex. 1.* *Find a solution in positive integers of* $x^2-61y^2=1$.

In Ex. 1, p. 127, $\sqrt{61}$ is expressed as a continued fraction, the number of quotients in the cycle being 11. Hence the smallest solution of the equation in question is (p_{22}, q_{22}). The mid-elements of the cycle are the 5th and 6th, and $p_5=164$, $q_5=21$, $p_6=453$, $q_6=58$. Hence by equations (F),

$$p_{11}=p_5q_6+p_6q_5=164\,.\,21+453\,.\,58=29718,\quad q_{11}=q_5^2+q_6^2=21^2+58^2=3805.$$

Using equations (O) and observing that $p_{11}^2-61q_{11}^2=-1$,

$$p_{22}=p_{11}^2+61q_{11}^2=2p_{11}^2+1=1766319049,\qquad q_{22}=2p_{11}q_{11}=226153980.$$

Thus the least solution is (1766319049, 226153980).

7. The Cycle belonging to $z=(\sqrt{N}+b)/r$. Suppose that

$$z>1,\quad b<\sqrt{N}<b+r,\quad N-b^2=rr',$$

where r' is a positive integer, then the simple continued fraction corresponding to z has no acyclic part (Art. 3), and the cycle can be calculated as follows.

Rule. *Let* (x, y) *be a solution in positive integers of any one of the equations*

$$x^2-Ny^2=\pm1\quad or\quad \pm4, \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

the latter pair being used only when r, r' *are both even and* N, b *are odd. Substitute* x/y *for* $\sqrt{N}$ *in the given surd. Express the result as a simple continued fraction with an even or an odd number of quotients according as the sign on the right of the chosen equation is* $+$ *or* $-$. *This fraction consists of one or more of the cycles belonging to* $(\sqrt{N}+b)/r$.

Proof. Since $N=b^2+rr'$, the surd $(\sqrt{N}+b)/r$ is the positive root of

$$rz^2-2bz-r'=0. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

(1) We shall prove that this equation can be written in the form

$$z=(pz+p')/(qz+q'),\ \text{where } p, q, p', q' \text{ are positive integers} \qquad \ldots\ldots\text{(C)}$$

such that $$pq'-p'q=\pm1 \quad\text{and}\quad q'\leqslant q. \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(D)}$$

For equation (C) is the same as $qz^2-(p-q')z-p'=0$, which is identical with (B) if

$$q=ry,\quad p-q'=2by,\quad p'=r'y, \qquad \ldots\ldots\ldots\ldots\ldots\ldots\text{(E)}$$

where y may be any rational.

* This problem was set by Fermat as a challenge to the English mathematicians of his time.

From (D), (E) we have $\frac{1}{4}(p+q')^2 = Ny^2 \pm 1 = x^2$, ...(F)

where x is rational. All possible cases are included in the following :

(A) x, y are positive integers such that $x^2 - Ny^2 = \pm 1$.

(B) $x = \xi/2$, $y = \eta/2$ where ξ, η are odd integers such that $\xi^2 - N\eta^2 = \pm 4$.

In case (B), r, r' are both even, for $q = ry$, $p' = r'y$. Hence $N - b^2$ is divisible by 4, and if N is odd so also is b.

In both cases, from (E) and (F), we find that

$$p = x + by, \quad q' = x - by, \quad \text{.....(G)}$$

and

$$p/q = (x/y + b)/r. \quad \text{.....(H)}$$

It remains to be shown that $q' \leqslant q$. This will be so if $x/y \leqslant b + r$.

Three cases must be considered :

(i) *If* $x^2 - Ny^2 = -1$ *or* $\xi^2 - N\eta^2 = -4$, then

$$x/y < \sqrt{N} < b + r \quad \text{and} \quad q' < q.$$

(ii) *If* $x^2 - Ny^2 = 1$, the least value of y is 1, and

$$x^2/y^2 = N + 1/y^2 \leqslant N + 1.$$

Now $N < (b+r)^2$, therefore $N \leqslant (b+r)^2 - 1$. Hence

$$x/y \leqslant \sqrt{N+1} \leqslant b + r \quad \text{and} \quad q' \leqslant q.$$

(iii) *If* $x = \xi/2$, $y = \eta/2$ *where* $\xi^2 - N\eta^2 = 4$, the least value of η is 1 and

$$x/y \leqslant \sqrt{N+4}.$$

Let $N = (b+r)^2 - k$ so that k is a positive integer, then $rr' = r(2b+r) - k$ where r, r' are even. Therefore k is divisible by 4, and 4 is its least value. Hence

$$x/y \leqslant \sqrt{N+4} \leqslant b + r \quad \text{and} \quad q' \leqslant q.$$

(2) It follows that if

$$\frac{p}{q} = a_1 + \frac{1}{a_2 +} \cdots \frac{1}{a_n}, \quad \text{.....(I)}$$

where n is even or odd according as $pq' - p'q = 1$ or -1, then p'/q' is the convergent immediately preceding p/q. (*H.A.*, XXIV, 12.) Now let z' be determined by

$$z = a_1 + \frac{1}{a_2 +} \cdots \frac{1}{a_n + \frac{1}{z'}},$$

then

$$z = \frac{pz' + p'}{qz' + q'} \quad \text{and} \quad \frac{pz' + p'}{qz' + q'} = \frac{pz + p'}{qz + q'}.$$

Hence $z' = z$ and *the fraction* (I) *consists of one or more of the cycles belonging to* z.

The rule can be used (as in Ex. 2) *to express any quadratic surd as a continued fraction, beginning at the stage where recurrence commences.*

Ex. 1. *Express* $(\sqrt{621}+21)/18$ *as a simple continued fraction.*

Since $21<\sqrt{621}<21+18$, there is no acyclic part. Also $18r'=621-21^2=180$, giving $r'=10$.

Thus r, r' are even and b is odd, also

$$25^2-621\,.\,1^2=4.$$

Using the rule, we substitute 25/1 for $\sqrt{621}$ in the given surd, and express the result as a simple continued fraction with an *even* number of quotients, thus

$$\frac{25+21}{18}=\frac{23}{9}=2+\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{4},$$

and

$$\frac{\sqrt{621}+21}{18}=2+\underset{*}{\frac{1}{1+}}\,\frac{1}{1+}\,\underset{*}{\frac{1}{4}}.$$

Ex. 2. *Express* $(\sqrt{13}+7)/4$ *as a simple continued fraction.*

Since $7>\sqrt{13}$, there is an acyclic part. The reckoning on the right shows that the second complete quotient is $(\sqrt{13}+1)/3$, and since $1>\sqrt{13}>1+3$, we can apply the rule. We have

b	7,	1
r	4,	3
a	2,	1

$$3^2-13\,.\,1^2=-4 \quad \text{and} \quad 18^2-13\,.\,5^2=-1.$$

Since $r=3$, an odd number, the first equation is useless. Taking the second, we substitute 18/5 for $\sqrt{13}$ in $(\sqrt{13}+1)/3$, and express the result as a simple continued fraction with an *odd* number of quotients, thus

$$\left(\frac{18}{5}+1\right)\frac{1}{3}=\frac{23}{15}=1+\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{6+}\,\frac{1}{1}.$$

This is the cycle belonging to the given surd, and

$$\frac{\sqrt{13}+7}{4}=2+\underset{*}{\frac{1}{1+}}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{6+}\,\underset{*}{\frac{1}{1}}.$$

EXERCISE X

1. Verify some of the following results, where the values of b, r, a are given as far as the middle of the first cycle:

(i) $\sqrt{13}$ { b . 0 . 3 . 1 . 2 ; r . 1 . 4 . 3 . 3 ; a . 3 . 1 . 1 . 1

(ii) $\sqrt{19}$ { b . 0 . 4 . 2 . 3 . 3 ; r . 1 . 3 . 5 . 2 . 5 ; a . 4 . 2 . 1 . 3 . 1

(iii) $\sqrt{31}$ { b . 0 . 5 . 1 . 4 . 5 . 5 ; r . 1 . 6 . 5 . 3 . 2 . 3 ; a . 5 . 1 . 1 . 3 . 5 . 3

(iv) $\sqrt{43}$ { b . 0 . 6 . 1 . 5 . 4 . 5 . 5 ; r . 1 . 7 . 6 . 3 . 9 . 2 . 9 ; a . 6 . 1 . 1 . 3 . 1 . 5 . 1

(v) $\sqrt{91}$ { b . 0 . 9 . 1 . 8 . 7 . 7 ; r . 1 . 10 . 9 . 3 . 14 . 3 ; a . 9 . 1 . 1 . 5 . 1 . 5

(vi) $\sqrt{109}$ { b . 0 . 10 . 8 . 7 . 5 . 9 . 7 . 8 . 10 ; r . 1 . 9 . 5 . 12 . 7 . 4 . 15 . 3 . 3 ; a . 10 . 2 . 3 . 1 . 2 . 4 . 1 . 6 . 6

(vii) $\sqrt{a^2+1}$ $\begin{matrix} b\,.\,0\,.\,a\,.\,a \\ r\,.\,1\,.\,1\,.\,1 \\ a\,.\,a\,.\,2a\,.\,2a \end{matrix}$ (viii) $\sqrt{a^2-1}$ $\begin{matrix} b\,.\ 0\ .\ a-1\ .\ a-1 \\ r\,.\ 1\ .\ 2(a-1)\,.\ 1 \\ a\,.\,a-1\,.\ 1\ .\ 2(a-1) \end{matrix}$

(ix) $\sqrt{a^2+2}$ $\begin{matrix} b\,.\,0\,.\,a\,.\,a \\ r\,.\,1\,.\,2\,.\,1 \\ a\,.\,a\,.\,a\,.\,2a \end{matrix}$ (x) $\sqrt{a^2-2}$ $\begin{matrix} b\,.\ 0\ .\ a-1\,.\,a-2\,.\,a-2 \\ r\,.\ 1\ .\ 2a-3\,.\ 2\ .\ 2a-3 \\ a\,.\,a-1\,.\ 1\ .\,a-2\,.\ 1 \end{matrix}$ $(a>2)$

(xi) $\sqrt{a(a+1)}$ $\begin{matrix} b\,.\,0\,.\,a\,.\,a \\ r\,.\,1\,.\,a\,.\,1 \\ a\,.\,a\,.\,2\,.\,2a \end{matrix}$ (xii) $\sqrt{a^2+4}$ $\begin{matrix} b\,.\,0\,.\ \ a\ \ .\,a-2\,.\,2 \\ r\,.\,1\,.\ \ 4\ \ .\ \ a\ \ .\,a \\ a\,.\,a\,.\,\frac{1}{2}(a-1)\,.\ 1\ .\,1 \end{matrix}$ $(a>1$ and odd$)$

(xiii) $\sqrt{a(a+4)}$ $\begin{matrix} b\,.\ 0\ .\,a+1\,.\ a-2\ .\,a.\ \ a \\ r\,.\ 1\ .\,2a-1\,.\ \ 4\ \ .\,a.\ \ 4 \\ a\,.\,a+1.\ \ 1\ \ .\,\frac{1}{2}(a-1)\,.\,2\,.\,\frac{1}{2}(a-1) \end{matrix}$ $(a>1$ and odd$)$

2. In certain cases, a solution of one of the equations $x^2-Ny^2=\pm1$ or ±4 can be written down at once; thus

if $N=a^2\pm1$, then $a^2-N\,1^2=\mp1$;
if $N=a^2\pm2$, then $(a^2\pm1)^2-Na^2=1$;
if $N=a(a+1)$, then $(2a+1)^2-N\,.\,2^2=1$;
if $N=a^2\pm4$, then $a^2-N\,.\,1^2=\mp4$.

Apply this to write down the integral solutions of $x^2-Ny^2=1$ when

$$N=51,\ 47,\ 56.$$

3. Find a solution of $x^2-109y^2=-4$, and apply the H.C.F. process to show that

$$\frac{\sqrt{109}+7}{10}=1+\underset{*}{\frac{1}{1+}}\,\frac{1}{2+}\,\frac{1}{1+}\,\frac{1}{9+}\,\frac{1}{1+}\,\underset{*}{\frac{1}{2}}.$$

4. Obtain the following:

(i) $\dfrac{\sqrt{17}+15}{8}=2+\underset{*}{\dfrac{1}{2+}}\,\dfrac{1}{1+}\,\dfrac{1}{1+}\,\underset{*}{\dfrac{1}{3}}$;

(ii) $\dfrac{\sqrt{61}+7}{6}=2+\underset{*}{\dfrac{1}{2+}}\,\underset{*}{\dfrac{1}{7}}$;

(iii) $\sqrt{\dfrac{13}{5}}=1+\underset{*}{\dfrac{1}{1+}}\,\dfrac{1}{1+}\,\dfrac{1}{1+}\,\dfrac{1}{1+}\,\underset{*}{\dfrac{1}{2}}$;

(iv) $\dfrac{\sqrt{19}+1}{6}=1+\underset{*}{\dfrac{1}{8+}}\,\dfrac{1}{2+}\,\dfrac{1}{1+}\,\dfrac{1}{3+}\,\underset{*}{\dfrac{1}{2}}$;

(v) $\sqrt{\dfrac{17}{3}}=2+\underset{*}{\dfrac{1}{2+}}\,\dfrac{1}{1+}\,\dfrac{1}{1+}\,\dfrac{1}{1+}\,\dfrac{1}{2+}\,\underset{*}{\dfrac{1}{4}}$.

5. Find two positive integral solutions of

(i) $5x^2-13y^2=7$, (ii) $5x^2-13y^2=-7$, (iii) $3x^2-17y^2=7$.

6. Find positive integral solutions of $x^2-621y^2=4$ and of $x^2-621y^2=1$. Referring to Art. 7, verify that if 623/25 and 7775/312 are substituted for $\sqrt{621}$ in the fraction $(\sqrt{621}+21)/18$, the first gives two cycles and the second three cycles of the fraction.

7. If $N=(2m+3)^2-4$, prove that

$$\frac{\sqrt{N}+2m-1}{4}=m+\underset{*}{\cfrac{1}{2+\cfrac{1}{m+\cfrac{1}{1+\cfrac{1}{4(m+1)+\cfrac{1}{1}}}}}}.$$

8. If a is odd, find a positive integral solution of

(i) $x^2-(a^2+4)y^2=a$; (ii) $x^2-(a^2+4)y^2=-a$.

9. Prove that $r_n \leqslant 2a_1$, and that if $r_n=2a_1$, then $a_n=1$ and a_n is the mid-term of the reciprocal part of the a cycle.

Show also that if N is an odd prime and $r_n=2a_1$, then N must be equal to 3.

[If $r_n=2a_1$, $a_n<(\sqrt{N}+b_n)/r_n \leqslant 1$, therefore $b_n+b_{n+1}=a_nr_n=2a_1$, so that $b_n=b_{n+1}$. Hence a_n is the mid-term of the reciprocal part of the a cycle. If N is an odd prime, we must have $a_n=a_1$ or a_1-1.

Hence $a_1=1$ or 2, and $N=3, 5, 7$. On trial it is found that $N=3$.]

10. If $r_n=r_{n+1}=a_1$, then $a_n=a_{n+1}=1$, so that a_n, a_{n+1} are the mid-terms of the reciprocal part of the a cycle.

[$a_n=I(a_1+b_n)/a_1=1$ or 2, according as $b_n \neq a_1$ or $b_n=a_1$. If $b_n=a_1$, $b_{n+1}=2a_1-b_n=a_1$, so that $b_n=b_{n+1}$. This is impossible. Hence $a_n=1$ and $a_{n+1}=I(a_1+b_{n+1})/a_1=1$.]

11. If a_1 is an odd prime, or a power of such a number, and $r_n=a_1$, then $a_n=1$.

[For $r_nr_{n+1}=N-b_{n+1}^2$, $r_{n-1}r_n=N-b_n^2$, therefore b_n and b_{n+1} are solutions of $x^2 \equiv N \pmod{a_1}$, and since each $\leqslant a_1$, and a_1 is an odd prime, $b_n+b_{n+1}=a_1$, therefore $a_n=(b_n+b_{n+1})/r_n=a_1/a_1=1$.]

12. If, after a certain stage, the simple continued fractions which are equivalent to two irrationals z and z' are identical, prove that

$$z'=(pz+p')/(qz+q') \quad \text{where} \quad pq'-p'q=\pm 1$$

where p, p', q, q' are integers. Show also that the converse is true.

13. If the number (c) of elements in the cycle belonging to $\sqrt{N}$ is even, (i) prove that $p_{c/2}/q_{c/2}=(p_c \pm 1)/q_c$, according as c is or is not divisible by 4.

(ii) By taking $N=21$, illustrate the fact that equations (J) of Art. 6, (5), (iv), are not necessarily true unless N is a prime, and verify the equations for $N=19$.

14. If the number (c) of elements in the cycle belonging to $\sqrt{N}$ is odd:

(i) Prove that N is the sum of two squares which are prime to one another. Also, by taking $N=205$, show that the converse of this is not generally true.

(ii) If $m=\frac{1}{2}(c-1)$ and $n=\frac{1}{2}(c+1)$, prove that

$$p_m^2+p_n^2=N(q_m^2+q_n^2)=Nq_c,$$
$$p_m^2+Nq_m^2=(2p_mq_mp_c+1)/q_c,$$
$$p_m^2-Nq_m^2=(p_mq_n+p_nq_m)/q_c,$$

and verify when $N=29$.

[(i) N is a factor of p_c^2+1.]

CHAPTER X

QUADRATIC RESIDUES

1. Quadratic Residues. (1) Choosing any number n as modulus, consider the squares $1^2, 2^2, 3^2, \ldots$ and the remainders $r_1, r_2, r_3, \ldots$ when these are divided by n.

If x is any number, $(n+x)^2 \equiv x^2 \pmod{n}$, therefore $r_{n+x} = r_x$, and the terms of the sequence $r_1, r_2, r_3, \ldots$ recur.

Again, $(n-x)^2 \equiv x^2 \pmod{n}$, therefore $r_{n-x} = r_x$. Hence, for any modulus n, not more than $\frac{1}{2}n$ or $\frac{1}{2}(n-1)$ of the numbers $1, 2, 3, \ldots n-1$ can be congruent (mod n) with a square, according as n is even or odd.

Since $(m+1)^2 = m^2 + 2m + 1$, we have $r_{m+1} \equiv r_m + 2m + 1 \pmod{n}$. Using this formula, the values of $r_1, r_2, r_3, \ldots$ can be calculated rapidly in succession.

Ex. 1. *If* $1^2, 2^2, 3^2, \ldots$ *are divided by* 17, *the remainders are*

1, 4, 9, 16, 8, 2, 15, 13, 15, 2, 8, 16, 9, 4, 1, 0, 1, ...

Having found that $r_8 = 8$, we have

$r_9 \equiv 8 + 11 \equiv 2$, $r_{10} \equiv 2 + 13 = 15$, $r_{11} \equiv 15 + 15 \equiv 13$, $r_{12} = r_{17-9} = r_8$, $r_{13} = r_7$, etc.

(2) A number is said to be a *quadratic residue* or a *non-residue* of a modulus n, according as it is or is not congruent (mod n) with some square.

From what has just been said, it appears that not more than $\frac{1}{2}n$ or $\frac{1}{2}(n-1)$ of the numbers $1, 2, 3, \ldots n-1$ are quadratic residues of n, according as n is even or odd.

Ex. 2. 1, 2, 4, 8, 9, 13, 15, 16 *are quadratic residues of* 17, *and* 3, 5, 6, 7, 10, 11, 12, 14 *are non-residues.*

(3) *For any modulus* n, *the product of two quadratic residues* (A, B) *is a residue.*

For if $A \equiv a^2$ and $B \equiv b^2 \pmod{n}$, then $AB \equiv (ab)^2 \pmod{n}$.

Again, *if* Ak^2 *is a quadratic residue of* n *and* k *is prime to* n, *then* A *is a residue of* n.

For let $Ak^2 \equiv a^2 \pmod{n}$, then, since k is prime to n, we can find x so that $kx \equiv a \pmod{n}$, and then $Ak^2 \equiv k^2x^2$ and $A \equiv x^2$.

For example, $5^2(-2) \equiv 7^2 \pmod{99}$ and 5 is prime to 99, therefore $-2 \equiv (\frac{7}{5})^2 \equiv 41^2 \pmod{99}$. It should be noticed that $2 \cdot 99 = 14^2 + 2$ and 2 is prime to 99, so that we also have $-2 \equiv 14^2$.

(4) Quadratic residues of a given number n and squares with which they are congruent may be found as follows. By the square root process, followed by suitable additions or subtractions, we find values of a, b so that $kn = b^2 \pm a$, where k is any number we may choose which is prime to n, and then $b^2 \equiv \mp a \pmod{n}$. Special attention is given to values of a which have square factors or are the products of small primes.

As will be explained later, this process is very useful in determining whether a large number is prime or composite. It also affords the readiest means of solving congruences of the form $x^2 \equiv A \pmod{p}$ where p is a prime.

NOTE. When no ambiguity can arise, a 'quadratic residue' is often spoken of as a 'residue.' The symbol aRn is used to denote that a is a quadratic residue of n and aNn indicates that a is a non-residue. This notation was introduced by Gauss.

Ex. 3. *Find four primes numerically less than* 100 *which are quadratic residues of* $n = 178979$.

Show also that -2 *is a residue, and find a square congruent with it.*

By the square root process, we find that

$$n = 423^2 + 50,$$

and so $423^2 \equiv -50 \pmod{n}$. Starting with this and proceeding both ways as on the right, we find the residues $-5^2 . 2$, $5^3 . 2 . 67$, $-2 . 11 . 79$.

In the same way, $3n = 733^2 - 352$, and 3 is prime to n, therefore $733^2 \equiv 352 = 4^2 . 2 . 11 \pmod{n}$.

Removing square factors which are prime to n and remembering that the product of two residues is a residue, we see that -2, -11, -67 and -79 are residues.

Again, $-2 \equiv \left(\frac{423}{5}\right)^2 \equiv \left(\frac{2n-423}{5}\right)^2 \equiv 71507^2$.

$427^2 \equiv \overline{3350} = 5^2 . 2 . 67$
$\overline{853}$
$426^2 \equiv \overline{2497}$
$\overline{851}$
$425^2 \equiv \overline{1646}$
$\overline{849}$
$424^2 \equiv \overline{797}$
$\overline{847}$
$423^2 \equiv -50 = -5^2 . 2$
$\overline{845}$
$422^2 \equiv \overline{-895}$
$\overline{843}$
$421^2 \equiv -\overline{1738} = -2 . 11 . 79$

2. Residues of a Prime Modulus. If p is an odd prime, (1) the squares $1^2, 2^2, 3^2, \ldots \{\frac{1}{2}(p-1)\}^2$ are mutually incongruent (mod p).

For if a^2, b^2 are any two of them $(a > b)$ and we suppose that $a^2 \equiv b^2$, we should have $a^2 - b^2$ divisible by p, and since p is a prime, $a+b$ or $a-b$ would be divisible. This is impossible, for $a+b$ and $a-b$ are both less than p.

(2) Half of the numbers 1, 2, 3, ... $p-1$ are quadratic residues of p, and the other half are non-residues.

For among these numbers there are $\frac{1}{2}(p-1)$ residues, namely those which are congruent with $1^2, 2^2, 3^2, \ldots \{\frac{1}{2}(p-1)\}^2$, and by Art. 1, (2), there are no more. Hence the remaining numbers are non-residues.

(3) **Products.** *For a prime modulus p, the product of two quadratic residues or of two non-residues is a residue: that of a residue and a non-residue is a non-residue.*

(i) Suppose that A and B are residues, and let $A \equiv a^2$ and $B \equiv b^2 \pmod{p}$. Then $AB \equiv (ab)^2$ and AB is a residue.

(ii) If A is a residue and B a non-residue, let $A \equiv a^2$ and suppose that $AB \equiv k^2 \pmod{p}$. Since a is prime to p we can find b so that $ab \equiv k \pmod{p}$, and then $a^2b^2 \equiv AB \equiv a^2B$. Hence $B \equiv b^2$, which is impossible, for B is a non-residue. Therefore AB is a non-residue.

(iii) Let A and B be non-residues. Among the numbers $1, 2, 3, \ldots p-1$ there are $\frac{1}{2}(p-1)$ residues, and if all of these are multiplied by A, the resulting products are non-residues and are mutually incongruent (mod p). Moreover, AB is not congruent with any of these products, hence if AB were a non-residue, there would be $\frac{1}{2}(p+1)$ non-residues incongruent two and two. This is impossible, and so AB is a residue.

(4) **Quotients.** *For a prime modulus p, the quotient $a/b \pmod{p}$ is a quadratic residue of p if a and b are both residues or if they are both non-residues. If either a or b is a residue and the other a non-residue, then $a/b \pmod{p}$ is a non-residue.*

For let $x = a/b \pmod{p}$, then $bx \equiv a$, and the result follows on considering different possibilities with regard to the product bx.

(5) **The Congruence $x^2 \equiv A \pmod{p}$.** Solutions exist, or there is no solution, according as A is or is not a quadratic residue of p. In the first case, among the numbers $1, 2, 3, \ldots \frac{1}{2}(p-1)$ there is just one of which the square is congruent with A. Denoting this number by a, it follows that a and $p-a$ are the only numbers of the set $1, 2, 3, \ldots p-1$ of which the squares are congruent with A. Hence the solution is $x \equiv \pm a \pmod{p}$. The value of a is most readily determined by the method of Art. 1 (4).

Ex. 1. *Solve* $x^2 \equiv A \pmod{179}$ *for* $A = -2, 3, 5, 13, 17, 19$.

Let $m = 179$ (a prime number). We find that $m = 13^2 + 10$, and so $13^2 \equiv -10$, $14^2 \equiv 17$. Also $2m = 18^2 + 34$, therefore $18^2 \equiv -34$, $19^2 \equiv 3$.

Hence $-2 \equiv \left(\frac{18}{14}\right)^2 \equiv \left(\frac{9}{7}\right)^2 \equiv \left(\frac{5 \cdot 4 \cdot 6}{7}\right)^2 \equiv 78^2$

and $5 \equiv \left(\frac{12}{8}\right)^2 \equiv 30^2$.

Again $13 \equiv 192 = 8^2 \cdot 3 \equiv (8 \cdot 19)^2 \equiv 27^2$,

$19 \equiv -160 \equiv 4^2(-10) \equiv (4 \cdot 13)^2 \equiv 52^2$.

Thus the solutions are $x \equiv \pm 78, \pm 19, \pm 30, \pm 27, \pm 14, \pm 52$.

If the solution is not obtained after a few operations of this kind, it is advisable to use the method of 'exclusion' described at the end of this chapter.

(6) **The Congruence $ax^2+bx+c\equiv 0 \pmod p$.** *If p is an odd prime and a is prime to p, this congruence can be put into the form $y^2\equiv A \pmod p$.*

For integers m, n can always be found so that $b\equiv 2ma \pmod p$ and $c\equiv na \pmod p$ and then, dividing by a, the congruence becomes

$$x^2+2mx+n\equiv 0 \quad \text{or} \quad (x+m)^2\equiv m^2-n \pmod p.$$

Ex. 2. *Find the general solution in integers of* $7x^2-5x+4=13y$.

The values of x are given by $7x^2-5x+4\equiv 0 \pmod{13}$.

Dividing by 7 and observing that $5/7 \pmod{13}=10$ and $4/7 \pmod{13}=8$, we have $x^2-10x+8\equiv 0$, and therefore $(x-5)^2\equiv 17\equiv 2^2 \pmod{13}$.

Hence $x-5\equiv \pm 2$ and $x\equiv 3$ or $7 \pmod{13}$. Thus the general solution of the equation is $x=13t+3$, $y=91t^2+37t+4$ or $x=13t+7$, $y=91t^2+93t+24$.

3. Forms of Primes with given Residues. It is important to be able to say whether a given number A is or is not a quadratic residue of a prime p. Here we shall consider the cases $A=-1, \pm 2, \pm 3$, which can be settled by Fermat's theorem, leaving the general question till later.

(1) *With regard to a prime p, -1 is a quadratic residue when p is of the form $4n+1$, and a non-residue when it is of the form $4n-1$.*

For $(-1)Rp$ or $(-1)Np$, according as the congruence $x^2+1\equiv 0 \pmod p$ has or has not a solution.

If $p=4n+1$, then x^2+1 is a factor of $x^{p-1}-1$. Now by Fermat's theorem the congruence $x^{p-1}-1\equiv 0 \pmod p$ has $p-1$ distinct solutions. Therefore $x^2+1\equiv 0 \pmod p$ has two solutions and $-1Rp$.

If $p=4n-1$ and x has such a value that $x^2\equiv -1 \pmod p$, we should have $x^{4n-2}\equiv (-1)^{2n-1}$, and therefore $x^{p-1}\equiv -1$. This is impossible, for by Fermat's theorem $x^{p-1}\equiv 1$. Hence in this case $-1Np$.

(2) We shall prove that $+2$ *is a quadratic residue of odd primes of the form $8n\pm 1$ and a non-residue of those of the form $8n\pm 3$.*

(i) Suppose that $p=8n+1$; then, by Fermat's theorem,

$$x^{8n}-1\equiv 0 \pmod p$$

has $8n$ distinct roots. Now x^4+1 is a factor of $x^{8n}-1$, therefore $x^4+1\equiv 0$ has four solutions. The last congruence may be written in either of the forms $(x^2+1)^2\equiv 2x^2$ or $(x^2-1)^2\equiv -2x^2$.

Hence each of the congruences, $(x^4+x^2)^2\equiv 2x^4\equiv -2$, $(x^2-x)^2\equiv -2x^4\equiv 2$ has solutions, and consequently both $+2$ and -2 are residues of p.

(ii) Let $p=8n\pm 3$, and suppose that, if possible, $2Rp$, then there are two roots less than p of $x^2\equiv 2 \pmod p$. If α is one of these, the other is $p-\alpha$, so that one root is odd and the other even. Let α be the odd root, then we have the equation $\alpha^2-2=pq$ where $q<p$, and therefore $2Rq$.

Again, α being odd, α^2 is of the form $8m+1$, and so we have an equation of the form $8m-1=(8n\pm 3)q$. Hence q is a prime of the form $8n\pm 3$, or else it has a prime factor of this form. Therefore in every case, if 2 is a residue of a prime of one of the forms $8n\pm 3$, it is also a residue of a smaller prime of one of these forms, and therefore of one smaller still, and so on.

Now the smallest primes of the forms $8n\pm 3$ are 3 and 5. Thus the argument shows that with the above supposition 2 must be a residue of either 3 or 5. But this is not the case, therefore 2 is a non-residue of primes of the forms $8n\pm 3$.

(iii) In a similar way we can show that if p is a prime of the form $8n-1$, then $(-2)Np$. Now by § (1), in this case $(-1)Np$, and the product of these non-residues is a residue, that is to say, $2Rp$.

(iv) This completes the proof of the statement in question, and applying the product theorem of Art. 2, we form the following table, where R stands for ' residue ' and N for ' non-residue ' :

Prime forms	$8n+1$	$8n-1$	$8n+3$	$8n-3$
-1	R	N	N	R
$+2$	R	R	N	N
-2	R	N	R	N

(3) *If p is an odd prime, -3 is a quadratic residue or a non-residue, according as p is of the form $3n+1$ or $3n-1$.*

For if $p=3n+1$, then x^3+1 is a factor of $x^{p-1}-1$. Consequently x^2+x+1 is a factor of $x^{p-1}-1$. Now $x^{p-1}-1\equiv 0 \pmod p$ has $p-1$ distinct roots, and therefore $x^2+x+1\equiv 0 \pmod p$ has two distinct roots. Moreover, 2 is prime to p, therefore the last congruence is the same as $y^2+3\equiv 0 \pmod p$ where $y=2x+1$.

Hence $y^2\equiv -3 \pmod p$ has two distinct roots and $(-3)Rp$.

But if $p=3n-1$ and y is such that $y^2\equiv -3 \pmod p$, we should have $x^2+x+1\equiv 0 \pmod p$ where $y=2x+1$. Consequently $x^3-1\equiv 0 \pmod p$ and $x^{3n}-1\equiv 0 \pmod p$, that is to say, $x^{p+1}\equiv 1 \pmod p$. Now by Fermat's theorem $x^{p-1}\equiv 1 \pmod p$, for x is prime to p, therefore $x^{p+1}\equiv x^{p-1} \pmod p$ and $x^2\equiv 1 \pmod p$.

Hence $x\equiv \pm 1 \pmod p$ and $x^2+x+1\equiv 3$ or 1.

But $x^2+x+1\equiv 0$, hence $y^2\equiv -3 \pmod p$ has no solution and $(-3)Np$.

Applying the product theorem of Art. 2, we have the following results :

Prime forms	$12n+1$	$12n-1$	$12n+5$	$12n-5$
-1	R	N	R	N
-3	R	N	N	R
$+3$	R	R	N	N

4. Residues of a Composite Modulus. (I) *For the modulus p^n where p is an odd prime, we have the following :*

(i) *Half of the numbers less than p^n and not divisible by p are quadratic residues of p^n, the other half are non-residues, so that there are $\frac{1}{2}(p^n-p)$ of each sort.*

Consider the numbers less than $\frac{1}{2}p^n$ and not divisible by p. There are $\frac{1}{2}(p^n-p)$ such numbers, and by Art. 2, (2), every residue not divisible by p is congruent with the square of one of them.

It is therefore sufficient to show that the squares of these numbers are incongruent, two and two.

Let a, b be two of them and suppose that $a^2 \equiv b^2 \pmod{p^n}$. Then $(a+b)(a-b)$ would be divisible by p^n.

Now $a+b$ and $a-b$ are not both divisible by p, for if this were so $2a$, and therefore also a, would be divisible by p. Moreover, neither $a+b$ nor $a-b$ is divisible by p^n, for each of these $< p^n$.

Thus a^2 is not congruent with $b^2 \pmod{p^n}$, and the result follows.

(ii) *With regard to numbers not divisible by p, a quadratic residue of p is a quadratic residue of p^n, and a non-residue of p is a non-residue of p^n.*

The second part of this statement is obvious. Consequently, if the first part were not true, among the numbers less than p^n and not divisible by p there would be more residues of p than of p^n, that is, more than $\frac{1}{2}(p^n-p)$. But the number of residues of p less than p^n is easily seen to be $\frac{1}{2}p^{n-1}(p-1)$. Thus the first part of the theorem is true.

(iii) *If $x^2 \equiv a^2 \pmod{p^n}$ where a is prime to p, then $x \equiv \pm a \pmod{p^n}$.*

For $(x+a)(x-a)$ is divisible by p^n. Also $x+a$ and $x-a$ are not both divisible by p, for if this were the case $2a$, and therefore also a, would be so divisible.

Hence $x+a$ or $x-a$ is divisible by p^n.

(iv) If ARp, the congruence $x^2 \equiv A \pmod{p^n}$ has two incongruent solutions, which can be obtained as follows :

Ex. 1. *Solve* (i) $x^2 \equiv 23 \pmod{49}$ *and* (ii) $x^2 \equiv 23 \pmod{343}$.

(i) We must have $x^2 \equiv 23 \equiv 2 \equiv 3^2 \pmod 7$, therefore $x = 7y \pm 3$ where

$$(7y \pm 3)^2 \equiv 23 \pmod{49}.$$

Hence $\pm 42y \equiv 14 \pmod{49}$ and $\pm 3y \equiv 1 \pmod 7$, giving $y \equiv \pm 5 \pmod 7$.
Thus $y = 7z \pm 5$ and $x = 49z \pm 38 \equiv \pm 11 \pmod{49}$, which is the solution.

(ii) We must have $x^2 \equiv 23 \pmod{49}$, and so by the preceding $x = 49t \pm 11$ where $(49t \pm 11)^2 \equiv 23 \pmod{343}$.

Hence $\pm 7^2 . 22t \equiv -98 \pmod{7^3}$ and $\pm 11t \equiv -1 \pmod 7$, giving $t \equiv \pm 5 \pmod 7$.
Thus $t = 7u \pm 5$ and $x = 343u \pm 256 \equiv \pm 87 \pmod{7^3}$, which is the solution.

(2) **The Modulus 2^n.** (i) Every number is a quadratic residue of 2.

Every odd number of the form $4k+1$ is a residue of 4, and those of the form $4k-1$ are non-residues. Hence if $x^2 \equiv a^2 \pmod 4$, then

$$x^2 \equiv 1 \pmod 4,$$

and x may be any odd number, so that there are two incongruent solutions.

For the modulus 2^n where $n \geqslant 3$, all odd numbers of the form $8k+1$ are quadratic residues and the others are non-residues.

The proof of this may be arranged as follows :

(α) *Every odd residue is of the form* $8k+1$. For if A is odd and

$$A \equiv a^2 \pmod{2^n},$$

then $A \equiv a^2 \pmod 8$; and, since a is odd, a^2 is of the form $8k+1$; hence, $A \equiv 1 \pmod 8$.

(β) *Every odd residue of 2^n is congruent with the square of an odd number less than 2^{n-2}.*

For if A is any odd residue of 2^n and $A \equiv a^2 \pmod{2^n}$, we can find x so that $a = m \cdot 2^{n-1} \pm x$ and $x < \frac{1}{2} \cdot 2^{n-1}$, and then $A \equiv x^2 \pmod{2^n}$ where x is an odd number.

(γ) *The squares of all odd numbers less than 2^{n-2} are mutually incongruent (mod 2^n).*

For let $a, b (a > b)$ be any two odd numbers less than 2^{n-2}, and suppose that $a^2 \equiv b^2 \pmod{2^n}$, then $(a+b)(a-b)$ is divisible by 2^n.

Now $a+b$ and $a-b$ are both divisible by 2, but only one of them is divisible by 4 : hence one of them is divisible by 2^{n-1}, which is impossible, for each is less than 2^{n-1}. Hence a^2 is not congruent with $b^2 \pmod{2^n}$.

(δ) There are 2^{n-3} odd numbers less than 2^{n-2}, hence there are 2^{n-3} odd quadratic residues of 2^n which are mutually incongruent. Also, of the numbers less than 2^n, there are 2^{n-3} of the form $8k+1$: all of these are therefore residues and the rest are non-residues.

(ii) *If $x^2 \equiv a^2 (mod\ 2^n)$ where a is odd and $n \geqslant 3$, then $x = 2^{n-1} \cdot t \pm a$, where t is any integer or zero, giving four incongruent solutions.*

For $(x+a)(x-a)$ is divisible by 2^n, therefore $x+a$ or $x-a$ is divisible by 2^{n-1}, as in § (1), (iii). Hence $x = 2^{n-1} \cdot t \pm a$, so that $x \equiv \pm a$ or $2^{n-1} \pm a \pmod{2^n}$, according as t is of the form $2m$ or $2m+1$.

Ex. 2. *Solve* $x^2 \equiv 17 (mod\ 32)$.

Solutions exist, for 17 is of the form $8k+1$, in fact $17 \equiv 7^2 \pmod{32}$. Hence $x = 16t \pm 7$, so that $x \equiv \pm 7, \pm 9 \pmod{32}$.

(3) **The Modulus 2n.** *If A is a quadratic residue of an odd modulus n, it is a residue of $2n$.*

For if $A \equiv a^2 \pmod{n}$, then $A \equiv (n-a)^2 \pmod{n}$, and since n is odd, just one of the two n, $n-a$ is even, and the same is true of $A-a^2$ and $A-(n-a)^2$. Also each of the last pair is divisible by n, hence A is congruent $\pmod{2n}$ with either a^2 or $(n-a)^2$, but not with both.

The converse theorem is obviously true, and it follows that *if n is odd, the congruence $x^2 \equiv A \pmod{2n}$ has the same number of incongruent solutions as $x^2 \equiv A \pmod{n}$.*

Ex. 3. *Solve* $x^2 \equiv 3 \pmod{26}$.

Here x is an odd number such that $x^2 \equiv 3 \equiv 4^2 \pmod{13}$, so that $x = 13y \pm 4$ where y is odd. Therefore

$$x = 13(2t+1) \pm 4 \equiv \pm 9 \pmod{26}.$$

(4) **The Modulus $\alpha\beta\gamma \ldots$.** Let $\alpha, \beta, \gamma, \ldots$ be different primes or powers of different primes, and let A be prime to all of these numbers, then *if A is a quadratic residue of each of $\alpha, \beta, \gamma, \ldots$ it is a quadratic residue of the product $\alpha\beta\gamma \ldots$, and conversely.*

For suppose that $A \equiv a^2, b^2, c^2, \ldots$ respectively with regard to the moduli $\alpha, \beta, \gamma, \ldots$. Since $\alpha, \beta, \gamma, \ldots$ are prime to one another, there is just one value x_1 of x, less than $\alpha\beta\gamma \ldots$, such that

$$x \equiv a \pmod{\alpha}, \quad x \equiv b \pmod{\beta}, \quad x \equiv c \pmod{\gamma}, \ldots,$$

and since $x_1^2 - A$ is divisible by each of $\alpha, \beta, \gamma, \ldots$, it is divisible by their product. Therefore x_1 is a solution of $x^2 \equiv A \pmod{\alpha\beta\gamma \ldots}$ and A is a residue of $\alpha\beta\gamma \ldots$. The converse theorem is obviously true.

(ii) To every set of values of $a, b, c, \ldots$ there corresponds a single value of x less than $\alpha\beta\gamma \ldots$. Hence if $n_1, n_2, n_3, \ldots$ are the numbers of incongruent solutions of $x^2 \equiv A$ to the moduli $\alpha, \beta, \gamma, \ldots$ respectively, the number of incongruent solutions of $x^2 \equiv A \pmod{\alpha\beta\gamma \ldots}$ is $n_1 n_2 n_3 \ldots$.

Combining this with the results of §§ (2), (3), we have the following:

If $n = 2^\kappa p^\lambda q^\mu \ldots$ where $p, q, \ldots$ are the odd prime factors of n, in order that the congruence $x^2 \equiv A \pmod{n}$ may have a solution, it is necessary and sufficient that A should be a quadratic residue of 2^κ and of $p, q, \ldots$.

If this is so, the number of incongruent solutions is 2^t, 2^{t+1}, 2^{t+2}, according as $\kappa < 2$, $\kappa = 2$, $\kappa > 2$, where t is the number of odd prime factors $p, q, \ldots$.

Ex. 4. *Solve* $x^2 \equiv 13 \pmod{153}$.

We have $153 = 3^2 \cdot 17$ and 13 is a residue of 3 and of 17. Hence solutions exist, and the number of incongruent roots is 2^2 or 4. The values of x are given by

$$x^2 \equiv 13 \equiv 2^2 \pmod{9}, \quad x^2 \equiv 13 \equiv 8^2 \pmod{17},$$

giving

$$x = 9y \pm 2 = 17z \pm 8.$$

Now if $x=9y+a=17z+b$, then $-z\equiv(a-b)\pmod 9$, so that $z=b-a+9t$ and $x\equiv 18b-17a\pmod{153}$. Putting $a=\pm 2$, $b=\pm 8$, we have $x\equiv \pm 25,\ \pm 43\pmod{153}$, giving the four solutions.

Or we may proceed as in the next example.

Ex. 5. *Solve* $x^2\equiv -41 \pmod{210}$.

We have $210=2\cdot 3\cdot 5\cdot 7$ and -41 is a residue of 3, 5, 7, therefore solutions exist and the number of incongruent roots is 2^3 or 8. Also x is an odd number, satisfying the congruences

$$x^2\equiv -41\equiv 1^2\pmod 3,\quad x^2\equiv -41\equiv 2^2\pmod 5,\quad x^2\equiv -41\equiv 1^2\pmod 7,$$

giving
$$x=3y\pm 1=5z\pm 2=7u\pm 1.$$

The odd numbers $\leqslant \frac{1}{2}.210$ which are of the form $7u\pm 1$ are

1, 13, 15, 27, 29, 41, 43, 55, 57, 69, 71, 83, 85, 97, 99,

Omitting multiples of 3 and numbers which are not of the form $5z\pm 2$ (i.e. those which do not end with 3 or 7), we are left with 13, 43, 83, 97. Hence

$$x\equiv \pm 13,\quad \pm 43,\quad \pm 83,\quad \pm 97\pmod{210}.$$

Or thus, if $x=3y+a=5z+b=7u+c$, we find that $x\equiv -35a+21b+15c\pmod{105}$.

Putting $a=\pm 1$, $b=\pm 2$, $c=\pm 1$, we have $x\equiv \pm 13,\ \pm 22,\ \pm 8,\ \pm 43\pmod{105}$, and since x is odd, it follows that

$$x\equiv \pm 13,\quad \pm 83,\quad \pm 97,\quad \pm 43\pmod{210}.$$

Ex. 6. *Solve* $x^2\equiv 73\pmod{304}$.

We have $304=2^4\cdot 19$, and 73 is a residue of 2^4, being of the form $8k+1$; it is also a residue of 19. Hence solutions exist, the number of distinct roots being 2^{1+2} or 8. They are given by

$$x^2\equiv 73\equiv 3^2\pmod{16},\quad x^2\equiv 73\equiv 4^2\pmod{19},$$

so that
$$x=8y\pm 3=19z\pm 4.$$

If $x=8y+a=19z+b$, then $3z\equiv a-b\pmod 8$, giving $z=5(b-a)+8t$ and

$$x=96b-95a+152t.$$

Hence $x\equiv 96b-95a$ or $x\equiv 96b-95a+152\pmod{304}$.

Putting $a=\pm 3$, $b=\pm 4$, we get the eight solutions,

$$x\equiv \pm 61,\quad \pm 99,\quad \pm 91,\quad \pm 53\pmod{304}.$$

Or by the method of Ex. 2.

5. Euler's Criterion.

Any number a is a quadratic residue or a non-residue of an odd prime p according as $a^{\frac{1}{2}(p-1)}$ is congruent with $+1$ or with -1.

Corresponding to any number r of the set $1, 2, 3, \ldots p-1$, there is a single number r', also belonging to the set, such that $rr'\equiv a\pmod p$.

This is merely another way of saying that the congruence

$$rx\equiv a\pmod p$$

has a single solution less than p.

(i) If aRp, the congruence $x^2\equiv a\pmod p$ has two solutions less than p. Denoting one of these by r, the other is $p-r$ and $r(p-r)\equiv -r^2\equiv -a$.

If, then, from the set $1, 2, 3, \ldots p-1$ we exclude r and $p-r$, the remaining $p-3$ numbers can be arranged in $\frac{1}{2}(p-3)$ pairs such that the product of each pair is congruent with a.

Therefore $(-a) \cdot a^{\frac{1}{2}(p-3)} \equiv \lfloor p-1$ or $a^{\frac{1}{2}(p-1)} \equiv -\lfloor p-1$.

Now 1 is a quadratic residue of every prime, and putting $a=1$, we have $\lfloor p-1 \equiv -1$, which is Wilson's theorem. Hence if aRp, $a^{\frac{1}{2}(p-1)} \equiv 1$.

(ii) If aNp, r' cannot be equal to r, for in that case we should have $r^2 \equiv a$, which is impossible. Hence the numbers $1, 2, 3, \ldots p-1$ can be arranged in $\frac{1}{2}(p-1)$ pairs such that the product of each pair is congruent with a.

Therefore, in this case, $a^{\frac{1}{2}(p-1)} \equiv \lfloor p-1 \equiv -1$.

NOTE. If a is prime to p, no matter whether it is a residue or a non-residue, it follows from the above that $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem. It also follows that -1 is a residue of primes of the form $4n+1$ and a non-residue of those of the form $4n-1$.

Ex. 1. *Examine whether* $+3$ *and* -3 *are residues or non-residues of* 37.

Here $\frac{1}{2}(p-1) = 18$ and, to the modulus 37,

$$(\pm 3)^{18} = 27^6 \equiv 1000^2 \equiv 1,$$

therefore 3 and -3 are residues of 37.

6. Gauss's Lemma. *If p is an odd prime and a is any number prime to p and if μ is the number of absolute least residues to the modulus p of the products $1 \cdot a$, $2 \cdot a$, $3a, \ldots \frac{1}{2}(p-1)a$ which are negative, then a is a residue or a non-residue of p according as μ is even or odd.*

Denote the absolute least residues by

$$a_1, \ a_2, \ldots a_\lambda, \ -b_1, \ -b_2, \ldots \ -b_\mu,$$

where every a and b is positive, then

$$a^{\frac{1}{2}(p-1)} \cdot \lfloor \tfrac{1}{2}(p-1) \equiv (-1)^\mu a_1 a_2 \ldots a_\lambda b_1 b_2 \ldots b_\mu.$$

Now consider the numbers $a_1, a_2, \ldots a_\lambda, b_1, b_2 \ldots b_\mu$. No two of them are equal, for in that case we should have ar congruent with as or $-as$, where r and s are less than $\frac{1}{2}p$, that is $a(r-s)$ or $a(r+s)$ would be divisible by p, which is impossible.

Hence $a_1, a_2, \ldots a_\lambda, b_1, b_2, \ldots b_\mu$ are the numbers $1, 2, 3, \ldots \frac{1}{2}(p-1)$ in some order or other. Therefore

$$a^{\frac{1}{2}(p-1)} \cdot \lfloor \tfrac{1}{2}(p-1) \equiv (-1)^\mu \cdot \lfloor \tfrac{1}{2}(p-1) \text{ and } a^{\frac{1}{2}(p-1)} \equiv (-1)^\mu,$$

since $\lfloor \frac{1}{2}(p-1)$ is prime to p.

Hence by Euler's criterion, $(-1)^\mu = +1$ or -1 according as aRp or aNp, which proves the lemma in question.

Ex. 1. *Prove that* 2 *is a quadratic residue of all primes of the form* $8n \pm 1$, *and is a non-residue of all primes of the form* $8n \pm 3$.

Consider the products $1 \cdot 2,\ 2 \cdot 2,\ 3 \cdot 2, \ldots \frac{1}{2}(p-1)2$. Let $2m$ be the least of these which is greater than $\frac{1}{2}p$, then the products which have negative absolute least residues are $2m$ and those which follow $2m$. If then μ is the number of such products, we have $\mu = \frac{1}{2}(p-1) - m + 1 = \frac{1}{2}(p+1) - m$, where

$$2(m-1) < \tfrac{1}{2}p < 2m \quad \text{or} \quad m - 1 < \tfrac{1}{4}p < m.$$

(i) If $p = 8n+1,\ m = 2n+1,\ \mu = 2n$. (ii) If $p = 8n-1,\ m = 2n,\ \mu = 2n$.
(iii) If $p = 8n+3,\ m = 2n+1,\ \mu = 2n+1$. (iv) If $p = 8n-3,\ m = 2n,\ \mu = 2n-1$,

and the results in question follow by Gauss's lemma.

7. Law of Quadratic Reciprocity. The following important theorem was stated by Legendre: the proof given below is due to Lange (except as regards the diagrammatic illustration).

If p and q are odd primes, then (i) *each is a residue or each a non-residue of the other if at least one of them is of the form* $4n+1$, *and* (ii) *p is a residue or a non-residue of q according as q is a non-residue or a residue of p when both are of the form* $4n-1$.

Suppose that $p < q$, and consider the sequences

$$1 \cdot q,\ 2q, \ldots rq, \ldots \tfrac{1}{2}(p-1)q, \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$
$$1 \cdot p,\ 2p, \ldots sp, \ldots \tfrac{1}{2}(q-1)p. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

These sets of numbers may be represented by the points of division of two scales set edge to edge, the zero points coinciding.

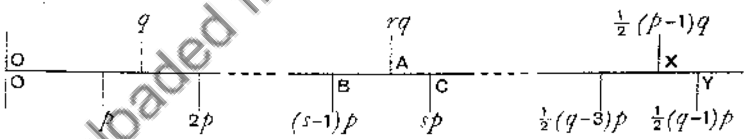


FIG. 48.

The diagram illustrates the case in which $p < q < 3p$; if $q > 3p$, more than one division of the p-scale will be outside the q-scale.

Let μ be the number of terms of the sequence (**A**) with negative absolute least residues (mod p). Every term of (**A**) lies between two consecutive terms of (**B**). Suppose that rq lies between $(s-1)p$ and sp, these numbers being represented by the points A, B, C; then BA and CA respectively represent the least positive and the numerically least negative residues of $rq \pmod p$.

Hence the absolute least residue of $rq \pmod p$ is negative if $AC < BA$, i.e. if $AC < \frac{1}{2}BC$ or if $sp - rq < \frac{1}{2}p$.

It follows that μ is the number of pairs of positive integers (r, s) which satisfy the conditions

$$r<\tfrac{1}{2}p, \quad s<\tfrac{1}{2}q, \quad 0<sp-rq<\tfrac{1}{2}p.$$

Again, let ν be the number of terms of the sequence (**B**) with negative absolute least residues (mod q).

If X, Y are the last points of division on the q- and p-scales,

$$XY=\tfrac{1}{2}(q-p)<\tfrac{1}{2}q.$$

Therefore XY represents the absolute least residue of $\frac{1}{2}(q-1)p \pmod q$, which is therefore positive. So also is the absolute least residue of any term of the sequence (**B**) greater than $\frac{1}{2}(p-1)q$, for its representative point is in XY.

Hence every term in (**B**) with a negative absolute least residue (mod q) lies between two consecutive terms of (**A**). Therefore, as above, ν is the number of pairs of positive integers (r, s) which satisfy the conditions

$$r<\tfrac{1}{2}p, \quad s<\tfrac{1}{2}q, \quad 0<rq-sp<\tfrac{1}{2}q,$$

i.e.,
$$r<\tfrac{1}{2}p, \quad s<\tfrac{1}{2}q, \quad -\tfrac{1}{2}q<sp-rq<0.$$

Now $sp-rq$ cannot be zero, therefore $\mu+\nu$ is the number of pairs of positive integers (r, s) which satisfy the conditions

$$r<\tfrac{1}{2}p, \quad s<\tfrac{1}{2}q, \quad -\tfrac{1}{2}q<sp-rq<\tfrac{1}{2}p. \quad \text{.....(C)}$$

Next let $r+r'=\frac{1}{2}(p+1)$ and $s+s'=\frac{1}{2}(q+1)$. Since r, s are positive, integers less than $\frac{1}{2}p$ and $\frac{1}{2}q$ respectively, so also are r', s'. Also if we substitute $\frac{1}{2}(p+1)-r'$ for r and $\frac{1}{2}(q+1)-s'$ for s in the last of the inequalities (**C**), we find that

$$-\tfrac{1}{2}q<\{\tfrac{1}{2}(q+1)-s'\}p-\{\tfrac{1}{2}(p+1)-r'\}q<\tfrac{1}{2}p.$$

Adding $\frac{1}{2}(q-p)$ to each of the unequals, we have $-\frac{1}{2}p<r'q-s'p<\frac{1}{2}q$, or $-\frac{1}{2}q<s'p-r'q<\frac{1}{2}p$; hence the pair (r', s') satisfy the conditions (**C**).

Again, the pairs (r, s), (r', s') are identical if $r=r'=\frac{1}{4}(p+1)$ and $s=s'=\frac{1}{4}(q+1)$. This can happen if both p and q are of the form $4n-1$, but not otherwise.

If then at least one of the two p, q is of the form $4n+1$, the solutions (r, s) of (**C**) can be arranged in pairs. Consequently $\mu+\nu$ is even, so that μ and ν are both even or both odd; and, by Gauss's lemma, qRp and pRq, or else qNp and pNq.

But if p and q are both of the form $4n-1$, the solutions (r, s) cannot be arranged in pairs, and $\mu+\nu$ is odd; therefore μ is even and ν odd, or *vice versa*; and, by Gauss's lemma, qRp and pNq, or else qNp and pRq.

The law of reciprocity, together with the supplementary theorems on the quadratic character of -1 and 2, completely settles the question as to whether any given number a is or is not a residue of a prime p. It also enables us to find the forms of primes of which a given prime is a residue.

Ex. 1. *Find the forms of primes of which* (i) $+5$, *and* (ii) -5, *is a residue.*

Since $+1$ and -1 are residues of 5, and $+2$ and -2 are non-residues, therefore all primes of the forms $5n \pm 1$ are residues of 5, and all primes of the forms $5n \pm 2$ are non-residues of 5.

Now 5 is of the form $4m+1$, therefore 5 *is a residue of all primes of the forms* $5n \pm 1$ *and a non-residue of all primes of the forms* $5n \pm 2$, *by the law of reciprocity.*

Using the theorems of Art. 2, we can now fill up the following table.

Forms	$20n+1$	$20n+3$	$20n+7$	$20n+9$	$20n-9$	$20n-7$	$20n-3$	$20n-1$
$+5$	R	N	N	R	R	N	N	R
-1	R	N	N	R	N	R	R	N
-5	R	R	R	R	N	N	N	N

Ex. 2. *Prove that* (i) $59 R 281$; (ii) $43 N 61$; (iii) $-43 R 103$.

(i) Both 59 and 281 are primes, and 281 is of the form $4n+1$. Hence $59 R 281$ if $281 R 59$, or if $45 R 59$, or if $5 R 59$, or if $4 R 5$, which is the case. Hence $59 R 281$.

(ii) $43 R 61$ if $61 R 43$, or if $18 R 43$, or if $2 R 43$.

Now 43 is of the form $8n+3$, therefore, by Art. 3, $2 N 43$ and $43 N 61$.

(iii) $-43 R 103$ if $60 R 103$, or if $15 R 103$.

Now $3 R 103$ if $103 N 3$, or if $1 N 3$, which is not the case, therefore $3 N 103$.

Also $5 R 103$ if $103 R 5$, or if $3 R 5$, which is not the case, therefore $5 N 103$.

Hence $15 R 103$ and $-43 R 103$.

In examples of this kind the reckoning is simplified by using the notation of Art. 8.

8. Legendre's Unities. Legendre introduced the following very convenient notation: *If p is an odd prime and a is any number, the symbol* $\left(\frac{a}{p}\right)$ *is to stand for* $+1$ *or* -1, *according as* aRp *or* aNp.

The law of reciprocity may be written in the form

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)},$$

where p, q are odd primes. For $\frac{1}{4}(p-1)(q-1)$ is even if p or q is of the form $4n+1$, and is odd if both are of the form $4n-1$.

The supplementary theorems relating to -1 and 2 may be written

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)} \quad \text{and} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}.$$

For $\frac{1}{2}(p-1)$ is even or odd according as p is of the form $4n+1$ or $4n-1$, i.e. according as $-1 Rp$ or $-1 Np$. Also $\frac{1}{8}(p^2-1)$ is even or odd according as p is of the forms $8n \pm 1$ or $8n \pm 3$, i.e. according as $2Rp$ or $2Np$.

Again, if a and b are any numbers, positive or negative, not divisible by p, $abRp$ if a and b are both residues or both non-residues and not otherwise, hence $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$, and so in general

$$\left(\frac{abc\ldots}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)\cdot\left(\frac{c}{p}\right)\ldots.$$

The convenience of this notation in working out such examples as the preceding is obvious. Thus, to investigate the quadratic character of -43 with regard to 103, we may proceed as follows:

$$\left(\frac{-43}{103}\right)=\left(\frac{-1}{103}\right)\cdot\left(\frac{43}{103}\right)=\left(\frac{103}{43}\right)=\left(\frac{17}{43}\right)=\left(\frac{43}{17}\right)=\left(\frac{9}{17}\right)=+1;$$

therefore $-43R103$.

9. Solution of $x^2\equiv A \pmod n$ by the Method of Exclusion. To solve this congruence is to find the integral solutions of the equation $x^2=ny+A$. We require values of y for which $ny+A$ is a square. These can be found by trial, and the number of trials which are actually necessary can be greatly reduced by the following considerations.

(i) It is sufficient to know the positive values of x which do not exceed $\frac{1}{2}n$, and so we need only consider values of y for which $-\frac{A}{n}<y<\frac{1}{4}n-\frac{A}{n}$.

(ii) Choose any number e greater than 2, which for this purpose is called an *excludent*, and let β be any non-residue of e.

If $ny+A$ is a square, it cannot be congruent (mod e) with β. Hence *we may exclude from trial all values of y which satisfy the congruence*

$$ny+A\equiv\beta \pmod e.$$

After using a properly chosen set of excludents, it will be found that the number of trials which have to be made is quite small.

NOTES. (i) It is easy to see that if e, e' are prime to one another, the use of these numbers in succession as excludents is equivalent to the use of ee'. Hence *only primes which are not divisors of n and powers of such primes should be used as excludents.*

(ii) If p is a prime and p^μ has been used as an excludent, the *use of the excludent $p^\nu(\nu>\mu)$ only rejects values of y for which $ny+A$ is a residue of p^μ and a non-residue of p^ν.*

(iii) *It is unnecessary to solve the congruence $ny+A\equiv\beta \pmod e$,* for this may be written in the form $y+a\equiv\beta/n \pmod e$ where $a=A/n \pmod e$.

Now β/n is a residue or a non-residue of e according as n is a non-residue or a residue. Hence, if $\alpha_1, \alpha_2, \ldots$, are the residues, and $\beta_1, \beta_2, \ldots$, are the non-residues, of e, the values of y which may be rejected are, (i) $\alpha_1-a, \alpha_2-a, \ldots$, when nNe, and (ii) $\beta_1-a, \beta_2-a, \ldots$, when nRe.

Ex. 1. *Find the general solution in integers of the equation* $x^2 = 157y + 109$.

Here $x^2 \equiv 109 \pmod{157}$, and it is easy to show that $109 R 157$, so that solutions exist. It is sufficient to take $x < \frac{1}{2} \cdot 157 < 79$ and $y < \frac{79^2 - 109}{157} < 40$.

Let $$V = 157y + 109.$$

Taking $\epsilon = 3$ and $\beta = 2$ (a non-residue of 3), we have $V \equiv y + 1 \pmod 3$, and if $y + 1 \equiv 2 \pmod 3$, then $y \equiv 1 \pmod 3$. Hence we may exclude values of y of the form $3m + 1$.

Taking $\epsilon = 4$ and $\beta = 2, 3$ (non-residues of 4), $V \equiv y + 1 \pmod 4$, and if $y + 1 \equiv 2, 3$, then $y \equiv 1, 2 \pmod 4$, so that we may exclude values of y of the forms $4m + 1$ and $4m + 2$.

Taking $\epsilon = 5$ and $\beta = 2, 3$ (non-residues of 5), $V \equiv 2y - 1$, and if $2y - 1 \equiv 2, 3$, then $2y \equiv 3, 4 \pmod 5$ and $y \equiv 4, 2 \pmod 5$. Hence we can exclude values of y of the forms $5m + 2$ and $5m + 4$.

If from the numbers 1, 2, 3, ... 39 we reject those of the forms mentioned above, the remaining numbers are 3, 8, 11, 12, 15, 20, 23, 24, 27, 32, 35, 36.

Taking $\epsilon = 7$ and $\beta = 3, 5, 6$ (non-residues of 7), $V \equiv 3y + 4 \pmod 7$, and if $3y + 4 \equiv \beta$ then $y - 1 \equiv \beta/3$, which is a residue. Hence we can reject values of y such that $y - 1 \equiv 1, 2, 4$ or $y \equiv 2, 3, 5 \pmod 7$. This excludes 3, 12, 23, 24, 32.

Taking $\epsilon = 8$, the non-residues of 8 are 2, 3, 5, 6, 7. Of these, 5 only is a residue of 4. Hence fresh numbers will be excluded only by taking $\beta = 5$.

Now $V \equiv 5y + 5 \pmod 8$, and if $5y + 5 \equiv 5$, then $y \equiv 0 \pmod 8$, and we can reject values of y of the form $8m$, namely 8, 24, 32. (The last two have already disappeared.) There remain 11, 15, 20, 27, 35, 36.

Taking $\epsilon = 11$ and $\beta = 2, 6, 7, 8, 10$ (non-residues of 11), $V \equiv 3y - 1$, and if $3y - 1 \equiv \beta \pmod{11}$, then $3y + 21 \equiv \beta$ and $y + 7 \equiv \beta/3$, which is a non-residue. Hence we can reject values of y such that $y + 7 \equiv 2, 6, 7, 8, 10$, or $y \equiv -5, -1, 0, 1, 3$, or $y \equiv 0, 1, 2, 3, 6$, thus excluding 11, 35 and 36. There remain 15, 20, 27.

Taking $\epsilon = 13$ and $\beta = 2, 5, 6, 7, 8, 11$ (non-residues of 13), $V \equiv y + 5 \pmod{13}$, and we can reject values of y such that $y \equiv -3, 0, 1, 2, 3, 6$. This excludes 15 and 27. The only remaining value of y is 20, which must give a solution.

In fact, $157 \cdot 20 + 109 = 57^2$, thus the solution of the congruence $x^2 \equiv 109 \pmod{157}$ is $x \equiv \pm 57 \bmod (157)$.

Hence $x = 157t \pm 57$ and $y = 157t^2 \pm 314t + 20$, which is the solution required.

EXERCISE XI

Solve the following congruences. (In each case the modulus is a prime.)

1. $x^2 \equiv A \pmod{79}$ for $A = 5, 13, 19$.
2. $x^2 \equiv A \pmod{103}$ for $A = 2, 7, 13$.
3. $x^2 \equiv A \pmod{157}$ for $A = -1, 109, 11, 17, 31$.
4. $x^2 \equiv A \pmod{179}$ for $A = 3, 5, 13, 19, 22$.
5. $x^2 \equiv A \pmod{197}$ for $A = 6, 7, -10$.
6. $x^2 \equiv A \pmod{229}$ for $A = 3, 5, 19$.
7. $x^2 \equiv A \pmod{2011}$ for $A = -2, 6, -10, -17$.
8. $x^2 \equiv A \pmod{10007}$ for $A = 2, 6, -17, -23$.

Solve the following, the modulus in each case being a composite number.

9. $x^2 \equiv 7 \pmod{58}$. **10.** $x^2 \equiv 5 \pmod{44}$. **11.** $x^2 \equiv -2 \pmod{99}$.

12. $x^2 \equiv 19 \pmod{135}$. **13.** $x^2 \equiv 51 \pmod{203}$. **14.** $x^2 \equiv -79 \pmod{1760}$.

15. $x^2 \equiv 23 \pmod{1001}$.

16. If p is a prime, the congruence $x^2 + x + 1 \equiv 0 \pmod{p}$ has solutions if, and only if, p is of the form $3n+1$. Also if x_1, x_2 are incongruent solutions, then $x_1 + x_2 \equiv -1 \pmod{p}$ and $x_1 x_2 \equiv 1 \pmod{p}$.

Find the general solution in integers of:

17. $x^2 + x + 1 \equiv 0 \pmod{73}$. **18.** $6x^2 + 7x - 4 \equiv 0 \pmod{71}$.

19. $3x^2 + 2x + 29 \equiv 0 \pmod{85}$. **20.** $6x^2 - x + 7 = 29y$.

21. $7x^2 - 11x - 3 = 31y$. **22.** $x^4 \equiv 4 \pmod{313}$.

23. Prove that $x^4 + x^2 + 1 \equiv 0 \pmod{19}$ has four incongruent solutions; find them.

24. Show that 6 is a quadratic residue of primes of the forms $24n \pm 1$, ± 5, and that -6 is a residue of those of the forms $24n+1$, 5, 7, 11.

25. Show that 10 is a quadratic residue of primes of the forms $40n \pm 1$, ± 3, ± 9, ± 13, and that -10 is a residue of those of the forms $40n+1$, 7, 9, 11, 13, 19, 23, 37.

26. For any prime p, prove that

(i) $7Rp$ if $p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$.
(ii) $11Rp$ if $p \equiv \pm 1, \pm 5, \pm 7, \pm 9, \pm 19 \pmod{44}$.
(iii) $13Rp$ if $p \equiv \pm 1, \pm 3, \pm 4 \pmod{13}$.
(iv) $17Rp$ if $p \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17}$.

27. Prove that -41 is a quadratic residue of 283, 307, 409.

28. Show that if a solution exists of the equation $x^2 = Ny + a$, where N is an odd prime number, then there are two solutions, and only two, for which $x < N$.

29. Show that, if a solution, (x, y), of the equation $x^2 = Ny + a$, where N is an odd prime exists, then the general solution is $X = mN \pm x$, $Y = m^2N \pm 2mx + y$.

Give the general solution, and the *first* four solutions of:

30. $x^2 = 13y + 23$. **31.** $x^2 = 23x + 13$. **32.** $x^2 = 97y + 22$.

In Exx. 33, 34, obtain the transformations indicated and give three solutions.

33. $x^2 = 21y + 123$, $u^2 = 7v + 2$. **34.** $x^2 = 21y + 112$, $u^2 = 3v + 1$.

35. Show that neither $x^2 - 11y = 2$ or 7, nor $x^2 - 13y = 2$ or 7 have any solutions; and that consequently $x^2 - 143y = 2$ or 7 have no solutions.

36. Show that $x^2 - 143y = 14$ may be reduced to $x^2 = 11u + 3$, or to $x^2 = 13v + 1$; hence that for solutions of the first equation x must be of the form $11m \pm 5$, and of the form $13n \pm 1$, and therefore of the form $143k \pm 27$, or $143k \pm 38$. Give the corresponding forms of y, and four solutions.

37. Verify, by the method of Ex. 36, the solutions of $x^2 = 153y + 13$, obtained in Art. 4, (4), Ex. 4; and give a general solution.

Use the method of excludents to solve the following equations:

38. $x^2 = 79y + 18$. **39.** $x^2 = 83y - 15$.

CHAPTER XI

INDETERMINATE EQUATIONS OF THE SECOND DEGREE

1. Solutions in Integers. In this chapter we consider equations of the second degree in x, y with integral coefficients, our object being to find any integral solutions which may exist.

It will be shown that the question can be made to depend on the solution in integers of an equation of one of the following types :

$$x^2 = my + n, \quad x^2 \pm Ny^2 = M, \quad xy = M,$$

where m, n, M, N are integers and N is positive and not a square. The first type has already been considered in the preceding chapter. With regard to the second type, the following theorems are of fundamental importance.

2. The Forms $x^2 \pm Ny^2$. It is supposed that N is a given positive integer which is not a square, and that x, y have any integral values.

(1) *The product of any two numbers of the form $x^2 + Ny^2$ can be expressed in the same form, and the same is true for numbers of the form $x^2 - Ny^2$.*

This follows from the identities

$$(x^2 + Ny^2)(x'^2 + Ny'^2) = (xx' \pm Nyy')^2 + N(xy' \mp x'y)^2,$$
$$(x^2 - Ny^2)(x'^2 - Ny'^2) = (xx' \pm Nyy')^2 - N(xy' \pm x'y)^2,$$

showing that in general the product can be expressed in the specified form in *two* ways. If, however, $xy' = x'y$, only one form is obtained, thus

$$(x^2 + Ny^2)^2 = (x^2 - Ny^2)^2 + N(2xy)^2.$$

Ex. 1. *Express* 91 *and* 91^2 *in the form* $x^2 + 3y^2$, *showing that this can be done in two ways.*

$$91 = 7 \cdot 13 = (2^2 + 3 \cdot 1^2)(1^2 + 3 \cdot 2^2) = (2 \cdot 1 \pm 3 \cdot 1 \cdot 2)^2 + 3(2 \cdot 2 \mp 1 \cdot 1)^2,$$

therefore
$$91 = 8^2 + 3 \cdot 3^2 = 4^2 + 3 \cdot 5^2,$$

and
$$91^2 = 37^2 + 3 \cdot 48^2 = 59^2 + 3 \cdot 40^2.$$

(2) *If $x^2 + Ny^2 = M_1 M_2$ and $M_1 = x_1^2 + Ny_1^2$, where x is prime to y and x_1 to y_1, then $M_2 = x_2^2 + Ny_2^2$, where x_2, y_2 are integers prime to one another, provided that M_1 is an odd prime, a power of an odd prime or twice such a number. Also numbers of the form $x^2 - Ny^2$ have similar properties.*

For $M_2 = (x^2 + Ny^2)/M_1 = (x^2 + Ny^2)(x_1^2 + Ny_1^2)/M_1^2 = x_2^2 + Ny_2^2$ where $x_2 = (xx_1 \pm Nyy_1)/M_1$ and $y_2 = (xy_1 \mp yx_1)/M_1$, both upper or both lower signs being taken.

Now $x^2y_1^2-y^2x_1^2=y_1^2(x^2+Ny^2)-y^2(x_1^2+Ny_1^2)=M_1(y_1^2M_2-y^2)$; therefore $(xy_1-yx_1)(xy_1+yx_1)$ is divisible by M_1; and, if M_1 is an odd prime p, at least one of the factors xy_1-yx_1 and xy_1+yx_1 is divisible by p. This gives an integral value for y_2; and if y_2 is an integer, so also is x_2.

Suppose that $M_1=p^r$, where p is an odd prime. Both xy_1-yx_1 and xy_1+yx_1 cannot be divisible by p, for if it were so, $2xy_1$ and $2yx_1$ would both be divisible by p, and so would xy_1 and yx_1. This is not the case, for x is prime to y and x_1 to y_1. Since $(xy_1-yx_1)(xy_1+yx_1)$ is divisible by p^r, it follows that one and only one of xy_1-yx_1 and xy_1+yx_1 is divisible by p^r, i.e. by M_1.

Next, let $M_1=2p^r$, then since $(xy_1-yx_1)(xy_1+yx_1)$ is divisible by 2, one and therefore *both* of xy_1-yx_1 and xy_1+yx_1 are divisible by 2.

As before, one of these is divisible by p^r, and therefore by $2p^r$, i.e. by M_1.

Thus, for one arrangement of signs, y_2 and consequently x_2 is an integer. Moreover,

$$x_1y_2-y_1x_2=\{x_1(xy_1\mp yx_1)-y_1(xx_1\pm Nyy_1)\}/M_1=\mp y.$$

Hence any common divisor of x_2, y_2 is a divisor of y: it is also a divisor of M_2, and therefore also of x. But x is prime to y, and so x_2 is prime to y_2.

This reasoning holds if $-N$ is substituted for N.

3. The Equation $x^2+Ny^2=M$. (1) It is supposed that M and N are integers, and that N is positive and not a square.

A solution (x', y') such that x' is prime to y' is called a *primitive solution*. Non-primitive solutions cannot exist unless M has a square factor, and any such solution can be obtained from a primitive solution of an equation of similar form.

Thus if $x^2-Ny^2=M$ and x, y have a common factor a, writing $x=aX$, $y=aY$ we have $X^2-NY^2=M/a^2$, so that M is divisible by a^2.

To find *all* the non-primitive solutions, *every* square factor a of M must be considered separately.

(2) The Case in which M is a Composite Number. If M_1 (or M_2) is of the form x^2+Ny^2, and if it is an odd prime, a power of an odd prime or twice such a number, then all the primitive solutions of $x^2+Ny^2=M_1M_2$ (if any exist) can be derived from those of $x^2+Ny^2=M_1$ and $x^2+Ny^2=M_2$.

For if (X, Y), (x_1, y_1) are primitive solutions of $x^2+Ny^2=M_1M_2$ and $x^2+Ny^2=M_1$ respectively, then by Art. 2 a primitive solution (x_2, y_2) of $x^2+Ny^2=M_2$ must exist such that

$$X^2+NY^2=(x_1^2+Ny_1^2)(x_2^2+Ny_2^2).$$

Ex. 1. *Find all the positive integral solutions of* $x^2+7y^2=7067$.

We have $7067=37\,.\,191$ and 37 (an odd prime) $=3^2+7\,.\,2^2$, thus if the equation has a solution, 191 must be of the form x^2+7y^2. On trial, we find $191=4^2+7\,.\,5^2$: moreover, 37 and 191 cannot be expressed in the form x^2+7y^2 in any other way. Thus

$$7067=(3^2+7\,.\,2^2)(4^2+7\,.\,5^2)=(3\,.\,4\pm7\,.\,2\,.\,5)^2+7(3\,.\,5\mp2\,.\,4)^2,$$

so there are just two solutions, namely (82, 7) and (58, 23).

4. The Equation $ax^2+by^2=M$, where a, b, M are Positive Integers. If any solutions exist, their number is obviously limited, and they can always be found as follows.

(1) **Method of Exclusion.** Choose one of the variables, say x (supposed to be positive), and let $V=(M-ax^2)/b$. We require values of x for which V is a square; and obviously the conditions

$$x<\sqrt{M/a} \quad \text{and} \quad x^2\equiv M/a \pmod{b}$$

must be satisfied. Writing down all values of x for which these conditions hold, the number of those which have to be actually tested may be reduced to something quite small as follows.

Choose any number e greater than 2 and not a factor of a (called an *excludent*), and let β be any non-residue of e. Since V is to be a perfect square, we may reject every x for which $V\equiv\beta \pmod{e}$.

All the remarks made in Art. 9 of the preceding chapter with regard to the choice of excludents hold good.

Ex. 1. *Search for positive integral solutions of*

(i) $10x^2+3y^2=2797$; (ii) $3x^2+7y^2=11506$.

(i) Let $V=(2797-10x^2)/3$, then V is to be a square, and we must have

$$x<\sqrt{280}<17 \quad \text{and} \quad x^2\equiv1 \pmod{3},$$

giving $x=3t\pm1$. Hence x must be one of the numbers

1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16. .....(A)

Taking $e=4$ and $\beta=2$, 3 (non-residues of 4), we have

$$V\equiv(1-2x^2)/(-1)\equiv-1+2x^2 \pmod{4},$$

and if $V\equiv2$, 3, then $2x^2\equiv3$, 0. The congruence $2x^2\equiv3$ is impossible, and if $2x^2\equiv0$, x is even, and so we can reject all even numbers from (A), leaving 1, 5, 7, 11, 13.

If $e=7$ and $\beta=3$, 5, 6 (non-residues of 7), then $V\equiv(-3-3x^2)/3\equiv-1-x^2 \pmod{7}$ and if $V\equiv3$, 5, 6, then $x^2\equiv3$, 1, 0. Now $3N7$ and if $x^2\equiv0$, 1, then $x=7t$, $7t\pm1$, and we can reject every x of these forms, i.e. 1, 7, leaving 5, 11, 13 as the only possible values of x. On trial we find that $x=11$ gives the solution (11, 23), and there is no other.

(ii) We can proceed exactly as in (i), or as follows: The equation may be written

$$X^2+21y^2=3\,.\,11506 \quad \text{where} \quad X=3x.$$

Now $3\,.\,11506=22\,.\,1569$ and $22=1^2+21\,.\,1^2$, moreover 22 is twice a prime, and

therefore if the given equation has a solution, integers (ξ, η) must exist so that

$$\xi^2 + 21\eta^2 = 1569.$$

We must have $\xi^2 \equiv 1569 \equiv 0 \pmod 3$ and $\xi^2 \equiv 1569 \equiv 1 \pmod 7$, hence ξ is a multiple of 3 of the form $7t \pm 1$. Also $\xi < \sqrt{1569} < 40$.

Writing down all multiples of 3 less than 40 and keeping only those of the form $7t \pm 1$, we have the numbers 6, 15, 27, 36, which are the only possible values of ξ.

Let $V = (1569 - \xi^2)/21$, then V is to be a square.

Let $\varepsilon = 5$ and $\beta = 2$, 3 (non-residues of 5), then $V \equiv (-1 - \xi^2)/1 \pmod 5$, and if $V \equiv 2$, 3, then $\xi^2 \equiv 2$, 1. So we reject every ξ such that $\xi^2 \equiv 1 \pmod 5$, or $\xi = 5t \pm 1$, i.e. the numbers 6, 36. We have left 15, 27 as the only possible values of ξ. Only the first of these gives the solution, (15, 8), and there is no other.

Thus we have $(3x)^2 + 21y^2 = (1^2 + 21 \cdot 1^2)(15^2 + 21 \cdot 8^2)$

$$= (1 \cdot 15 \pm 21 \cdot 1 \cdot 8)^2 + 21(1 \cdot 8 \mp 1 \cdot 15)^2,$$

giving $x = 7 \cdot 8 \pm 5 = 61$, 51, $y = 15 \mp 8 = 7$, 23; so there are just two solutions, viz. (61, 7) and (51, 23).

5. The Equation $x^2 - Ny^2 = M$. (1) As before, it is supposed that $\sqrt{N}$ is irrational. The nth complete quotient in the process of expressing $\sqrt{N}$ as a simple continued fraction is denoted by

$$(\sqrt{N} + b_n)/r_n,$$

the nth convergent is p_n/q_n, and c is the number of elements in the cycle. We have

$$p_n^2 - Nq_n^2 = = (-1)^n r_{n+1}.$$

Hence, if for some value of n, $M = (-1)^n r_{n+1}$, then (p_n, q_n) is a primitive solution of $x^2 - Ny^2 = M$.

It will be shown that if $|M| < \sqrt{N}$, and also under certain other conditions, *all* the primitive solutions can be obtained in this way.

Theorem. *If $0 < M < \sqrt{N}$ and (p, q) is any primitive solution of $x^2 - Ny^2 = \pm M$, then p/q is a convergent of the simple continued fraction equal to $\sqrt{N}$.*

(i) If $p^2 - Nq^2 = M$, then $p - \sqrt{N}q = M/(p + \sqrt{N}q) > 0$ and

$$0 < p - \sqrt{N}q < M/(2\sqrt{N}q) < 1/2q.$$

Hence

$$0 < p/q - \sqrt{N} < 1/2q^2.$$

Moreover, p is prime to q, for (p, q) is a primitive solution, therefore p/q is a convergent to $\sqrt{N}$. (*H.A.*, Ch. XXIV, 23.)

(ii) If $p^2 - Nq^2 = -M$, then $\sqrt{N}q - p = M/(\sqrt{N}q + p) > 0$ and

$$0 < \sqrt{N}q - p < M/2p < \sqrt{N}/2p.$$

Hence

$$0 < q/p - 1/\sqrt{N} < 1/2p^2.$$

Consequently q/p is a convergent to $1/\sqrt{N}$ and p/q is a convergent to $\sqrt{N}$.

6. General Solution of $x^2 - Ny^2 = \pm 1$.

(i) *If* (p, q) *is the least positive integral solution of* $x^2 - Ny^2 = 1$, *the general solution is given by*

$$x + \sqrt{N}y = (p + \sqrt{N}q)^t \quad \text{where} \quad t = 0, 1, 2, 3, \ldots .$$

(ii) *If* (p', q') *is the least solution of* $x^2 - Ny^2 = -1$, *the general solution is given by*

$$x + \sqrt{N}y = (p' + \sqrt{N}q')^{2t+1}.$$

For if (x, y) is a solution of either of these equations, x must be prime to y; and by the last theorem $x = p_n$, $y = q_n$ where p_n/q_n is a convergent to $\sqrt{N}$.

Also $p_n^2 - Nq_n^2 = (-1)^n r_{n+1}$ and $r_{n+1} = 1$ if, and only if, $n = tc$, where c is the number of elements in the period belonging to $\sqrt{N}$ and

$$t = 0, 1, 2, \ldots .$$

The general solution of $x^2 - Ny^2 = 1$ is (p_{tc}, q_{tc}) when c is even, and (p_{2tc}, q_{2tc}) when c is odd.

The general solution of $x^2 - Ny^2 = -1$ is $(p_{(2t+1)c}, q_{(2t+1)c})$ when c is odd, and there is no solution when c is even.

Also $p_{tc} + \sqrt{N}q_{tc} = (p_c + \sqrt{N}q_c)^t$ (equation (P), p. 132), whence the results in question immediately follow.

7. The Equation $x^2 - Ny^2 = M$, where $|M| < \sqrt{N}$.

(1) **General Solution.** *If* (p, q) *is the least solution of* $x^2 - Ny^2 = 1$ *and* (x_1, y_1), (x_2, y_2), $\ldots$, (x_k, y_k) *are the primitive solutions of* $x^2 - Ny^2 = M$ *less than* (p, q), *then all the primitive solutions of the latter equation are given by*

$$x + \sqrt{N}y = (x_m + \sqrt{N}y_m)(p + \sqrt{N}q)^t,$$

where $m = 1, 2, 3, \ldots k$ *and* t *is any positive integer.*

For since $|M| < \sqrt{N}$, every primitive solution is of the type (p_m, q_m), where p_m/q_m is a convergent to $\sqrt{N}$ such that $(-1)^m r_{m+1} = M$.

Also for every t, $r_{m+tc+1} = r_{m+1}$, where c is the number of elements in the cycle belonging to $\sqrt{N}$.

Hence if (p_m, q_m) is a solution, so also is (p_{m+tc}, q_{m+tc}) when c is even, and (p_{m+2tc}, q_{m+2tc}) when c is odd.

Also the least solution (p, q) of $x^2 - Ny^2 = 1$ is (p_c, q_c) or (p_{2c}, q_{2c}), according as c is even or odd, and by equation (Q), p. 132,

$$p_{m+tc} + \sqrt{N}q_{m+tc} = (p_m + \sqrt{N}q_m)(p_c + \sqrt{N}q_c)^t,$$

whence the result in question.

(2) Primitive solutions less than (p, q) are connected as follows: *If (X, Y) is a primitive solution less than (p, q), then a solution (ξ, η), also less than (p, q), is given by*

$$\xi + \sqrt{N}\eta = \pm(X - \sqrt{N}Y)(p + \sqrt{N}q),$$

where the upper or lower sign is to be taken according as $M \gtrless 0$.

For we may take $X = p_m$, $Y = q_m$ where $m < c$ or $2c$, according as c is even or odd and $M = (-1)^m r_{m+1}$. If $m + n = tc$, then $r_{m+1} = r_{n+1}$, and taking $t = 1$ or 2 according as c is even or odd, we have

$$M = (-1)^m r_{m+1} = (-1)^n r_{n+1}.$$

Thus (p_n, q_n) is a solution less than (p, q), and by equation (H), p. 130,

$$p_n + \sqrt{N}q_n = (-1)^m(p_m - \sqrt{N}q_m)(p + \sqrt{N}q),$$

giving the result in question.

Ex. 1. *Find the general solution of* $x^2 - 13y^2 = 3$.

For $\sqrt{13}$ we find that $c = 5$, $p_5 = 18$, $q_5 = 5$, thus the least solution (p, q) of

$$x^2 - 13y^2 = 1$$

is given by $p + \sqrt{13}q = (18 + \sqrt{13} \cdot 5)^2$. Also $(4, 1)$ is a solution of $x^2 - 13y^2 = 3$, and the only other solution less than (p, q) is given by $x + \sqrt{13}y = (4 - \sqrt{13})(p + \sqrt{13}q)$.

Hence the general solution is given by

$$x + \sqrt{13}y = (4 \pm \sqrt{13})(18 + \sqrt{13} \cdot 5)^{2t},$$

where $t = 0, 1, 2, \ldots$.

8. The Equation $x^2 - Ny^2 = M$ where $|M| > \sqrt{N}$.

(1) We shall prove that *if $|M| > \sqrt{N}$, all the primitive solutions of $x^2 - Ny^2 = M$ can be derived from those of one or more equations of the same form in which $|M| < \sqrt{N}$.*

Suppose that (x, y) is any primitive solution and let $M' = |M|$. Since x is prime to y, y must be prime to M': also $x^2 \equiv Ny^2 \pmod{M'}$, and therefore $(x/y)^2 \equiv N \pmod{M'}$.

Hence N is a quadratic residue of M', and at least one pair of numbers L_1, M_1 exists such that

$$L_1^2 = MM_1 + N \quad \text{and} \quad 0 < L_1 \leqslant \tfrac{1}{2}|M|. \qquad \ldots\ldots\ldots\ldots\ldots\ldots (A)$$

For one such pair, $x \equiv \pm L_1 y \pmod{M'}$, and we may write

$$x = \pm(L_1 y + M y_1). \qquad \ldots\ldots\ldots\ldots\ldots\ldots (B)$$

Substituting for x in the given equation and using (A),

$$M_1 y^2 + 2L_1 y y_1 + M y_1^2 = 1 \quad \text{and} \quad (yM_1 + L_1 y_1)^2 - N y_1^2 = M_1.$$

Let $x_1 = \pm(yM_1 + L_1 y_1)$, then $x_1^2 - N y_1^2 = M_1$, and by (B),

$$x = \pm(\pm L_1 x_1 - N y_1)/M_1, \quad y = (\pm x_1 - L_1 y_1)/M_1, \qquad \ldots\ldots\ldots\ldots\ldots\ldots (C)$$

where both upper or both lower signs are to be taken inside the brackets.

It follows that

$$xy_1 \pm yx_1 = \pm 1, \quad \text{.....(D)}$$

so that $|x_1|$ is prime to $|y_1|$ and $(|x_1|, |y_1|)$ is a primitive solution of

$$x^2 - Ny^2 = M_1. \quad \text{.....(E)}$$

Again, if $|L_1| < \sqrt{N}$, then $|M_1| = (N - L_1^2)/M' < N/M' < \sqrt{N}$, and if $|L_1| > \sqrt{N}$, $|M_1| = (L_1^2 - N)/M' < L_1^2/M' < \frac{1}{4}|M|$.

Thus it has been shown that if $|M| > \sqrt{N}$, corresponding to any primitive solution (x, y) of $x^2 - Ny^2 = M$, there is a primitive solution (x_1, y_1) of $x^2 - Ny^2 = M_1$, where $|M_1|$ < the greater of $\sqrt{N}$ and $\frac{1}{4}|M|$, from which x, y may be derived by equations (C).

Hence the primitive solutions of the given equation may be found as follows:

Rule. Find all the integral solutions (L_1, M_1), (L_1', M_1') ... of

$$x^2 = My + N$$

such that for every L_1, $0 < L_1 \leqslant \frac{1}{2}|M|$. For every M_1, take in order the primitive solutions (x_1, y_1) of

$$x^2 - Ny^2 = M_1,$$

and the corresponding values of $|x|$, $|y|$ given by

$$x + \sqrt{N}y = (L_1 \pm \sqrt{N})(x_1 + \sqrt{N}y_1)/M_1, \quad \text{.....(D)}$$

which is equivalent to

$$x = (L_1x_1 \pm Ny_1)/M_1, \quad y = (L_1y_1 \pm x_1)/M_1; \quad \text{.....(E)}$$

these give the same values of $|x|$, $|y|$ as equations (C). Every $(|x|, |y|)$ so obtained is a *rational* solution of $x^2 - Ny^2 = M$, for

$$x^2 - Ny^2 = (x_1^2 - Ny_1^2)(L_1^2 - N)/M_1^2 = M,$$

and it has been shown that every primitive solution must occur among them.

If $|M_1| > \sqrt{N}$, then $|M_1| < \frac{1}{4}|M|$, and in the same way the primitive solutions of $x^2 - Ny^2 = M_1$ can be derived from those of one or more equations of the type $x^2 - Ny^2 = M_2$ where $|M_2|$ < the greater of $\sqrt{N}$ and $\frac{1}{4}|M_1|$. Continuing thus the primitive solutions of $x^2 - Ny^2 = M$ can be derived from those of one or more equations of the type $x^2 - Ny^2 = M_r$ where $|M_r| < \sqrt{N}$.

NOTE. *If integral solutions are given by* both *signs in equation* (A), *then* $2N$ *must be divisible by* $|M_1|$.

For if (ξ, η), (ξ', η') are the solutions, by equations (B), $\xi \pm \xi'$ and $\eta \pm \eta'$ must be divisible by $|M_1|$. Hence $2Ny_1$ and $2x_1$ must be divisible by $|M_1|$, and since x_1 is prime to y_1, N must be divisible by $|M_1|$ or $\frac{1}{2}|M_1|$ according as $|M_1|$ is odd or even.

Ex. 1. *Find the general solution of* $x^2-29y^2=91$ *and deduce the four least solutions.*

We first express $\sqrt{29}$ as a simple continued fraction. The values of r, a, p, q are shown on the right, also $c=5$. Let $k=70+13\sqrt{29}$.

$\sqrt{29}$

r	1	4	5	5	4	1	
a	5	2	1	1	2	10	
p	5	11	16	27	70		
q	1	2	3	5	13		

The solutions (L_1, M_1) of $x^2=91y+29$ such that $0<L_1<\frac{1}{2}.91$ are $L_1=22, 43$, $M_1=5, 20$.

(i) *Let* $L_1=22$, $M_1=5$ and $x_1^2-29y_1=5$, then

$$x_1+\sqrt{29}y_1=(11\pm2\sqrt{29})\,.\,k^{2t}$$

and

$$x+\sqrt{29}y=(L_1\pm\sqrt{29})(x_1+\sqrt{29}y_1)/M_1$$
$$=(22\pm\sqrt{29})(11\pm2\sqrt{29})\,k^{2t}/5.$$

Like signs give

$$x+\sqrt{29}y=(60\pm11\sqrt{29})\,k^{2t}, \quad \text{.....(A)}$$

and, since $2\,.\,29$ is not divisible by M_1, unlike signs must give fractional values of x, y.

(ii) *Let* $L_1=43$, $M_1=20$ and $x_1^2-29y^2=20$. Since $20>\sqrt{29}$, we require the solutions (L_2, M_2) of $x^2=20y+29$ such that $0<L_2\leqslant\frac{1}{2}.20$. These are $L_2=3, 7$, $M_2=-1, 1$.

Taking $L_2=3$, $M_2=-1$ and $x_2^2-29y_2^2=-1$, we have

$$x_2+\sqrt{29}y_2=k^{2t+1},$$
$$x_1+\sqrt{29}y_1=(3\pm\sqrt{29})\,k^{2t+1},$$
$$x+\sqrt{29}y=(43\pm\sqrt{29})(3\pm\sqrt{29})\,k^{2t+1}/20.$$

Unlike signs give

$$x+\sqrt{29}y=(5\pm2\sqrt{29})\,k^{2t+1}, \quad \text{.....(B)}$$

and, since $2\,.\,29$ is not divisible by M_1, like signs must give fractional values of x, y.

Taking $L_2=7$, $M_2=1$ and $x_2^2-29y_2^2=1$, we have

$$x_2+\sqrt{29}y_2=k^{2t},$$
$$x_1+\sqrt{29}y_1=(7\pm\sqrt{29})\,k^{2t},$$
$$x+\sqrt{29}y=(43\pm\sqrt{29})(7\pm\sqrt{29})\,k^{2t}/20,$$

giving fractional values of x, y. Thus the general solution ($|x|, |y|$) is contained in equations (A), (B). Putting $t=0$ and 1, the least solutions are (60, 11), (404, 75), (1104, 205), (7480, 1389).

(2) If $|M|>\sqrt{N}$ and (p_m, q_m) is a solution of $x^2-Ny^2=M$ where p_m/q_m is a convergent to $\sqrt{N}$, the question arises as to whether every primitive solution is of this type. It will be shown that this is certainly the case *if* N *is a prime and* $|M|$ *is an odd prime, a power of an odd prime, twice such a number or equal to* 4.

This depends on the following:

(i) We have $M=(-1)^m r_{m+1}$; and $b_{m+1}^2=-r_m r_{m+1}+N$, by Art. 6.

Hence the equation $L_1^2=MM_1+N$ is satisfied if $L_1=\pm b_{m+1}$ and $M_1=(-1)^{m-1}r_m$.

Again, $r_{m+1}>\sqrt{N}$, and therefore $r_m<\sqrt{N}$. Hence all the primitive solutions of $x^2-Ny^2=M_1$ are given by $x=p_{n-1}$, $y=q_{n-1}$ where

$$n=m+tc \quad \text{or} \quad m+2tc, \quad \text{according as } c \text{ is even or odd.}$$

It follows that *rational solutions of* $x^2 - Ny^2 = M$ *are given by*

$$x = \left| \frac{b_{m+1}p_{n-1} \pm Nq_{n-1}}{r_m} \right|, \quad y = \left| \frac{b_{m+1}q_{n-1} \pm p_{n-1}}{r_m} \right|. \quad \text{.....(A)}$$

Again, $b_{n+1} = b_{m+1}$, $r_n = r_m$, and by equations (**D**) on p. 129,

$$r_n p_n = b_{n+1}p_{n-1} + Nq_{n-1} \quad \text{and} \quad r_n q_n = b_{n+1}q_{n-1} + p_{n-1}.$$

Hence *the upper signs give the solutions* (p_n, q_n), *and by* § (1), *the lower signs give fractional solutions unless* $2N$ *is divisible by* r_m.

(ii) If $|M|$ is as described above, $\pm b_{m+1}$ are the only solutions of $x^2 \equiv N (\mathrm{mod}\, |M|)$, and all the positive integral solutions are given by equations (**A**). Hence *all the solutions of* $x^2 - Ny^2 = M$ *are of the type* (p_n, q_n) *when* $|M|$ *is as described above and* $2N$ *is not divisible by* r_m.

(iii) *If* $r_m = 1$, then $m = 1$, $M = -r_2$ and the solutions given by (**A**) are

$$x = |a_1 p_{tc} \pm Nq_{tc}|, \quad y = |a_1 q_{tc} \pm p_{tc}|.$$

The upper signs give $x = p_{tc+1}$, $y = q_{tc+1}$, and by equations (**M**) on p. 131,

$$p_{tc-1} = Nq_{tc} - a_1 p_{tc} \quad \text{and} \quad q_{tc-1} = p_{tc} - a_1 q_{tc},$$

so that the lower signs give $x = p_{tc-1}$, $y = q_{tc-1}$.

(iv) *If* N *is a prime and* $r_m = 2$, then by Art. 6, (1), (iii), on p. 128, c is even and $m = \frac{1}{2}c + 1$; thus the upper signs in (**A**) give $x = p_{\frac{1}{2}kc+1}$, $y = q_{\frac{1}{2}kc+1}$, where k is any odd number.

The lower signs give the solutions $x = p_{\frac{1}{2}kc-1}$, $y = q_{\frac{1}{2}kc-1}$; for it is easy to show that for elements of the first cycle the solution is $(p_{\frac{1}{2}c-1}, q_{\frac{1}{2}c-1})$.

Thus, if we put $\frac{1}{2}c$ for n in equations (**C**) of Art. 6, (4), on p. 129, and note that $b_m = b_{m+1}$, from Art. 6, (1), (iii), on p. 128, we have

$$Nq_{\frac{1}{2}c} = r_{\frac{1}{2}c+1}q_{\frac{1}{2}c-1} - b_{\frac{1}{2}c+1}q_{\frac{1}{2}c} = r_{\frac{1}{2}c+1}p_{\frac{1}{2}c-1} + b_{\frac{1}{2}c+2}p_{\frac{1}{2}c},$$

$$p_{\frac{1}{2}c} = r_{\frac{1}{2}c+1}q_{\frac{1}{2}c-1} + b_{\frac{1}{2}c+1}q_{\frac{1}{2}c} = r_{\frac{1}{2}c+1}q_{\frac{1}{2}c-1} + b_{\frac{1}{2}c+2}q_{\frac{1}{2}c};$$

hence $(Nq_{\frac{1}{2}c} - b_{\frac{1}{2}c+2}p_{\frac{1}{2}c})/r_{\frac{1}{2}c+1} = p_{\frac{1}{2}c-1}$, $(p_{\frac{1}{2}c} - b_{\frac{1}{2}c+2}q_{\frac{1}{2}c})/r_{\frac{1}{2}c+1} = q_{\frac{1}{2}c-1}$.

The statement at the head of this section follows from (ii), (iii) and (iv).

9. The Case in which M is a Composite Number.

(1) If (x_1, y_1), (x_2, y_2) are solutions of $x^2 - Ny^2 = M_1$, and $x^2 - Ny^2 = M_2$ respectively, then two solutions of $x^2 - Ny^2 = M_1 M_2$ are given by

$$x + \sqrt{N}y = (x_1 \pm \sqrt{N}y_1)(x_2 + \sqrt{N}y_2), \quad \text{.....(A)}$$

or

$$x = x_1x_2 \pm Ny_1y_2, \quad y = x_1y_2 \pm y_1x_2. \quad \text{.....(B)}$$

For if equation (A) holds, then, since $\sqrt{N}$ is irrational,

$$x - \sqrt{N}y = (x_1 \mp \sqrt{N}y_1)(x_2 - \sqrt{N}y_2);$$

and therefore $x^2 - Ny^2 = (x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = M_1 M_2$.

Further, if M_1 is prime to M_2 and (x_1, y_1), (x_2, y_2) are primitive solutions, so also is (x, y). For from equations (B),

$$xx_2 - Nyy_2 = x_1 M_2, \quad xy_2 - yx_2 = -y_1 M_2,$$
$$xx_1 \pm Nyy_1 = x_2 M_1, \quad xy_1 \pm yx_1 = x_2 M_1;$$

and since x_1 is prime to y_1, and x_2 to y_2, any common factor of x, y divides M_1 and M_2.

(2) If M_1 (or M_2) is of the form $x^2 - Ny^2$ and is an odd prime, a power of an odd prime or twice such a number, then all the primitive solutions $(|x|, |y|)$ of $x^2 - Ny^2 = M_1 M_1$ (if any exist) can be derived from the equation

$$x + \sqrt{N}y = (x_1 + \sqrt{N}y_1)(x_2 + \sqrt{N}y_2),$$

where $(|x_1|, |y_1|)$, $(|x_2|, |y_2|)$ are primitive solutions of $x^2 - Ny^2 = M_1$ and $x^2 - Ny^2 = M_2$, respectively, and every x, y may have positive or negative values.

This follows from the preceding and from reasoning similar to that in the preceding article.

Again, if $-M_1$ is of the form $x^2 - Ny^2$, any primitive solutions of $x^2 - Ny^2 = M_1 M_2$ which may exist can be derived from those of

$$x^2 - Ny^2 = -M_1 \quad \text{and} \quad x^2 - Ny^2 = -M_2.$$

Ex. 1. *Give the general solutions of* $x^2 - 29y^2 = 7$ *and* $x^2 - 29y^2 = 13$, *and deduce that of* $x^2 - 29y^2 = 91$.

Proceeding as in Ex. 1, p. 160, we find that the general solutions of the first two equations are respectively given by

$$x + \sqrt{29}y = (6 \pm \sqrt{29})k^{2t} \quad \text{and} \quad x + \sqrt{29}y = (4 \pm \sqrt{29})k^{2t+1},$$

where $k = 70 + \sqrt{29 \cdot 13}$; and, as 7 is a prime, the general solution of $x^2 - 29y^2 = 91$ is given by

$$x + \sqrt{29}y = (6 \pm \sqrt{29})(4 \pm \sqrt{29})k^{2t+1}.$$

It is not difficult to show that this result is equivalent to that already obtained.

Ex. 2. *Verify that the result obtained in the last example may be got by using the equations* $x^2 - 29y^2 = -7$ *and* $x^2 - 29y^2 = -13$.

The general solutions of these equations are

$$x + \sqrt{29} = (6 \pm \sqrt{29})k^{2t+1} \quad \text{and} \quad x + \sqrt{29}y = (4 \pm \sqrt{29})k^{2t}, \text{ etc.}$$

10. Other Methods. Some of the results obtained in this chapter can be derived in a more elementary way from the following inequalities.

If (x_1, y_1), (x_2, y_2) *are positive solutions of* $x^2 - Ny^2 = M$ *such that* $x_1 + \sqrt{N}y_1 > x_2 + \sqrt{N}y_2$, *then* $x_1 > x_2$, $y_1 > y_2$ *and* $x_1/y_1 < x_2/y_2$.

For $x_1^2 - Ny_1^2 = x_2^2 - Ny_2^2$ and $x_1 + \sqrt{N}y_1 > x_2 + \sqrt{N}y_2$; therefore $x_2 - \sqrt{N}y_2 > x_1 - \sqrt{N}y_1$. Hence $x_1 + x_2 + \sqrt{N}(y_1 - y_2) > x_1 + x_2 - \sqrt{N}(y_1 - y_2)$, so that $y_1 > y_2$.

Also $x_1^2 - x_2^2 = N(y_1^2 - y_2^2) > 0$, therefore $x_1 > x_2$.

Again, $x_1 - \sqrt{N}y_1 < x_2 - \sqrt{N}y_2$ and $y_1 > y_2$, therefore

$$x_1/y_1 - \sqrt{N} < x_2/y_2 - \sqrt{N} \quad \text{and} \quad x_1/y_1 < x_2/y_2.$$

Ex. 1. *If* (p, q), (X, Y) *are solutions of* $x^2 - Ny^2 = 1$ *such that*

$$(p + \sqrt{N}q)^k < X + \sqrt{N}Y < (p + \sqrt{N}q)^{k+1},$$

where k *is any positive integer, then there exists a solution* (P, Q) *of this equation such that* $P < p$ *and* $Q < q$.

For let $X' + \sqrt{N}Y' = (p + \sqrt{N}q)^k$, then by equation (P), p. 132, (X', Y') is a solution and

$$1 < P + \sqrt{N}Q < p + \sqrt{N}q$$

where $P + \sqrt{N}Q = (X + \sqrt{N}Y)/(X' + \sqrt{N}Y')$. Since $\sqrt{N}$ is irrational, we have also

$$P - \sqrt{N}Q = (X - \sqrt{N}Y)/(X' - \sqrt{N}Y'),$$

and therefore $$P^2 - NQ^2 = (X^2 - NY^2)/(X'^2 - NY'^2) = 1.$$

Hence (P, Q) is a solution; and, by the theorem above, $P < p$ and $Q < q$.

Ex. 2. *Deduce the general solution of* $x^2 - Ny^2 = 1$ *from the last example.*

If (p, q) is the least solution, then solutions are given by

$$\xi + \sqrt{N}\eta = (p + \sqrt{N}q)^t \quad \text{where} \quad t = 1, 2, 3, \ldots; \quad \ldots\ldots\ldots\ldots\ldots\ldots(\mathrm{A})$$

and if a solution (X, Y) exists which is not included among these, we should have

$$(p + \sqrt{N}q)^k < X + \sqrt{N}Y < (p + \sqrt{N}q)^{k+1}$$

for some value of k. Consequently (p, q) would not be the least solution, and therefore the general solution is given by (A).

11. The General Quadratic. The foregoing results may be applied to the question of finding solutions in integers of the equation

$$ax^2 + 2hxy + by^2 + 2gx + 2fy + c = 0.$$

Let $C = ab - h^2$, $F = gh - af$, $G = fh - bg$ and

$$\Delta = abc + 2fgh - af^2 - bg^2 - ch^2.$$

If $C \neq 0$, the equation may be written in one of the forms

$$C(ax + hy + g)^2 + (Cy - F)^2 + a\Delta = 0 \quad \text{where} \quad a \neq 0,$$

$$C(hx + by + f)^2 + (Cx - G)^2 + b\Delta = 0 \quad \text{where} \quad b \neq 0.$$

If $a = 0$, $b = 0$ and $h \neq 0$, the form is

$$2(hx + f)(hy + g) + ch - 2fg = 0.$$

If $C = 0$, the forms are

$$(ax + hy + g)^2 - 2Fy + B = 0 \quad (a \neq 0),$$

$$(hx + by + f)^2 - 2Gx + A = 0 \quad (b \neq 0),$$

where $A = bc - f^2$, $B = ca - g^2$.

Thus the equation can be written in one of the forms

$$X^2+CY^2=M, \quad XY=M, \quad X^2=mY,$$

where M, m are integers and X, Y are linear functions of x, y with integral coefficients, in the last two equations Y involving only x or only y. Now if x, y are integers, so also are X, Y, and we can find integral solutions (X, Y) of any of these equations (if such exist) by the foregoing methods. Having done this, those solutions must be selected which render x, y integral. In this way, no solution can escape discovery.

Four distinct cases arise according as $\sqrt{-C}$ is real and rational, real and irrational, imaginary or zero.

(i) *If* $\sqrt{-C}$ *is rational*, then $ax^2+2hxy+by^2$ is the product of two linear factors with rational coefficients, the equation can be put in the form $XY=M$, and we proceed as follows.

Ex. 1. *Find all the integral solutions of*

$$S=6x^2+7xy-3y^2-19x-y-25=0.$$

We have $6x^2+7xy-3y^2=(2x+3y)(3x-y)$, and we may assume that

$$S=(2x+3y+h)(3x-y+k)-M.$$

Equating coefficients, we find that $h=-5$, $k=-2$, $M=35$, and the equation may be written in the form $XY=35$ where $X=2x+3y-5$, $Y=3x-y-2$.

If x, y are integers, so are X, Y; thus we require integral solutions of $XY=35$ which yield integral values of x, y. Now $11x=X+3Y+11$, $11y=3X-2Y+11$, and x, y are integers if $X+3Y\equiv 0 \pmod{11}$; for $3X-2Y\equiv 3(X+3Y) \pmod{11}$.

The possibilities are as follows.

X	5,	−5,	7,	−7,	35,	−35,	1,	−1
Y	7,	−7,	5,	−5,	1,	−1,	35,	−35
$X+3Y$	26,	−26,	22,	−22,	38,	−38,	106,	−106
x			3,	−1				
y			2,	0				

Hence the solutions are $(3, 2)$, $(-1, 0)$.

(ii) *If* $\sqrt{-C}$ *is real and irrational,* the equation is of the form

$$X^2-(-C)Y^2=M,$$

and we use the method of Art. 3 or of Art. 8.

Ex. 2. *Search for positive integral solutions of*

$$S=2x^2-7xy+4y^2+3x+6y-14=0.$$

Here
$$8S=(4x-7y+3)^2-17y^2+90y-121,$$
$$136S=17(4x-7y+3)^2-(17y-45)^2-32.$$

Hence the equation may be written

$$X^2-17Y^2=-32, \quad \text{.....(A)}$$

where
$$X=17y-45, \qquad Y=4x-7y+3.$$

By the method of Art. 8, for equation (A) we find the primitive solutions (11, 3), (45, 11), (771, 187), etc., and the non-primitive solutions (6, 2), (74, 18), (470, 114), ..., so that possible values of X are ± 6, ± 11, ± 45, ± 74, ± 470, etc. Now $17y = X + 45$, we therefore select values of X for which $X \equiv -45 \equiv 6 \pmod{17}$, and proceed as follows.

$X = 17y - 45 =$	$+6,$		$-11,$		$-45,$		$+74,$		$+771,$ etc.
$y =$	3,		2,		0,		7,		48
$Y = 4x - 7y + 3 =$	2,	$-2,$	3,	$-3,$	11,	$-11,$	18,	$-18,$	187, -187
$4x + 3 =$	23,	19,	17,	11,	11,	...,	67,	31,	523, 109
$x =$	5,	4,	...,	2,	2,	...,	16,	7,	130, ...

giving the solutions (2, 0), (2, 2), (4, 3), (5, 3), (7, 7), (16, 7), (130, 48), etc. In this way no solution can be missed.

(iii) *If* $C > 0$ the solution depends on that of $X^2 + CY^2 = M$, and we apply the method of Art. 3 in the same way as above.

(iv) *If* $C = 0$ the solution depends on $X^2 = mY$, and the general solution can be found as in the following.

Ex. 3. *Find the general solution in integers of*

$$S = 9x^2 - 12xy + 4y^2 - 6x - 31y - 20 = 0.$$

Here
$$\begin{aligned} S &= (3x - 2y)^2 - 6x - 31y - 20 \\ &= (3x - 2y)^2 - 2(3x - 2y) + 1 - 35y - 21 \\ &= (3x - 2y - 1)^2 - 7(5y + 3). \end{aligned}$$

Hence the equation may be written

$$X^2 = 7Y, \quad \text{.....(A)}$$

where
$$X = 3x - 2y - 1, \quad Y = 5y + 3. \quad \text{.....(B)}$$

From (A), $X^2 \equiv 0 \pmod 7$; therefore $X = 7u$, $Y = 7u^2$.
From (B), $Y = 7u^2 \equiv 3 \pmod 5$; hence $u^2 \equiv 4 \pmod 5$ and $u = 5v \pm 2$.
Hence $5y + 3 = 7(5v \pm 2)^2$, so that

$$y = 35v^2 \pm 28v + 5; \quad \text{also} \quad X = 3x - 2y - 1 = 35v \pm 14; \quad \text{.....(C)}$$

and we have
$$3x = 70v^2 + 91v + 25 \quad \text{or} \quad 70v^2 - 21v - 3,$$

according as the upper or lower signs are taken.

In the first case

$$70v^2 + 91v + 25 \equiv v^2 + v + 1 \equiv 0 \pmod 3;$$

i.e.
$$(2v + 1)^2 \equiv 0, \quad 2v \equiv -1, \quad v \equiv 1 \pmod 3, \quad v = 3t + 1.$$

Hence we find that

$$x = 21(10t^2 + 11t) + 62, \quad y = 21(15t^2 + 14t) + 68. \quad \text{.....(D)}$$

In the second case, when the lower signs are taken,

$$70v^2 - 21v - 3 \equiv 0 \pmod 3, \quad v \equiv 0 \pmod 3, \quad v = 3t,$$

and we find that

$$x = 21(10t^2 - t) - 1, \quad y = 21(15t^2 - 4t) + 5. \quad \text{.....(E)}$$

The general solution is contained in (D) and (E), where t is any integer or zero.

EXERCISE XII

1. Find all the positive integral solutions of:

(i) $3x^2+10y^2=2077$; (ii) $5x^2+11y^2=1984$;
(iii) $5x^2+13y^2=6138$; (iv) $x^2+10y^2=1859$.

2. Show that all the positive integral solutions $(|x|, |y|)$ of $x^2-13y^2=12$ are given by

$$x+\sqrt{13}y=(\sqrt{13}\pm 1)k^{2t+1}, \quad (5\pm\sqrt{13})k^{2t}, \quad 2(4\pm\sqrt{13})k^{2t},$$

where $k=18+\sqrt{13}\,.\,5$ and $t=0, 1, 2, \ldots$.

3. (i) Show that all the positive integral solutions $(|x|, |y|)$ of

$$x^2-13y^2=153$$

are given by

$$x+\sqrt{13}y=(19\pm\sqrt{13}\,.\,4)k^{2t}, \quad (59\pm\sqrt{13}\,.\,16)k^{2t}, \quad 3(15\pm\sqrt{13}\,.\,4)k^{2t},$$

where $k=18+\sqrt{13}\,.\,5$, and give the four least primitive solutions.

(ii) Deduce the primitive solutions of $x^2-13y^2=153$ from those of $x^2-13y^2=9$, $x^2-13y^2=17$, showing that they are given by

$$x+\sqrt{13}y=(2\pm\sqrt{13})(15\pm\sqrt{13}\,.\,4)k^{2t+1}.$$

Verify that the same result may be obtained from the pair $x^2-13y^2=-9, -17$, and that it is equivalent to that in (i).

4. If c is the number of elements in the cycle belonging to $\sqrt{N}$, then

$$x^2=N(y^2+1)$$

has solutions if c is odd and $x^2=N(y^2+2)$ has solutions if c is of the form $4m+2$. Find the least positive integral solutions of

(i) $x^2=29(y^2+1)$; (ii) $x^2=43(y^2+2)$.

For the equations 5-12, prove that the general solution $(|x|, |y|)$ in positive integers is given as under, where $t=0, 1, 2, \ldots$; and give the two least solutions in each case.

5. If $x^2-7y^2=-6$, then $x+\sqrt{7}y=(\sqrt{7}\pm 1)(8+\sqrt{7}\,.\,3)^t$.

6. If $x^2-7y^2=42$, then $x+\sqrt{7}y=(7\pm\sqrt{7})(8+\sqrt{7}\,.\,3)^t$.

7. If $x^2-7y^2=197$, then $x+\sqrt{7}y=(15\pm\sqrt{7}\,.\,2)(8+\sqrt{7}\,.\,3)^t$.

8. If $x^2-19y^2=30$ and $k=\frac{1}{2}(13+\sqrt{19}\,.\,3)^2$, then

$$x+\sqrt{19}y=(7\pm\sqrt{19})k^t \quad \text{or} \quad (31\pm\sqrt{19}\,.\,7)k^t.$$

9. If $x^2-19y^2=229$, then $x+\sqrt{19}y=(20\pm\sqrt{19}\,.\,3)k^t$.

10. If $x^2-31y^2=18$ and $k=\frac{1}{2}(39+\sqrt{31}\,.\,7)^2$, then

$$x+\sqrt{31}y=(7\pm\sqrt{31})k^t \quad \text{or} \quad 3(39+\sqrt{31}\,.\,7)k^t.$$

11. If $x^2-15y^2=49$ and $k=4+\sqrt{15}$, then $x+\sqrt{15}y=(8\pm\sqrt{15})k^t$ or $7k^t$.

12. If $x^2-22y^2=179$, then $x+\sqrt{22}y=(27\pm\sqrt{22}\,.\,5)(14+\sqrt{22}\,.\,3)^{2t}/2^t$.

13. If $x^2-(a^2-2)y^2=2$ where $a>2$, then

$$x+\sqrt{(a^2-2)}\,.\,y=(a+\sqrt{a^2-2})^{2t+1}/2^t.$$

14. If $x^2-a(a+4)y^2=-a$ where $a>1$ and is odd, then

$$x+\sqrt{a(a+4)}\,.\,y=\tfrac{1}{2}\{a(a+3)+\sqrt{a(a+4)}\,.\,(a+1)\}\{p+\sqrt{a(a+4)}q\}^t$$

where $p=\frac{1}{2}(a^3+6a^2+9a+2)$ and $q=\frac{1}{2}(a+1)(a+3)$.

15. Find all the positive integral solutions of:

(i) $3xy-7x-5y+11=0$;
(ii) $x^2-2xy-3y^2-x+15y-22=0$;
(iii) $x^2+3xy-7y-81=0$;
(iv) $x^2+y^2-2x+3y-33=0$;
(v) $x^2-6xy+9y^2+5x-12y=0$;
(vi) $3x^2+5xy-12y^2-18x+11y-9=0$;
(vii) $3x^2+y^2+8x-10y-19=0$;
(viii) $6x^2+8xy-13x-12y+19=0$.

16. Find two integral solutions of:

(i) $7x^2-y^2+4x-8y-15=0$; (ii) $x^2-6xy-2y^2+11x-44y+24=0$

CHAPTER XII

PRIMITIVE ROOTS

(*Continued from* H.A., *Chap. XXVI*)

1. Theorem. *If p is an odd prime and d is $p-1$, or any divisor of it, then $\phi(d)$ of the numbers* $1, 2, 3, \ldots p-1$ *belong to the index d.*

Let $d_1 (=1)$, d_2, d_3, ... d_λ $(=p-1)$ be the divisors of $p-1$, then by *H.A.*, Ch. XXVI, 2, (6), on p. 424,

$$\phi(d_1)+\phi(d_2)+\phi(d_3)+\ldots+\phi(d_\lambda)=p-1.$$

Hence it is sufficient to show that not more than $\phi(d)$ of the numbers less than p belong to any particular divisor d.

Suppose that a belongs to the index d, and consider the numbers $a^0, a^1, a^2, \ldots a^m, \ldots a^{d-1}$ and their residues

$$r_0,\ r_1,\ r_2, \ldots r_m, \ldots r_{d-1}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

The congruence $x^d \equiv 1 \pmod p$ has at most d incongruent roots, and it is satisfied by each of these residues. Hence all the numbers belonging to the index d are included in the set (**A**).

Further, if m and d have a common divisor f so that $m=nf$, $d=ef$, then $me=nd$ and $(a^m)^e=(a^d)^n \equiv 1 \pmod p$.

Consequently r_m belongs to the index e, which is less than d. Hence the only numbers in the set (**A**) which belong to the index d are those with a suffix prime to d; i.e. not more than $\phi(d)$ of the numbers less than p belong to the index d. This establishes the truth of the theorem.

In particular, *an odd prime modulus p has $\phi(p-1)$ primitive roots*, for such roots belong to the index $p-1$. Moreover, *if a is any primitive root, the complete set is congruent (mod p) with $a^h, a^k, a^l, \ldots$ where $h, k, l, \ldots$ are the numbers less than $p-1$ and prime to it.*

2. The process of finding a primitive root is one of trial, as in Ex. 1.

Ex. 1. *Find a primitive root of* 73 ; *and deduce the index and period of the root* 10.

To a modulus 73, the residues of powers of 2 are, in order, 1, 2, 4, 8, 16, 32, 64, 55, 37, 1 ; hence 2 is a subordinate root belonging to the index 9.

Now, as has been proved above, each of these residues belongs to an index which is equal to or less than 9 ; hence none of them can be primitive roots. For a second trial, therefore, we choose a number, say 3, which is not included in these residues.

The residues of powers of 3 are 1, 3, 9, 27, 8, 24, 72, ... ; and, since 72 is the residue of 3^6, the residue of 3^{12} is 1. Hence 3 is a subordinate root belonging to an index 12, and the residues are 1, 3, 9, 27, 8, 24, -1, -3, -9, -27, -8, -24, $+1$, ...

For a third trial take a number not included in the residues of the powers of 2 or of 3, say 5. We have $5^4 \equiv 41$, $5^8 \equiv 2$, $5^{12} \equiv 9$, $5^{24} \equiv 8$, $5^{36} \equiv -1$; hence 5 is a primitive root of 73, and all the others can be found at once.

Again, $10 \equiv 5^9$ and $10^m \equiv 5^{9 \cdot m}$, hence $72/9 = 8$ is the least value of m for which $10^m \equiv 1$ and 10 belongs to the index 8. Also the residues of 10^0, 10^1, 10^2, ... , 10^7 are congruent with 5^0, 5^9, $5^{9 \cdot 2}$, ... , $5^{9 \cdot 7}$, and are therefore 1, 10, 27, 51, 72, 63, 46, 22, which is the required period. These residues are the remainders in the process of expressing 1/73 as a decimal.

Alternatively. When n is not large, if $1/n$ is converted into a decimal, and $n-1$ figures occur in the period, then 10 is a primitive root, and the remainders are the residues of powers of 10. If there are $(n-1)/t$ figures in the period, where $t = 2, 3, 4, 6, 8, 9$ or 12, then a primitive root can be very readily obtained by writing down the quadratic residues in order (by the addition of the successive odd numbers), and then if necessary obtaining from them the residues of the cubes. For, if 10 belongs to an index $(n-1)/t$ or d, there is at least one primitive root, g, such that $g^t \equiv 10$.

Thus the period for 1/41 consists of 5 figures ; hence we seek a solution of $g^5 \equiv 10$; and from the quadratic residues of 41, we find $g^4 = \pm 16$, $g^2 = \pm 4$, ± 5, $g = \pm 2$, ± 18, ± 13, ± 6. For these, $2^{10} \equiv -1$, $18^5 \equiv 1$, and 2, 39, 18, 23, are subordinate roots ; but $13^{10} \equiv 10 \cdot 13^2 \equiv 9$, $13^{30} \equiv -1$, $6^{10} \equiv 10 \cdot 36 \equiv -9$, $6^{20} \equiv -1$; hence ± 13, ± 6, i.e. 6, 13, 28, 35, are all primitive roots.

Similarly, for 73 we require solutions of $g^9 \equiv 10$; and from the residues of the cubes we have $g^3 \equiv -21$, -22, -30, giving $g \equiv 5, 28, 40$; 7, 10, 56 ; 14, 20, 39 ; and of these it will be found that 5, 14, 20, 28, 39, 40, are primitive roots.

3. Gauss's 'Index' Notation. (1) Let p be an odd prime and g any primitive root of p which we choose as a *base.*

If x is any number prime to p, among the numbers 1, 2, 3, ... $p-1$, we can find one number ι and one only such that $x \equiv g^\iota \pmod{p}$.

The number ι is called the *index* of x to the *base* g, and is denoted by $ind_g\, x$. The fundamental theorems for indices are as follows :

(i) *If* $g^{\iota'} \equiv g^\iota (mod\ p)$, *then* $\iota' \equiv \iota (mod\ p-1)$.

For if $\iota' > \iota$, $g^{\iota'-\iota} \equiv 1 \pmod{p}$ and since g is a primitive root,

$$\iota' - \iota = p-1, \quad \text{or a multiple of } p-1.$$

(ii) $ind_g(xy) \equiv ind_g\, x + ind_g\, y (mod\ p-1)$.

(iii) $ind_g\, x^n \equiv n\ .\ ind_g\, x (mod\ p-1)$.

For let $\text{ind}_g\, x = \iota$, $\text{ind}_g\, y = j$ and $\text{ind}_g\, (xy) = k$, then $x \equiv g^\iota \pmod{p}$, $y \equiv g^j \pmod{p}$ and $xy \equiv g^{\iota+j} \pmod{p}$.

Hence, by the preceding, $k \equiv \iota + j \pmod{p-1}$. This proves Theorem (ii) and Theorem (iii) is an immediate consequence.

Thus indices can be used in connection with congruences in much the same way as logarithms are used in ordinary reckoning.

PRIMITIVE ROOTS AND INDICES

p	g	$x=$	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89
3	2	$i=$	1																							
5	2		1	3																						
7	3		2	1	5																					
11	2		1	8	4	7																				
13	6		5	8	9	7	11																			
17	10		10	11	7	9	13	12																		
19	10		17	5	2	12	6	13	8																	
23	10		8	20	15	21	3	12	17	5																
29	10		11	27	18	20	23	2	17	15	24															
31	17		12	13	20	4	29	23	1	22	21	27														
37	5		11	34	1	28	6	13	5	25	21	15	27													
41	6		26	15	22	39	3	31	33	9	36	7	28	32												
43	28		39	17	5	7	6	40	16	29	20	25	32	35	18											
47	10		30	18	17	38	27	3	42	29	39	43	5	24	25	37										
53	26		25	9	31	38	46	28	42	41	39	6	45	22	33	30	8									
59	10		25	32	34	44	45	23	14	22	27	4	7	41	2	13	53	28								
61	10		47	42	14	23	45	20	49	22	39	25	13	33	18	41	40	51	17							
67	12		29	9	39	7	61	23	8	26	20	22	43	44	19	63	64	3	54	5						
71	62		58	18	14	33	43	27	7	38	5	4	13	30	55	44	17	59	29	37	11					
73	5		8	6	1	33	55	59	21	62	46	35	11	64	4	51	31	53	5	58	50	44				
79	29		50	71	34	19	70	74	9	10	52	1	76	23	21	47	55	7	17	75	54	33	4			
83	50		3	52	81	24	72	67	4	59	16	36	32	60	38	49	69	13	20	34	53	17	43	47		
89	30		72	87	18	7	4	65	82	53	31	29	57	77	67	59	34	10	45	19	32	26	68	46	27	
97	10		86	2	11	53	82	83	19	27	79	47	26	41	71	44	60	14	65	32	51	25	20	42	91	18

With regard to the table opposite, the following points should be noticed:

(i) The first column contains the odd primes (p) less than 100, which are taken as moduli. Opposite to each of these, in the second column, is a primitive root (g).

If it happens that 10 is a primitive root, this number is chosen; otherwise we choose the primitive root for which 10 has the least index.

The row at the top contains the primes $x=2, 3, 5, \ldots$; and below are the indices ι corresponding to the various moduli, so that $x \equiv g^{\iota} \pmod{p}$.

(ii) The figures in the table may be calculated as follows: taking, for example, $p=43$, $g=28$, we find that $10 \equiv 28^2 \pmod{43}$. If, then, 1/43 and 28/43 are expressed as decimals, the remainders, starting with 1 and 28, are the numbers corresponding to the indices 0, 2, 4, 6, ... and 1, 3, 5, 7, ... respectively, and so we find

$$\begin{aligned} \text{ind}\, x = {} & 1, \quad 3, \quad 5, \quad 7, \ldots; \qquad 2, \quad 4, \quad 6, \quad 8, \ldots; \\ x = {} & 28, \quad 22, \quad 5, \quad 7, \ldots; \qquad 10, \quad 14, \quad 11, \quad 24, \ldots . \end{aligned}$$

(iii) In virtue of Theorems (ii), (iii), it is only necessary to record the indices of primes. We can thus find the index of any number, or the number corresponding to any index.

(iv) *The table shows whether any prime number x up to 89 is a quadratic residue or a non-residue of any odd prime modulus less than* 100.

For if xRp, a number y exists so that $y^2 \equiv x \pmod{p}$, and therefore $2 \text{ ind}\, y \equiv \text{ind}\, x \pmod{p-1}$. Hence xRp or xNp, according as $\text{ind}\, x$ is even or odd. For instance, 17, 19, 23, 29 are quadratic residues of 67, for the corresponding indices 8, 26, 20, 22 are even.

4. Application to Congruences. In every case the modulus p is supposed to be a prime.

(1) **The Linear Congruence.** If p is an odd prime, the congruence $ax \equiv b \pmod{p}$ has a single incongruent solution given by

$$\text{ind}\, a + \text{ind}\, x \equiv \text{ind}\, b \pmod{p-1} \quad \text{or} \quad \text{ind}\, x \equiv \text{ind}\, b - \text{ind}\, a \pmod{p-1}.$$

Thus,
$$\text{ind}\, b/a \equiv \text{ind}\, b - \text{ind}\, a \pmod{p-1}.$$

Ex. 1. *Solve* $40x \equiv 21 \pmod{43}$.

We have $\text{ind}\, x \equiv \text{ind}\, 21 - \text{ind}\, 40 \pmod{42}$, and since $21 = 3 \cdot 7$ and $40 = 2^3 \cdot 5$,

$$\text{ind}\, x \equiv 17 + 7 - (3 \cdot 39 + 5) \equiv 28 \pmod{42}.$$

Now 28 does not occur among the indices of primes, and so we look for the two or more indices whose sum $\equiv 28 \pmod{42}$. We find

$$28 = 17 + 5 + 6 = \text{ind}\, 3 + \text{ind}\, 5 + \text{ind}\, 11, \quad \text{or} \quad 28 = 4 \cdot 7 = 4 \text{ ind}\, 7;$$

$$x \equiv 3 \cdot 5 \cdot 11 \pmod{43} \equiv 165 \equiv 36 \pmod{43}, \quad \text{or} \quad x \equiv 7^4 \equiv 6^2 \equiv 36 \pmod{43}.$$

(2) **The Congruence $x^n \equiv a \pmod p$.** This relation is often written in the form $x \equiv \sqrt[n]{a} \pmod p$. Any solutions which may exist are given by

$$n \cdot \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}.$$

Moreover, any value of $\operatorname{ind} x$ which satisfies the last congruence corresponds to a solution of the first. The possible cases are as follows:

(i) If n is prime to $p-1$, there is a single solution.

(ii) If δ is the highest common divisor of n and $p-1$, and $\operatorname{ind} a$ is divisible by δ, there are δ incongruent solutions; but, if $\operatorname{ind} a$ is not divisible by δ, there is no solution.

All this follows at once from Art. 3.

Ex. 2. *Solve* (i) $x^5 \equiv 19 \pmod{79}$; (ii) $x^{21} \equiv 2 \pmod{31}$.

(i) $2 \operatorname{ind} x \equiv \operatorname{ind} 19 \equiv 10 \pmod{78}$, hence $\operatorname{ind} x \equiv 5, 44 \pmod{78}$.

If $\operatorname{ind} x \equiv 5 \equiv 83 \equiv 76 + 7 \equiv \operatorname{ind} 31 + \operatorname{ind} 53 \pmod{78}$, then $x \equiv 31 \cdot 53 \equiv 63 \pmod{79}$.

If $\operatorname{ind} x \equiv 44 \equiv 34 + 10 \equiv \operatorname{ind} 5 + \operatorname{ind} 19 \pmod{78}$, then $x \equiv 5 \cdot 19 \equiv 16 \pmod{79}$. Thus $x \equiv \pm 16 \pmod{79}$.

(ii) The highest common divisor of 21 and 30 is 3, and we may expect three incongruent solutions. We have $21 \operatorname{ind} x \equiv \operatorname{ind} 2 \equiv 12 \pmod{30}$, hence

$$\operatorname{ind} x \equiv 2, 12, 22 \pmod{30}.$$

If $\operatorname{ind} x \equiv 2 \equiv 32 \equiv 12 + 20 \equiv \operatorname{ind} 2 + \operatorname{ind} 5 \pmod{30}$, then $x \equiv 2 \cdot 5 \equiv 10 \pmod{31}$.

If $\operatorname{ind} x \equiv 12, 22 \pmod{30}$, then $x \equiv 2, 19 \pmod{31}$.

Thus the solutions are $x \equiv 2, 10, 19 \pmod{31}$.

EXERCISE XIII

1. For the congruence $x^3 \equiv a \pmod p$, where p is an odd prime, prove that (i) if p is of the form $3m+1$, there are three solutions or there is no solution, according as $\operatorname{ind} a$ is or is not divisible by 3; (ii) if p is of the form $3m-1$, there is one solution.

2. Solve (i) $x^3 \equiv 31 \pmod{37}$; (ii) $x^3 \equiv 2 \pmod{71}$.

3. If p is an odd prime, show that the congruence

$$x^4 + x^3 + x^2 + x + 1 \equiv 0 \pmod p$$

has four solutions or no solution, according as p is or is not of the form $5m+1$. Solve the congruence when $p = 41$.

4. Solve (i) $x^{11} \equiv 11 \pmod{19}$; (ii) $x^{15} \equiv 11 \pmod{19}$; (iii) $x^{21} \equiv 2 \pmod{31}$; (iv) $x^{20} \equiv 43 \pmod{97}$.

5. Use the tables to show that 7 is the smallest primitive root of 71: also find the values of $\operatorname{ind}_{62} 10$ and $\operatorname{ind}_7 10$.

6. Show that the indices given in the tables for $p = 79$, $g = 29$ may be found as follows: express $a/79$ as a decimal for $a = 1, 29, 51, 57, 73, 63$. The remainders (starting with 1, 29, etc.) are the numbers corresponding to the indices in the six groups $(0, 6, 12, \ldots)$, $(1, 7, 13, \ldots)$, $(2, 8, 14, \ldots)$, $\ldots$ $(5, 11, 17, \ldots)$ respectively.

CHAPTER XIII

THE EQUATION $x^n - 1 = 0$

NOTE. Most of this Chapter is taken from Gauss's *Recherches Arithmétiques*.

1. The Equation $x^n - 1 = 0$, where n is an Odd Prime.

Gauss discovered a remarkable process in which the solution of the equation, $x^n - 1 = 0$, is made to depend on that of equations of lower degree. His method requires the use of a primitive root of n, and the first step is to divide the set of imaginary roots into groups of a special kind.

(1) Let α be any imaginary root of $x^n - 1 = 0$; then the complete set of imaginary roots is

$$\alpha,\ \alpha^2,\ \alpha^3,\ \ldots\ \alpha^{n-1}, \qquad \text{.....(A)}$$

For convenience α^λ is denoted by $[\lambda]$, so that

$$[0] = 1, \quad [\lambda] \times [\mu] = [\lambda + \mu], \quad [\lambda]^\mu = [\lambda\mu].$$

Also $[\lambda] = [\mu]$ if and only if $\lambda \equiv \mu \pmod{n}$, for $\alpha^n = 1$.

(2) *Let g be any primitive root of n; then, except as regards order, the set* (A) *is the same as*

$$[1],\ [g],\ [g^2],\ \ldots\ [g^{n-2}]. \qquad \text{.....(B)}$$

More generally, the set (A) *is the same as*

$$[\lambda],\ [\lambda g],\ [\lambda g^2],\ \ldots\ [\lambda g^{n-2}], \qquad \text{.....(C)}$$

where λ is any number not divisible by n.

For, apart from order, $\lambda,\ \lambda g,\ \lambda g^2,\ \ldots\ \lambda g^{n-2} \equiv 1,\ 2,\ 3,\ \ldots\ n-1 \pmod{n}$.

(3) *If λ is not divisible by n and $[\lambda g^\mu] = [\lambda g^\nu]$, then $\mu \equiv \nu \pmod{n-1}$, and conversely.*

For if $[\lambda g^\mu] = [\lambda g^\nu]$, then $\lambda g^\mu \equiv \lambda g^\nu \pmod{n}$. Therefore $g^{\mu-\nu} \equiv 1 \pmod{n}$, and, since g is a primitive root, $\mu - \nu$ is equal to or is a multiple of $n-1$. The converse is obviously true.

(4) *Let e be any divisor of $n-1$, and let $n-1 = ef$. Suppose that G, g are any two primitive roots of n and $G^e = H$, $g^e = h$. Then, except as regards order, the two sets of roots*

$$[\lambda],\ [\lambda H],\ [\lambda H^2],\ \ldots\ [\lambda H^{f-1}] \quad \textit{and} \quad [\lambda],\ [\lambda h],\ [\lambda h^2]\ \ldots\ [\lambda h^{f-1}]$$

are identical.

For no two roots of either set are equal, hence it is sufficient to show

that for any number $\mu < f$ there is a number $\nu < f$ such that $[\lambda h^\nu] = [\lambda H^\mu]$.

Let $G = g^\omega$, then $[\lambda h^\nu] = [\lambda H^\mu]$ if $h^\nu \equiv H^\mu \pmod n$, that is if

$$g^{\nu e} \equiv g^{\mu\omega e} \pmod n,$$

or if $\nu e \equiv \mu\omega e \pmod{n-1}$, or if $\nu \equiv \mu\omega \pmod f$.

Hence if ν is the least positive residue of $\mu\omega \pmod f$, then

$$[\lambda h^\nu] = [\lambda H^\mu].$$

(5) Thus the group $[\lambda]$, $[\lambda h]$, $[\lambda h^2]$, ... $[\lambda h^{f-1}]$ consists of exactly the same roots, no matter what primitive root g may stand for. This group is called a *period, and is denoted by* (f, λ).

The symbol (f, λ) is also used to denote the *sum* of the f roots in the period, so that

$$(f, \lambda) = [\lambda] + [\lambda h] + [\lambda h^2] + \ldots + [\lambda h^{f-1}],$$

whence we have $$(f, 0) = (f, kn) = f.$$

(6) Since $\lambda h^f = \lambda g^{n-1} \equiv \lambda$, $\lambda h^{f+1} \equiv \lambda h \pmod n$, etc., we have

$$(f, \lambda) = (f, \lambda h) = (f, \lambda h^2) = \ldots .$$

Thus if $[\lambda']$ is any root in the period (f, λ), then

$$(f, \lambda') = (f, \lambda).$$

(7) The complete period (A) of the imaginary roots is made up of the periods

$$(f, 1),\ (f, g),\ (f, g^2),\ \ldots\ (f, g^{e-1}).$$

More generally, (A) consists of the periods

$$(f, \lambda),\ (f, \lambda g),\ (f, \lambda g^2),\ \ldots\ (f, \lambda g^{e-1}),$$

where λ is any number not divisible by n.

In particular, the period (A) is represented by $(n-1, 1)$ or by $(n-1, \lambda)$.

(8) *The product of the roots in any period* (f, λ) *is equal to* 1, *excepting the case in which the period consists of a single root.*

For, denoting the product by P, we have

$$P = [\lambda + \lambda h + \lambda h^2 + \ldots + \lambda h^{f-1}] \quad \text{where} \quad h = g^e$$

and $$\lambda + \lambda h + \ldots + \lambda h^{f-1} = \lambda \cdot \frac{h^f - 1}{h - 1} = \lambda \frac{g^{ef} - 1}{g^e - 1}.$$

Now $g^{ef} - 1 = g^{n-1} - 1 \equiv 0 \pmod n$, and since g is a primitive root, g^e is not congruent with 1 $\pmod n$ unless $e = n-1$, in which case the period consists of a single root. Excepting this case, it follows that

$$\lambda + \lambda h + \ldots + \lambda h^{f-1} \equiv 0 \pmod n \quad \text{and} \quad P = [0] = 1.$$

(9) *The equation* $x^{19} - 1 = 0$. (i) Here $n - 1 = 3 \cdot 3 \cdot 2$, and it will be

shown that the solution depends on that of two cubic equations and one quadratic.

Taking $g=2$, a primitive root of 19, the least positive residues of $2^0, 2^1, 2^2, \dots 2^{17} \pmod{19}$ are

Index	0 . 1 . 2 . 3 . 4 . 5 . 6 . 7 . 8 . 9 . 10 . 11 . 12 . 13 . 14 . 15 . 16 . 17.
Residue	1 . 2 . 4 . 8 . 16 . 13 . 7 . 14 . 9 . 18 . 17 . 15 . 11 . 3 . 6 . 12 . 5 . 10.

The complete set (A) of imaginary roots, forming the period (18, 1), is made up of three periods each of 6 roots, thus

$$(18,1)\begin{cases}(6,1)=[1]+[8]+[7]+[18]+[11]+[12]=p_1,\\(6,2)=[2]+[16]+[14]+[17]+[3]+[5]=p_2,\\(6,4)=[4]+[13]+[9]+[15]+[6]+[10]=p_3.\end{cases}$$

The reader should notice such equalities as

$$(6,1)=(6,8)=(6,7), \quad (6,2)=(6,3)=(6,5).$$

Again, the periods (6, 1), (6, 2), (6, 4) are made up of three periods each of 2 roots, thus :

$$(6,1)\begin{cases}(2,1)=[1]+[18]=q_1,\\(2,8)=[8]+[11]=q_2,\\(2,7)=[7]+[12]=q_3.\end{cases} \qquad (6,2)\begin{cases}(2,2)=[2]+[17]=r_1,\\(2,16)=[16]+[3]=r_2,\\(2,14)=[14]+[5]=r_3.\end{cases}$$

$$(6,4)\begin{cases}(2,4)=[4]+[15]=s_1,\\(2,13)=[13]+[6]=s_2,\\(2,9)=[9]+[10]=s_3.\end{cases}$$

The next step is to find the equations of which the roots are (6, 1), (6, 2), (6, 4) and (2, 1), (2, 8), (2, 7).

To do this we require an easy way of finding such products as

$$(f,\lambda)\times(f,\mu).$$

and we shall return to this equation later.

(10) **Products.** *Let* (f,λ), (f,μ) *be two sums of* f *roots, identical or different, and let*

$$(f,\lambda)=[\lambda]+[\lambda']+[\lambda'']+\dots,$$

then
$$(f,\lambda)\times(f,\mu)=(f,\lambda+\mu)+(f,\lambda'+\mu)+(f,\lambda''+\mu)+\dots,$$

the series being continued to f *terms.*

As in the preceding, $n-1=ef$, g is a primitive root of n and $h=g^e$. Thus

$$(f,\lambda)=[\lambda]+[\lambda h]+[\lambda h^2]+\dots, \quad (f,\mu)=[\mu]+[\mu h]+[\mu h^2]+\dots$$

and
$$(f,\lambda)=(f,\lambda h)=(f,\lambda h^2)=\dots.$$

Hence

$$(f,\lambda)\times(f,\mu)=[\mu].(f,\lambda)+[\mu h].(f,\lambda h)+[\mu h^2].(f,\lambda h^2)+\dots.$$

Expanding each term and noting that $[\lambda].[\mu]=[\lambda+\mu]$, the product is equal to

$$\left.\begin{array}{l}[\lambda+\mu] \quad +[\lambda h+\mu] \quad +[\lambda h^2+\mu] \quad +\ldots+[\lambda h^{f-1}+\mu] \\ +[\lambda h+\mu h] \quad +[\lambda h^2+\mu h] \quad +[\lambda h^3+\mu h] \quad +\ldots+[\lambda h^f+\mu h] \\ +[\lambda h^2+\mu h^2]+[\lambda h^3+\mu h^2]+[\lambda h^4+\mu h^2]+\ldots+[\lambda h^{f+1}+\mu h^2] \\ +\text{etc., to } f \text{ rows.}\end{array}\right\} \quad \ldots\ldots\text{(D)}$$

Adding by columns, the product is equal to

$$(f, \lambda+\mu)+(f, \lambda h+\mu)+(f, \lambda h^2+\mu)+\ldots+(f, \lambda h^{f-1})+\mu), \quad \ldots\ldots\text{(E)}$$

which is the result stated in the enunciation, for

$$\lambda'+\mu \equiv \lambda h+\mu, \quad \lambda''+\mu \equiv \lambda h^2+\mu \pmod{n}, \text{ etc.}$$

(11) Every term in (E) is identical with one of the set

$$(f, 0), \quad (f, 1), \quad (f, g), \quad (f, g^2), \quad \ldots \quad (f, g^{e-1}).$$

Therefore $(f, \lambda)\times(f, \mu)$ may be expressed in the form

$$a_0(f, 0)+a_1(f, 1)+a_2(f, g)+a_3(f, g^2)+\ldots+a_e(f, g^{e-1}), \quad \ldots\ldots\text{(F)}$$

or in the form

$$a_0(f, 0)+a_1(f, k)+a_2(f, kg)+a_3(f, kg^2)+\ldots+a_e(f, kg^{e-1}), \quad \ldots\ldots\text{(G)}$$

where $a_0, a_1, a_2, \ldots$ are positive integers or zero and k is any number not divisible by n.

Thus, for the equation $x^{19}-1=0$, we have

$$(6, 1)=[1]+[8]+[7]+[18]+[11]+[12];$$

$$\begin{aligned}\therefore\ (6, 1)^2 &= (6, 2)+(6, 9)+(6, 8)+(6, 19)+(6, 12)+(6, 13) \\ &= (6, 2)+(6, 4)+(6, 1)+(6, 0)+(6, 1)+(6, 4) \\ &= 6+2(6, 1)+(6, 2)+2(6, 4).\end{aligned}$$

$$\begin{aligned}(6, 1)\times(6, 2) &= (6, 3)+(6, 10)+(6, 9)+(6, 20)+(6, 13)+(6, 14) \\ &= (6, 2)+(6, 4)+(6, 4)+(6, 1)+(6, 4)+(6, 2) \\ &= (6, 1)+2(6, 2)+3(6, 4).\end{aligned}$$

Again, the expression (D) contains f^2 terms, and each of the periods $(f, 0)$, $(f, 1)$, ... consists of f of these terms.

Hence $$f^2=a_0f+a_1f+a_2f+\ldots;$$

therefore $$a_0+a_1+a_2+\ldots+a_e=f. \quad \ldots\ldots\text{(H)}$$

Moreover, $a_0=1$ *or* 0 *according as* s *is or is not divisible by* e, *where* $-\mu/\lambda \equiv g^s \pmod{n}$ *and* $0 \leqslant s < n$. *Also if* $\lambda=\mu$, *then* $a_0=1$ *or* 0 *according as* f *is even or odd.*

For just one value of s satisfies the conditions, and if $(f, \lambda h^x+\mu)=(f, 0)$, then $\lambda h^x+\mu \equiv 0 \pmod{n}$ and $h^x=g^{ex} \equiv g^s \pmod{n}$.

Therefore $$ex \equiv s \pmod{ef}.$$

This congruence has a single solution $<f$ or no solution, according as s is or is not divisible by e, which proves the first part.

If $\lambda=\mu$, then $s=\frac{1}{2}ef$, and there is one solution or no solution, according as f is even or odd.

(12) Hence if $\lambda, \mu, \nu, \ldots$ are any whole numbers, any rational integral function u of (f, λ) (f, μ), (f, ν), ... can be expressed in the form

$$a_0+a_1(f, k)+a_2(f, kg)+a_3(f, kg^2)+\ldots+a_e(f, kg^{e-1}),$$

where k is any number not divisible by n and $a_0, a_1, a_2, \ldots$ are definite numbers. Also if the coefficients in u are whole numbers, so also are $a_0, a_1, a_2, \ldots$.

(13) The complete period $(n-1, 1)$ of imaginary roots is made up of the e periods

$$(f, \lambda), (f, \lambda g), (f, \lambda g^2), \ldots (f, \lambda g^{e-1}),$$

where λ is any number not divisible by n.

These periods will be denoted by $p_1, p_2, p_3, \ldots p_e$.

Theorem. *If u is any symmetric function of $p_1, p_2, \ldots p_e$ with integral coefficients, the value of u is a definite whole number.*

By the preceding

$$u=a_0+a_1p_1+a_2p_2+\ldots+a_ep_e$$

where $a_0, a_1, \ldots$ are integers or zero; and there is only one way of expressing u in this form.

Again, if λg is written for λ, then p_1 is changed to p_2, p_2 to p_3, ... p_e to p_1, and the value of u is unaltered. Hence

$$u=a_0+a_1p_2+a_2p_3+\ldots+a_ep_1,$$

and since the expression for u is unique,

$$a_1=a_2=a_3=\ldots=a_e$$

and $$u=a_0+a_1(p_1+p_2+\ldots+p_e)=a_0-a_1,$$

Hence *if the equation whose roots are $p_1, p_2, p_3, \ldots p_e$ is*

$$x^e+Ax^{e-1}+Bx^{e-2}+\ldots+K=0,$$

then $A, B, \ldots K$ are whole numbers.

Here $A=-(p_1+p_2+\ldots+p_e)=1$, and we shall prove that

$$\Sigma p_1^2=n-f \text{ or } -f \text{ and } B=\Sigma p_1p_2=-\tfrac{1}{2}(n-1-f) \text{ or } \tfrac{1}{2}(1+f), \quad \ldots\ldots(\text{I})$$

according as f is even or odd.

Let $$p_1^2=a_0f+a_1p_1+a_2p_2+\ldots+a_ep_e.$$

We may change p_1 to p_2, p_2 to p_3, ... p_e to p_1; hence we have

$$p_2^2=a_0f+a_1p_2+a_2p_3+\ldots+a_ep_1,$$

with $e-2$ similar equations, namely,

$$p_3^2 = a_0 f + a_1 p_3 + a_2 p_4 + \ldots + a_e p_2,$$
$$p_4^2 = a_0 f + a_1 p_4 + a_2 p_5 + \ldots + a_e p_3,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$p_e^2 = a_0 f + a_1 p_e + a_2 p_1 + \ldots + a_e p_{e-1};$$

whence, by addition, $\Sigma p_1^2 = a_0 ef + (a_1 + a_2 + \ldots + a_e) \cdot \Sigma p_1$

$$= a_0(n-1) - (f - a_0)$$
$$= a_0 n - f,$$

and $$2\Sigma p_1 p_2 = (\Sigma p_1)^2 - \Sigma p_1^2 = 1 + f - a_0 n.$$

Also by (11) $a_0 = 1$ or 0, according as f is even or odd.

(14) *If* (f, λ), (f, μ) *are any periods of* f *roots, then* (f, μ) *can be expressed in the form*

$$a_0 + a_1 p_1 + a_2 p_1^2 + \ldots + a_{e-1} p_1^{e-1},$$

where $p_1 = (f, \lambda)$ *and* $a_0, a_1, \ldots$ *are definite rational numbers.*

For with the notation of (13),

$$0 = 1 + p_1 + p_2 + \ldots + p_e,$$

and by (10) we can find $e-2$ equations of the form

$$p_1^2 = b_0 + b_1 p_1 + b_2 p_2 + \ldots + b_e p_e,$$
$$p_1^3 = c_0 + c_1 p_1 + c_2 p_2 + \ldots + c_e p_e,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$p_1^{e-1} = k_0 + k_1 p_1 + k_2 p_2 + \ldots + k_e p_e,$$

where the constants are whole numbers, independent of λ.

Let $(f, \mu) = p_r$, then by eliminating $e-2$ of the periods $p_2, p_3, \ldots p_e$ we can obtain the equation

$$M p_r = l_0 + l_1 p_1 + l_2 p_1^2 + \ldots + l_{e-1} p_1^{e-1},$$

where M, l_0, l_1, etc., are rationals independent of λ.

It will be found that M is never zero, but a general proof of this statement is too long to give here.

(15) Let $n - 1 = ef = ef_1 f_2$ and $h = g^e$, then

$$(f, \lambda) = [\lambda] + [\lambda h] + [\lambda h^2] + \ldots + [h\lambda^{f-1}],$$
$$(f_1, \lambda) = [\lambda] + [\lambda h^{f_2}] + [\lambda h^{2f_2}] + \ldots + [\lambda h^{(f_1-1)f_2}].$$

Therefore (f, λ) is made up of the f_2 periods

$$(f_1, \lambda), \quad (f_1, \lambda h), \quad (f_1, \lambda h^2), \ldots \quad (f_1, \lambda h^{f_2-1}). \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(J)}$$

Denote these by $q_1, q_2, q_3, \ldots q_{f_2}$; and observe that if λh is written for λ, then q_1 is changed to q_2, q_2 to q_3, $\ldots$, q_{f_2} to q_1.

We shall prove that *if u is a symmetric function of $q_1, q_2, \dots q_{f_2}$ with integral coefficients, then*

$$u=a_0+a_1(f,\lambda)+a_2(f,\lambda g)+a_3(f,\lambda g^2)+\dots+a_e(f,\lambda g^{e-1}), \quad \dots\dots(\mathrm{K})$$

where $a_0, a_1, a_2, \dots$ are integers or zero.

For by (12)

$$u=a_0+a_1(f_1,\lambda)+a_2(f_1,\lambda g)+a_3(f_1,\lambda g^2)+\dots+a_{ef_2}(f,\lambda g^{ef_2-1}),$$

where a_0, a_1, a_2, etc., are definite whole numbers.

Let λh, that is λg^e, be written for λ. Since u is a symmetric function of $q_1, q_2, \dots q_{f_2}$, its value is unaltered.

Also, if $r \leqslant e(f_2-1)$, the term $a_r(f,\lambda g^{r-1})$ becomes $a_r(f,\lambda g^{e+r-1})$, and since the expression for u is unique, it follows that $a_r=a_{e+r}$.

Hence $u=a_0+\sum_{s=1}^{s=e} a_s A_s$ where

$$A_s=(f_1,\lambda g^{s-1})+(f_1,\lambda g^{s-1}.h)+(f_1,\lambda g^{s-1}.h^2)+\dots \text{ to } f_2 \text{ terms}$$
$$=(f,\lambda g^{s-1}).$$

In particular, *any symmetric function of the roots which compose the period (f,λ), with integral coefficients, can be expressed as in* (K).

For in this case $f_1=1$.

(16) *The equation* $x^{19}-1=0$. Using the notation of (9), we proceed to find the equation of which the roots are p_1, p_2, p_3, where

$$p_1=(6,1), \quad p_2=(6,2), \quad p_3=(6,4).$$

We have $p_1+p_2+p_3=-1$; and, as in (11), $p_1p_2=p_1+2p_2+3p_3$.

If the roots of $x^{19}-1=0$ are written $[\lambda]$, $[\lambda g]$, $[\lambda g^2]$, ... where $g=2$, $\lambda=1$, the substitution of λg for g is equivalent to the cyclic substitution (p_1, p_2, p_3). So in the last equation, we may change p_1 to p_2, p_2 to p_3 and p_3 to p_1. Hence

$$p_2p_3=p_2+2p_3+3p_1 \quad \text{and} \quad p_3p_1=p_3+2p_1+3p_2;$$
$$\Sigma p_1p_2=(1+2+3)(-1)=-6.$$

This also follows from (13), (I), by putting $n=19$, $f=6$.

Again $p_1p_2p_3=p_1(p_2+2p_3+3p_1)=-p_1(3+2p_2+p_3)$;

therefore $p_1p_2p_3=-3p_1-2(p_1+2p_2+3p_3)-(p_3+2p_1+3p_2)=7$.

Hence the equation whose roots are p_1, p_2, p_3 is

$$x^3+x^2-6x-7=0. \quad \dots\dots(\mathrm{L})$$

Now p_1 may be taken as *any* root of this equation, and then p_2, p_3 are determined by

$$p_1+p_2+p_3=-1, \quad p_1^2=6+2p_1+p_2+2p_3, \text{ as found in (11)};$$

from which, $p_2=4-p_1^2$, $p_3=-5-p_1+p_1^2$.

By Horner's method one root of (L) is $-1{\cdot}2218761623$, and taking this as the value of p_1, we find that

$$p_2 = 2{\cdot}5070186441, \quad p_3 = -2{\cdot}2851424818.$$

We next find the equation of which the roots are q_1, q_2, q_3, where

$$q_1 = (2, 1), \quad q_2 = (2, 8), \quad q_3 = (2, 7).$$

We have $q_1 + q_2 + q_3 = (6, 1) = p_1$ and $(2, 1) = [1] + [18]$, thus

$$q_1 q_2 = (2, 1) \times (2, 8) = (2, 9) + (2, 26) = (2, 9) + (2, 7) = s_3 + q_3.$$

Representing the roots of $x^{19} - 1 = 0$ as in the preceding, the substitution of λg^3 for λ involves the cyclic substitutions (q_1, q_2, q_3), (r_1, r_2, r_3), (s_1, s_2, s_3).

Therefore $$q_2 q_3 = s_1 + q_1 \quad \text{and} \quad q_3 q_1 = s_2 + q_2,$$

and $$\Sigma q_1 q_2 = (6, 4) + (6, 1) = p_3 + p_1.$$

Also $$q_1 q_2 q_3 = (2, 1)\{(2, 4) + (2, 1)\},$$

and
$$(2, 1) \times (2, 4) = (2, 5) + (2, 22) = (2, 14) + (2, 16),$$
$$(2, 1) \times (2, 1) = (2, 2) + (2, 0) = (2, 2) + 2.$$

Therefore $$q_1 q_2 q_3 = 2 + (6, 2) = 2 + p_2.$$

Hence the equation whose roots are q_1, q_2, q_3 is

$$x^3 - p_1 x^2 + (p_1 + p_3)x - (2 + p_2) = 0. \quad \text{.....(M)}$$

Now q_1 may be taken as *any* root of this equation, and then all the periods $(2, 2)$, $(2, 3)$, ... $(2, 9)$ are expressed in terms of q_1 by the equations; for, if $[1]$ is denoted by a, $q_1 = a + \dfrac{1}{a}$

and $(2, 2) = a^2 + \dfrac{1}{a^2} = q_1^2 - 2,$ $\qquad (2, 3) = a^3 + \dfrac{1}{a^3} = q_1^3 - 3q_1,$

$(2, 4) = a^4 + \dfrac{1}{a^4} = q_1^4 - 4q_1^2 + 2,$ $\qquad (2, 5) = a^5 + \dfrac{1}{a^5} = q_1^5 - 5q_1^3 + 5q_1,$

and so on.

Using the values already given for p_1, p_2, p_3, we find that one root of equation (M) is $-1{\cdot}3545631433$, and this is taken as the value of q_1.

Again, we must have $[1] = \cos\omega + \iota \sin\omega$ where $\omega = \dfrac{2k\pi}{19}$ and k is a positive integer. Hence $[18] = \cos\omega - \iota \sin\omega$ and

$$(2, 1) = 2\cos\omega, \quad (2, \lambda) = 2\cos\lambda\omega.$$

Since $\cos\omega = \frac{1}{2}q_1 = -0{\cdot}6772 \ldots$, reference to any trigonometrical table shows that $k = 7$, thus

$$(2, 1) = 2\cos\frac{14\pi}{19}, \quad (2, 8) = 2\cos\frac{2\pi}{19}.$$

Hence we can show that

$$2\cos\frac{2\pi}{19} = 1{\cdot}8916344834.$$

Finally, [1], [18] are the roots of $x^2-q_1x+1=0$, ...(N)

giving $$x=\tfrac{1}{2}q_1\pm\frac{i}{2}\sqrt{(4-q_1^2)}.$$

Thus the complete solution of $x^{19}-1=0$ depends on that of equations (L), (M) and (N).

It should be noticed that the periods (2, 2), (2, 16), (2, 14) which compose (6, 2) are the roots of

$$x^3-p_2x^2+(p_2+p_1)x-(2+p_3)=0,$$

obtained by the cyclic substitution (p_1, p_2, p_3) from equation (M).

Similarly (2, 4), (2, 13), (2, 9) composing (6, 4) are the roots of

$$x^3-p_3x^2+(p_3+p_2)x-(2+p_1)=0.$$

If (2, 2), etc., are found in this way, they can be identified by the method explained in Exercise XIV, Exx. 2, 3.

(17) *The equation* $x^{17}-1=0$. Since $17-1=2^4$, we may expect that solution to depend on four quadratic equations.

Taking $g=3$, a primitive root of 17, the least positive residues of 3^0, 3^1, 3^2, etc., are as below.

Index	0 . 1 . 2 . 3 . 4 . 5 . 6 . 7 . 8 . 9 . 10 . 11 . 12 . 13 . 14 . 15.
Residue	1 . 3 . 9 . 10 . 13 . 5 . 15 . 11 . 16 . 14 . 8 . 7 . 4 . 12 . 2 . 6.

The set of irrational roots is divided into periods as follows.

$$p_1=(8,1)\begin{cases} q_1=(4,1)\begin{cases}(2,1)=z_1\\(2,13)=z_4\end{cases}\\ q_3=(4,9)\begin{cases}(2,9)=z_8\\(2,15)=z_2\end{cases}\end{cases}\qquad p_2=(8,2)\begin{cases} q_2=(4,3)\begin{cases}(2,3)=z_3\\(2,5)=z_5\end{cases}\\ q_4=(4,10)\begin{cases}(2,10)=z_7\\(2,11)=z_6.\end{cases}\end{cases}$$

(i) If the roots of $x^{17}-1=0$ are denoted by $[k]$, $[kg]$, $[kg^2]$, ... where $k=1$, $g=3$, the substitution of kg for k is equivalent to the transposition (p_1p_2), and involves the cyclic substitution $(q_1q_2q_3q_4)$.

(ii) By (13), or using the rule in (10),

p_1, p_2 are the roots of $x^2+x-4=0$. .....(O)

We choose p_1 as the positive root, so that

$$p_1=-\tfrac{1}{2}+\tfrac{1}{2}\sqrt{17}=\ \ 1{\cdot}5615528128,$$
$$p_2=-\tfrac{1}{2}-\tfrac{1}{2}\sqrt{17}=-2{\cdot}5615528128.$$

(iii) We now find the equation of which the roots are q_1, q_3, the periods composing p_1. We have $q_1+q_3=p_1$, and

$$q_1q_3=(4,10)+(4,22)+(4,25)+(4,13)=p_1+p_2=-1.$$

Thus q_1, q_3 are the roots of $x^2-p_1x-1=0$. .....(P)

We choose q_1 as the positive root, so that

$$q_1 = \tfrac{1}{2}p_1 + \sqrt{(p_1^2+4)} = \tfrac{1}{2}p_1 + \tfrac{1}{2}\sqrt{(8-p_1)} = 2{\cdot}0494811777,$$
$$q_3 = \tfrac{1}{2}p_1 - \sqrt{(8-p_1)} = -0{\cdot}4879283649.$$

Making the substitution (i) in equation (P),

q_2, q_4 are the roots of $x^2 - p_2x - 1 = 0$. .....(Q)

To identify these, we can easily show that

$$(q_1 - q_3)(q_2 - q_4) = 2(p_1 - p_2) > 0,$$

so that $q_2 > q_4$ and

$$q_2 = \tfrac{1}{2}p_2 + \tfrac{1}{2}\sqrt{(8-p_2)} = \quad 0{\cdot}3441507314,$$
$$q_4 = \tfrac{1}{2}p_2 - \tfrac{1}{2}\sqrt{(8-p_2)} = -2{\cdot}9057035442.$$

(iv) To find the equation of which the roots are z_1, z_4, the periods composing q_1, we have $z_1 + z_4 = q_1$ and $z_1 z_4 = q_2$, hence

z_1, z_4 are the roots of $x^2 - q_1x + q_2 = 0$. .....(R)

Taking z_1 as the greater root, it is easily shown that

$$q_1^2 - 4q_2 = 4 + q_3 - 2q_2,$$

so that

$$z_1 = \tfrac{1}{2}q_1 + \tfrac{1}{2}\sqrt{(4 + q_3 - 2q_2)} = 1{\cdot}8649444588,$$
$$z_4 = \tfrac{1}{2}q_1 - \tfrac{1}{2}\sqrt{(4 + q_3 - 2q_2)} = 0{\cdot}1845367189.$$

It follows from (i) and (R) that

z_3, z_5 are the roots of $x^2 - q_2x + q_3 = 0$, ...(S)

z_8, z_2 are the roots of $x^2 - q_3x + q_4 = 0$, ...(T)

z_7, z_6 are the roots of $x^2 - q_4x + q_1 = 0$. .....(U)

To identify these, we find that

$$(z_1 - z_4)(z_3 - z_5) = q_3 - q_4 > 0, \quad (z_3 - z_5)(z_8 - z_2) = q_4 - q_1 < 0,$$
$$(z_8 - z_2)(z_7 - z_6) = q_1 - q_2 > 0,$$

so that z_3, z_2, z_6 are the greater roots of (S), (T), (U).

Thus every z can be calculated, and if this is done it will be found that z_1 is the greatest, and consequently

$$\cos\frac{2\pi}{17} = \tfrac{1}{2}z_1 = 0{\cdot}9324722294.$$

With appropriate changes, equations (O)-(U) are the same as those of *H.A.*, Art. 5, (K), ... 174.

In the same way ... *equation* $x^n - 1 = 0$ *can be solved by quadratic equations if* n *is a prime* ... *the form* $2^n + 1$.

(18) *The periods* $(m, 1)$ ... *and* (m, g) *where* $n - 1 = 2m$. These periods make up the complete set of ... imaginary roots of $x^n - 1 = 0$.

Also, $(m, 1)=[1]+[g^2]+[g^4]+\ldots=[1]+[R]+[R']+\ldots,$

$(m, g)=[g]+[g^3]+[g^5]+\ldots=[N]+[N']+[N'']+\ldots,$

where R, R', ... and N, N', ... are respectively the residues and the non-residues of n. For obviously 1, R, R', ... are residues; they are all different, and their number is $\frac{1}{2}(n-1)$. Hence N, N', ..., which are all different from one another and from 1, R, R', ..., are non-residues.

Again, $(m, 1)+(m, g)=-1$, and putting $f=m$ in (13), (I), we have

$$(m, 1)\times(m, g)=-\tfrac{1}{2}(2m-m)=-\tfrac{1}{4}(n-1) \text{ when } m \text{ is even},$$

$$(m, 1)\times(m, g)=\tfrac{1}{2}(1+m)=\tfrac{1}{4}(n+1) \text{ when } m \text{ is odd}.$$

Hence, according as n is of the form $4k+1$ or $4k-1$, *the equation of which the roots are* $(m, 1)$, (m, g) *is*

$$x^2+x-\tfrac{1}{4}(n-1)=0 \quad \text{or} \quad x^2+x+\tfrac{1}{4}(n+1)=0; \quad \ldots\ldots\ldots\ldots(\mathrm{V})$$

and

$$\{(m, 1)-(m, g)\}^2=+n \quad \text{or} \quad -n, \quad \ldots\ldots\ldots\ldots(\mathrm{W})$$

(19) *If n is an odd prime, $n-1=2m$ and $u=x^{n-1}+x^{n-2}+\ldots+x+1$, then polynomials X, Y of degrees m and $m-1$ respectively and with integral coefficients can be found such that $4u=X^2-nY^2$ or $4u=X^2+nY^2$ according as n is of the form $4k+1$ or $4k-1$.*

Let the equations, of which the roots are those contained in the periods $(m, 1)$ and (m, g) respectively, be

$$z\equiv x^m+a_1x^{m-1}+a_2x^{m-2}+\ldots+a_m=0, \quad \ldots\ldots\ldots\ldots(\mathrm{X})$$

$$z'\equiv x^m+a_1'x^{m-1}+a_2'x^{m-2}+\ldots+a_m'=0. \quad \ldots\ldots\ldots\ldots(\mathrm{Y})$$

Now, by (15), a_1, a_2, ..., a_m, can be expressed as $A+B(m, 1)+C(m, g)$, where A, B, C are whole numbers; for they are symmetric functions with integral coefficients of the roots in $(m, 1)$. Therefore

$$z=R+S(m, 1)+T(m, g),$$

where R, S, T are polynomials in x with integral coefficients.

If the roots of $u=0$ are represented by $[\lambda]$, $[\lambda g]$, $[\lambda g^2]$, etc., where $\lambda=1$, and λg is substituted for λ, then $(m, 1)$ is changed to (m, g), (m, g) to $(m, g^2)=(m, 1)$ and z to z'. Hence $z'=R+S(m, g)+T(m, 1)$.

Therefore, $z+z'=2R+(S+T)\{(m, 1)+(m, g)\}=2R-S-T$,

$$z-z'=(S-T)\{(m, 1)-(m, g)\}.$$

Also $u=zz'$ and $\{(m, 1)-(m, g)\}^2=\pm n$, therefore $4u=X^2\mp nY^2$,

where $X=2R-S-T$, $Y=S-T$, and the upper or lower sign is to be taken according as n is of the form $4k+1$ or $4k-1$.

It is easily seen that the highest terms in X are $2x^m+x^{m-1}$, that in Y being x^{m-1}. In calculating the coefficients of z, z', observe that the interchange of $(m, 1)$ and (m, g) transforms $a_1, a_2, \ldots$ into $a_1', a_2', \ldots$.

Also by (8), $$a_m = a_m' = (-1)^m.$$

Again, if $[\lambda]$ is any root in $(m, 1)$, then since $\lambda g^m \equiv -\lambda \pmod n$, the root $[-\lambda]$ belongs to $(m, 1)$ or (m, g), according as m is even or odd.

Hence *if m is even*, $z=0$ is a reciprocal equation and $a_{m-r}=a_r$.

If m is odd, z is transformed into z' by writing $1/x$ for x in z and multiplying by x^m. Therefore $a_{m-r}=-a_r'$.

The values of $a_1, a_2, \ldots$ may be found as follows: let s_r be the sum of the rth powers of the roots in $(m, 1)$, then $s_r=(m, 1)$ or (m, g), *according as* $[r]$ *belongs to* $(m, 1)$ *or to* (m, g). For if $[\lambda]$ is any root in $(m, 1)$ and $r \equiv g^s \pmod n$, then $[r\lambda]$ belongs to $(m, 1)$ or (m, g), according as s is even or odd. Hence we can find $a_1, a_2, \ldots$ by Newton's theorem.

Ex. 1. *If $u=x^{18}+x^{17}+\ldots+x+1$, it is required to express $4u$ in the form X^2+19Y^2.*
Here $n=19$, $m=9$, and, taking $g=2$, we have

$$(9, 1)=[1]+[4]+[16]+[7]+[9]+[17]+[11]+[6]+[5],$$
$$(9, 2)=[2]+[8]+[13]+[14]+[18]+[15]+[3]+[12]+[10].$$

Let $p=(9, 1)$, $q=(9, 2)$, then we find that $p^2=4p+5q$ and $-pq=5$.
Let the equations whose roots are those in $(9, 1)$, $(9, 2)$ respectively be

$$z=x^9+a_1x^8+a_2x^7+\ldots+a_8x-1=0,$$
$$z'=x^9+a_1'x^8+a_2'x^7+\ldots+a_8'-1=0,$$

and let s_r be the sum of the rth powers of the roots of $z=0$, then

$$s_1=p, \quad s_2=q, \quad s_3=q, \quad s_4=p.$$

Using Newton's theorem, a_1, a_2, a_3, a_4 are given by

$$p+a_1=0, \qquad q+a_1p+2a_2=0,$$
$$q+a_1q+a_2p+3a_3=0, \qquad p+a_1q+a_2q+a_3p+4a_4=0.$$

The values of $a_1', a_2', \ldots$ are found from those of $a_1, a_2, \ldots$ by interchanging p and q, also $a_8=-a_1'$, $a_7=-a_2'$, $a_6=-a_3'$, $a_5=-a_4'$. Hence

$$\begin{array}{lll} a_1=-p, & a_1'=-q, & a_8=q, \\ a_2=-2, & a_2'=-2, & a_7=2, \\ a_3=2+p, & a_3'=2+q, & a_6=-(2+q), \\ a_4=2-p, & a_4'=2-q, & a_5=q-2. \end{array}$$

Substituting the values of $a_1, a_2, \ldots$ in z and writing $z=R+Sp+Tq$, we find that

$$R=x^8-2x^7+2x^6+2x^5-2x^4-2x^3+2x^2-1,$$
$$S=-x^6+x^5-x^3, \qquad T=x^4-x^3+x.$$

Writing $X=2R-S-T$, $Y=T-S$, it follows that

$$4u=X^2+19Y^2,$$

where

$$X=2x^9+x^8-4x^7+3x^6+5x^5-3x^3+4x^2-x-2,$$
$$Y=x^8-x^6+x^5+x^4-x^3+x.$$

EXERCISE XIV

1. If α is an imaginary root of $x^7-1=0$ and $p_1=\alpha+\alpha^2+\alpha^4$, $p_2=\alpha^3+\alpha^6+\alpha^5$, show that the equation whose roots are p_1, p_2 is $x^2+x+2=0$, and find the equations whose roots are α, α^2, α^4 and α^3, α^6, α^5 respectively. Hence obtain the identity

$$4(x^6+x^5+x^4+x^3+x^2+x+1)=X^2+7Y^2,$$

where $$X=2x^3+x^2-x-2, \quad Y=x^2+x.$$

2. *For the equation* $x^{13}-1=0$, take $g=2$, a primitive root of 13, and let

$$p_1=(4,1), \quad p_2=(4,2), \quad p_3=(4,4).$$

Prove that (i) $p_1p_2=-1+p_2$.

(ii) The equation of which the roots are p_1, p_2, p_3 is $x^3+x^2-4x+1=0$. The smaller positive root is 0·2738905 ... . *Take this as* p_1 and show that

$$p_2=2-2p_1-p_1^2=1\cdot37720\ldots,$$
$$p_3=-1-p_1-p_2=-2\cdot65109\ldots.$$

(iii) Show that (2, 1), (2, 8) are the roots of $x^2-p_1x+p_2=0$;
show that (2, 2), (2, 3) are the roots of $x^2-p_2x+p_1=0$;
show that (2, 4), (2, 6) are the roots of $x^2-p_3x+p_2=0$.

Take (2, 1) *as the positive root* of the first of these equations. *To identify the roots* (2, 2) *and* (2, 4), prove that

$$\{(2,1)-(2,8)\}\{(2,2)-(2,3)\}=p_1-p_3>0,$$
$$\{(2,2)-(2,3)\}\{(2,4)-(2,6)\}=p_2-p_1>0.$$

Therefore (2, 2) and (2, 4) are the greater of the roots of the second and third quadratics.

(iv) Show that $(2,1)=1\cdot77091\ldots=2\cos\dfrac{2\pi}{13}$.

(v) Show that the equation of which the roots are those in the period (6, 1) is

$$x^6-px^5+2x^4-(p+1)x^3+2x^2-px+1=0,$$

where $p=(6,1)$. Hence find polynomials X, Y with integral coefficients such that

$$4(x^{13}-1)/(x-1)=X^2-13Y^2.$$

3. For the equation $x^{17}-1=0$, taking $g=3$, $p=(8,1)$, $q=(8,3)$, show that the equation of which the roots are those in the period (8, 1) is

$$x^8-px^7+(3+q)x^6+(3-p)x^5+(3+2q)x^4+(3-p)x^3+(3+q)x^2-px+1=0.$$

Hence find polynomials X, Y with integral coefficients such that

$$4(x^{17}-1)/(x-1)=X^2-17Y^2.$$

4. Let n be an odd prime. Of the numbers $1, 2, 3, \ldots n-1$, let $R, R', \ldots$ be quadratic residues and $N, N', \ldots$ non-residues of n. Prove that if $\theta=2\pi/n$ and k is any whole number not divisible by n, then

$$\Sigma\cos kR\theta-\Sigma\cos kN\theta=\pm\sqrt{n} \quad \text{or} \quad 0,$$
$$\Sigma\sin kR\theta-\Sigma\sin kN\theta=\quad 0 \quad \text{or} \quad \pm\sqrt{n},$$

according as n is of the form $4k+1$ or $4k-1$, the upper or lower sign being taken according as k is a quadratic residue, or a non-residue of n.

[This follows from (18), equation (W).]

CHAPTER XIV

SUM OF TWO OR MORE SQUARES. FACTORS OF LARGE NUMBERS

1. Sum of Two Squares. (1) *Every odd number which is the sum of two squares is of the form* $4n+1$.

For if a^2+b^2 is odd, one of the two a, b is odd and the other even, so that $a^2+b^2\equiv 1 \pmod 4$.

(2) *If a is prime to b, every factor of a^2+b^2 is the sum of two squares.*

For let p be any prime factor of a^2+b^2, and suppose that $a^2+b^2=pq$. Let α, β be the absolute least residues of a, b to the modulus q, then

$$\alpha^2+\beta^2\equiv 0 \pmod q,$$

so that $\alpha^2+\beta^2=qq'$ where $qq'\leqslant 2(\frac{1}{2}q)^2$ and $q'\leqslant\frac{1}{2}q$.

Also $pq^2q'=(a^2+b^2)(\alpha^2+\beta^2)=(a\alpha+b\beta)^2+(a\beta-b\alpha)^2$.

Now $a\equiv\alpha$ and $b\equiv\beta \pmod q$, therefore $a\beta-b\alpha\equiv 0 \pmod q$.

Hence also $a\alpha+b\beta\equiv 0 \pmod q$, and, dividing the last equation by q^2, we have an equation of the form $pq'=h^2+k^2$ where $q'<q$.

If h, k have a common factor g, q' must be divisible by g^2, for p is a prime. Thus we can find an equation $pq_1=x^2+y^2$ where $q_1<q$ and x is prime to y.

By continuing the process, as often as may be necessary, we can express p as the sum of two squares. It follows that every factor of a^2+b^2 is the sum of two squares, of which one may be zero.

(3) *If a is prime to b, every odd factor of a^2+b^2 is of the form* $4n+1$.

This follows from the last two theorems.

Ex. 1. *Given that* $34\cdot 1489=225^2+1$, *express* 1489 *as the sum of two squares.*

Here, $\dfrac{225^2+1}{34}=\dfrac{(225^2+1^2)(5^2+3^2)}{34^2}=\dfrac{(225\cdot 5-1\cdot 3)^2+(225\cdot 3+1\cdot 5)^2}{34^2}=33^2+20^2$.

Alternatively, the absolute least residue of 225 (mod 34) is -13; also we have $(-13)^2+1^2=5\cdot 34$; thus $5\cdot 34^2\cdot 1489=(-225\cdot 13+1\cdot 1)^2+(225\cdot 1+1\cdot 13)^2$, as in (2); hence $5\cdot 1489=86^2+7^2$.

Again $5=1^2+2^2$, therefore $5^2\cdot 1489=(86\cdot 1+7\cdot 2)^2+(86\cdot 2-7\cdot 1)^2$; hence

$$1489=20^2+33^2.$$

Ex. 2. *Given that* $1489=20^2+33^2$, *solve the congruence* $x^2+1\equiv 0 \pmod{1489}$.

Since 20 is prime to 1489, $(\frac{33}{20})^2+1\equiv 0 \pmod{1489}$.

Also $\frac{33}{20}\equiv -\frac{28}{5}\equiv 225$, therefore $x=\pm 225$.

(4) *Any prime p of the form $4n+1$ is the sum of two squares.*

For, in this case, the congruence $x^2 \equiv -1 \pmod{p}$ has a solution; for -1 is a quadratic residue of a prime of form $4n+1$; that is to say, integers x, y can be found so that $x^2+1^2=py$. Hence, by (2), p is the sum of two squares.

(5) To express a given number as the sum of two squares, or to show that this is impossible, we can use the square root process with suitable additions or subtractions. In case of a large number, it is advisable to use the method of exclusion.

Ex. 3. *Express* 19109 *as the sum of two squares, showing that this can be done in two ways.*

First Method. With this a table of squares is advisable.

1'91'09 (138		$19109 = 138^2 + 65$
1		548
23 | 91		$= 136^2 + 613$
69		540
268 | 2209 $= 47^2$		$134^2 + 1153$
2144		.....
65		$= 130^2 + 2209 = 47^2$
		.....
		$= 122^2 + 4225 = 65^2$.

Hence $19109 = 130^2 + 47^2 = 122^2 + 65^2$.

Method of Exclusion. Let $m = 19109 = x^2 + y^2$ $(x<y)$, then $2x^2 < m$ and $x < 97$. Let ω denote the set of numbers 1, 2, 3, ... 96. Let $V = m - x^2$, then V is to be a square. Choosing any excludent e of which β is a non-residue, we can omit from ω values of x such that $V \equiv \beta \pmod{e}$. If $e=3$, $\beta=2$, for instance, we can omit every x for which $V \equiv 2 - x^2 \equiv 2 \pmod 3$ or $x \equiv 0 \pmod 3$. Thus we can exclude all multiples of 3. After using 5, 7, 8, 11, 13, 17, 19 as excludents, it will be found that the only numbers left are 23, 47, 65, 68. On trial, we find that, if $x=47$ or 65, then V is a square, giving the same result as before.

(6) *Any number (n) which can be expressed as the sum of two squares in more than one way is a composite number.*

If the number has a square factor, we suppose this to have been removed and we assume that $n = a^2 + b^2 = a'^2 + b'^2$, where a is prime to b and a' to b'.

Thus in each of the pairs (a, b), (a', b') one number is odd and the other even. Let a, a' be even and $a<a'$, then b, b' are odd and $b>b'$.

Hence we may write $n = a^2 + b^2 = (a+2gx)^2 + (b-2gy)^2$, where $2g$ is the greatest common divisor of $a'-a$ and $b-b'$, so that x is prime to y.

Therefore $x(a+gx)=y(b-gy)=xyt$, where t is an integer,

and consequently $a=yt-gx, \quad b=xt+gy,$

so that $n=a^2+b^2=(g^2+t^2)(x^2+y^2),$

showing that n is a composite number.

Ex. 4. *Given that* $19109=122^2+65^2=130^2+47^2$, *find the prime factors of* 19100.
With the notation in the text,

$$a=122, \quad a'=130, \quad b=65, \quad b'=47,$$
$$2gx=a'-a=8, \quad 2gy=b-b'=18,$$

where $2g=2$, the highest common divisor of 8 and 18, thus

$$g=1, \quad x=4, \quad y=9, \quad t=(a+gx)/y=14;$$

therefore $19109=(1^2+14^2)(4^2+9^2)=197 \cdot 97.$

(7) **The Equation $x^2=y^2+z^2$.** If any two of x, y and z have a common factor, it must be a factor of the third number, and may be removed by division.

We shall therefore suppose that x, y *and* z *are prime to one another.*

Now y and z cannot both be odd, for then x^2 would be of the form $4m+2$, which is impossible: and since y is prime to z, one of these must be even and the other odd. Suppose that y is even, then z and x are both odd.

Again, x^2-y^2 is the square of an odd number, therefore $x+y$ and $x-y$ are both odd. Also any common divisor of these is a common divisor of $2x$ and $2y$, and therefore of x and y, which are prime to one another. Hence $x+y$ and $x-y$ are prime to one another, and both are squares.

Let $x+y=r^2$ and $x-y=s^2$, then $z=rs$ where r, s are odd and prime to one another, then $r+s$ and $r-s$ are both even; and if we write

$$r+s=2m, \quad r-s=2n \quad \text{or} \quad r=m+n, \quad s=m-n,$$

it follows that m is prime to n, and we have

$$x+y=(m+n)^2, \quad x-y=(m-n)^2, \quad z=m^2-n^2,$$

giving the general solution, namely

$$x=m^2+n^2, \quad y=2mn, \quad z=m^2-n^2,$$

where m, n are any two numbers prime to one another.

(8) *A prime* (p) *of the form* $4n+1$ *can be expressed as the sum of two squares in one way only, and the same is true for the square of such a prime.*

The first part follows from (4) and (5). As to the second part, x and y are determined uniquely by $p=x^2+y^2$ and then $p^2=(x^2-y^2)^2+(2xy)^2$.

Moreover, x is prime to y, and so, by (7), there is no other way of expressing p^2 in this form.

A similar statement does *not* apply to powers of p higher than the second, thus

$$p^3=(x^3-3xy^2)^2+(3x^2y-y^3)^2=(px)^2+(py)^2.$$

Hence we derive a useful test as to whether a number of the form $4n+1$ is or is not a prime: *if the number can be expressed uniquely as the sum of two squares, it is a prime or the square of a prime.*

2. The Congruence $x^2+y^2+1\equiv 0 \pmod p$. We shall prove that *if p is a prime, solutions of this congruence always exist, provided that when p is of the form $4n+1$ or when $p=2$, zero values of x, y are admitted.*

If h can be found so that h and $-(h+1)$ are quadratic residues of p, solutions are given by $x^2\equiv h$, $y^2\equiv -(h+1)$, for then $x^2+y^2\equiv -1 \pmod p$.

(i) *Let p be a prime of the form $4n-1$.* Of the numbers less than p, $\frac{1}{2}(p-1)$ are quadratic residues and the rest are non-residues. Hence at least one of the set $1, 2, 3, \ldots \frac{1}{2}(p+1)$ is a non-residue, and since 1 is a residue, there must be two consecutive numbers h and $h+1$ such that hRp and $(h+1)Np$.

Also $(-1)Np$, for p is of the form $4n-1$, therefore $-(h+1)Rp$ and solutions of the congruence exist, neither x nor y being zero.

(ii) *If p is a prime of the form $4n+1$,* then $(-1)Rp$, and if $(-1)\equiv a^2$, solutions of the congruence are $(\pm a, 0)$. Of course, solutions may exist in which neither x nor y is zero; thus, if $p=197$, we find that $-10\equiv 37^2$ and so $3^2+37^2+1\equiv 0 \pmod{197}$.

If $p=2$, a solution is $(1, 0)$.

Ex. 1. *Find solutions of* $x^2+y^2+1\equiv 0 (mod\ 199)$.

We require values of h such that h and $-(h+1)$ are quadratic residues of 199. It is easy to show that such values are 2, 5, 14, 16. Proceeding as in Ex. (13) (I), we obtain the results on the right, showing that $2\equiv 20^2$, $-3\equiv 14^2$,

$$5\equiv(\tfrac{18}{5})^2\equiv 76^2, \qquad -6\equiv(20.14)^2\equiv 81^2,$$
$$14\equiv 2.7\equiv(20.\tfrac{24}{14})^2\equiv(\tfrac{41}{7})^2\equiv 51^2,$$
$$-15\equiv(14.76)^2\equiv 69^2, \qquad -17\equiv(\tfrac{23}{2})^2\equiv 88^2.$$

Thus solutions are (20, 14), (76, 81), (51, 69), (4, 88).

$14^2\equiv -3 \pmod{199}$.
$18^2\equiv 5^2.5$.
$20^2\equiv 2$.
$23^2\equiv -2^2.17$.
$24^2\equiv -3.7$.

3. Sum of Four Squares. (1) *The product of two numbers each of which is the sum of four squares can be expressed as the sum of four squares.*

For if $m=x^2+y^2+z^2+w^2$, $m'=x'^2+y'^2+z'^2+w'^2$, then

$$mm'=\begin{vmatrix} x+\iota y, & z+\iota w \\ -z+\iota w, & x-\iota y \end{vmatrix}\cdot\begin{vmatrix} y'+\iota x', & w'+\iota z' \\ -w'+\iota z', & y'-\iota x' \end{vmatrix},$$

and, expanding the right-hand side,

$$mm'=(xx'+yy'+zz'+ww')^2+(yz'-zy'+xw'-wx')^2$$
$$+(zx'-xz'+yw'-wy')^2+(xy'-yx'+zw'-wz')^2.$$

On the right-hand side we may change the sign of any of the letters, and so, in general, the product can be expressed as the sum of four squares in several ways.

(2) *Any number can be expressed in the form* $x^2+y^2+z^2+w^2$, *zero values of* x, y, z, w *being admissible.*

Taking first the case of an odd prime p, suppose that we have an equation

$$pq=x^2+y^2+z^2+w^2,$$

where x, y, z, w are known numbers. Let x', y', z', w' be the absolute least residues of x, y, z, w to the modulus q, then $\Sigma x'^2\equiv 0 \pmod q$ and

$$x'^2+y'^2+z'^2+w'^2=qq',$$

where $qq'\leqslant 4(\frac{1}{2}q)^2$, so that $q'\leqslant q$.

If $q'=q$ then q must be even, and each of x', y', z', w' equal to $\pm\frac{1}{2}q$. Hence x, y, z, w are all divisible by $\frac{1}{2}q$ and pq by $\frac{1}{4}q^2$. Thus $4p$ is divisible by q, and since p is an odd prime, the only possible values of q are 2 and 4.

If $q=2$, then $2p=x^2+y^2+z^2+w^2$, so that just two of x, y, z, w, say x, y, are odd and

$$p=\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+\left(\frac{z+w}{2}\right)^2+\left(\frac{z-w}{2}\right)^2,$$

the numbers in brackets being integers or zero.

If $q=4$, then $4p=x^2+y^2+z^2+w^2$ and each of x, y, z, w must be odd, thus

$$2p=\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+\left(\frac{z+w}{2}\right)^2+\left(\frac{z-w}{2}\right)^2.$$

It is easily seen that two of the numbers in brackets are odd and two are even integers or zero, and thus (as in the previous case) we can express p as the sum of four squares.

Turning to the general case in which $q'<q$, we have

$$\begin{aligned}pq^2q'=&(xx'+yy'+zz'+ww')^2+(yz'-zy'+xw'-wx')^2\\&+(zx'-xz'+yw'-wy')^2+(xy'-yx'+zw'-wz')^2,\end{aligned}$$

and since $x, y, z, w\equiv x', y', z', w'$ respectively (mod q), the numbers in the last three brackets $\equiv 0 \pmod q$. Hence the number in the first bracket $\equiv 0 \pmod q$, and, dividing by q^2, we have an equation of the form

$$pq'=X^2+Y^2+Z^2+W^2, \text{ where } q'<q.$$

Thus, given an odd prime (p) and an equation of the form

$$pq=x^2+y^2+z^2+w^2,$$

where $q\neq 1$, we can always find an equation of the same form with a smaller q, and by repeating the process we can express p as the sum of four squares.

Now it has been shown that, for any prime p, a relation of the form $x^2+y^2+1^2+0^2\equiv 0 \pmod p$ exists. Hence every prime and consequently every composite number can be expressed in the specified form.

Ex. 1. *Given that* $-17\equiv 631^2 \pmod{2011}$, *express* 2011 *as the sum of four squares.*

We find that
$$631^2+4^2+1^2=198\,.\,2011.$$
The absolute least residues of 631, 4, 1 (mod 198) are 37, 4, 1, and
$$37^2+4^2+1^2=198\,.\,7,$$
therefore
$$198^2\,.\,7\,.\,2011=(631\,.\,37+4\,.\,4+1\,.\,1)^2+0^2+(37\,.\,1-631\,.\,1)^2+(631\,.\,4-37\,.\,4)^2.$$
Hence
$$7\,.\,2011=118^2+3^2+12^2.$$
The absolute least residues of 118, 3, 12 (mod 7) are -1, 3, -2, and
$$7\,.\,2=(-1)^2+3^2+(-2)^2;$$
therefore
$$7^2\,.\,2\,.\,2011=(-118+9-24)^2+(-6-36)^2+(-12+236)+(354+3)^2.$$
Hence
$$2\,.\,2011=19^2+6^2+32^2+51^2,$$
and
$$2011=\left(\frac{51+19}{2}\right)^2+\left(\frac{51-19}{2}\right)^2+\left(\frac{32+6}{2}\right)^2+\left(\frac{32-6}{2}\right)^2$$
$$=35^2+16^2+19^2+13^2.$$

(3) It is obvious that not every number can be expressed as the sum of three squares; for instance, 7 cannot be so expressed. To express a number as the sum of three squares (when possible) or as the sum of four squares, it is preferable to use the square root process rather than the general theory.

Ex. 2. *Show that* 63211 *can be expressed as the sum of three squares and express it in this way.*

We have
$$\begin{aligned} 63211&=251^2+\ 210\\ &\qquad\quad\ 501\\ &=250^2+\ 711\\ &\qquad\quad\ 499\\ &=249^2+1210 \end{aligned}$$
Now $1210=11^2\,.\,10=11^2(3^2+1^2)$, therefore
$$63211=249^2+33^2+11^2.$$

Ex. 3. *Express* 10007 *as the sum of four squares in three ways.*

Let $m=10007$, by the square root process,
$$m=99^2+206=99^2+14^2+3^2+1^2,$$
$$2m=139^2+9\,.\,77=139^2+9^2+24^2+6^2,$$
therefore
$$m=74^2+65^2+15^2+9^2.$$
Again
$$3m=172^2+437=172^2+20^2+6^2+1^2$$
and
$$3\,.\,1=1^2+(-1)^2+0^2+1^2,$$
therefore
$$3^2m=(172-20+1)^2+(6+172-1)^2+(6+20+1)^2+(-172-20+6)^2$$
and
$$m=51^2+59^2+9^2+62^2.$$

4. Factors of Large Numbers. To discover whether a large number (N) is or is not a prime, and in the latter case to find its factors, is a problem of great interest and of considerable difficulty. The methods given below should be used in the order given; the first is tentative, and should not be carried on to more than two or three subtractions; if this does not quickly give the desired result, the method of exclusion in the other two methods will be successful in all cases.

(1) General Methods. (i) Let N be an odd number, and suppose that $N=ab$; then a and b are odd numbers, $a+b$ and $a-b$ are even numbers, and

$$N=[\tfrac{1}{2}(a+b)]^2-[\tfrac{1}{2}(a-b)]^2;$$

and, in particular,

$$N=[\tfrac{1}{2}(N+1)]^2-[\tfrac{1}{2}(N-1)]^2.$$

Thus an odd number can be expressed as the difference of two squares; and, in this way, it can be factorised. The easiest way is to use the square-root process as follows, it being assumed that a table of squares is available.

Ex. 1. Let $N=123456789$; then $N/9=13717421$. From the working in the margin, where the last figure in the square root is taken as 4 instead of 3, *in order to give the least possible negative number as 'remainder'*, we find that

$$\begin{aligned} N/9 &= 3704^2-2195 \\ &\quad -7409 \quad (=2\times 3704+1) \\ &= 3705^2-9604 \\ &= 3705^2-98^2 = 3607\times 3803 \end{aligned}$$

```
3 ) 13717421 ( 3704
    9
67 ) 471
     469
7404 ) 27421
       29616
       -2195
```

Therefore, $123456789=3^2\,.\,3607\,.\,3803$; and it will be found that the last two factors are primes.

When, as in the above example, the factors are nearly equal, the desired result will be obtained after two or three subtractions: if not, we may proceed as follows. Suppose that $N=ab$, and that roughly $a=kb$, where $k=2, 3, 4, \ldots$: then apply the square-root process to kN or $4kN$, according as k is odd or even, and not proceeding to more than two or three subtractions, as in the next examples.

Ex. 2. Let $N=130381$. Here the square-root process, applied to N, does not give a ready result; but, on applying it to $8N$, we find that

$$8N=1043048=1022^2-1436=1023^2-3481=1023^2-59^2.$$

Ex. 3. Let $N=766879$. Here the square-root process applied to N and $8N$ fails to give a ready result; but we have

$$3N=2300637=1517^2-652=1518^2-3687=1519^2-6724=1519^2-82^2.$$

If the above tentative method fails, either of the following methods will succeed in all cases.

(ii) The square-root process would always succeed if carried on to a sufficient number of subtractions; but in general the number of subtractions would be large. The work can, however, be shortened by the use of quadratic residues, as in the next example.

Ex. 4. Let $N = 107399 = 328^2 - 185$; then we suppose that $(328+x)^2 - N = y^2$.

Hence, *to mod* 8, $x^2 + 1 \equiv 0$, 1, or 4 (the residues of 8), that is, $x^2 \equiv -1$, 0, or 3; and, since -1 and 3 are not residues of 8, it follows that $x = 4n$.

Again, *to mod* 3, $(1+x)^2 - 2 \equiv 0$ or 1 (residues of 3), i.e. $(1+x)^2 \equiv 2$ or 0; from which it follows that $x = 3k + 2$.

Also, *to mod* 5, $(3+x)^2 - 4 \equiv 0$, 1, or 4 (residues of 5), i.e. $(3+x)^2 \equiv 4$, 0, or 3; from which it follows that $x + 3 \equiv \pm 2$, or 0, i.e. $x \equiv 0$, 2, or 4 (mod 5).

Writing down the multiples of 4 in order, and erasing numbers of the forms $3n$, $3n+1$, $5n+1$, $5n+3$, we have left 20, 32, 44, 80, 92, 104, out of all numbers less than 120; and, the use of mod 7 will reduce these further to 32, 92, only.

On trying $x = 32$, we find that $y^2 = 107399 - 360^2 = 22201 = 149^2$; and thus

$$107399 = 360^2 - 149^2 = 211 \cdot 509.$$

(iii) Denote the aggregate of primes less than $\sqrt{N}$ by ω. If N is not divisible by any of these, it is a prime; and the question may be settled by dividing N by each of these primes. The number of trials which actually have to be made can be very much reduced by the *method of exclusion*.

For, if a is a quadratic residue of N, and $a \equiv b^2 \pmod{N}$, then $a \equiv b^2 \pmod{p}$, when p is a prime factor of N. Hence we may exclude from the aggregate ω any prime p of which a is a non-residue.

Ex. 5. Let $N = 178979$; here neither 3 nor 5 is a factor; and, since the remainder on dividing N by 1001 is $(979 - 178)$, or 801, which is not divisible by 7, 11, or 13, neither of these primes is a factor of N.

Now, in Ex. 3 on p. 138, it has been found that -2, -11, -67, and -79 are quadratic residues of N; and we form the table on the right (see Ch. X, 7, 8). The first column contains primes (p) for which -2 is a residue; the letters R, N, in the second column indicate that -11 is a residue, or non-residue of the corresponding number in the first column, and similarly for the third and fourth columns; the numbers -2, -11, -67, and -79 being the values of a used as excludents.

-2	-11	-67	-79
17	N		
19	N		
41	N		
43	N		
59	R	R	N
67	R	N	
73	N		
83	N		
89	R	R	R
...	...	...	...

Hence it appears that 89 is the least prime of which -2, -11, -67, -79 are all residues; and on trial we find that

$$178979 = 89 \cdot 2011.$$

The reckoning also shows that 2011 has no factor less than its square root, so that it is a prime.

(2) **The Forms $x^n \pm 1$.** (i) *Any common factor of $x^m - 1$ and $x^n - 1$ is a factor of $x^g - 1$, where g is the greatest common divisor of m and n.*

Integers u, v can be found so that $mu - nv = g$. Let p be a prime which is a factor of $x^m - 1$ and of $x^n - 1$, so that $x^m \equiv 1$ and $x^n \equiv 1 \pmod{p}$, then

$$x^{nv}(x^g - 1) = x^{mu} - x^{nv} \equiv 0 \pmod{p}.$$

Now x is prime to p, therefore p is a divisor of $x^g - 1$.

(ii) *If n is an odd prime, every odd prime factor (p) of x^n-1 which is not a factor of $x-1$ is of the form $2kn+1$.*

For by Fermat's theorem, since x is prime to p, $x^{p-1}-1\equiv 0 \pmod p$. Hence, by the last theorem, p is a factor of x^g-1, where g is the greatest common divisor of n and $p-1$.

Now as n and p are odd primes, either $p-1$ is prime to n or is an even multiple of n. In the first case, $g=1$ and p is a factor of $x-1$. In the second case, p is of the form $2kn+1$.

(iii) *If n is a prime, every prime factor (p) of $x^{n^r}-1$ which is not a factor of $x^{n^{r-1}}-1$ is of the form kn^r+1.*

For, reasoning as in (ii), it will be seen that p is a factor of x^g-1 where g is the greatest common divisor of n^r and $p-1$.

Since n is a prime, g must be a power of n. Also g cannot be n^{r-1} or any lower power of n, for then p would be a factor of $x^{n^{r-1}}-1$, which is not the case. Hence $g=n^r$ and $p-1$ is a multiple of n^r, which proves the theorem.

Ex. 2. *Prove that $2^{17}-1$ is a prime.*

If p is any prime factor of $2^{17}-1$, by Theorem (ii) p is of the form $34k+1$. And since $2^{18}\equiv 2 \pmod p$, 2 is a quadratic residue of p. Hence p is of the form $8k\pm 1$. It follows easily that p must be of one of the forms $136t+1$, $136t+103$.

Again, $2^{17}-1=131071<370^2$, hence we need only try as possible factors 137 and 239, which are the only primes of the above forms less than 370. On trial it is found that neither of these is a factor of $2^{17}-1$, which is therefore a prime.

(iv) *Every odd prime factor p of x^n+1 is a factor of x^g+1 where g is the greatest common divisor of $\frac{1}{2}(p-1)$ and n.*

For p is a factor of $x^{2n}-1$, and by Fermat's theorem it is a factor of $x^{p-1}-1$. Also $2g$ is the greatest common divisor of $p-1$ and $2n$, hence by (i) p is a factor of $x^{2g}-1$. Now p is not a factor of x^g-1, for then it would be a factor of x^n-1, and this is not so, for p is an odd factor of x^n+1. Hence p is a factor of x^g+1.

(v) *If n is a prime, every odd prime factor p of x^n+1 which is not a factor of $x+1$ is of the form $2kn+1$.*

For $\frac{1}{2}(p-1)$ is prime to n or is a multiple of n. Using the previous notation, it follows that $g=1$ or else $\frac{1}{2}(p-1)$ is a multiple of n, and the theorem follows from (iv).

(vi) *Every odd prime factor p of $x^{2^n}+1$ is of the form $2^{n+1}.k+1$.*

For p is a factor of $x^{2^{n+1}}-1$, but not of $x^{2^n}-1$, and the theorem follows from (iii).

Ex. 3. *Prove that $2^{35}+1$ is not a prime, and find its factors.*

Any prime factor of $2^{35}+1$ is a factor of $2^{70}-1$ but not of $2^{35}-1$, and is therefore

of the form 2^6k+1. The primes of this form are 193, 257, 449, 641, 769, 1153, 1217, 1409, 1601, 2113, 2689, etc.

It will be found that $2^{32}+1=4294967297=641\,.\,6700417$.

The latter factor $<2600^2$, and on trial it will be found that it is not divisible by any of the above primes less than 2600. Thus 6700417 is a prime.

Ex. 4. *Find the factors of* $10^{11}+1$.

Here every prime factor other than 11 is of the form $22n+1$; also -10 is a quadratic residue of each prime factor.

Hence, the factors other than 11 are of the forms $440r+1$, 23, 89, 133, 287, 331, 397, 419: for these are the numbers which are of the form $22n+1$, as well as of one of the forms $40m+1$, 7, 9, 11, 13, 19, 23, 37, for which -10 is a residue.

Trying 11 and 23, we find that $10^{11}+1=11^2\,.\,23\,.\,35932447$, the last factor being prime to 11 and 23.

We next try in succession the numbers 89, 331, 397, 419, 463, 727, 859, 881, 1013, etc.: the 28th of the series, 4093, proves to be a factor of 35932447, giving a quotient 8779. If the latter were not a prime, its factors, one of which must be less than 100, would have been found already. Hence $10^{11}+1=11^2\,.\,23\,.\,4093\,.\,8779$.

EXERCISE XV

1. Express 23^2+4^2 in another way as the sum of two squares.

2. Show that each of the following numbers can be expressed as the sum of two squares in two ways. Hence express each as the product of prime factors.

(i) 3161; (ii) 6109; (iii) 28013.

3. Show that 2, -3, 10, -11 are quadratic residues of 31. Hence find two solutions of $x^2+y^2+1\equiv 0 \pmod{31}$.

4. If a is prime to $2b$, any factor of a^2+2b^2 is of the form x^2+2y^2.

[Let p be a prime factor of a^2+2b^2 and suppose that $a^2+2b^2=pq$. Since a is odd, so are p and q. Let α, β be the absolutely least residues of a, b to the modulus q, then $\alpha+2\beta^2=qq'$ where $qq'\leqslant\frac{3}{4}q^2$, so that $q'<q$.]

[Proceed as in Art. 3 (2), noting all possible cases.]

5. Every prime of the form $8n+1$ or $8n+3$ can be expressed in the form x^2+2y^2.

[For -2 is a quadratic residue of any prime p of the form $8n+1$ or $8n+3$. Hence a can be found so that $a^2+2\,.\,1^2$ is divisible by p; by Ex. 1, p is of the form x^2+2y^2.]

6. Every prime of the form $6n+1$ can be put into the form x^2+3y^2.

7. If a is prime to $2b$, any prime factor of a^2-2b^2 is of the same form, and a similar theorem holds with regard to $2a^2-b^2$.

In this connection, note the identity $x^2-2y^2=2(x+y)^2-(x+2y)^2$.

8. Every prime of the form $8n\pm1$ can be expressed in either of the forms x^2-2y^2, $2x^2-y^2$.

9. Any prime of the form $8n+1$ can be expressed in each of the forms x^2+y^2, x^2+2y^2, x^2-2y^2, $2x^2-y^2$. Express 3001 in each of these ways.

10. Show that $\frac{1}{4}(x^2+y^2+z^2+w^2)$ is equal to each of the following expressions:

(i) $\left(\frac{-x+y+z+w}{4}\right)^2+\left(\frac{x-y+z+w}{4}\right)^2+\left(\frac{x+y-z+w}{4}\right)^2+\left(\frac{x+y+z-w}{4}\right)^2$;

(ii) $\left(\frac{x+y+z+w}{4}\right)^2+\left(\frac{y+z-x-w}{4}\right)^2+\left(\frac{z+x-y-w}{4}\right)^2+\left(\frac{x+y-z-w}{2}\right)^2$;

and that, if x, y, z, w are all odd numbers, all the expressions in brackets in either (i) *or* (ii) are integers.

11. Given that -10 is a quadratic residue of 2011, obtain a solution of

$$x^2+y^2+1\equiv 0 \pmod{2011}.$$

Hence express 2011 as the sum of three squares.

[We find that $569^2+3^2+1^2=161\,.\,2011$, hence

$$35\,.\,2011=265^2+12^2+4^2 \quad \text{and} \quad 11\,.\,2011=109^2+96^2+32^2,$$

giving $$2011=39^2+21^2+7^2.]$$

12. Given that $10\,.\,1103=102^2+25^2+1$, express 1103 as the sum of four squares.

13. If $m=10007$, we have $5m=233^2+306=223^2+15^2+9^2$. Use this to express 10007 as the sum of four squares.

14. Given that $-17\equiv 245^2 \pmod{10007}$, express 10007 as the sum of four squares.

15. Show that 770 can be expressed as the sum of three squares in eight ways. Give all the results.

16. Prove that $2^{13}-1$ and $2^{19}-1$ are primes.

[$2^{13}-1=8191$, $2^{19}-1=524287$.]

17. Find the prime factors of $2^{11}-1$.

18. Use the fact that $2^{2n}+1=(2^n+1)^2-2^{n+1}$ to find factors of $2^{2n}+1$ when n is odd.

19. Express $2^{28}+1$ as the product of primes.

20. Prove that $10^9-1=3^4\,.\,37\,.\,333667$, showing that the last factor is a prime.

[Let $m=333667$, then since $10^9-1=1000^3-1$, any prime factor of m is of the form $6k+1$. Also $10^{10}\equiv 10 \pmod{m}$ and $10Rm$. Using the square root process, we can now find easily that -2, -5, -31, 41 and 61 are residues of m, etc., as in Art. 4 (iii).]

21. Obtain small quadratic residues of 29951, and express this number as the product of primes.

22. Prove that any prime factor of $10^{11}-1$ other than 3 is of one of the forms $440k+1$, 67, 89, 111, 133, 199, 243, 397.

23. Show that $1\,.\,2\,.\,3\,.\,5\,.\,7\,.\,11\,.\,13+1=30031$ is a composite number, and find its prime factors.

24. We have $2^{11}+3^{11}=5m$, where $m=35839$. Prove that $-6Rm$, and obtain other small quadratic residues of m, using the results to prove that m is a prime.

[$2^{12}\equiv -6\,.\,3^{10} \pmod{m}$. Other residues are 2, -3, 10, -11, 41, -47.]

CHAPTER XV

GENERAL THEORY OF CONTINUED FRACTIONS

1. General Form. We shall consider fractions of the form

$$F=\frac{b_1}{a_1+}\frac{b_2}{a_2+}\cdots\frac{b_n}{a_n+}\cdots, \qquad \text{.....(A)}$$

where the a's and b's may be any real numbers.

Observe that an a may be zero, and yet the fraction may have a definite value. If one of the b's is zero, the fraction terminates.

Moreover, it has been explained in *H.A.*, XXIV (1), that we may, without any loss of generality, suppose that every a is positive.

For the fraction F, p_n and q_n are defined by

$$p_n=a_np_{n-1}+b_np_{n-2}, \quad q_n=a_nq_{n-1}+b_nq_{n-2},$$

with the initial values

$$p_0=0, \quad q_0=1, \quad p_1=b_1, \quad q_1=a_1.$$

This being so, p_n/q_n is the nth convergent, *not necessarily in its lowest terms.*

2. Equivalent Continued Fractions. Two continued fractions are said to be *equivalent* when their corresponding convergents are equal.

We proceed to consider certain transformations by means of which the fraction F may be converted into an equivalent fraction.

(1) *If* b_r, a_r, b_{r+1} *are all multiplied by the same number* k, *then* p_r, p_{r+1}, p_{r+2}, ... *and* q_r, q_{r+1}, q_{r+2}, ... *are all multiplied by* k, *and the value of any convergent is unaltered.*

For if p_n'/q_n' is the nth convergent of

$$\frac{b_1}{a_1+}\cdots\frac{b_{r-1}}{a_{r-1}+}\frac{kb_r}{ka_r+}\frac{kb_{r+1}}{a_{r+1}+}\frac{b_{r+2}}{a_{r+2}+}\cdots,$$

then $p_n'=p_n$ and $q_n'=q_n$, for $n<r$ and

$$p_r'=ka_rp_{r-1}+kb_rp_{r-2}=kp_r,$$
$$p_{r+1}'=a_{r+1}p_r'+kb_{r+1}p_{r-1}=kp_{r+1},$$
$$p_{r+2}'=a_{r+2}p_{r+1}'+b_{r+2}p_r'=kp_{r+2},$$

and so on, with similar results for the q's, and the theorem follows.

(2) It will be seen that, by continued application of the above, *any convergent of*

$$\frac{k_1b_1}{k_1a_1+}\,\frac{k_1k_2b_2}{k_2a_2+}\,\frac{k_2k_3b_3}{k_3a_3+}\ \dots\ \frac{k_{n-1}k_nb_n}{k_na_n+}\ \dots \quad \text{.....(B)}$$

is equal to the corresponding convergent of F, that is to say, the forms (B), (A) *are equivalent.*

Also if p_n'/q_n' is the nth convergent (unreduced) of the fraction (B), by § (1)

$$p_n' = k_1k_2 \dots k_np_n \quad \text{and} \quad q_n' = k_1k_2 \dots k_nq_n,$$

thus *the values of* a_na_{n-1}/b_n *and* a_nq_{n-1}/b_nq_{n-2} *are unaltered by the transformation.*

(3) *Any continued fraction of the form* (A), *in which the a's and b's are rational numbers, can be transformed into an equivalent fraction of the same form, in which the a's and b's are integers.*

For in (B) we can choose the k's so that every numerator and every denominator is a whole number.

(4) *Any continued fraction of the form* (B) *can be transformed into an equivalent fraction of the form*

$$\frac{1}{f_1+}\,\frac{1}{f_2+}\ \dots\ \frac{1}{f_n+}\ \dots \quad \text{.....(C)}$$

For we can choose the k's so that

$$k_1b_1 = k_1k_2b_2 = \dots\ k_{n-1}k_nb_n = \dots = 1,$$

and then if $f_1 = k_1a_1$, $f_2 = k_2a_2$, etc., we find that

$$f_1 = a_1/b_1, \quad f_2 = b_1a_2/b_2, \quad f_3 = b_2a_3/b_1b_3, \quad f_4 = b_1b_3a_4/b_2b_4,$$

and

$$f_n = \frac{b_1b_3b_5 \dots b_{n-1}a_n}{b_2b_4 \dots b_n} \quad \text{or} \quad \frac{b_2b_4 \dots b_{n-1}a_n}{b_1b_3 \dots b_n},$$

according as n is even or odd.

3. Euler's Rule for the Formation of Convergents.

To obtain the values of p_n and q_n for the continued fraction,

$$\frac{1}{f_1+}\,\frac{1}{f_2+}\,\frac{1}{f_3+}\ \dots,$$

the rule is as follows: *The first term of* q_n *is* $f_1f_2f_3 \dots f_n$. *To obtain the other terms, omit from this product, in all possible ways, one or more pairs of consecutive f's. If n is even and all the pairs are omitted, the corresponding term is unity. Also* p_n *is obtained from* $f_2f_3 \dots f_n$ *by exactly the same rule.*

For example,

$$q_4 = f_1f_2f_3f_4 + f_3f_4 + f_1f_4 + f_1f_2 + 1,$$
$$p_4 = f_2f_3f_4 + f_4 + f_2.$$

Proof of the rule for the q's. Let S_0^n stand for $f_1 f_2 \dots f_n$; let S_r^n denote the sum of all the terms which can be formed from S_0^n by omitting r pairs of consecutive f's, and let $S_m^{2m}=1$. Then we have to show that

$$q_n = S_0^n + S_1^n + S_2^n + \dots + S_r^n, \quad \dots\dots\dots\dots(\mathbf{A})$$

where $r=\frac{1}{2}n$ or $\frac{1}{2}(n-1)$, according as n is even or odd. We shall first show that

$$S_r^n = f_n S_r^{n-1} + S_{r-1}^{n-2}, \text{ where } 1 \leqslant r \leqslant \tfrac{1}{2}n. \quad \dots\dots\dots\dots(\mathbf{B})$$

To prove this, consider first the terms of S_r^n which contain f_n. The sum of these is f_n times the sum of the terms which can be formed from $f_1 f_2 \dots f_{n-1}$ by omitting r pairs of consecutive f's, and is therefore $f_n S_r^{n-1}$.

Next consider the terms of S_r^n which do not contain f_n. Since f_n is absent, so also is f_{n-1}; hence the terms are obtained from $f_1 f_2 \dots f_{n-2}$, by omitting $r-1$ pairs of consecutive f's, and their sum is S_{r-1}^{n-2}. This proves equation (**B**). We have also

$$S_0^n = f_n S_0^{n-1} \quad \text{and} \quad S_m^{2m}=1. \quad \dots\dots\dots\dots(\mathbf{C})$$

Now equation (**A**) holds for $n=2, 3$ and, using equations (**B**), (**C**) with recurrence formula, we have

$$q_4 = f_4 q_3 + q_2 = f_4 S_0^3 + (f_4 S_1^3 + S_0^2) + S_1^2 = S_0^4 + S_1^4 + S_2^4,$$

$$q_5 = f_5 q_4 + q_3 = f_5 S_0^4 + (f_5 S_1^4 + S_0^3) + (f_5 S_2^4 + S_1^3) = S_0^5 + S_1^5 + S_2^5;$$

and so on to any extent.

The rule for the p's follows from the fact that p_n is the same function of $f_2, f_3, \dots f_n$ as q_{n-1} is of $f_1, f_2, \dots f_{n-1}$.

For p_n is given by the difference equation $p_n = f_n p_{n-1} + p_{n-2}$ with the initial values $p_1=1$, $p_2=f_2$, and all of these equations hold if we change the p's into q's and decrease every suffix by unity.

4. Some important Inequalities. *For the continued fraction*

$$\frac{1}{f_1+}\,\frac{1}{f_2+}\,\frac{1}{f_3+}\cdots,$$

where $f_1, f_2, f_3, \dots$ *are* positive *rationals, the following inequalities hold:*

(i) $q_n < (1+f_1)(1+f_2)\dots(1+f_n)$,

(ii) $q_{2n+1} > f_1 + f_3 + f_5 + \dots f_{2n+1}$ *and* $q_{2n} > 1$.

The first inequality is due to the fact that q_n consists of some but not all of the terms in the expansion of $(1+f_1)(1+f_2)\dots(1+f_n)$.

Again, with the notation of Art. 3, we have

$$S_n^{2n+1} = f_1 + f_3 + \dots f_{2n+1} \quad \text{and} \quad S_n^{2n}=1.$$

Hence the other inequalities follow from Euler's rule.

5. Properties of p_n and q_n. For the fraction

$$F=\frac{b_1}{a_1+}\frac{b_2}{a_2+}\frac{b_3}{a_3+}\cdots\frac{b_n}{a_n+}\cdots,$$

by the recurrence formulae $p_nq_{n-1}-p_{n-1}q_n=-b_n(p_{n-1}q_{n-2}-p_{n-2}q_{n-1})$,

hence, $p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}b_nb_{n-1}\ldots b_2(p_1q_0-p_0q_1)$.

Now $p_0=0$, $q_0=1$, $p_1=b_1$, therefore

$$p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}b_1b_2\ldots b_n, \quad \ldots\ldots\ldots\ldots\text{(A)}$$

and

$$\frac{p_n}{q_n}-\frac{p_{n-1}}{q_{n-1}}=(-1)^{n-1}\frac{b_1b_2\ldots b_n}{q_nq_{n-1}}. \quad \ldots\ldots\ldots\ldots\text{(B)}$$

In the last formula, put $n-1$, $n-2$, ... 1 in succession for n and add; then since $p_0/q_0=0$, we have

$$\frac{p_n}{q_n}=\frac{b_1}{q_1}-\frac{b_1b_2}{q_1q_2}+\frac{b_1b_2b_3}{q_2q_3}-\ldots+(-1)^{n-1}\frac{b_1b_2\ldots b_n}{q_{n-1}q_n}. \quad \ldots\ldots\ldots\ldots\text{(C)}$$

Again, by the recurrence formulae,

$$p_nq_{n-2}-p_{n-2}q_n=a_n(p_{n-1}q_{n-2}-p_{n-2}q_{n-1})=(-1)^na_nb_1b_2\ldots b_{n-1};$$

therefore

$$\frac{p_n}{q_n}=\frac{p_{n-2}}{q_{n-2}}+(-1)^n\frac{a_nb_1b_2\ldots b_{n-1}}{q_nq_{n-2}}. \quad \ldots\ldots\ldots\ldots\text{(D)}$$

6. Infinite Continued Fractions. For convenience we repeat certain definitions given in *H.A.*, XXIV (3).

If p_1/q_1, p_2/q_2, ... are the convergents of an infinite continued fraction F, *the fraction is said to be convergent, divergent or oscillatory, according as the sequence* p_1/q_1, p_2/q_2, ... *converges, diverges or oscillates.*

If the sequence converges, the *value* of F is defined as $\lim p_n/q_n$, and we write $F=\lim p_n/q_n$. If the sequence does not converge, F has no definite value and is to be regarded merely as defining the sequence of convergents. If F and F' are equivalent continued fractions, they both converge to the same limit, or else both diverge or both oscillate.

7. Residual Fractions. Consider the fraction

$$F=\frac{b_1}{a_1+}\frac{b_2}{a_2+}\cdots\frac{b_m}{a_m+}\frac{b_{m+1}}{a_{m+1}+},$$

and let

$$z_m=a_m+\frac{b_{m+1}}{a_{m+1}+}\frac{b_{m+2}}{a_{m+2}+}\cdots,$$

then z_m is called the mth residual fraction, and the following question arises: *If it is known that* z_m *is convergent, under what circumstances can we conclude that* F *is convergent?*

Obviously if z_1 converges to any value but zero, F is convergent. Let $m>1$ and suppose that z_m is convergent, then

$$F=\frac{b_1}{a_1+}\cdots\frac{b_{m-1}}{a_{m-1}+}\frac{b_m}{z_m}=\frac{z_mp_{m-1}+b_mp_{m-2}}{z_mq_{m-1}+b_mq_{m-2}}.$$

Hence F is convergent, provided that

$$z_mq_{m-1}+b_mq_{m-2}\neq 0.$$

Thus the convergence of z_m involves the convergence of F in the following cases :

(i) if every a and every b is positive ;

(ii) if the a's and b's are rational numbers and z_m is irrational.

8. Two Main Classes. We shall consider chiefly the forms

$$\frac{b_1}{a_1+}\frac{b_2}{a_2+}\cdots\frac{b_n}{a_n+}\cdots \quad\text{and}\quad \frac{b_1}{a_1-}\frac{b_2}{a_2-}\cdots\frac{b_n}{a_n-}\cdots,$$

where the a's and b's are positive. These are called fractions of the *first* and *second* class respectively. In those of the first class every element is preceded by the sign $+$, in those of the second class every element after the first is preceded by the sign $-$.

Continued Fractions of the First Class

9. Properties of the Convergents. We consider the fraction

$$F=\frac{b_1}{a_1+}\frac{b_2}{a_2+}\frac{b_3}{a_3+}\cdots,$$

where the a's and b's are positive.

(1) *The p's and q's are all positive, and if every $a\geqslant 1$ then p_n and q_n increase with n. Also, if the a's and b's are positive integers, p_n and q_n tend to infinity with n.*

All this follows from the equation

$$p_n-p_{n-1}=(a_n-1)p_{n-1}+b_np_{n-2},$$

and the similar equation connecting the q's.

(2) *The even convergents form an increasing sequence, the odd convergents form a decreasing sequence, and every even convergent is less than any odd convergent.*

For if $u_n=p_n/q_n$, it follows from equations (B), (D) of Art. 5 that u_n-u_{n-1} and u_n-u_{n-2} are of opposite signs. Therefore u_n lies between u_{n-1} and u_{n-2}.

Now $u_2<u_1$, and consequently $u_2<u_3<u_1$; $u_2<u_4<u_3$, $u_4<u_5<u_3$, and so on. Hence

$$u_2<u_4<u_6<\ldots<u_5<u_3<u_1. \quad\ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

(3) *A continued fraction of the first class written in the form*

$$F=\frac{1}{f_1+}\frac{1}{f_2+}\frac{1}{f_3+}\cdots$$

is convergent if at least one of the series

$$f_1+f_3+f_5+\ldots,\quad f_2+f_4+f_6+\ldots$$

is divergent. If both series are convergent, then the fraction oscillates.

Proof. Suppose that $f_1+f_3+f_5+\ldots$ *is divergent,* and let u_n denote the nth convergent of F. By Art. 4 we have

$$q_{2n-1}>f_1+f_3+\ldots f_{2n-1} \quad \text{and} \quad q_{2n}>1.$$

Therefore $q_{2n}q_{2n-1}\to\infty$ and, using equation (B) of Art. 5,

$$u_{2n}-u_{2n-1}=-1/q_{2n}q_{2n-1}\to 0.$$

Hence F is convergent. (Art. 9 (3).)

Next, suppose that $f_2+f_4+f_6+\ldots$ *is divergent,* then it follows as before that

$$\frac{1}{f_2+}\frac{1}{f_3+}\frac{1}{f_4+}\cdots$$

is convergent, and therefore F is convergent.

Lastly, suppose that both series are convergent, then $f_1+f_2+f_3+\ldots$ is convergent, and therefore the infinite product $(1+f_1)(1+f_2)(1+f_3)\ldots$ converges to a limit l. Using the first inequality of Art. 4,

$$q_r<(1+f_1)(1+f_2)\ldots(1+f_r)<l,$$

and therefore $q_{2n}q_{2n-1}<l^2$. Hence

$$u_{2n-1}-u_{2n}=1/q_{2n}q_{2n-1}>1/l^2.$$

Therefore $u_{2n}-u_{2n-1}$ does not tend to zero and F oscillates. (Art. 9.)

(4) The question of the convergence of the fraction

$$\frac{b_1}{a_1+}\frac{b_2}{a_2+}\cdots\frac{b_n}{a_n+}\cdots,$$

where the a's and b's are all positive, can be completely settled by applying the conditions of § (3) to the fraction

$$\frac{1}{f_1+}\frac{1}{f_2+}\cdots\frac{1}{f_n},$$

where $$f_n=\frac{b_1b_3b_5\ldots b_{n-1}a_n}{b_2b_4\ldots b_n} \quad \text{or} \quad \frac{b_2b_4\ldots b_{n-1}a_n}{b_1b_3\ldots b_n},$$

according as n is even or odd.

Special cases, which cover many instances with which we are concerned, are the following.

(5) *If a_n, b_n are polynomials in n which are positive for $n \geqslant 1$ and of degrees r, s respectively, then the continued fraction*

$$F = \frac{b_1}{a_1+}\frac{b_2}{a_2+}\cdots\frac{b_n}{a_n+}\cdots$$

is convergent or oscillates according as $s \leqslant 2(r+1)$ or $s > 2(r+1)$.

Let $a_n = \lambda(n^r + hn^{r-1} + h'n^{r-2} + \ldots)$, $b_n = \mu(n^s + kn^{s-1} + k'n^{s-2} + \ldots)$, and let f_n have the same meaning as in the last section.

Considering the convergence of $f_1 + f_3 + f_5 + \ldots$, and denoting the nth term of this series by t_n, we have

$$\frac{t_n}{t_{n+1}} = \frac{f_{2n-1}}{f_{2n+1}} = \frac{a_{2n-1}}{a_{2n+1}} \cdot \frac{b_{2n+1}}{b_{2n}}.$$

Now
$$\frac{a_{2n-1}}{a_{2n+1}} = \left(\frac{1-\frac{1}{2n}}{1+\frac{1}{2n}}\right)^r \cdot \frac{1 + \frac{h}{2n}\left(1-\frac{1}{2n}\right)^{-1} + \frac{h'}{4n^2}\left(1-\frac{1}{2n}\right)^{-2} + \ldots}{1 + \frac{h}{2n}\left(1+\frac{1}{2n}\right)^{-1} + \frac{h'}{4n^2}\left(1+\frac{1}{2n}\right)^{-2} + \ldots}.$$

Expanding this in powers of $1/n$, we find that

$$\frac{a_{2n-1}}{a_{2n+1}} = \left(1 - \frac{p}{n} + \ldots\right)\left(1 + \frac{0}{n} + \ldots\right) = 1 - \frac{p}{n} + \text{higher powers of } 1/n.$$

Similarly
$$\frac{b_{2n+1}}{b_{2n}} = 1 + \frac{s}{2n} + \text{higher powers of } 1/n,$$

and therefore
$$\frac{t_n}{t_{n+1}} = 1 + \frac{s-2r}{2} \cdot \frac{1}{n} + \text{higher powers of } 1/n.$$

Hence, by Gauss's test, the series $f_1 + f_3 + f_5 + \ldots$ is divergent or convergent, according as $(s-2r)/2 \leqslant 1$ or $(s-2r)/2 > 1$. (*H.A.*, XX, 5.)

In just the same way it can be shown that $f_2 + f_4 + f_6 + \ldots$ is divergent or convergent under exactly the same conditions. This completes the proof of the theorem.

(6) *If a_n and b_n are rational functions of n which are positive for $n \geqslant 1$, the fraction*

$$F = \frac{b_1}{a_1+}\frac{b_2}{a_2+}\cdots\frac{b_n}{a_n+}\cdots$$

*is convergent or oscillates according as the series $\Sigma(a_n a_{n-1}/b_n)^{\frac{1}{2}}$ is divergent or convergent.**

For by means of Art. 2, (2), we can transform F into an equivalent continued fraction,

$$F' = \frac{d_1}{c_1+}\frac{d_2}{c_2+}\cdots\frac{d_n}{c_n+}\cdots,$$

* It should be noticed that this test includes the preceding.

where c_n, d_n are polynomials in n. Now by Art. 2, (2), we have

$$a_n a_{n-1}/b_n = c_n c_{n-1}/d_n.$$

Hence, if r, s are the degrees in n of c_n, d_n, the ratio of the nth terms of the series $\Sigma(a_n a_{n-1}/b_n)^{\frac{1}{2}}$ and $\Sigma n^{-(s-2r)/2}$ is finite.

Therefore $\Sigma(a_n a_{n-1}/b_n)^{\frac{1}{2}}$ is divergent if and only if $(s-2r)/2 \leqslant 1$. But F', and therefore also F, is convergent if and only if $(s-2r)/2 \leqslant 1$, which proves the statement in question.

Ex. 1. *Examine for convergence*

(i) $\dfrac{1^2}{2+}\dfrac{3^2}{2+}\dfrac{5^2}{2+}\cdots$.

(ii) $\dfrac{\frac{1}{2}}{\frac{2}{3}+}\dfrac{\frac{3}{4}}{\frac{4}{5}+}\dfrac{\frac{5}{6}}{\frac{6}{7}+}\cdots$.

(iii) $\dfrac{x}{2+}\dfrac{x}{3+}\dfrac{2x}{2+}\dfrac{2x}{5+}\dfrac{3x}{2+}\dfrac{3x}{7+}\cdots$.

(i) Here $a_n a_{n-1}/b_n = 4/(2n-1)^2$, therefore $\Sigma(a_n a_{n-1}/b_n)^{\frac{1}{2}}$ is divergent and F is convergent.

(ii) Here $a_n = 2n/(2n+1)$, $b_n = (2n-1)/2n$, therefore $a_n a_{n-1}/b_n \to 1$ and $\Sigma a_n a_{n-1}/b_n$ is divergent, therefore F is convergent.

(iii) Here F is equivalent to $\dfrac{1}{2/x+}\dfrac{1}{3+}\dfrac{1}{2/2x+}\dfrac{1}{5+}\dfrac{1}{2/3x+}\dfrac{1}{7+}\cdots$ and the series $3+5+7+\ldots$ is divergent, therefore F is convergent.

Continued Fractions of the Second Class

11. The General Continued Fraction of the Second Class.

This is of the form

$$F = \frac{b_1}{a_1-}\frac{b_2}{a_2-}\cdots\frac{b_n}{a_n-}\cdots,$$

where the a's and b's may have *any* positive values.

The recurrence formulae are

$$p_n = a_n p_{n-1} - b_n p_{n-2}, \quad q_n = a_n q_{n-1} - b_n q_{n-2},$$

with the initial values $p_0 = 0$, $q_0 = 1$, $p_1 = b_1$, $q_1 = a_1$.

Proceeding as in Art. 5, we have the following:

$$p_n q_{n-1} - p_{n-1} q_n = b_1 b_2 \ldots b_n, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{b_1 b_2 \ldots b_n}{q_n q_{n-1}}, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{a_n b_1 b_2 \ldots b_{n-1}}{q_n q_{n-2}}, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

$$\frac{p_n}{q_n} = \frac{b_1}{q_1} + \frac{b_1 b_2}{q_1 q_2} + \frac{b_1 b_2 b_3}{q_2 q_3} + \ldots + \frac{b_1 b_2 \ldots b_n}{q_{n-1} q_n}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(D)}$$

Observe that, in calculating successive convergents by the rules of formation, p_n/q_n must not be reduced in any way, and each of the numbers must retain its own sign; thus, if $p_n=5$ and $q_n=-6$, the convergent must not be written as $(-5)/6$.

If the a's and b's are integers, the p's and q's are integers, positive or negative; their absolute values do not necessarily tend to infinity with n, even if F is convergent; nor, if all the q's tend to infinity with n, is F necessarily convergent.

12. A Test of Convergence. For continued fractions of the second class there is no general test of convergence. But *if after a certain stage all the q's are positive and $b_nq_{n-2}/q_n<k$, where $0<k<1$, then the fraction of the second class,*

$$F=\frac{b_1}{a_1-}\,\frac{b_2}{a_2-}\cdots\frac{b_n}{a_n-}\cdots,$$

is convergent; but if $b_nq_{n-2}/q_n\geqslant 1$, then F is divergent.

For the series (D) of the preceding article is a series of positive terms (u_r), and $u_n/u_{n-1}=b_nq_{n-2}/q_n$; hence the result follows by d'Alembert's test.

It should be noted that the value of b_nq_{n-2}/q_n is unaltered by the transformation in Art. 2, (2).

13. The 'Restricted' Type. If, in the fraction

$$F=\frac{b_1}{a_1-}\,\frac{b_2}{a_2-}\cdots\frac{b_n}{a_n-}\cdots,$$

the a's and b's are positive and $a_n\geqslant b_n+1$, for all values of n, then (i) *the fraction is convergent*; (ii) *if $a_n=b_n+1$ for every n, and the series $1+b_1+b_1b_2+\ldots+b_1b_2\ldots b_n+\ldots$ converges and has a sum s, then $F=1-1/s$, but if the series diverges, then $F=1$*; (iii) *If $a_n>b_n+1$ for one or more values of n, then $0<F<1$.*

The truth of these statements depends on the following properties of the fraction, when it is supposed that $a_n\geqslant b_n+1$ and that p_r/q_r is the rth convergent.

(1) *The quantities p_n and q_n are positive and increase with n.*

For $p_n-p_{n-1}=(a_n-1)p_{n-1}-b_np_{n-2}\geqslant b_n(p_{n-1}-p_{n-2})$; and this holds if we put $n-1$, $n-2$, ... 2 in succession for n, therefore

$$p_n-p_{n-1}\geqslant b_nb_{n-1}\ldots b_2(p_1-p_0)\geqslant b_nb_{n-1}\ldots b_2b_1.$$

Also, $q_n-q_{n-1}\geqslant b_nb_{n-1}\ldots b_2(q_1-q_0)\geqslant b_nb_{n-1}\ldots b_2(a_1-1)\geqslant b_nb_{n-1}\ldots b_2b_1.$

Therefore

$$p_n>p_{n-1}\quad\text{and}\quad q_n>q_{n-1}.$$

(2) *The convergents form an increasing sequence of positive numbers.*

For $p_n/q_n - p_{n-1}/q_{n-1} = b_1 b_2 \dots b_n/q_n q_{n-1}$, and the p's and q's are positive.

(3) In § (1) it has been shown that, for every n,

$$p_n - p_{n-1} \geqslant b_1 b_2 \dots b_n \quad \text{and} \quad q_n - q_{n-1} \geqslant b_1 b_2 \dots b_n;$$

hence,

$$p_n \geqslant b_1 + b_1 b_2 + \dots + b_1 b_2 \dots b_n, \quad \text{......(A)}$$

$$q_n \geqslant 1 + b_1 + b_1 b_2 + \dots + b_1 b_2 \dots b_n. \quad \text{......(B)}$$

(4) *If* $a_r = b_r + 1$ *for* $r \leqslant n$, the sign $=$ must be taken everywhere in the last section, and

$$p_n = b_1 + b_1 b_2 + \dots + b_1 b_2 \dots b_n, \quad \text{......(C)}$$

$$q_n = 1 + b_1 + b_1 b_2 + \dots + b_1 b_2 \dots b_n. \quad \text{......(D)}$$

(5) *If* $a_r = b_r + 1$ *for all values of* n, then equations (C), (D) are true for all values of n. Hence

$$q_n - p_n = 1 \quad \text{and} \quad p_n/q_n = 1 - 1/q_n.$$

Therefore $p_n/q_n \to 1 - 1/s$ or 1, according as the series for q_n converges to a sum s or is divergent. This proves the second part of the theorem.

(6) *Let m be the least value of n for which* $a_n > b_n + 1$; let $a_m - b_m - 1 = \eta$, so that $\eta > 0$; also suppose that $v_n = (1-k)q_n - p_n$, where k is a constant to be chosen later. Then, by § (4), $v_n = 1 - kq_n$ for $n \leqslant m-1$. ......(E)

Choose k provisionally so that $0 < k < 1/q_{m-1}$; then v_{m-1} is positive,

and $$v_m - v_{m-1} = (a_m - 1)v_{m-1} - b_m v_{m-2} = \eta v_{m-1} + b_m(v_{m-1} - v_{m-2}).$$

Thus, $$v_m - v_{m-1} = \eta - k(\eta q_{m-1} + b_m q_{m-1} - b_m q_{m-2}) \quad \text{by (E)}$$

$$= \eta - k\{(a_m - 1)q_{m-1} - b_m q_{m-2}\} = \eta - k(q_m - q_{m-1}).$$

Now $$q_m = a_m q_{m-1} - b_m q_{m-2} > (a_m - b_m) q_{m-1} > (\eta + 1) q_{m-1};$$

hence, $\eta/(q_m - q_{m-1}) < 1/q_{m-1}$; therefore, if we take $0 < k < \eta/(q_m - q_{m-1})$, we shall have $v_{m-1} > 0$ and $v_m > v_{m-1}$. Also $v_n - v_{n-1} \geqslant b_n(v_{n-1} - v_{n-2})$ for all values of n, therefore $v_n > v_{m-1} > 0$ for $n \geqslant m$.

Therefore $(1-k)q_n > p_n$ for $n \geqslant m$; hence, $p_n/q_n < 1 - k$; and, since p_n/q_n increases with n and is positive, it tends to a positive limit less than unity.

This proves the third part of the theorem.

NOTE. In the proof usually given of part (iii) (see Chrystal's *Algebra*, Vol. 2, p. 511) no attention is paid to the main difficulty. It is merely shown that $p_n/q_n \leqslant 1 - 1/q_n$. Now q_n may tend to infinity, and then we could not assign a constant k such that $p_n/q_n < k < 1$; and the only conclusion we could make is that $F \leqslant 1$.

14. Another Type. (1) Consider the fraction

$$F=\frac{b_1x}{a_1-}\,\frac{b_2x}{a_2-}\cdots\frac{b_nx}{a_n-}\cdots,$$

where $0<x\leqslant 1$, the a's and b's are positive, $a_{2n-1}\geqslant b_{2n-1}+b_{2n}$, and $a_{2n}\geqslant 2$ for all values of n.

We shall prove that the fraction is always convergent and that

$$F\leqslant 2xs/(1+2s) \quad or \quad F\leqslant x;$$

according as the series $b_1/b_2+b_1b_3/b_2b_4+\ldots$ *converges to a sum* s *or is divergent.*

(1) From the given relations, $q_2-q_1=(a_2-1)\,q_1-b_2xq_0\geqslant q_1-b_2\geqslant b_1$, therefore

$$q_2>q_1>b_2q_0>0. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

Assume that $q_{2n-2}>q_{2n-3}>b_{2n-2}q_{2n-4}>0$, then

$$q_{2n-1}=a_{2n-1}q_{2n-2}-b_{2n-1}xq_{2n-3}\geqslant(b_{2n-1}+b_{2n})q_{2n-2}-b_{2n-1}q_{2n-3},$$

therefore $\quad q_{2n-1}-b_{2n}q_{2n-2}\geqslant b_{2n-1}(q_{2n-2}-q_{2n-3})>0. \quad \ldots\ldots\ldots\ldots\text{(B)}$

Again, $\quad q_{2n}=a_{2n}q_{2n-1}-b_{2n}xq_{2n-2}\geqslant 2q_{2n-1}-b_{2n}q_{2n-2},$

therefore $\quad q_{2n}-q_{2n-1}\geqslant q_{2n-1}-b_{2n}q_{2n-2}>0. \quad \ldots\ldots\ldots\ldots\text{(C)}$

Thus $q_{2n}>q_{2n-1}>b_{2n}q_{2n-2}>0$; and it follows by induction that all of the above relations hold for every n.

Again, from (B) and (C), $q_{2n}-q_{2n-1}\geqslant b_{2n-1}(q_{2n-2}-q_{2n-3})$, $\ldots\ldots\ldots\ldots\text{(D)}$ and by a succession of similar steps

$$q_{2n}-q_{2n-1}\geqslant b_{2n-1}b_{2n-3}\ldots b_3(q_2-q_1). \quad \ldots\ldots\ldots\ldots\ldots\text{(E)}$$

Let $P_n=b_1b_3\ldots b_{2n-1}$, $Q_n=b_2b_4\ldots b_{2n}$, then since $q_2-q_1\geqslant b_1$ we have from (B) and (E),

$$q_{2n}-q_{2n-1}\geqslant P_n \quad \text{and} \quad q_{2n-1}-b_{2n}q_{2n-2}\geqslant P_n, \quad \ldots\ldots\ldots\ldots\text{(F)}$$

whence by addition

$$q_{2n}-b_{2n}q_{2n-2}\geqslant 2P_n \quad \text{and} \quad q_{2n}/Q_n-q_{2n-2}/Q_{n-1}\geqslant 2P_n/Q_n. \quad \ldots\ldots\text{(G)}$$

Also $q_2/Q_1\geqslant(2b_1+b_2)/b_2$; hence we find that $q_{2n}/Q_n\geqslant 2s_n+1$, $\ldots\ldots\text{(H)}$ where s_n is the sum to n terms of the series

$$\frac{b_1}{b_2}+\frac{b_1b_3}{b_2b_4}+\frac{b_1b_3b_5}{b_2b_4b_6}+\ldots \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(I)}$$

(2) It has been proved that every q is positive, therefore p_n/q_n *increases with* n *and is positive.* (See Art. 11, Equation B.)

(3) *Let* $v_n=q_n-p_n/x$, then $v_n=a_nv_{n-1}-b_nxv_{n-2}$ and $v_0=1$,

$$v_1=a_1-b_1x\geqslant b_2, \quad v_2-v_1=(a_2-1)v_1-b_2xv_0\geqslant 0.$$

Thus $v_2 \geqslant v_1 \geqslant b_2 v_0$, and by steps exactly similar to those in § (1) we can show that $v_{2n} - v_{2n-1} \geqslant v_{2n-1} - b_{2n} v_{2n-2} \geqslant 0$.

Hence $v_{2n} \geqslant b_{2n} v_{2n-2}$, and so $v_{2n} \geqslant Q_n$. .....(J)

(4) Thus $q_{2n} - p_{2n}/x \geqslant Q_n$, hence by § (2) and the relation (H),

$$\frac{p_{2n-1}}{q_{2n-1}} < \frac{p_{2n}}{q_{2n}} \leqslant x\left(1 - \frac{Q_n}{q_{2n}}\right) \leqslant x\left(1 - \frac{1}{1+2s_n}\right).$$

Hence, if the series $\Sigma P_n/Q_n$ converges to a sum s and $l = 2xs/(1+2s)$, then $p_n/q_n \leqslant l$, and by § (2), $p_n/q_n \to k \leqslant l$. Also if the series is divergent, $p_n/q_n < x$ and $p_n/q_n \to k \leqslant x$. This proves the theorem.

(5) For the particular case in which $x = 1$, $a_{2n-1} = b_{2n-1} + b_{2n}$, and $a_{2n} = 2$ for all values of n, the a's and b's being all positive, we have

$$F = \frac{b_1}{a_1 -} \frac{b_2}{a_2 -} \cdots \frac{b_n}{a_n -} \cdots = 2s/(1+2s) \quad \text{or} \quad 1,$$

according as the series $b_1/b_2 + b_1 b_3/b_2 b_4 + \ldots$ *converges to a sum* s *or is divergent.*

Here the sign $=$ replaces $\geqslant$ or $\leqslant$ in the previous reckoning. (For examples, see Exercise XVI, Exx. 5–8.)

15. Some Fractions which converge to Irrational Limits.

(1) *If the* a*'s and* b*'s are positive integers and if* $a_n \geqslant b_n$ *for* $n \geqslant m$, *where* m *is a given integer, then the fraction*

$$x_1 = \frac{b_1}{a_1 +} \frac{b_2}{a_2 +} \cdots \frac{b_n}{a_n +} \cdots$$

converges to an irrational limit.

Proof. Let $x_r = \dfrac{b_r}{a_r +} \dfrac{b_{r+1}}{a_{r+1} +} \cdots \dfrac{b_n}{a_n +} \cdots$. Then, since the a's and b's are positive integers and, after a certain stage, $a_n \geqslant b_n$, it follows that every x_r is convergent (Art. 10(2)). Also, if x_m is irrational, so is x_1.

Suppose that x_m *is rational*, and let $x_m = k_1/k_0$ where k_1, k_0 are positive integers. Then, since $x_m < b_m/a_m$, we have $x_m < 1$ and $k_1 < k_0$.

Also $x_m = \dfrac{b_m}{a_m + x_{m+1}}$, therefore $x_{m+1} = \dfrac{b_m}{x_m} - a_m = \dfrac{b_m k_0 - a_m k_1}{k_1}$.

Let $x_{m+1} = k_2/k_1$ where $k_2 = b_m k_0 - a_m k_1$, then k_2 is a positive integer, and since $x_{m+1} < 1$ we have $k_2 < k_1$.

Proceeding in this way, we should arrive at an infinite decreasing sequence of positive integers. Since no such sequence exists, x_m and consequently x_1 must be irrational.

(2) *If the a's and b's are positive integers and if* $a_n \geqslant b_n + 1$ *for* $n \geqslant m$, *the sign* $>$ *occurring indefinitely often, then the fraction*

$$x_1 = \frac{b_1}{a_1 -}\,\frac{b_2}{a_2 -}\,\cdots\,\frac{b_n}{a_n -}\,\cdots$$

converges to an irrational limit.

Proof. Choose any integer r, such that $r \geqslant m$, then, since the condition $a_n > b_n + 1$ holds infinitely many times, it must hold for values of n greater than r. Let

$$x_r = \frac{b_r}{a_r -}\,\frac{b_{r+1}}{a_{r+1} -}\,\cdots\,\frac{b_n}{a_n -}\,\cdots,$$

then, by Theorem (iii) of Art. 13, the fractions x_m, x_{m+1}, x_{m+2}, ... are convergent, and their values are positive numbers less than unity.

Suppose that x_m *is rational*, and let $x_m = k_1/k_0$ where k_1, k_0 are positive integers. Then since $x_m < 1$, we have $k_1 < k_0$. Also

$$x_m = \frac{b_m}{a_m - x_{m+1}}, \quad \text{therefore} \quad x_{m+1} = a_m - \frac{b_m}{x_m} = \frac{a_m k_1 - b_m k_0}{k_1}.$$

Let $x_{m+1} = k_2/k_1$, where $k_2 = a_m k_1 - b_m k_0$, then k_2 is a positive integer, and since $x_{m+1} < 1$, we have $k_2 < k_1$.

Continuing thus, we should obtain an infinite decreasing sequence of positive integers which is non-existent. Consequently x_m is irrational.

Again, if p_r/q_r is the rth convergent of x_1,

$$x_1 = \frac{b_1}{a_1 -}\,\frac{b_2}{a_2 -}\,\cdots\,\frac{b_{m-1}}{a_{m-1} -}\,\frac{1}{1/x_m} = \frac{p_{m-1} - x_m p_{m-2}}{q_{m-1} - x_m q_{m-2}};$$

and since x_m is irrational, so also is x_1 unless $p_{m-1}/q_{m-1} = p_{m-2}/q_{m-2}$. This cannot occur, on account of equation (B) of Art. 11, therefore x_1 is irrational.

Ex. 1. *Given that* $\tan x = \dfrac{x}{1 -}\,\dfrac{x^2}{3 -}\,\dfrac{x^2}{5 -}\,\cdots\,\dfrac{x^2}{2n-1 -}\,\cdots$, *prove that* π *is irrational.*

If π is rational, so also is $\pi/4$. Assume that $\pi/4 = r/s$ where r, s are integers, and let $x = r/s$, then

$$1 = \frac{r/s}{1 -}\,\frac{r^2/s^2}{3 -}\,\frac{r^2/s^2}{5 -}\,\cdots = \frac{r}{s -}\,\frac{r^2}{3s -}\,\frac{r^2}{5s -}\,\cdots.$$

Choose m so that $2m - 1 > (r^2 + 1)/s$, then for the last continued fraction $a_n > b_n + 1$, provided that $n \geqslant m$. Hence this fraction converges to an irrational limit and cannot be equal to unity; therefore π cannot be rational.

EXERCISE XVI

1. Prove that

$$\frac{a_1}{a_1 +}\,\frac{a_2}{a_2 -}\,\frac{a_3}{a_3 +}\,\cdots\,\frac{a_n}{a_n} = \frac{1}{1 +}\,\frac{1}{a_1 +}\,\frac{a_1}{a_2 +}\,\frac{a_2}{a_3 +}\,\cdots\,\frac{a_{n-2}}{a_{n-1}}.$$

2. For the fraction $\frac{b_1}{a_1+}\frac{b_2}{a_2+}\frac{b_3}{a_3+}\cdots$, prove that

$$\frac{p_n}{p_{n-1}}=a_n+\frac{b_n}{a_{n-1}+}\frac{b_{n-1}}{a_{n-2}+}\cdots\frac{b_3}{a_2},$$

$$\frac{q_n}{q_{n-1}}=a_n+\frac{b_n}{a_{n-1}+}\frac{b_{n-1}}{a_{n-2}+}\cdots\frac{b_2}{a_1}.$$

3. Test for convergence:

(i) $\frac{1^2}{1+}\frac{2^2}{1+}\frac{3^2}{1+}\cdots$; (ii) $\frac{2}{1+}\frac{1^3\cdot 3}{1+}\frac{2^3\cdot 4}{1+}\cdots\frac{n^3(n+2)}{1+}\cdots$;

(iii) $\frac{x}{1+}\frac{x(x+1)}{2+}\frac{x(x+2)}{3+}\cdots\frac{x(x+n-1)}{n+}\cdots$;

(iv) $\frac{a}{b+}\frac{c}{d+}\frac{a}{b+}\frac{c}{d+}\cdots$.

4. If $a>1$, prove that

(i) $\frac{1}{a-}\frac{a}{a+1-}\frac{a+1}{a+2-}\frac{a+2}{a+3-}\cdots=\frac{1}{a-1}$;

(ii) $\frac{a}{a-}\frac{a+1}{a+1-}\frac{a+2}{a+2-}\cdots=\frac{a-1}{a-2}$.

[Follows at once from Art. 13 and Ex. 1.]

5. If $t+m$ and $t-m+1$ are positive, prove that the fraction

$$F=\frac{t+m}{2t+1-}\frac{t-m+1}{2-}\frac{t+m+1}{2t+3-}\frac{t-m+2}{2-}\frac{t+m+2}{2t+5-}\cdots$$

is convergent, and that $F=1+m/t$ or $F=1$, according as $m<0$ or $m\geqslant 0$.

6. Prove that $\frac{1}{3-}\frac{2}{2-}\frac{2}{5-}\frac{3}{2-}\frac{3}{7-}\cdots=1$.

Hence show that $\frac{1}{1-}\frac{1}{2-}\frac{1}{3-}\frac{2}{2-}\frac{2}{5-}\frac{3}{2-}\frac{3}{7-}\cdots$ is divergent.*

7. Prove that

$$\frac{1-m}{3-}\frac{2+m}{2-}\frac{2-m}{5-}\frac{3+m}{2-}\frac{3-m}{7-}\cdots=1-m \quad \text{or} \quad 1,$$

according as $m>0$ or $m\leqslant 0$. Hence show that the fraction

$$F=\frac{1}{1+}\frac{m}{1-}\frac{1+m}{2-}\frac{1-m}{3-}\frac{2+m}{2-}\frac{2-m}{5-}\cdots$$

is convergent if $m>0$ and divergent if $m<0$. Also if $m<0$, then $F=0$, and if $m=0$, then $F=1$.*

8. Prove that: (i) $\frac{1}{3-}\frac{2}{2-}\frac{3}{7-}\frac{4}{2-}\cdots\frac{2n-1}{4n-1-}\frac{2n}{2-}\cdots=1$;

and that (ii) $\frac{1}{3-}\frac{2}{2-}\frac{1}{4-}\frac{3}{2-}\cdots\frac{1}{n-}\frac{n-1}{2-}\cdots=\frac{2e-4}{2e-3}$.

* This result is required in the last part of this chapter.

9. Given that

$$\frac{e^x-e^{-x}}{e^x+e^{-x}}=\frac{x}{1+}\,\frac{x^2}{3+}\,\frac{x^2}{5+}\cdots\frac{x^2}{2n-1+}\cdots,$$

prove that any rational power of e is irrational.

Series and Continued Fractions

16. Fraction equivalent to a Series. (1) A continued fraction F is said to be *equivalent* to a series S when, for all values of n, the nth convergent of F is equal to the sum to n terms of S.

It follows that if S converges to a sum s, then F converges to the limit s, and we write $S=F$.

(2) **Euler's Transformation.** *Given a series*

$$S=u_1+u_2+\ldots u_n+\ldots,$$

it is required to find an equivalent continued fraction.

Denote the sum to n terms of the series by s_n. Take $u_1/1$ as the first convergent of the fraction, and let

$$s_2=u_1/(1-x_1),$$

then
$$x_1=1-u_1/s_2=u_2/(u_1+u_2)$$

and
$$s_2=\frac{u_1}{1-}\,\frac{u_2}{u_1+u_2}.$$

In this equation, writing u_2+u_3 for u_2, we have

$$s_3=\frac{u_1}{1-}\,\frac{u_2+u_3}{u_1+u_2+u_3}=\frac{u_1}{1-}\,\frac{u_2}{u_1+u_2-x_2},$$

where
$$\frac{u_2+u_3}{u_1+u_2+u_3}=\frac{u_2}{u_1+u_2-x_2}=\frac{u_3}{u_3+x_2},$$

and therefore
$$x_2=\frac{u_1u_3}{u_2+u_3}.$$

Hence
$$s_3=\frac{u_1}{1-}\,\frac{u_2}{u_1+u_2-}\,\frac{u_1u_3}{u_2+u_3}.$$

In this equation, put u_3+u_4 for u_3, therefore

$$s_4=\frac{u_1}{1-}\,\frac{u_2}{u_1+u_2-}\,\frac{u_1(u_3+u_4)}{u_2+u_3+u_4}=\frac{u_1}{1-}\,\frac{u_2}{u_1+u_2-}\,\frac{u_1u_3}{u_2+u_3-x_3},$$

where
$$\frac{u_3+u_4}{u_2+u_3+u_4}=\frac{u_3}{u_2+u_3-x_3}\quad\text{and, as before,}\quad x_3=\frac{u_2u_4}{u_3+u_4}.$$

Hence
$$s_4=\frac{u_1}{1-}\,\frac{u_2}{u_1+u_2-}\,\frac{u_1u_3}{u_2+u_3-}\,\frac{u_2u_4}{u_3+u_4}.$$

This process can be continued to any extent, and shows that

$$u_1+u_2+\ldots+u_n=\frac{u_1}{1-}\,\frac{u_2}{u_1+u_2-}\,\frac{u_1u_3}{u_2+u_3-}\,\ldots\,\frac{u_{n-2}u_n}{u_{n-1}+u_n}, \quad \ldots\ldots\ldots(\mathrm{A})$$

and this is Euler's transformation.

Equation (A) may also be written in the form

$$u_1+u_2+\ldots+u_n=\frac{u_1}{1-}\,\frac{u_2/u_1}{1+u_2/u_1-}\,\frac{u_3/u_2}{1+u_3/u_2-}\,\ldots\,\frac{u_n/u_{n-1}}{1+u_n/u_{n-1}}. \quad \ldots\ldots(\mathrm{B})$$

By changing the signs of u_2, u_4, u_6, ... in these equations, we find that

$$u_1-u_2+u_3-\ldots+(-1)^{n-1}u_n=\frac{u_1}{1+}\,\frac{u_2}{u_1-u_2+}\,\frac{u_1u_3}{u_2-u_3+}\,\ldots\,\frac{u_{n-2}u_n}{u_{n-1}-u_n} \quad \ldots\ldots(\mathrm{C})$$

$$=\frac{u_1}{1+}\,\frac{u_2/u_1}{1-u_2/u_1+}\,\frac{u_3/u_2}{1-u_3/u_2+}\,\ldots\,\frac{u_n/u_{n-1}}{1-u_n/u_{n-1}}. \quad \ldots\ldots\ldots\ldots(\mathrm{D})$$

If in (B) and (D) we put $u_n=a_1a_2a_3\ldots a_n$, it follows that

$$a_1+a_1a_2+a_1a_2a_3+\ldots+a_1a_2\ldots a_n$$

$$=\frac{a_1}{1-}\,\frac{a_2}{1+a_2-}\,\frac{a_3}{1+a_3-}\,\ldots\,\frac{a_n}{1+a_n}, \quad \ldots\ldots\ldots\ldots\ldots(\mathrm{E})$$

$$a_1-a_1a_2+a_1a_2a_3+\ldots+(-1)^{n-1}a_1a_2\ldots a_n$$

$$=\frac{a_1}{1+}\,\frac{a_2}{1-a_2+}\,\frac{a_3}{1-a_3+}\,\ldots\,\frac{a_n}{1-a_n}. \quad \ldots\ldots\ldots\ldots\ldots(\mathrm{F})$$

Again, by writing u_nx^n for u_n in (A) and (C), we find that

$$u_1x+u_2x^2+\ldots u_nx^n$$

$$=\frac{u_1x}{1-}\,\frac{u_2x}{u_1+u_2x-}\,\frac{u_1u_3x}{u_2+u_3x-}\,\ldots\,\frac{u_{n-2}u_nx}{u_{n-1}+u_nx}, \quad \ldots\ldots\ldots\ldots(\mathrm{G})$$

$$u_1x-u_2x^2+\ldots+(-1)^{n-1}u_nx^n$$

$$=\frac{u_1x}{1+}\,\frac{u_2x}{u_1-u_2x+}\,\frac{u_1u_3x}{u_2-u_3x+}\,\ldots\,\frac{u_{n-2}u_nx}{u_{n-1}-u_nx}. \quad \ldots\ldots\ldots\ldots(\mathrm{H})$$

Ex. 1. *Express* $1-1/e$ *as a continued fraction.*

[We have $1-1/e=1/\underline{|1}-1/\underline{|2}+1/\underline{|3}-1/\underline{|4}+\ldots$. Hence, by equation (D),

$$1-1/e=\frac{1}{1+}\,\frac{1/2}{1/2+}\,\frac{1/3}{2/3+}\,\frac{1/4}{2/4+}\ldots=\frac{1}{1+}\,\frac{1}{1+}\,\frac{2}{2+}\,\frac{3}{3+}\ldots.]$$

Ex. 2. *If* S *stands for* $\underline{|1}+\underline{|2}+\underline{|3}+\ldots+\underline{|n}$, *prove that*

$$F_n=\frac{1}{2+}\,\frac{2}{3+}\,\frac{3}{4+}\ldots\frac{n-1}{n}=\frac{S}{S+1},$$

and deduce that $F_\infty=1$.

[In (A), put $u_1=1$, $u_2=u_1$, $u_3=2u_2$, $u_4=3u_2$, etc.; and show that $1+S=1/(1-F_n)$. Cf. also Art. 13.]

17. Quotient of Two Series. Let u_0 and v_0 denote two convergent power series, with sums s and s'. If a continued fraction F converges to the limit s/s', we say that u_0/v_0 *is equal to* F.

(1) Let $u_0 = 1 + a_1x + a_2x^2 + \dots$, $v_0 = 1 + b_1x + b_2x^2 + \dots$; using the H.C.F. process, we have

f_1/x	u_0	v_0	1
	f_1v_1	u_0	
f_3/x	xu_1	xv_1	f_2
	xf_3v_2	xf_2u_1	
	x^2u_2	x^2v_2	f_4
	.....	.....	

where the constants f_1, f_2, ... are chosen so that the absolute terms of $u_0 - f_1v_1$, $v_1 - f_2u_1$, ... are zero. Since u_0, v_0 are convergent series, so are u_1, v_1, u_2, v_2, etc., and we have the equations

$$\begin{aligned} v_0 &= u_0 + xv_1, & u_0 &= f_1v_1 + xu_1, \\ v_1 &= f_2u_1 + xv_2, & u_1 &= f_3v_2 + xu_2, \\ &\dots\dots\dots\dots, & &\dots\dots\dots\dots, \\ v_n &= f_{2n}u_n + xv_{n+1}, & u_n &= f_{2n+1}v_{n+1} + xu_{n+1}. \end{aligned}$$

Therefore $v_0/u_0 = 1 + xv_1/u_0$, $u_0/v_1 = f_1 + xu_1/v_1$, etc.; and so we find that

$$\frac{u_0}{v_0} = \frac{1}{1+}\,\frac{x}{u_0/v_1} = \frac{1}{1+}\,\frac{x}{f_1+}\,\frac{x}{v_1/u_1} = \frac{1}{1+}\,\frac{x}{f_1+}\,\frac{x}{f_2+}\,\frac{x}{u_1/v_2}, \text{ etc.,}$$

and generally

$$\frac{u_0}{v_0} = \frac{1}{1+}\,\frac{x}{f_1+}\,\frac{x}{f_2+}\cdots\frac{x}{f_{2n-1}+}\,\frac{x}{v_n/u_n} = \frac{1}{1+}\,\frac{x}{f_1+}\cdots\frac{x}{f_{2n}+}\,\frac{x}{u_n/v_{n+1}}.$$

In obtaining these equations u_0, v_1, u_1, v_2, u_2, ... are used as divisors; it is also assumed that $v_0 \neq 0$. *If, then, x has such a value that $u_0 = 0$ or $v_0 = 0$, no such reckoning is possible. But if $v_n = 0$ or $u_n = 0 (n \geqslant 1)$, the fraction terminates.* When $v_n = 0$, the last element is x/f_{2n-2} (or $1/1$ if $n = 1$), and when $u_n = 0$, the last element is x/f_{2n-1}.

(2) Thus if u_0, v_0 are convergent power series, with sums s, s' different from zero, by using the H.C.F. process we can obtain a set of equations of the form

$$\frac{u_0}{v_0} = \frac{b_1}{a_1+}\,\frac{b_2x}{a_2+}\cdots\frac{b_{n-1}x}{a_{n-1}+}\,\frac{b_nx}{z_n},$$

where z_n is the ratio of two convergent series, leading to the fraction

$$F = \frac{b_1}{a_1+}\,\frac{b_2x}{a_2+}\cdots\frac{b_nx}{a_n+}\cdots.$$

Disregarding the exceptional case mentioned above, F is an infinite continued fraction, and there are three distinct possibilities :

(i) F may converge to the limit s/s', in which case we say that u_0/v_0 *is equal to* F; (ii) F may converge to a limit different from s/s'; or (iii) F may be non-convergent.

(3) **Criterion for Equality.** *To find a criterion as to whether* u_0/v_0 *is or is not equal to* F, consider the fractions

$$F' = \frac{b_{m+1}x}{a_{m+1}+}\frac{b_{m+2}x}{a_{m+2}+}\cdots\frac{b_{n-1}x}{a_{n-1}+}\frac{b_nx}{z_n}, \qquad F'' = \frac{b_{m+1}x}{a_{m+1}+}\frac{b_{m+2}x}{a_{m+2}+}\cdots\frac{b_nx}{a_n+}\cdots.$$

If, for any value of m, *it can be shown that* F'' *is convergent and that* $F'=F''$, *then*

$$\frac{u_0}{v_0} = \frac{b_1}{a_1+}\cdots\frac{b_mx}{a_m+F'} = \frac{b_1}{a_1+}\cdots\frac{b_mx}{a_m+F''} = F.$$

Let P_r/Q_r be the rth convergent of F'', then

$$F' - \frac{P_{n-2}}{Q_{n-2}} = \frac{z_nP_{n-1}+b_nxP_{n-2}}{z_nQ_{n-1}+b_nxQ_{n-2}} - \frac{P_{n-2}}{Q_{n-2}},$$

whence it readily follows that

$$F' - \frac{P_{n-2}}{Q_{n-2}} = \frac{1}{1+\epsilon_n}\left(\frac{P_{n-1}}{Q_{n-1}} - \frac{P_{n-2}}{Q_{n-2}}\right),$$

where

$$\epsilon_n = \frac{b_nx}{z_n}\cdot\frac{Q_{n-2}}{Q_{n-1}}.$$

Suppose that F'' *is convergent,* then $P_{n-1}/Q_{n-1} - P_{n-2}/Q_{n-2} \to 0$, and therefore $F' - P_{n-2}/Q_{n-2} \to 0$, provided that $1+\epsilon_n$ is never zero. Under these circumstances, $F'=F''$ and $u_0/v_0 = F$.

In order, then, to prove that F *converges and is equal to* u_0/v_0, *it is sufficient to show that, for some value of* m, F'' *is convergent, and that, as* $n\to\infty$, ϵ_n *always differs from* -1 *by a finite quantity.*

In particular, if $x>0$ *and* a_n, b_n, z_n *are all positive for* $n>m$, *then* $u_0/v_0 = F$, *provided only that* F'' *is convergent.*

(4) **A Special Case.** In the preceding, we may take $v_0=1$, and then, if the conditions of § (3) are satisfied, *we can find an infinite continued fraction* $F(x)$ *which is equal to* u_0.

But if $u_0=0$ for $x=x_1$, *we are not justified in assuming that* $F(x_1)=0$ without proving that u_0 and $F(x)$ are continuous at $x=x_1$.

In general, it will be found that the fraction $F(x)$ found in this way is of a simpler character than the fraction equivalent to u_0 found by Euler's method.

The process, however, presents some difficulty in practice; for in order to get the general form of the partial quotients, the remainders in the H.C.F. process have to be generalised, as in the example below. In Arts. 17 and 21, general theorems are given for the transformation of a series and a quotient of two series; and it will be found preferable to substitute in these for any special cases that are required.

Ex. 1. *Given that* $\tan^{-1}x = x - x^3/3 + x^5/5 - \dots$, *when* $0 < x \leqslant 1$, *find a continued fraction for* $\tan^{-1} x$.

The several remainders in the H.C.F. process are found to be multiples of

$$v_r = \Sigma_{n=1}^{\infty} (-1)^{n-1} n(n+1) \dots (n+r-2) x^{2n} / (2n+2r-3)(2n+2r-1) \dots (2n+4r-5),$$

$$u_r = \Sigma_{n=1}^{\infty} (-1)^{n-1} n(n+1) \dots (n+r-2) x^{2n} / (2n+2r-1)(2n+2r+1) \dots (2n+4r-3);$$

and, once this generalisation has been made, it is easy to show that

$$(2r-1)v_r/u_r = 4r - 1 + (2r)^2x^2/(ru_r/v_{r+1}),\ ru_r/v_{r+1} = 4r + 1 + (2r+1)^2x^2/((2r+1)v_{r+1}/u_{r+1}).$$

From which it follows immediately that

$$(2r-1)v_r/u_r = 4r - 1 + \frac{(2r)^2x^2}{4r+1+} \frac{(2r+1)^2x^2}{4r+3+} \frac{(2r+2)^2x^2}{4r+5+} \frac{(2r+3)^2x^2}{4r+7+} \dots;$$

i.e.,
$$v_1/u_1 = 3 + \frac{2^2x^2}{5+} \frac{3^2x^2}{7+} \frac{4^2x^2}{9+} \frac{5^2x^2}{11+} \dots;$$

and, writing $\lfloor n+r-2 / \lfloor n-1$ for $n(n+1)\dots(n+r-2)$, and remembering that $\lfloor 0 = 1$, we have $v_1 = 1 - x^2/3 + x^4/5 - \dots$, and $u_1 = 1/3 - x^2/5 + x^4/7 - \dots$, from which it follows that $\tan^{-1}x = xv_1$, and $v_1 + x^2u_1 = 1$.

Hence,
$$\tan^{-1}x = \frac{x}{1+} \frac{x^2}{v_1/u_1} = \frac{x}{1+} \frac{x^2}{3+} \frac{2^2x^2}{5+} \frac{3^2x^2}{7+} \frac{4^2x^2}{9+} \frac{5^2x^2}{11+} \dots,$$

where the fraction is continued to infinity, because it is convergent and satisfies the criterion for equality given in Art. 16.

18. Lambert's Transformation. *If* a *is any real number except zero or a negative integer,* m *is a positive integer, and*

$$u_m = 1 + \frac{x}{1\,.\,(a+m)} + \frac{x^2}{1\,.\,2(a+m)(a+m+1)} + \frac{x^3}{1\,.\,2\,.\,3(a+m)(a+m+1)(a+m+2)} + \dots,$$

then
$$\frac{u_1}{u_0} = \frac{a}{a+} \frac{x}{a+1+} \frac{x}{a+2+} \dots \frac{x}{a+n+} \dots,$$

where x *may have any value which does not make* u_0 *or* u_1 *equal to zero.*

It is easy to show that the series u_m converges for all values of x, and that $u_m - u_{m+1} = xf_{m+1}u_{m+2}$ where $f_{m+1} = 1/(a+m)(a+m+1)$.

In particular,
$$u_0 - u_1 = xf_1u_2, \quad u_1 - u_2 = xf_2u_3, \text{ etc.}$$

Therefore
$$\frac{u_0}{u_1} = 1 + \frac{xf_1}{u_1/u_2} = 1 + \frac{xf_1}{1+} \frac{xf_2}{u_2/u_3}.$$

Continuing in this way and substituting the values of $f_1, f_2, \ldots$ we get

$$\frac{u_1}{u_0}=\frac{1}{1+}\,\frac{x/a(a+1)}{1+}\,\frac{x/(a+1)(a+2)}{1+}\cdots\frac{x/(a+n-1)(a+n)}{u_n/u_{n+1}},$$

and therefore

$$\frac{u_1}{u_0}=\frac{a}{a+}\,\frac{x}{a+1+}\,\frac{x}{a+2+}\cdots\frac{x}{(a+n)u_n/u_{n+1}}.$$

We are thus led to the infinite continued fraction

$$F=\frac{a}{a+}\,\frac{x}{a+1+}\cdots\frac{x}{a+n+}\cdots.$$

(i) *Let* $x>0$. Choose m so that $m+a>0$, then u_n is positive for $n\geqslant m$.

Let

$$F'=\frac{x}{a+m+1+}\,\frac{x}{a+m+2+}\cdots\frac{x}{a+m+n+}\cdots$$

$$=\frac{1}{(a+m+1)/x+}\,\frac{1}{a+m+2+}\,\frac{1}{(a+m+3)/x+}\,\frac{1}{a+m+4+}\cdots.$$

Now the series $1/(a+m+2)+1/(a+m+4)+\ldots$ is divergent, therefore F' is convergent, and by Art. 7 F converges and is equal to u_1/u_0.

(ii) *Let* $x<0$ and let $x=-y$, then

$$u_m=1-\frac{y}{1\,.\,(a+m)}+\frac{y^2}{1\,.\,2(a+m)(a+m+1)}-\cdots,$$

$$\frac{u_1}{u_0}=\frac{a}{a-}\,\frac{y}{a+1-}\,\frac{y}{a+2-}\cdots\frac{y}{(a+n)u_n/u_{n+1}}$$

and

$$F=\frac{a}{a-}\,\frac{y}{a+1-}\cdots\frac{y}{a+n-}\cdots.$$

Let

$$F'=\frac{y}{a+m+1-}\,\frac{y}{a+m+2-}\cdots\frac{y}{a+m+n-}\cdots,$$

where m is chosen so that $a+m>y$, then F' is convergent by Art. 13. Let P_r/Q_r be the rth convergent of F', and let

$$\epsilon_n=\frac{y}{(a+m+n)u_{m+n}/u_{m+n+1}}\cdot\frac{Q_{n-2}}{Q_{n-1}}.$$

By Art. 13 (1), Q_r is positive and increases with r, therefore

$$0<Q_{n-2}/Q_{n-1}<1.$$

Also for $r\geqslant m$, we have $u_r>1-y/(a+r)>0$ and $0<u_{r+1}<1$;

therefore

$$u_r/u_{r+1}>1-y/(a+r)>0.$$

Hence

$$(a+m+n)u_{m+n}/u_{m+n+1}>a+m+n-y>0$$

and

$$0<\epsilon_n<y/(a+m+n-y).$$

Therefore $\epsilon_n\to 0$, and the conditions of Art. 17 (3) are satisfied, so that $u_1/u_0=F$.

19. Tan x and tanh x as Fractions. Putting $a=\frac{1}{2}$ and substituting $-x^2/4$ for x in the last article, we find that

$$u_0=\cos x,\ u_1=\frac{1}{x}\sin x,\ \text{and}\ \frac{u_1}{u_0}=\frac{1/2}{1/2-}\,\frac{x^2/4}{3/2-}\,\frac{x^2/4}{5/2-}\cdots,$$

provided that neither u_0 nor u_1 is zero; and hence

$$\tan x=\frac{x}{1-}\,\frac{x^2}{3-}\,\frac{x^2}{5-}\cdots\frac{x^2}{2n-1-}\cdots,$$

the case in which x is a multiple of π being excluded.

Again, if $a=\frac{1}{2}$ and we substitute $x^2/4$ for x, we find that

$$u_0=\cosh x,\ \text{and}\ u_1=\sinh x/x;$$

hence,

$$\tanh x=\frac{x}{1+}\,\frac{x^2}{3+}\,\frac{x^2}{5+}\cdots\frac{x^2}{2n-1+}\cdots.$$

20. Properties of Hypergeometric Series. In a classical memoir on this subject Gauss expressed the quotient of two hypergeometric series as a continued fraction.

Gauss's transformation is given in the next article, and the following properties of such series are required.

Let $$F(\alpha,\beta,\gamma,x)=1+\frac{\alpha\beta}{1\cdot\gamma}x+\frac{\alpha(\alpha+1)\cdot\beta(\beta+1)}{1\cdot 2\gamma(\gamma+1)}+\ldots.$$

(1) *The series is convergent* if $|x|<1$, or if $x=1$ and $\gamma>\alpha+\beta$, or if $x=-1$ and $\gamma+1>\alpha+\beta$. (See *H.A.*, XX, 7.)

(2) The reader can easily verify the following equalities:

$$F(\alpha,\beta+1,\gamma+1,x)-F(\alpha\beta\gamma x)=\frac{\alpha(\gamma-\beta)}{\gamma(\gamma+1)}xF(\alpha+1,\beta+1,\gamma+2,x),\ldots\text{(A)}$$

$$F(\alpha+1,\beta,\gamma+1,x)-F(\alpha,\beta,\gamma,x)=\frac{\beta(\gamma-\alpha)}{\gamma(\gamma+1)}xF(\alpha+1,\beta+1,\gamma+2,x).\ldots\text{(B)}$$

(3) *Note on the Gamma Function.* For positive values of n, the function $\Gamma(n)$ may be defined by

$$\Gamma(n)=\int_0^\infty e^{-x}x^{n-1}dx.$$

Thus if n is positive, so is $\Gamma(n)$. Also it can be shown that

$$\Gamma(n+1)=n\Gamma(n)\quad\text{and}\quad\Gamma(1)=0.$$

Hence, if n is a positive integer, $\Gamma(n)=\underline{|n-1}$.

Further, it is proved in treatises on the Integral Calculus that if l and m are positive,

$$\int_0^1 x^{l-1}(1-x)^{m-1}dx=\frac{\Gamma(l)\Gamma(m)}{\Gamma(l+m)}.\ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

(4) *If the series* $F(\alpha, \beta, \gamma, x)$ *is convergent and* α, γ, $\gamma-\alpha$ *are positive,*

$$F(\alpha, \beta, \gamma, x)=\frac{\Gamma(\gamma)}{\Gamma(\alpha)\Gamma(\gamma-\alpha)}\int_0^1 t^{\alpha-1}(1-t)^{\gamma-\alpha-1}.(1-xt)^{-\beta}\,dt, \quad \ldots\ldots(\mathbf{D})$$

To prove this, we expand $(1-xt)^{-\beta}$ and integrate term by term, using equation (C). It follows that $F(\alpha, \beta, \gamma, x)$ *is positive for all values of* x *for which the series is convergent if* α, γ, $\gamma-\alpha$ *are all positive.*

(5) If the values of the letters are restricted as in § (4), the following equalities are an immediate consequence of equation (D):

$$\gamma F(\alpha, \beta, \gamma, x)-(\gamma-\alpha)F(\alpha, \beta+1, \gamma+1, x)=\alpha(1-x)F(\alpha+1, \beta+1, \gamma+1, x),$$
$$\gamma F(\alpha, \beta, \gamma, x)-(\gamma-\beta)F(\alpha+1, \beta, \gamma+1, x)=\beta(1-x)F(\alpha+1, \beta+1, \gamma+1, x).$$

By equating coefficients we can show that these equations hold if $|x|<1$ or if $x=1$ and $\gamma>\alpha+\beta+1$, or if $x=-1$ and $\gamma>\alpha+\beta$.

21. Gauss's Transformation for the quotient of two hypergeometric series. Let

$$F(\alpha, \beta, \gamma, x)=1+\frac{\alpha\beta}{1.\gamma}x+\frac{\alpha(\alpha+1)\beta(\beta+1)}{1.2\gamma(\gamma+1)}x^2+\ldots,$$

and suppose the series to be convergent. Let

$$v_r=F(\alpha+r, \beta+r, \gamma+2r, x) \quad \text{and} \quad u_r=F(\alpha+r, \beta+r+1, \gamma+2r+1, x),$$

so that $u_0/v_0=F(\alpha, \beta+1, \gamma+1, x)/F(\alpha, \beta, \gamma, x)$, then Gauss's transformation is

$$\frac{u_0}{v_0}=\frac{1}{1-}\frac{k_1x}{1-}\frac{k_2x}{1-}\cdots\frac{k_{2n-1}x}{1-}\frac{k_{2n}x}{v_n/u_n}=\frac{1}{1-}\frac{k_1x}{1-}\cdots\frac{k_{2n}x}{1-}\frac{k_{2n+1}x}{u_n/v_{n+1}},$$

where $$k_{2r+1}=\frac{(\alpha+r)(\gamma-\beta+r)}{(\gamma+2r)(\gamma+2r+1)}, \quad k_{2r}=\frac{(\beta+r)(\gamma-\alpha+r)}{(\gamma+2r-1)(\gamma+2r)}.$$

Proof. Referring to the conditions of Art. 20, (1), it will be seen that, since v_0 is convergent, so also are u_0, v_1, u_1, v_2, u_2, etc. Writing $\alpha+n$, $\beta+n$, $\gamma+2n$ for α, β, γ in equation (A), and substituting $\alpha+n$, $\beta+n+1$, $\gamma+2n+1$ for α, β, γ in equation (B), we find that

$$u_n-v_n=k_{2n+1}xv_{n+1}, \quad \text{and} \quad v_{n+1}-u_n=k_{2n+2}xu_{n+1}.$$

In particular, $u_0-v_0=k_1xv_1$, $v_1-u_0=k_2xu_1$, $u_1-v_1=k_3xv_2$, etc.

$$\frac{u_0}{v_0}=\frac{1}{1-}\frac{k_1x}{u_0/v_1}=\frac{1}{1-}\frac{k_1x}{1-}\frac{k_2x}{v_1/u_1}=\frac{1}{1-}\frac{k_1x}{1-}\frac{k_2x}{1-}\frac{k_3x}{u_1/v_2},$$

and so on, to any extent. This proves the transformation.

NOTE. The fraction $u_0/v_0=F(\alpha, \beta+1, \gamma+1, x)/F(\alpha, \beta, \gamma, x)$ is often denoted by $G(\alpha, \beta, \gamma, x)$.

22. Gauss's Infinite Continued Fraction. *If the series* $v_0 = F(\alpha, \beta, \gamma, x)$ *is convergent, then the fraction*

$$G = \frac{1}{1-}\frac{k_1 x}{1-}\frac{k_2 x}{1-}\cdots\frac{k_n x}{1-}\cdots,$$

is convergent and $u_0/v_0 = G$*; except perhaps when* $x = 1$*, in which case* u_0/v_0 *may or may not be equal to* G.

(i) *First let* $-1 \leqslant x < 0$ and let $x = -y$, then $0 < y \leqslant 1$, and

$$\frac{u_0}{v_0} = \frac{1}{1+}\frac{k_1 y}{1+}\cdots\frac{k_{n-1} y}{1+}\frac{k_n y}{z_n} \quad \text{and} \quad G = \frac{1}{1+}\frac{k_1 y}{1+}\cdots\frac{k_n y}{1+}\cdots,$$

where $z_{2r} = v_r/u_r$ and $z_{2r+1} = u_r/v_{r+1}$.

By Art. 4 (4), z_r is positive for sufficiently large values of r; so also is k_r. Choose m so that k_r and z_r are positive for $r \geqslant 2m+1$, and consider

$$G' = \frac{k_{2m+1} y}{1+}\frac{k_{2m+2} y}{1+}\cdots\frac{k_{2m+n} y}{1+}\cdots.$$

By Art. 10 (3), this fraction is equivalent to $\dfrac{1}{f_1+}\dfrac{1}{f_2+}\cdots\dfrac{1}{f_n+}\cdots$, where

$$f_{2n} = \frac{k_{2m+1}k_{2m+3}\cdots k_{2m+2n-1}}{k_{2m+2}k_{2m+4}\cdots k_{2m+2n}}, \quad f_{2n+1} = \frac{k_{2m+2}k_{2m+4}\cdots k_{2m+2n}}{k_{2m+1}k_{2m+3}\cdots k_{2m+2n+1}}\cdot\frac{1}{y}.$$

Hence, by Art. 10 (3), G' is convergent if at least one of the series

$$f_1 + f_3 + f_5 + \ldots, \qquad f_2 + f_4 + f_6 + \ldots$$

is divergent. For the first of these, applying the test of Art. 16 (3), we have

$$\frac{f_{2n-1}}{f_{2n+1}} = \frac{k_{2m+2n-1}}{k_{2m+2n}} = \frac{(\alpha+m+n)(\alpha-\beta+m+n)(\gamma+2m+2n-1)}{(\gamma+2m+2n+1)(\beta+m+n)(\gamma-\alpha+m+n)}$$

by expanding in powers of $1/n = 1 + \dfrac{1}{n}(2\alpha - 2\beta - 1) + \ldots$.

Hence, $f_1 + f_3 + \ldots$ is divergent if $2\alpha - 2\beta - 1 \leqslant 1$, or if $\alpha \leqslant \beta + 1$.

Similarly, $f_2 + f_4 + \ldots$ is divergent if $2\beta + 1 - 2\alpha \leqslant 1$, or if $\alpha \geqslant \beta$.

Therefore at least one of the series diverges and G' is convergent. Also k_r and z_r are positive for $r \geqslant 2m+1$, hence by Art. 17 (3), G converges and is equal to u_0/v_0.

(ii) *Suppose that* $0 < x < 1$. It is easily seen that Gauss's transformation may be written

$$\frac{u_0}{v_0} = \frac{\gamma}{\gamma-}\frac{l_1 x}{\gamma+1-}\frac{l_2 x}{\gamma+2-}\cdots\frac{l_{n-1} x}{\gamma+n-1-}\frac{l_n x}{(\gamma+n)z_n},$$

where $l_{2r} = (\beta+r)(\gamma-\alpha+r)$ and $l_{2r+1} = (\alpha+r)(\gamma-\beta+r)$.

Let $$G=\frac{\gamma}{\gamma-}\frac{l_1x}{\gamma+1-}\cdots\frac{l_nx}{\gamma+n-}\cdots,$$ and consider

$$G'=\frac{l_{2m+1}x}{\gamma+2m+1-}\frac{l_{2m+2}x}{\gamma+2m+2-}\cdots\frac{l_{2m+n}x}{\gamma+2m+n-}\cdots.$$

Let m be chosen so that $l_r>0$ for $r>2m$, and so that

$$m>\beta-\gamma,\quad \alpha+m+1>0 \quad\text{and}\quad \beta+m+1>0.$$

Then if P_r/Q_r is the rth convergent of G',

$$Q_1=\gamma+2m+1>(\beta+m+1)Q_0, \quad\text{for}\quad m>\beta-\gamma \quad\text{and}\quad Q_0=1,$$
$$Q_2=(\gamma+2m+2)Q_1-(\beta+m+1)(\gamma-\alpha+m+1)xQ_0$$
$$>(\gamma+2m+2)Q_1-(\gamma-\alpha+m+1)Q_1>(\alpha+m+1)Q_1,$$
$$Q_3=(\gamma+2m+3)Q_2-(\alpha+m+1)(\gamma-\beta+m+1)xQ_1$$
$$>(\gamma+2m+3)Q_2-(\gamma-\beta+m+1)Q_2>(\beta+m+2)Q_2.$$

Continuing in this way, we can show that

$$Q_{2n-1}>(\beta+m+n)Q_{2n-2} \quad\text{and}\quad Q_{2n}>(\alpha+m+n)Q_{2n-1},$$

and since Q_1 is positive, so is every Q. Applying the test of convergence of Art. 12, we have to consider the expression $\eta_r=l_{2m+r}xQ_{r-2}/Q_r$.

By the preceding,

$$\eta_{2n}=l_{2m+2n}x\cdot\frac{Q_{2n-2}}{Q_{2n}}<\frac{\gamma-\alpha+m+n}{\alpha+m+n}\cdot x,$$

$$\eta_{2n+1}=l_{2m+2n+1}x\cdot\frac{Q_{2n-1}}{Q_{2n+1}}<\frac{\gamma-\beta+m+n}{\beta+m+n+1}\cdot x.$$

Each of these fractions tends to x as $n\to\infty$, hence, after a certain stage, $\eta_r<k$ where $x<k<1$, therefore G' is convergent.

Again, applying the test of Art. 17 (3), we consider the expression

$$\epsilon_r=\frac{l_{2m+r}x}{(\gamma+2m+r)z_{2m+r}}\cdot\frac{Q_{r-2}}{Q_{r-1}}.$$

If in equations of Art. 20 (5) we write $\alpha+r$, $\beta+r$, $\gamma+2r$ and $\alpha+r$, $\beta+r+1$, $\gamma+2r+1$ respectively for α, β, γ, we shall find that $z_{2r}(\gamma+2r)>\gamma-\alpha+r$ and $z_{2r+1}(\gamma+2r+1)>\gamma-\beta+r$ for $r>2m$.

Hence, using the above inequalities,

$$\epsilon_{2n}<\frac{(\beta+m+n)(\gamma-\alpha+m+n)x}{\gamma-\alpha+m+n}\cdot\frac{1}{\beta+m+n},$$

$$\epsilon_{2n+1}<\frac{(\alpha+m+n)(\gamma-\beta+m+n)x}{\gamma-\beta+m+n}\cdot\frac{1}{\alpha+m+n}.$$

Thus $\epsilon_r<x<1$ and the criterion of Art. 17 (3) holds, so that G is convergent and is equal to u_0/v_0.

23. Special Cases. (1) If in Art. 20 we write $\alpha=l$, $\beta=0$, $\gamma=m-1$ where $m\neq 1$, we have

$$u_0=F(l,\,1,\,m,\,x)=1+\frac{l}{m}x+\frac{l(l+1)}{m(m+1)}x^2+\ldots$$

and $v_0=F(l,\,0,\,m-1,\,x)=1$. Hence we can express the series u_0 as a continued fraction.

(2) **The Logarithmic Series.** If $-1<x\leqslant 1$, we have

$$\frac{1}{x}\log(1+x)=1-\frac{1}{2}x+\frac{1}{3}x^2-\ldots=F(1,\,1,\,2,\,-x).$$

In Art. 21, let $\alpha=1$, $\beta=0$, $\gamma=1$, and write $-x$ for x, then

$$u_0=\frac{1}{x}\log(1+x),\quad v_0=1,$$

and by Art. 22,

$$u_0=\frac{1}{1+}\,\frac{k_1x}{1+}\,\frac{k_2x}{1+}\cdots\frac{k_nx}{1+}\cdots,$$

where $k_{2r}=r/2(2r+1)$ and $k_{2r+1}=(r+1)/2(2r+1)$; therefore

$$\log(1+x)=\frac{x}{1+}\,\frac{\frac{1}{2}x}{1+}\,\frac{\frac{1}{2.3}x}{1+}\,\frac{\frac{2}{2.3}x}{1+}\,\frac{\frac{2}{2.5}x}{1+}\,\frac{\frac{3}{2.5}x}{1+}\,\frac{\frac{3}{2.7}x}{1+}\cdots$$

$$=\frac{x}{1+}\,\frac{x}{2+}\,\frac{x}{3+}\,\frac{2x}{2+}\,\frac{2x}{5+}\,\frac{3x}{2+}\,\frac{3x}{7+}\cdots\frac{nx}{2+}\,\frac{nx}{2n+1+}\cdots.$$

When $x=-1$, the fraction is divergent (see Exercise XVI, Ex. 6).

(3) **The Binomial Series.** Assuming that the series is convergent, we have

$$(1-x)^{-m}=1+mx+\frac{m(m+1)}{1.2}x^2+\ldots=F(m,\,1,\,1,\,x).$$

If in Art. 21 we write $\alpha=m$, $\beta=0$, $\gamma=0$, then $v_n=F(m+n,\,n,\,2n,\,x)$ for $n\geqslant 1$ and $u_n=F(m+n,\,n+1,\,2n+1,\,x)$ for $n\geqslant 0$.

Thus $u_0=(1-x)^{-m}$ and v_0 is *undefined*. Now $u_0-1=mxv_1$, and therefore we may take $v_0=1$ and $k_1=m$. The rest of the k's are given by the equations of Art. 21, whence

$$k_{2r}=(r-m)/2(2r-1)\quad\text{and}\quad k_{2r+1}=(r+m)/2(2r+1).$$

Hence, as the series is convergent, we have (except perhaps when $x=1$),

$$(1-x)^{-m}=\frac{1}{1-}\,\frac{mx}{1-}\,\frac{\frac{1-m}{2.1}x}{1-}\,\frac{\frac{1+m}{2.3}x}{1-}\,\frac{\frac{2-m}{2.3}x}{1-}\,\frac{\frac{2+m}{2.5}x}{1-}\cdots$$

$$=\frac{1}{1-}\,\frac{mx}{1-}\,\frac{(1-m)x}{2-}\,\frac{(1+m)x}{3-}\,\frac{(2-m)x}{2-}\,\frac{(2+m)x}{5-}\cdots.$$

Changing the sign of m, we have

$$(1-x)^m = 1 + \frac{mx}{1-} \frac{(1+m)x}{2-} \frac{(1-m)x}{3-} \frac{(2+m)x}{2-} \frac{(2-m)x}{5-} \cdots;$$

the only doubt being as to what happens when $x=1$. It follows from Ex. XVI, Ex. 7, that in this case the last fraction converges to zero, or is divergent according as $m>0$ or $m<0$. Thus the last two equations are true for all values of m.

(4) **The Exponential Series.** Putting x/m for x in § (3), we find that

$$\left(1-\frac{x}{m}\right)^{-m} = \frac{1}{1-} \frac{x}{1-} \frac{(1/m-1)x}{2-} \frac{(1/m+1)x}{3-} \frac{(2/m-1)x}{2} \cdots - \frac{\{(n-1)/m+1\}x}{2n-1-} \frac{(n/m-1)x}{2v_n/u_n}, \quad \text{.....(A)}$$

where $v_0=1$, $v_n = F(m+n, n, 2n, x/m)$ for $n \geqslant 1$ and

$$u_n = F(m+n, n+1, 2n+1, x/m).$$

Now as $m \to \infty$, $\lim (1-x/m)^{-m} = e^x$; also

$$\lim v_n = 1 + \frac{n}{2n} \cdot \frac{x}{\underline{1}} + \frac{n(n+1)}{2n(2n+1)} \cdot \frac{x^2}{\underline{2}} + \cdots,$$

$$\lim u_n = 1 + \frac{n+1}{2n+1} \cdot \frac{x}{\underline{1}} + \frac{(n+1)(n+2)}{(2n+1)(2n+2)} \cdot \frac{x^2}{\underline{2}} + \cdots \text{.....(B)}$$

Since the continued fraction in (A) *terminates*, we may give the numerators and denominators of the various elements their limiting values, therefore

$$e^x = \frac{1}{1-} \frac{x}{1+} \frac{x}{2-} \frac{x}{3+} \frac{x}{2-} \frac{x}{5+} \cdots - \frac{x}{2n-1+} \frac{x}{2v_n/u_n}, \quad \text{.....(C)}$$

where v_n, u_n denote the series in equations (B) and the v's and u's are connected by

$$u_n - v_n = \frac{1}{2(2n+1)} x v_{n+1}, \quad v_{n+1} - u_n = \frac{1}{2(2n+1)} x u_{n+1}. \quad \text{.....(D)}$$

It should be noticed that, for sufficiently large values of n, both u_n and v_n are positive, for they are the limits of positive functions.

By applying the test of Art. 17, we can now show that

$$e^x = \frac{1}{1-} \frac{x}{1+} \frac{x}{2-} \frac{x}{3+} \frac{x}{2-} \frac{x}{5+} \cdots \frac{x}{+2-} \frac{x}{2n-1+} \cdots.$$

[The method of applying the test is indicated in Ex. XVII, 17.]

By changing the sign of x and inverting, we have also

$$e^x = 1 + \frac{x}{1-} \frac{x}{2+} \frac{x}{3-} \frac{x}{2+} \frac{x}{5-} \cdots \frac{x}{-2+} \frac{x}{2n-1-} \cdots.$$

EXERCISE XVII

1. If n is a positive integer or if the series for $(1+x)^n$ is convergent, prove that

(i) $(1+x)^n = \dfrac{1}{1-}\ \dfrac{nx}{1+nx-}\ \dfrac{1\,.\,(n-1)x}{2+(n-1)x-}\ \dfrac{2(n-2)x}{3+(n-2)x-}\ \ldots$;

(ii) $\dfrac{1}{1-}\ \dfrac{n}{n+1-}\ \dfrac{1\,.\,(n-1)}{n+1-}\ \dfrac{2(n-2)}{n+1-}\ \ldots = 2^n$ where $n > -1$;

(iii) $\dfrac{1}{1+}\ \dfrac{n}{1-n+}\ \dfrac{1\,.\,(n-1)}{3-n+}\ \dfrac{2(n-2)}{5-n+}\ \ldots = 0$ where $n > 0$.

Verify the last when $n = 3$.

2. Prove that:

(i) $e^x = \dfrac{1}{1-}\ \dfrac{x}{1+x-}\ \dfrac{x}{2+x-}\ \dfrac{2x}{3+x-}\ \ldots$; (ii) $\dfrac{1}{3-}\ \dfrac{2}{4-}\ \dfrac{3}{5-}\ \ldots = \dfrac{e-2}{e-1}$;

(iii) $\dfrac{2}{2+}\ \dfrac{3}{3+}\ \dfrac{4}{4+}\ \ldots = e-2$; (iv) $\dfrac{1}{2+}\ \dfrac{2}{3+}\ \dfrac{3}{4+}\ \ldots = \dfrac{3-e}{e-2}$.

3. Prove that:

(i) $\log(1+x) = \dfrac{x}{1+}\ \dfrac{1^2x}{2-x+}\ \dfrac{2^2}{3-2x+}\ \dfrac{3^2}{4-3x+}\ \ldots$;

(ii) $\dfrac{1^2}{1+}\ \dfrac{2^2}{1+}\ \dfrac{3^2}{1+}\ \ldots = \dfrac{1}{\log 2} - 1$.

4. Prove that

$$\frac{\sin x}{x} = \frac{1}{1+}\ \frac{x^2}{2\,.\,3-x^2+}\ \frac{2\,.\,3x^2}{4\,.\,5-x^2+}\ \frac{4\,.\,5x^2}{6\,.\,7-x^2+}\ \ldots .$$

5. Prove that $\dfrac{1}{1-}\ \dfrac{a}{a+1-}\ \dfrac{a+1}{a+2-}\ \ldots\ \dfrac{a+n-1}{a+n}$

$$= 1 + a + a(a+1) + a(a+1)(a+2) + \ldots \text{ to } n+1 \text{ terms.}$$

6. Prove that $\dfrac{1}{1+}\ \dfrac{x}{1+}\ \dfrac{x(x+1)}{2+}\ \dfrac{x(x+2)}{3+}\ \ldots\ \dfrac{x(x+n-1)}{n+}\ \ldots$

is equivalent to $1 - \dfrac{x}{x+1} + \dfrac{x^2}{(x+1)(x+2)} - \dfrac{x^3}{(x+1)(x+2)(x+3)} + \ldots$.

Hence show that when $x = 2$ the value of the fraction is $(e^2+1)/2e^2$.

7. (i) $\dfrac{1}{1+}\ \dfrac{1^4}{3+}\ \dfrac{2^4}{5+}\ \ldots\ \dfrac{(n-1)^4}{2n-1+}\ \ldots = 1 - \dfrac{1}{2^2} + \dfrac{1}{3^2} - \dfrac{1}{4^2} + \ldots = \dfrac{\pi^2}{12}$;

(ii) $\dfrac{1}{1-}\ \dfrac{1^4}{5-}\ \dfrac{2^4}{13-}\ \ldots\ \dfrac{(n-1)^4}{2n^2-2n+1-}\ \ldots = 1 + \dfrac{1}{2^2} + \dfrac{1}{3^2} + \dfrac{1}{4^2} + \ldots = \dfrac{\pi^2}{6}$.

8. $\dfrac{2}{1+}\ \dfrac{1^3\,.\,3}{1+}\ \dfrac{2^3\,.\,4}{1+}\ \ldots\ \dfrac{n^3(n+2)}{1+}\ \ldots$ is equivalent to the series

$$2/1 - 3/2 + 4/3 - 5/4 + \ldots .$$

Hence show that the fraction oscillates between $\log 2$ and $1 + \log 2$.

9. If

$$v_r=\Sigma_{n=1}^{\infty}(-x)^{n-1}\frac{\lfloor r+n-1}{\lfloor n-1\,\lfloor 2r+n-1}, \quad u_r=\Sigma_{n=1}^{\infty}(-x)^{n-1}\frac{\lfloor r+n-2}{\lfloor n-1\,\lfloor 2r+n-2},$$

prove that

(i) $u_r-2v_r=xu_{r+1}$, and $v_r-(2r+1)u_{r+1}=-xv_{r+1}$;

(ii) $v_0/u_1=1-\dfrac{x}{2+}\dfrac{x}{3-}\dfrac{x}{2+}\dfrac{x}{5-}\cdots$, where $v_0=e^{-x}$, $u_1=(1-e^{-x})/x$;

(iii) $e^x=1+\dfrac{x}{1-}\dfrac{x}{2+}\dfrac{x}{3-}\dfrac{x}{2+}\dfrac{x}{5-}\dfrac{x}{2+}\dfrac{x}{7-}\cdots$.

10. If $v_r=r\left\{\dfrac{\lfloor r-1}{\lfloor 2r}+\dfrac{\lfloor r}{\lfloor 2r+1}(m-r-1)x+\dfrac{\lfloor r+1}{\lfloor 2r+2}\dfrac{(m-r-1)(m-r-2)}{\lfloor 2}x^2+\cdots\right\}$,

$$u_r=\frac{\lfloor r-1}{\lfloor 2r-1}+\frac{\lfloor r}{\lfloor 2r}(m-r)x+\frac{\lfloor r+1}{\lfloor 2r+1}\frac{(m-r)(m-r-1)}{\lfloor 2}x^2+\cdots,$$

prove that (i) $u_r-2v_r=(m+r)xu_{r+1}$, and $v_r-(2r+1)u_{r+1}=-(m-r-1)xv_{r+1}$,

(ii) $u_0=(1+x)^m$, $u_1=\{(1+x)^m-1\}/mx$, $u_1-(m-1)xv_1=1$;

(iii) $(1+x)^m=1+\dfrac{mx}{1-}\dfrac{(m-1)x}{2+}\dfrac{(m+1)x}{3-}\dfrac{(m-2)x}{2+}\dfrac{(m+2)x}{5-}\cdots$.

11. If $v_r=2^r\left\{\dfrac{\lfloor r}{\lfloor 2r}-\dfrac{\lfloor r+1}{\lfloor 2r+2}\dfrac{\lfloor x^2}{\lfloor 1}+\dfrac{\lfloor r+2}{\lfloor 2r+4}\dfrac{\lfloor x^4}{\lfloor 4}-\cdots\right\}$, prove that

(i) $v_r-(2r+1)v_{r+1}=-x^2v_{r+2}$, $v_0=\cos x$, and $v_1=\sin x/x$,

(ii) $\tan x=xv_1/u_1=\dfrac{x}{1-}\dfrac{x^2}{3-}\dfrac{x^2}{5-}\dfrac{x^2}{7-}\cdots$.

12. If $v_r=\Sigma_{n=1}^{\infty}\dfrac{r+n-1}{\lfloor n-1\,\lfloor 2r+n}x^{n-1}$, $u_r=\Sigma_{n=1}^{\infty}\dfrac{r+n-1}{n-1}\dfrac{r+n}{2r+n-1}x^{n-1}$,

prove that (i) $v_r-2u_r=xv_{r+1}$, and $(r+1)u_r-(2r+3)v_{r+1}=(r+1)xu_{r+1}$,

(ii) $v_0=\dfrac{1}{x}\log(1+x)$, $u_0=x-\log(1+x)/x^2$, and $v_0+xu_0=1$,

(iii) $\log(1+x)=xv_0/(v_0+xu_0)=\dfrac{x}{1+}\dfrac{x}{2+}\dfrac{x}{3+}\dfrac{2x}{2+}\dfrac{2x}{5+}\dfrac{3x}{2+}\dfrac{3x}{7+}\cdots$.

13. If $0<x\leqslant 1$, show that $(6x+3x^2)/(6+6x+x^2)$ is an approximation in defect to $\log(1+x)$ with an error less than $x^5/180$.

Hence show that $\log_e 1{\cdot}1=63/661$ with an error in defect less than ·00000006.

[The expression is the fourth convergent to the fraction in Ex. 12 (iii).]

14. Given that $\tan^{-1}x=xF(\frac{1}{2},\ 1,\ \frac{3}{2},\ -x^2)$, show that

$$\tan^{-1}x=\frac{x}{1+}\frac{1^2x}{3+}\frac{2^2x}{5+}\cdots\frac{n^2x}{2n+1+}\cdots.$$

15. Given that $\tanh^{-1}x=xF(\frac{1}{2},\ 1,\ \frac{3}{2},\ x^2)$, prove that

$$\tanh^{-1}x=\frac{1}{2}\log\frac{1+x}{1-x}=\frac{x}{1-}\frac{1^2x}{3-}\frac{2^2x}{5-}\cdots\frac{n^2x}{2n+1-}\cdots.$$

16. Let $F=\dfrac{x}{a_1-}\dfrac{x}{a_2+}\dfrac{x}{a_3-}\dfrac{x}{a_4+}\cdots$, where the signs are alternately positive and negative. Prove that, if (i) all the q's are positive and (ii) if, after a certain stage, $x^2q_{n-2}q_{n-3}/q_nq_{n-1}<1$, and (iii) $x^n/q_nq_{n-1}\to 0$, then F is convergent.

This completes the proof in Art. 23 (4), showing that

$$e^x=\frac{1}{1-}\frac{x}{1+}\frac{x}{2-}\frac{x}{3+}\cdots\frac{x}{2-}\frac{x}{2n-1+}\cdots.$$

17. Let $0<x<2m-1$ and let v_r, u_r be defined as in Art. 23, then if

$$F'=\frac{x}{2-}\frac{x}{2m+1+}\frac{x}{2-}\frac{x}{2m+3+}\cdots\frac{x}{2-}\frac{x}{(2m+2n-1)u_{m+n-1}/v_{m+n}},$$

$$F''=\frac{x}{2-}\frac{x}{2m+1+}\cdots\frac{x}{2-}\frac{x}{2m+2n-1+}\cdots,$$

show that F'' is convergent and is equal to F'.

[Let P_r/Q_r be the rth convergent of F'', and assume that Q_{2n-2} and Q_{2n-3} are positive; then $Q_{2n-1}=2Q_{2n-2}+xQ_{2n-3}$, so $Q_{2n-1}>2Q_{2n-2}$ and $Q_{2n-1}>xQ_{2n-3}$.

Also $$Q_{2n}=(2m+2n-1)Q_{2n-1}-xQ_{2n-2}>\{2(x+2n)-x\}Q_{2n-2},$$

therefore $Q_{2n}>(x+4n)Q_{2n-2}$. Now $Q_0>0$, $Q_1>0$; hence $Q_n>0$.

(ii) Referring to Ex. 16, it is obvious that $x^2Q_{n-2}Q_{n-3}/Q_nQ_{n-1}\to 0$. Also

$$0<\frac{x^{2n}}{Q_{2n}Q_{2n-1}}<\frac{x^2}{(1+2\,.\,4/x)(1+3\,.\,4/x)\ldots(1+n\,.\,4/x)}\to 0,$$

therefore $x^{2n}/Q_{2n}Q_{2n-1}$ (and similarly $x^{2n-1}/Q_{2n-1}Q_{2n-2}$) tends to zero. Therefore F'' is convergent.

Again, the conditions of Art. 17 (3) hold, for

$$0<-\epsilon_{2n}=\frac{x}{(2m+2n-1)u_{m+n-1}/v_{m+n}}\cdot\frac{Q_{2n-2}}{Q_{2n-1}}<\frac{2m-1}{2(2m+2n-1)},$$

therefore $\epsilon_{2n}\to 0$; also ϵ_{2n+1} is positive. Therefore $F'=F''$.]

Next, let $0<y<2m-1$, and let

$$F'=\frac{y}{2+}\frac{y}{2m+1-}\frac{y}{2+}\frac{y}{2m+3-}\cdots\frac{y}{+2m+2n-1-}\frac{y}{2v_{m+n}/u_{m+n}},$$

$$F''=\frac{y}{2+}\frac{y}{2m+1-}\frac{y}{2+}\frac{y}{2m+3}\cdots\frac{y}{+2m+2n-1-}\frac{y}{2+}\cdots.$$

If P_r/Q_r is the rth convergent of F'', prove that

(i) Every Q is positive and

$$Q_{2n}>(y+2n)Q_{2n-1},\quad Q_{2n}>yQ_{2n-2},\quad Q_{2n+1}>(y+4n)Q_{2n-1}.$$

(ii) Hence show that F'' is convergent and equal to F'.

[The first part is similar to that in the preceding case.

For the last part, take m so that v_{m+n} and u_{m+n} are positive for $n\geqslant 0$, then by equation (D) of Art. 23 (4), when $x=-y$, we have $v_{m+n}>u_{m+n}$ and

$$0<-\epsilon_{2n+1}=\frac{y}{2v_{m+n}/u_{m+n}}\cdot\frac{Q_{2n-1}}{Q_{2n}}<\frac{y}{2(y+2n)},\ \text{therefore}\ \epsilon_{2n+1}\to 0,\ \text{etc.}]$$

CHAPTER XLVIII

LINEAR TRANSFORMATION

1. Definitions. Let a set of variables $x, y, \ldots$ be connected with a new set $X, Y, \ldots$ by the equations

$$x = l_1X + m_1Y + n_1Z + \ldots ,$$
$$y = l_2X + m_2Y + n_2Z + \ldots ,$$
$$z = l_3X + m_3Y + n_3Z + \ldots .$$
$$\ldots\ldots\ldots\ldots\ldots\ldots .$$

These equations constitute a *linear substitution*. The effect of such a substitution is a *linear transformation*, of which the determinant $(l_1m_2n_3 \ldots)$ is the *modulus*; this determinant will be denoted by μ. Solving for $X, Y, \ldots$ we obtain what is called the *inverse substitution*, namely

$$\mu X = L_1x + L_2y + L_3z + \ldots ,$$
$$\mu Y = M_1x + M_2y + M_3z + \ldots ,$$
$$\mu Z = N_1x + N_2y + N_3z + \ldots ,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots ,$$

where L_r, M_r, N_r, are the cofactors of l_r, m_r, n_r, in (l_1, m_2, n_3).

The substitution is said to be *orthogonal* if

$$x^2 + y^2 + z^2 + \ldots = X^2 + Y^2 + Z^2 + \ldots .$$

In connection with the linear transformation of polynomials the word *quantic* is used to denote a homogeneous polynomial. Quantics of the second, third, fourth, ... degrees are called *quadratics, cubics, quartics, ...*; quantics in two, three, ... variables are called *binary, ternary, ... quantics.*

A function of *the coefficients* of a quantic u is called an *invariant* if when u is transformed by a linear substitution the same function of the new coefficients is equal to the original function multiplied by a power of the modulus of transformation.

Thus the vanishing of an invariant is the condition that the quantic possesses some property which is unaffected by linear transformation.

A *covariant* is a function of the *coefficients of a quantic and also of the variables* such that, after a linear transformation, the same function of the new coefficients and variables is equal to the original function multiplied by a power of the modulus of transformation.

We may also have functions of the coefficients of several quantics which possess properties similar to those just described, and which are called covariants or invariants according as they do or do not contain the variables. Thus $ac'+a'c-2bb'$ is an invariant and $(ab')x^2+(ac')xy+(bc')y^2$ is a covariant of the quadratics $ax^2+2bxy+cy^2$, $a'x^2+2b'xy+c'y^2$, as has been shown on pp. 26, 27.

2. Formation of Invariants. Let the quantic

$$u \equiv (a, b, \ldots)(x, y)^n$$

be transformed into $u' \equiv (a', b', \ldots)(X, Y)^n$ .....(A)

by the substitution $x = lX + mY, \quad y = l'X + m'Y.$ .....(B)

Let $\alpha, \beta, \ldots$ be the values of x/y for which $u=0$ and let $\alpha', \beta', \ldots$ be the corresponding values of X/Y, so that

$$\alpha = \frac{l\alpha' + m}{l'\alpha' + m'} \quad \text{and} \quad \alpha' = \frac{-m + \alpha m'}{l - \alpha l'}. \quad \ldots\ldots(C)$$

Then $x - \alpha y = lX + mY - \alpha(l'X + m'Y) = (l - \alpha l')X + (m - \alpha m')Y$

i.e. $x - \alpha y = (l - \alpha l')(X - \alpha' Y),$ .....(D)

with similar values for $x - \beta y$, etc.

And since $u = a(x-\alpha y)(x-\beta y)\ldots$ and $u' = a'(X-\alpha' Y)(X-\beta' Y)\ldots$,

it follows that $a' = a(l-\alpha l')(l-\beta l')\ldots$ .....(E)

Now an invariant is unchanged by the substitution $x = X + hY$, $y = Y$: it is therefore *a function of the differences* $\alpha - \beta$, etc., and we have

$$\alpha' - \beta' = \frac{-m + \alpha m'}{l - \alpha l'} - \frac{-m + \beta m'}{l - \beta l'} = \frac{(\alpha - \beta)(lm' - l'm)}{(l - \alpha l')(l - \beta l')}, \quad \ldots\ldots(F)$$

with similar values for $\beta' - \gamma'$, etc.

We are now in a position to discover invariants.

(1) *The Quadratic.* From (E), (F) we get $a'^2(\alpha' - \beta')^2 = (lm')^2 \cdot a^2(\alpha - \beta)^2$.

Therefore (as proved in Ch. II, 9) $a'c' - b'^2 = (lm')^2(ac - b^2)$. .....(G)

(2) *The Cubic.* In the same way we have

$$(\beta' - \gamma')^2(\gamma' - \alpha')^2(\alpha' - \beta')^2 = \frac{(\beta - \gamma)^2(\gamma - \alpha)^2(\alpha - \beta)^2(lm')^6}{(l - \alpha l')^4(l - \beta l')^4(l - \gamma l')^4},$$

hence $a'^4(\beta' - \gamma')^2(\gamma' - \alpha')^2(\alpha' - \beta')^2 = (lm')^6 a^4(\beta - \gamma)^2(\gamma - \alpha)^2(\alpha - \beta)^2,$

that is to say, $\Delta' = (lm')^6 \Delta,$ .....(H)

therefore the discriminant Δ is an invariant.

(3) *The Quartic.* If $I = ae - 4bd + 3c^2$, $J = ace + 2bcd - ad^2 - c^3 - eb^2$, it is shown on pp. 187, 188 of *Higher Algebra* that, if $\alpha, \beta, \gamma, \delta$ are the roots of the quartic, and

$$P = (\beta - \gamma)(\alpha - \delta), \quad Q = (\gamma - \alpha)(\beta - \delta), \quad R = (\alpha - \beta)(\gamma - \delta).$$

then the roots of the equation $4t^3 - It + J = 0$ are

$$\tfrac{1}{12}a(Q - R), \quad \tfrac{1}{12}a(R - P), \quad \tfrac{1}{12}a(P - Q).$$

Hence, $\quad 24I = a^2(P^2 + Q^2 + R^2), \quad 432J = -a^3(Q - R)(R - P)(P - Q),$

If accented letters refer to u', by equations (E), (F), it is easily seen that

$$a'P' = (lm')^2 aP, \quad a'Q' = (lm')^2 aQ, \quad a'R' = (lm')^2 aR,$$

and therefore $\qquad I' = (lm')^4 I, \quad J' = (lm')^6 J,$

so that I and J are invariants.

We draw the following general conclusion. Let L be a symmetric function of $\alpha, \beta, \ldots$ of order ϖ, involving the differences only, so that L is a single term or the sum of terms of the form

$$h(\alpha - \beta)^p(\gamma - \alpha)^q(\beta - \gamma)^r \ldots;$$

then *if all of $\alpha, \beta, \gamma, \ldots$ occur the same number of times in every term, $a^\varpi L$ is an invariant.*

3. Formation of Covariants.

Let

$$u = (a_0, a_1, a_2, \ldots a_n \between x, y)^n = a_0(x - \alpha y)(x - \beta y)(x - \gamma y) \ldots,$$

then (1) *If $f(\alpha, \beta, \ldots)$ is a symmetric function of $\alpha, \beta, \ldots$ of order ϖ and weight w involving only the differences of $\alpha, \beta, \ldots$ and*

$$v = \frac{u^\varpi}{y^w} f\left(\frac{1}{x - \alpha y}, \frac{1}{x - \beta y}, \ldots\right); \quad \text{.......................(A)}$$

then in general v is a covariant of degree $n\varpi - 2w$ in which $a_0^\varpi f(\alpha, \beta, \ldots)$ is the coefficient of the highest power of x.

But if $n\varpi = 2w$, then v is equal to $a_0^\varpi f(\alpha, \beta, \ldots)$ and is an invariant.

Proof. The function $f(\alpha, \beta, \ldots)$ consists of terms of the form

$$c = m(\alpha - \beta)^p(\alpha - \gamma)^q(\beta - \gamma)^r \ldots,$$

and, since it is of weight w, we have $\quad p + q + r + \ldots = w.$

Now $$\frac{1}{x - \alpha y} - \frac{1}{x - \beta y} = \frac{(\alpha - \beta)y}{(x - \alpha y)(x - \beta y)};$$

therefore the part of v arising from the term c is

$$C = u^\varpi m \left\{\frac{\alpha - \beta}{(x - \alpha y)(x - \beta y)}\right\}^p \left\{\frac{\alpha - \gamma}{(x - \alpha y)(x - \gamma y)}\right\}^q \ldots.$$

In the denominator of the last expression, the number of times which a factor such as $x - \alpha y$ occurs is the same as the number of factors in c which contain α. This number cannot exceed ϖ, the order of $f(\alpha, \beta, \ldots)$.

Therefore C is equal to $a_0^{\varpi} c$ multiplied by factors of the form $(x - \lambda y)^k$, where k is a positive integer or zero.

Hence v is an *integral* function. Its degree in x, y is obviously $n\varpi - 2w$, and the coefficient of the highest power of x is $a_0^{\varpi} f(\alpha, \beta, \ldots)$.

If, however, $n\varpi = 2w$, then $v = a_0^{\varpi} f(\alpha, \beta, \ldots)$.

Next, let u be transformed by the substitution

$$x = lX + mY, \quad y = l'X + m'Y,$$

and let accented letters refer to u'. Then by equations (C), (E) of Art. 2,

$$\frac{\alpha' - \beta'}{(X - \alpha' Y)(X - \beta' Y)} = \mu \cdot \frac{\alpha - \beta}{(x - \alpha y)(x - \beta y)}, \qquad \text{(B)}$$

where $\mu = lm' - l'm$. Therefore

$$C' = \mu^{p+q+r+\ldots} C \quad \text{and} \quad v' = \mu^{w} v,$$

so that v is a covariant or an invariant.

The function v can be expressed in terms of the coefficients of u by means of the following theorem :

(2) *If* $a_0^{\varpi} f(\alpha, \beta, \ldots) = \phi(a_0, a_1, a_2, \ldots a_n)$, *then*

$$v = (-1)^{w} y^{-w} \phi(u_n, u_{n-1}, \ldots u_1, a_0), \qquad \text{(C)}$$

where $\qquad u_r = (a_0, a_1, a_2, \ldots, a_r)$.

For, by the use of Taylor's Theorem (see *H.A.*, p. 305, Ex. 20), it can be shown that the equation whose roots are $\alpha y - x$, $\beta y - x$, ... is

$$(a_0, u_1, u_2, \ldots u_n \between t, 1)^n = 0 ;$$

therefore the equation whose roots are $1/(\alpha y - x)$, $1/(\beta y - x)$, ... is

$$(u_n, u_{n-1}, \ldots u_1, a_0 \between t, 1)^n = 0 ;$$

hence, $$u^{\varpi} f\left(\frac{1}{\alpha y - x}, \frac{1}{\beta y - x}\right) = \phi(u_n, u_{n-1}, \ldots u_1, a_0),$$

whence the result in question. Observe that *the coefficient of the leading term in v is* $\phi(a_0, a_1, \ldots a_n)$. This is called the *source* of the covariant.

(3) For practical purposes, theorem (A) may be stated thus :

Rule. *Express* $f(\alpha, \beta, \ldots)$ *in terms of* $\alpha - \beta$, $\alpha - \gamma$, ... *and for* $\alpha - \beta$ *write* $(\alpha - \beta)/(x - \alpha y)(x - \beta y)$, *making similar substitutions for* $\alpha - \gamma$, ... *The result when multiplied by u^{ϖ} is a covariant or an invariant.*

In any particular case it will be seen that the proof depends on equation (B) without reference to the general theorem. Instances occur in the next three articles.

4. The Hessian. Considering the binary quantic,

$$u=(a_0, a_1, a_2, \dots a_n\mathfrak{x}x, y)^n=a_0(x-\alpha y)(x-\beta y)\dots$$

we have $$a_0^2\Sigma(\alpha-\beta)^2=-n^2(n-1)(a_0a_2-a_1^2).$$

Let **H** be defined by $$-n^2(n-1)\mathbf{H}=u^2\Sigma\left\{\frac{\alpha-\beta}{(x-\alpha y)(x-\beta y)}\right\}^2, \quad \dots\dots(\mathbf{A})$$

then by the preceding, $\mathbf{H}'=(lm'-l'm)^2\mathbf{H}$,

and $$\mathbf{H}=y^{-2}(u_nu_{n-2}-u_{n-1}^2)=\frac{1}{y^2}\begin{vmatrix} u_{n-2} & u_{n-1} \\ u_{n-1} & u_n \end{vmatrix}.$$

In this determinant subtract x times the top row from the bottom and divide by y, then subtract x times the right-hand column from the left and divide by y. Thus it will be found that

$$\mathbf{H}=\begin{vmatrix} (a_0, a_1, \dots a_{n-2}\mathfrak{x}x, y)^{n-2}, & (a_1, a_2, \dots a_{n-1}\mathfrak{x}x, y)^{n-2} \\ (a_1, a_2, \dots a_{n-1}\mathfrak{x}x, y)^{n-2}, & (a_2, a_3, \dots a_n\mathfrak{x}x, y)^{n-2} \end{vmatrix}, \quad \dots\dots(\mathbf{B})$$

which is the same as $$n^2(n-1)^2\mathbf{H}=\begin{vmatrix} \dfrac{\partial^2u}{\partial x^2}, & \dfrac{\partial^2u}{\partial x\,\partial y} \\ \dfrac{\partial^2u}{\partial x\,\partial y}, & \dfrac{\partial^2u}{\partial y^2} \end{vmatrix}. \quad \dots\dots(\mathbf{C})$$

The last determinant is called the *Hessian* of u.

5. Covariants of the Cubic. For the binary cubic,

$$u=(a, b, c, d\mathfrak{x}x, y)^3=a(x-\alpha y)(x-\beta y)(x-\gamma y),$$

(i) we have $$a^2\Sigma(\alpha-\beta)^2=-18(ac-b^2)=-18H.$$

The *covariant* **H** is defined by

$$-18\mathbf{H}=u^2\Sigma\left\{\frac{\alpha-\beta}{(x-\alpha y)(x-\beta y)}\right\}^2=a^2\Sigma(\alpha-\beta)^2(x-\gamma y)^2,$$

and, by (**B**) above, $$\mathbf{H}=\begin{vmatrix} ax+by & bx+cy \\ bx+cy & cx+dy \end{vmatrix}.$$

(ii) The *Cubic Covariant* **G**. Take the equality

$$a^3(\beta+\gamma-2\alpha)(\gamma+\alpha-2\beta)(\alpha+\beta-2\gamma)=27(a^2d-3abc+2b^3)=27G,$$

and observe that $$a(\beta+\gamma-2\alpha)=a\{(\gamma-\alpha)-(\alpha-\beta)\}.$$

Let v_1, v_2, v_3 be defined by $$v_1=u\left\{\frac{\gamma-\alpha}{(x-\gamma y)(x-\alpha y)}-\frac{\alpha-\beta}{(x-\alpha y)(x-\beta y)}\right\}$$

i.e., $$v_1=a\{(\gamma-\alpha)(x-\beta y)-(\alpha-\beta)(x-\gamma y)\},$$

and similar equations for v_2 and v_3; then, by equation (**B**) of Art. 3,

$$v_1'=(lm')v_1, \quad v_2'=(lm')v_2, \quad v_3'=(lm')v_3.$$

We therefore define the *cubic covariant* $\mathbf{G}$ by $27\mathbf{G} = v_1 v_2 v_3$.

Also, by Art. 3, (2), $\mathbf{G} = (-1)^3 y^{-3}(u_3^2 a - 3u_3 u_2 u_1 + 2u_2^3)$,

where $u_3 = u, \quad u_2 = ax^2 + 2bxy + cy^2, \quad u_1 = ax + by.$

(iii) *If* α', β', γ' *are the values of* x/y *given by* $G = 0$, *then*

$$(\alpha'\alpha, \beta\gamma), \quad (\beta'\beta, \gamma\alpha), \quad (\gamma'\gamma, \alpha\beta)$$

are harmonic.

For if $v_1 = 0$, then $(\alpha' - \beta)/(\alpha' - \gamma) \cdots (\alpha - \beta)/(\alpha - \gamma)$, etc.

6. Covariants of the Quartic. For the binary quartic,

$$u = (a, b, c, d, e)(x, y)^4 = a(x - \alpha y)(x - \beta y)(x - \gamma y)(x - \delta y),$$

(i) We have $a^2\Sigma(\alpha - \beta)^2 = -48(ac - b^2) = -48H,$

and the *covariant* $\mathbf{H}$ is defined by

$$-48\mathbf{H} = u^2\Sigma\left\{\frac{\alpha - \beta}{(x - \alpha y)(x - \beta y)}\right\}^2 = a^2\Sigma(\alpha - \beta)^2(x - \gamma y)^2(x - \delta y)^2.$$

As in Art. 4, $\mathbf{H} = \begin{vmatrix} ax^2 + 2bxy + cy^2 & bx^2 + 2cxy + dy^2 \\ bx^2 + 2cxy + dy^2 & cx^2 + 2dxy + ey^2 \end{vmatrix}.$

(ii) The *Sextic Covariant* $\mathbf{G}$. Consider the equality

$$a^3(\beta + \gamma - \alpha - \delta)(\gamma + \alpha - \beta - \delta)(\alpha + \beta - \gamma - \delta) = 32(a^2 d - 3abc + 2b^3) = 32G.$$

Let v_1, v_2, v_3 be defined by

$$\begin{aligned} v_1 &= u\left\{\frac{\beta - \alpha}{(x - \beta y)(x - \alpha y)} + \frac{\gamma - \delta}{(x - \gamma y)(x - \delta y)}\right\} \\ &= a\{(\beta - \alpha)(x - \gamma y)(x - \delta y) + (\gamma - \delta)(x - \alpha y)(x - \beta y)\} \\ &= a[(\beta + \gamma - \alpha - \delta)x^2 - 2(\beta\gamma - \alpha\delta)xy + \{\beta\gamma(\alpha + \delta) - \alpha\delta(\beta + \gamma)\}y^2], \end{aligned}$$

and similar equations for v_2 and v_3; then, by equations (B) of Art. 3,

$$v_1' = (lm')v_1, \quad v_2' = (lm')v_2, \quad v_3 = (lm')v_3.$$

We therefore define the *sextic covariant* $\mathbf{G}$ by $32\mathbf{G} = v_1 v_2 v_3$.

By Art. 3, (2), $\mathbf{G} = -y^{-3}(u_4^2 u_1 - 3u_4 u_3 u_2 + 2u_3^3),$

where $u_4 = u, \quad u_3 = ax^3 + 3bx^2 y + 3cxy^2 + y^3$

$$u_2 = ax^2 + 2bxy + cy^2, \quad u_1 = ax + by,$$

(iii) *If* $y = 1$, *the points given by* $\mathbf{G} = 0$ *are the foci of the three involutions determined by the points* $\alpha, \beta, \gamma, \delta$ *taken in pairs.*

For the equation $v_1 = 0$ gives the foci of the involution in which the points β, γ and α, δ are corresponding pairs. (Ex. 17 (ii), on p. 19.)

7. Homographic Transformation. Let $u \equiv (a, b, \ldots)(x, 1)^n$ be transformed to $u' = (a', b', \ldots)(X, 1)^n$ by the following process. Write $x = (lX + m)/(l'X + m')$, and multiply by $(l'X + m')^n$ to remove fractions. This is called a homographic transformation; then the coefficients $a', b', \ldots$ have the same values as in Art. 2, but in this case u is not equal to u'.

As in Art. 1, a function $f(a, b, \ldots)$ of the coefficients is an *invariant* if

$$f(a', b', \ldots) = (lm' - l'm)^w f(a, b, \ldots).$$

Again, a function $f(x, a, b, \ldots)$ is a *covariant* if when it is transformed by the above substitution and rendered integral it is equal to $f(X, a', b', \ldots)$ divided by some power of $lm' - l'm$. Such covariants are obtained by putting $y = 1$ in the previous results.

8. Some Properties of Covariants and Invariants. Let

$$u = (a_0, a_1, \ldots a_n)(x, y)^n = a_0(x - \alpha y)(x - \beta y)\ldots;$$

then we have the following properties.

(1) *To interchange a_0 and a_n, a_1 and a_{n-1}, a_2 and a_{n-2}, etc., in an invariant I is to multiply it by $(-1)^w$. To make these interchanges in a covariant v, at the same time interchanging x and y, is to multiply it by $(-1)^w$.*

For the substitution $x = Y$, $y = X$, of which the modulus is -1, changes u into $(a_n, a_{n-1}, a_{n-2}, \ldots a_0)(X, Y)^n$.

Let $I = \phi(a_0, a_1, \ldots a_n)$, then since I is an invariant,

$$\phi(a_n, a_{n-1}, \ldots a_0) = (-1)^w \phi(a_0, a_1, \ldots a_n).$$

Let $v = \psi(a_0, a_1, \ldots a_n, x, y)$, then since v is a covariant,

$$\psi(a_n, a_{n-1}, \ldots a_0, X, Y) = (-1)^w \psi(a_0, a_1, \ldots a_n, x, y);$$

$$\therefore \psi(a_n, a_{n-1}, \ldots a_0, y, x) = (-1)^w \psi(a_0, a_1, \ldots a_n, x, y).$$

(2) *If $v \equiv (b_0, b_1, \ldots b_m)(x, y)^m$ is a covariant, the coefficients of terms equidistant from the beginning and end are connected as follows:*

If $b_r = F(a_0, a_1, \ldots a_n)$, then $b_{m-r} = (-1)^w F(a_n, a_{n-1}, \ldots a_0)$.

This is an immediate consequence of the last theorem.

(3) *Any invariant I satisfies the equations,* $DI = 0$, $D'I = 0$, ...**(A)**

and any covariant v satisfies $y\dfrac{\partial v}{\partial x} = Dv$, $x\dfrac{\partial v}{\partial y} = D'v$, ...**(B)**

where D, D' are defined by

$$D = a_0\frac{\partial}{\partial a_1} + 2a_1\frac{\partial}{\partial a_2} + 3a_2\frac{\partial}{\partial a_3} + \ldots + na_{n-1}\frac{\partial}{\partial a_n},$$

$$D' = na_1\frac{\partial}{\partial a_0} + (n-1)a_2\frac{\partial}{\partial a_1} + (n-2)a_3\frac{\partial}{\partial a_2} + \ldots + a_n\frac{\partial}{\partial a_{n-1}}.$$

We give a proof of the second theorem: that of the first is similar. Consider the substitution $x = X + hY$, $y = Y$, of which the modulus (μ) is unity. This transforms u into

$$(a_0, A_1, A_2, \dots A_n \mid X, Y)^n,$$

where $A_1 = a_1 + a_0 h$, $A_2 = a_2 + 2a_1 h + a_0 h^2$, etc.

Let $v = \psi(a_0, a_1, a_2, \dots a_n, x, y)$, then since v is a covariant and $\mu = 1$,

$$\psi(a_0, A_1, A_2, \dots A_n, X, Y) = \psi(a_0, a_1, a_2, \dots a_n, x, y).$$

If $A_1, A_2, \dots$ have the above values and $X = x - hy$, $Y = y$, the last equation holds for all values of h. Let the left-hand side be expanded in powers of h. By the extension of Taylor's theorem, the coefficient of h is

$$a_0 \frac{\partial v}{\partial a_1} + 2a_1 \frac{\partial v}{\partial a_2} + \dots + n a_{n-1} \frac{\partial v}{\partial a_n} - y \frac{\partial v}{\partial x}.$$

Equating this to zero, we have the first equation in question. The second follows from the first on account of theorem (A).

(4) *The coefficients of the covariant* $v = (b_0, b_1, \dots b_m \mid x, y)^m$ *satisfy the equations*

$$Db_0 = 0, \quad Db_1 = b_0, \quad Db_2 = 2b_1, \dots \quad Db_m = b_{m-1}, \quad \text{(C)}$$

$$D'b_0 = mb_1, \quad D'b_1 = (m-1)b_2, \quad D'b_2 = (m-2)b_3, \dots \quad D'b_m = 0, \dots\dots \text{(D)}$$

hence, $$v = b_0 x^m + D'b_0 x^{m-1} y + \frac{1}{\lfloor 2} D'^2 b_0 x^{m-2} y^2 + \frac{1}{\lfloor 3} D'^3 b_0 x^{m-3} y^3 + \dots . \quad \dots \text{(E)}$$

For we have

$$y \frac{\partial v}{\partial x} = ym(b_0, b_1, \dots b_{m-1} \mid x, y)^{m-1}$$

$$= mb_0 x^{m-1} y + m(m-1) b_1 x^{m-2} y^2 + \frac{m(m-1)(m-2)}{\lfloor 2} b_2 x^{m-3} y^3 + \dots ;$$

and $$Dv = Db_0 x^m + mDb_1 x^{m-1} y + \frac{m(m-1)}{\lfloor 2} Db_2 x^{m-2} y^2 + \dots ;$$

and since $y \dfrac{\partial v}{\partial x} = Dv$, the coefficients of corresponding terms in these expansions are equal.

This proves the first set of equations: the others follow in the same way from the equation $x \dfrac{\partial v}{\partial y} = D'v$.

(5) *If any coefficient of a covariant* v *is given, the other coefficients may be calculated by using equations* (C), (D).

Again, since $Db_0 = 0$, *the coefficient of the leading term in a covariant is a function of the differences of* $\alpha, \beta, \dots$.

Ex. 1. *The cubic covariant* G *of the cubic* $(a, b, c, d\,(x, y)^3$ *is*

$$(b_0, b_1, b_2, b_3\,(x, y)^3,$$

where
$$b_0 = a^2d - 3abc + 2b^3, \qquad b_1 = abd + b^2c - 2ac^2,$$
$$b_2 = -d^2a + 3dcb - 2c^3, \quad b_3 = -dca - c^2b + 2db^2.$$

By Art. 5, $b_0 = a^2d - 3abc + 2b^3$, and using equations (D) above,

$$3b_1 = \left(3b\frac{d}{da} + 2c\frac{d}{db} + d\frac{d}{dc}\right)(a^2d - 3abc + 2b^2)$$
$$= 3b(2ad - 3bc) + 2c(-3ac + 6b^2) + d(-3ab);$$
$$\therefore\ b_1 = abd + b^2c - 2ac^2.$$

Again, b_0 is of weight 3, therefore b_3 is derived from $-b_0$ and b_2 from $-b_1$ by interchanging a, d and b, c.

Ex. 2. *For the quartic* $(a, b, c, d, e\,(x, y)^4$ *the sextic covariant* G *is*

$$b_0x^6 + b_1x^5y + b_2x^4y^2 + \ldots + b_6y^6,$$
$$b_0 = a^2d - 3abc + 2b^3, \qquad b_1 = a^2e + 2abd - 9ac^2 + 6b^2c,$$
$$b_2 = 5abc - 15acd + 10b^2d, \qquad b_3 = -10ad^2 + 10b^2e,$$

and b_6, b_5, b_4 *are derived from* $-b_0, -b_1, -b_2$ *by interchanging* a, e *and* b, d.

(6) *Every invariant of a covariant is an invariant of the original quantic.*

This follows directly from the definitions, and the formal proof is left to the reader.

9. Identities connecting Covariants.

The covariant of which $\phi(a_0, a_1, \ldots a_n)$ is the leading coefficient is $(-y)^{-w}\phi(u_n, u_{n-1}, \ldots u_0)$. If, however, $\phi(a_0, a_1, \ldots a_n)$ is an invariant, then

$$(-y)^{-w}\phi(u_n, u_{n-1}, \ldots u_0) \equiv \phi(a_0, a_1, \ldots a_n).$$

We draw the following conclusion: *Corresponding to any identical relation connecting symmetric functions of* $\alpha, \beta, \ldots$ *which involve the differences only, there exists a relation connecting the corresponding covariants or invariants and the quantic itself.*

Ex. 1. *For the cubic* $u = (a, b, c, d\,(x, y)^3$ *prove the identity*

$$\mathrm{G}^2 + 4\mathrm{H}^3 = u^3\Delta.$$

The leading coefficients of G, H are G, H and

$$G^2 + 4H^3 = a^2\Delta \text{ (see } H.A., \text{ p. 179).}$$

If in this identity we substitute u_3, u_2, u_1, u_0 for a, b, c, d, then G, H, Δ, a become $(-y)^{-3}\mathrm{G}$, $(-y)^{-2}\mathrm{H}$, $(-y)^{-6}\Delta$, u respectively, whence the result in question.

It should be noticed that in all such cases the factor $(-y)^{-w}$ disappears, for all terms in the given identity must be of the same weight.

Ex. 2. *For the quartic* $u = (a, b, c, d, e\,(x, y)^4$ *prove that*

$$\mathrm{G}^2 + 4\mathrm{H}^3 = u^2\mathrm{H}I - u^3J.$$

This follows in the same way from the identity

$$G^2 + 4H^3 = a^2(HI - aJ) \text{ (see } H.A., \text{ p. 188).}$$

10. A System of Two Quantics. Let

$$\left.\begin{aligned} u &= (a, b, \dots)(x, y)^m = a(x-\alpha_1 y)(x-\alpha_2 y)\dots(x-\alpha_m y) \\ v &= (a', b', \dots)(x, y)^n = a'(x-\beta_1 y)(x-\beta_2 y)\dots(x-\beta_n y) \end{aligned}\right\}, \quad \dots\dots\dots(\mathrm{A})$$

then (1) *the resultant of* $u=0$, $v=0$ *is an invariant.*

For suppose that u, v are transformed to

$$\begin{aligned} U &= (A, B, \dots)(X, Y)^m = A(X-\alpha_1' Y)(X-\alpha_2' Y)\dots, \\ V &= (A', B', \dots)(X, Y)^n = A'(X-\beta_1' Y)(X-\beta_2' Y)\dots, \end{aligned}$$

by the substitution $x=\lambda X+\mu Y$, $y=\lambda' X+\mu' Y$.

Let R, R' be the resultants of $u=0$, $v=0$, and $U=0$, $V=0$ respectively, so that

$$R = a^n a'^m \Pi(\alpha_r-\beta_s), \quad R' = A^n A'^m \Pi(\alpha_r'-\beta_s').$$

Now, as in Art. 9 (1), on p. 26,

$$A = a\Pi(\lambda-\alpha_r\lambda'), \quad A' = a'\Pi(\lambda-\beta_s\lambda'),$$

and

$$\alpha_r'-\beta_s' = \frac{(\lambda\mu'-\lambda'\mu)(\alpha_r-\beta_s)}{(\lambda-\alpha_r\lambda')(\lambda-\beta_s\lambda')}.$$

Moreover, the product $\Pi(\alpha_r'-\beta_s')$ contains mn factors, of which n involve α_r' and m involve β_s'. Therefore

$$\Pi(\alpha_r'-\beta_s') = \frac{(\lambda\mu'-\lambda'\mu)^{mn}\Pi(\alpha_r-\beta_s)}{\Pi(\lambda-\alpha_r\lambda')^n\Pi(\lambda-\beta_s\lambda')^m},$$

and consequently

$$R' = (\lambda\mu'-\lambda'\mu)^{mn}R, \quad \dots\dots\dots(\mathrm{B})$$

so that R is an invariant.

We now consider methods of finding covariants and invariants of the system u, v.

(2) We can extend the rule of Art. 3, (3), so as to find covariants of the system u, v as follows: suppose that $f(\alpha_1, \alpha_2, \dots \beta_1, \beta_2, \dots)$ is a function such that

(i) it is symmetric with regard to each of the sets $\alpha_1, \alpha_2, \dots$ and $\beta_1, \beta_2, \dots$ and of orders ϖ, ϖ' in $\alpha_1, \alpha_2, \dots$ and $\beta_1, \beta_2, \dots$ respectively;

(ii) it involves only the differences of $\alpha_1, \alpha_2 \dots \beta_1, \beta_2 \dots$.

Rule. *For every difference such as* $\alpha_r-\beta_s$ *substitute*

$$(\alpha_r-\beta_s)/(x-\alpha_r y)(x-\beta_s y).$$

The result when multiplied by $u^{\varpi}v^{\varpi'}$ *is a covariant or an invariant, and in the former case the coefficient of the highest power of* x *is*

$$a^{\varpi}a'^{\varpi'}f(\alpha_1, \alpha_2 \dots \beta_1, \beta_2 \dots).$$

Ex. 1. *For the quantics* u, v *find the covariant corresponding to* $\Sigma(\alpha_r - \beta_s)$, *and prove that it can be written in the form*

$$J \equiv \frac{\partial u}{\partial x}\frac{\partial v}{\partial y} - \frac{\partial u}{\partial y}\frac{\partial v}{\partial x}.$$

Applying the rule, the covariant is

$$uv\Sigma\frac{\alpha_r - \beta_s}{(x-\alpha_r y)(x-\beta_s y)},$$

which is equal to

$$uv\left\{\Sigma\frac{\alpha_r}{x-\alpha_r y}\cdot\Sigma\frac{1}{x-\beta_s y} - \Sigma\frac{\beta_s}{x-\beta_s y}\cdot\Sigma\frac{1}{x-\alpha_r y}\right\}.$$

Taking logarithms and differentiating equations (A) with regard to x and y, we have

$$\frac{1}{u}\frac{\partial u}{\partial x} = \Sigma\frac{1}{x-\alpha_r y}, \quad \frac{1}{u}\frac{\partial u}{\partial y} = -\Sigma\frac{\alpha_r}{x-\alpha_r y},$$

with two similar equations. Whence the result in question follows at once. This covariant J is called the *Jacobian* of u, v.

(3) If $u = (a, b, \ldots)(x, y)^n$, $v = (a', b', \ldots)(x, y)^n$, and we substitute $a + ka'$, $b + kb'$, ... for a, b in any invariant I of u, then the coefficient of every power of k in the result is an invariant. By the extension of Taylor's theorem, the coefficient of k^r is

$$\frac{1}{\lfloor r}\left(a'\frac{\partial}{\partial a} + b'\frac{\partial}{\partial b} + \ldots\right)^r I.$$

Hence *if the operation* $a'\dfrac{\partial}{\partial a} + b'\dfrac{\partial}{\partial b} + \ldots$ *is performed any number of times on* I, *the result is an invariant of* u, v.

Thus $ac - b^2$ is an invariant of $ax^2 + 2bx + c$, $a'x^2 + 2b'x + c'$ and

$$\left(a'\frac{\partial}{\partial a} + b'\frac{\partial}{\partial b} + c'\frac{\partial}{\partial c}\right)(ac - b^2) = a'c - 2b'b + c'a;$$

therefore the last expression is an invariant.

11. Some General Theorems. (1) If variables $x', y', \ldots$ are transformed according to the same rules as $x, y, \ldots$, the two sets of variables are said to be *cogredient*. Thus if

$$x = lX + mY, \quad y = l'X + m'Y,$$
$$x' = lX' + mY', \quad y' = l'X' + m'Y',$$

then x', y' are cogredient with x, y. From these equations we have

$$x + kx' = l(X + kX') + m(Y + kY'),$$
$$y + ky' = l'(X + kX') + m'(Y + kY').$$

Hence if the quantic $u \equiv f(x, y)$ is transformed into $U \equiv F(X, Y)$ by the above substitution, then $f(x + kx', y + ky')$ is transformed into $F(X + kX', Y + kY')$, so that these expressions are identically equal.

Equating the coefficients of k^r, we have, by Taylor's theorem,

$$\left(x'\frac{\partial}{\partial x}+y'\frac{\partial}{\partial y}\right)^r u=\left(X'\frac{\partial}{\partial X}+Y'\frac{\partial}{\partial Y}\right)^r U.$$

Hence *if* $\left(x'\dfrac{\partial}{\partial x}+y'\dfrac{\partial}{\partial y}\right)^r u$ *is regarded as a quantic in* x', y', *then any of its invariants is a covariant of* u.

For example, $\left(x'\dfrac{\partial}{\partial x}+y'\dfrac{\partial}{\partial y}\right)^2 = u_{xx}x'^2+2u_{xy}x'y'+u_{yy}y'^2,$

where u_{xx}, u_{xy}, u_{yy} stand for $\dfrac{\partial^2 u}{\partial x^2}$, $\dfrac{\partial^2 u}{\partial x\,\partial y}$, $\dfrac{\partial^2 u}{\partial y^2}$;

therefore $u_{xx}u_{yy}-u_{xy}^2$ is a covariant of u, for it is an invariant of the right-hand side regarded as a quadratic in x', y' (cf. Art. 9, p. 26).

Similar reasoning proves that *if* u *is a quantic in* $x, y, z, \ldots$ *and*

$$v=\left(x'\frac{\partial}{\partial x}+y'\frac{\partial}{\partial y}+z'\frac{\partial}{\partial z}+\ldots\right)^r u,$$

where $x', y', z', \ldots$ *are cogredient with* $x, y, z, \ldots$, *then if* v *is regarded as a quantic in* $x', y', z', \ldots$, *any of its invariants is a covariant of* u.

For example, if u is a quantic in x, y, z,

$$\left(x'\frac{\partial}{\partial x}+y'\frac{\partial}{\partial y}+z'\frac{\partial}{\partial z}\right)^2 u = u_{xx}x'^2+u_{yy}y'^2+u_{zz}z'^2+2u_{yz}y'z' \\ +2u_{zx}z'x'+2u_{xy}x'y';$$

therefore the determinant

$$\begin{vmatrix} u_{xx} & u_{xy} & u_{xz} \\ u_{xy} & u_{yy} & u_{yz} \\ u_{zx} & u_{yz} & u_{zz} \end{vmatrix}$$

is a covariant of u, for it is an invariant of the right-hand side regarded as a quadratic in x', y', z' (Art. 15, p. 35). This determinant is called the *Hessian*.

(2) Let the quantic u be transformed to U by the substitution

$$x=lX+mY, \quad y=l'X+m'Y.$$

If $\mu=lm'-l'm$, we have

$$\mu X=m'x-my, \quad \mu Y=-l'x+ly.$$

Therefore

$$\frac{\partial u}{\partial x}=\frac{\partial U}{\partial X}\cdot\frac{\partial X}{\partial x}+\frac{\partial U}{\partial Y}\cdot\frac{\partial Y}{\partial x}=\frac{\partial U}{\partial X}\cdot\frac{m'}{\mu}-\frac{\partial U}{\partial Y}\cdot\frac{l'}{\mu},$$

$$\frac{\partial u}{\partial y}=\frac{\partial U}{\partial X}\cdot\frac{\partial X}{\partial y}+\frac{\partial U}{\partial Y}\cdot\frac{\partial Y}{\partial y}=-\frac{\partial U}{\partial X}\cdot\frac{m}{\mu}+\frac{\partial U}{\partial Y}\cdot\frac{l}{\mu}.$$

Hence $\mu\dfrac{\partial}{\partial y}=l\dfrac{\partial}{\partial Y}+m\left(-\dfrac{\partial}{\partial X}\right)$, $\mu\left(-\dfrac{\partial}{\partial x}\right)=l'\dfrac{\partial}{\partial Y}+m'\left(-\dfrac{\partial}{\partial X}\right)$,

showing that, *apart from the factor* μ, *the symbols* $\dfrac{\partial}{\partial y}$, $-\dfrac{\partial}{\partial x}$ *are cogredient with* x, y.

It follows that *if* $\dfrac{\partial}{\partial y}$, $-\dfrac{\partial}{\partial x}$ *are substituted for* x, y *in a quantic* u *or in any of its covariants, we obtain an operator which if applied to* u *or to any covariant of* u *produces a covariant or an invariant. If the operator is applied to another quantic* u' *we obtain a covariant or an invariant of* u, u'.

Ex. 1. *Let* $u=(a, b, c, d)(x, y)^3$, $u'=(a', b', c', d')(x, y)^3$, *and suppose that these are transformed to* $U=(A, B, C, D)(X, Y)^3$, $U'=(A', B', C', D')(X, Y)^3$.

Substituting $\mu\dfrac{\partial}{\partial y}$, $-\mu\dfrac{\partial}{\partial x}$ for x, y in u, we have by the preceding,

$$\mu^3\left(a, b, c, d\right)\left(\frac{\partial}{\partial y}, -\frac{\partial}{\partial x}\right)=\left(A, B, C, D\right)\left(\frac{\partial}{\partial Y}, -\frac{\partial}{\partial X}\right).$$

Applying these operators to u', U' respectively, we have

$$6\mu^3\{ad'-a'd-3(bc'-b'c)\}=6\{AD'-A'D-3(BC'-B'C)\},$$

showing that $ad'-a'd-3(bc'-b'c)$ is an invariant.

12. The Jacobian. (1) The following notation is used:

Let $u, v, w, \ldots$ be k functions of k variables $x, y, z, \ldots$, then

$$J=\begin{vmatrix} u_x & u_y & u_z \ldots \\ v_x & v_y & v_z \ldots \\ w_x & w_y & w_z \ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \end{vmatrix}=\frac{d(u, v, w, \ldots)}{d(x, y, z, \ldots)}$$

where $u_x, u_y, \ldots$ stand for $\dfrac{\partial u}{\partial x}, \dfrac{\partial u}{\partial y}, \ldots$. The function J is called the *Jacobian* of $u, v, w, \ldots$ (with regard to $x, y, z, \ldots$).

In the next three sections we consider two functions of two variables, and by similar reasoning we can show that corresponding theorems hold for k functions of k variables ($k=3, 4, \ldots$).

(2) *If* u, v *are functions of* x, y, *and* x, y *are functions of* X, Y, *then*

$$\frac{d(u, v)}{d(x, y)}=\frac{d(u, v)}{d(X, Y)}\cdot\frac{d(X, Y)}{d(x, y)}.$$

For the right-hand side is equal to

$$\begin{vmatrix} u_X, & u_Y \\ v_X, & v_Y \end{vmatrix}\cdot\begin{vmatrix} X_x, & Y_x \\ X_y, & Y_y \end{vmatrix}=\begin{vmatrix} u_X X_x+u_Y Y_x, & u_X X_y+u_Y Y_y \\ v_X X_x+v_Y Y_x, & v_X X_y+v_Y Y_y \end{vmatrix}=\begin{vmatrix} u_x, & u_y \\ v_x, & v_y \end{vmatrix},$$

which is the left-hand side.

(3) In particular, if we put $u=x$, $v=y$ and observe that $\dfrac{d(x,y)}{d(x,y)}=1$, it follows that

$$\frac{d(x,y)}{d(X,Y)}\cdot\frac{d(X,Y)}{d(x,y)}=1.$$

(4) Again, if $x=lX+mY$, $y=l'X+m'Y$, then

$$\frac{d(x,y)}{d(X,Y)}=lm'-l'm \quad\text{and}\quad \frac{d(u,v)}{d(X,Y)}=(lm'-l'm)\frac{d(u,v)}{d(x,y)},$$

so that *the Jacobian is a covariant.*

(5) *If* $u, v, w, \ldots$ *are* k *quantics in* k *variables* $x, y, z, \ldots$, *then any solution of the system* $u=0$, $v=0$, $w=0, \ldots$ *other than* $x=0$, $y=0$, $z=0, \ldots$ *also satisfies the equation* $J=0$, *and if* $u, v, w, \ldots$ *are of the same degree, it also satisfies the equations* $\dfrac{\partial J}{\partial x}=0$, $\dfrac{\partial J}{\partial y}=0$, $\dfrac{\partial J}{\partial z}=0, \ldots$.

We shall prove this for the case in which $k=3$, similar reasoning applying in all cases. Let u, v, w be quantics of degrees n_1, n_2, n_3 in x, y, z, then by Euler's theorem of homogeneous functions,

$$xu_x+yu_y+zu_z=n_1u, \quad xv_x+yv_y+zv_z=n_2v, \quad xw_x+yw_y+zw_z=n_3w;$$

therefore
$$xJ=n_1uU_x+n_2vV_x+n_3wW_x, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

and two similar equations, where $U_x, V_x, \ldots$ are the cofactors of $u_x, v_x, \ldots$ in J.

Hence if u, v, w are all zero, so also are xJ, yJ, zJ, whence the first part of the theorem.

Next let u, v, w be all of degree n. Differentiating equation (A) with regard to x,

$$x\frac{\partial J}{\partial x}+J=n\left(u\frac{\partial U_x}{\partial x}+v\frac{\partial V_x}{\partial x}+w\frac{\partial W_x}{\partial x}\right)+n(u_xU_x+v_xV_x+w_xW_x),$$

therefore
$$x\frac{\partial J}{\partial x}=n\left(u\frac{\partial U_x}{\partial x}+v\frac{\partial V_x}{\partial x}+w\frac{\partial W_x}{\partial x}\right)+(n-1)J,$$

with two similar equations, and the second part of the theorem follows.

13. The Hessian. (1) If u is a quantic in k variables $x, y, z, \ldots$, the *Hessian* is defined as the Jacobian of $u_x, u_y, u_z, \ldots$ with regard to $x, y, z, \ldots$, that is to say, it is equal to

$$\frac{d(u_x,u_y,u_z,\ldots)}{d(x,y,z,\ldots)}=\begin{vmatrix} u_{xx} & u_{xy} & u_{xz}\ldots \\ u_{yx} & u_{yy} & u_{yz}\ldots \\ u_{zx} & u_{zy} & u_{zz}\ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \end{vmatrix}.$$

(2) *The Hessian is a covariant or, in the case of the quadratic, an invariant.*

We shall prove this for the case in which u is a function of two variables, x, y, using a method which applies in all cases.

Let u be transformed to U by the substitution

$$x = lX + mY, \quad y = l'X + m'Y,$$

and let $\mu = lm' - l'm$, then

$$\frac{d(U_X, U_Y)}{d(X, Y)} = \frac{d(U_X, U_Y)}{d(x, y)} \cdot \frac{d(x, y)}{d(X, Y)} = \mu \frac{d(U_X, U_Y)}{d(x, y)}, \quad \ldots\ldots\ldots\ldots (\mathrm{A})$$

where in the second and third expressions U_X, U_Y are supposed to be expressed in terms of x, y. Now

$$U_X = \frac{\partial u}{\partial x} \cdot \frac{\partial x}{\partial X} + \frac{\partial u}{\partial y} \cdot \frac{\partial y}{\partial X} = lu_x + l'u_y,$$

$$U_Y = \frac{\partial u}{\partial x} \cdot \frac{\partial x}{\partial Y} + \frac{\partial u}{\partial y} \cdot \frac{\partial y}{\partial Y} = mu_x + m'u_y;$$

therefore

$$\frac{d(U_X, U_Y)}{d(x, y)} = \begin{vmatrix} lu_{xx} + l'u_{yx}, & lu_{xy} + l'u_{yy} \\ mu_{xx} + m'u_{yx}, & mu_{xy} + m'u_{yy} \end{vmatrix} = \begin{vmatrix} l, & l' \\ m, & m' \end{vmatrix} \cdot \begin{vmatrix} u_{xx}, & u_{xy} \\ u_{xy}, & u_{yy} \end{vmatrix}.$$

Hence, by (A),

$$\frac{d(U_X, U_Y)}{d(X, Y)} = \mu^2 \cdot \frac{d(u_x, u_y)}{d(x, y)},$$

which proves the theorem.

14. Canonical Forms. The question arises as to what is the simplest form to which a quantic can be brought by linear transformation. Any such form must contain explicitly or implicitly as many constants as the quantic. For instance, *if u is a binary cubic,* the form

$$X^3 + Y^3,$$

where $X = lx + my$, $Y = l'x + m'y$ contains the requisite number of constants. It has been shown (*H.A.*, p. 182) that in general u can be so expressed, and this is taken as the *canonical form of the cubic.*

The exceptional case is when u contains a square factor; it can then be expressed in the form X^2Y.

15. The Quartic. (1) *If u is a binary quartic,* and we assume that

$$u = X^4 + 6\lambda X^2Y^2 + Y^4,$$

where $X = lx + my$, $Y = l'x + m'y$, it will be seen that, by equating coefficients, we have five equations to determine l, m, l', m', λ. But it may happen that these equations are inconsistent.

(2) *Any quartic u which does not contain a cube factor can be expressed in the form*

$$X^4 + 6\lambda X^2Y^2 + Y^4, \quad \text{.....(A)}$$

and in general this can be done in three ways.

For if u have no factor which is a perfect cube, we may assume that $u = vv'$ where v, v' are quadratic functions with no common factor. We can then determine the constants, so that

$$v = \xi^2 + \eta^2, \quad v' = A\xi^2 + B\eta^2,$$

where $\xi = lx + my$, $\eta = l'x + m'y$, and then

$$u = A\xi^4 + (A + B)\xi^2\eta^2 + B\eta^4.$$

By writing $A^{\frac{1}{4}}\xi = X$, $B^{\frac{1}{4}}\eta = Y$, we can now express u in the required form, which is called the *canonical form of the quartic*.

In general, the transformation can be effected in three different ways, corresponding to the three ways of expressing u as the product of quadratic factors. In practice we proceed as follows:

(3) **Reduction of the Quartic to its Canonical Form.** Consider the problem of reducing any quartic u to the form

$$a\xi^4 + 6c\xi^2\eta^2 + e\eta^4$$

by the substitution $x = l\xi + m\eta$, $y = l'\xi + m'\eta$.

We have seven constants at our disposal which are to satisfy five equations, so we may assume that

$$lm' - l'm = 1. \quad \text{.....(B)}$$

Since I and J are invariants of u, we have

$$ae + 3c^2 = I, \quad ace - c^3 = J, \quad \text{.....(C)}$$

and, eliminating ae, it follows that c is one root of the equation

$$4t^3 - It + J = 0. \quad \text{.....(D)}$$

Moreover, if $\mathbf{H}$ is the Hessian of u,

$$\mathbf{H} = ac\xi^4 + (ae - 3c^2)\xi^2\eta^2 + ce\eta^4, \quad \text{.....(E)}$$

and

$$u = a\xi^4 + 6c\xi^2\eta^2 + e\eta^4,$$

therefore

$$\mathbf{H} - cu = (ae - 9c^2)\,\xi^2\eta^2. \quad \text{.....(F)}$$

Hence, if t_1 is a root of (D), then $\mathbf{H} - t_1u$ is a perfect square and ξ, η are factors of its square root. We can thus determine ξ, η so that equation (B) is satisfied, and then a, e are easily found (as in the next example).

Finally, if $\sqrt{a}\xi^2 = X^2$, $\sqrt{e}\eta^2 = Y^2$, we have

$$u = X^4 + 6\frac{c}{\sqrt{ae}}X^2Y^2 + Y^4.$$

NOTE. The modulus of transformation from x, y to X, Y is $1/\sqrt[4]{ae}$.

Ex. 1. *Reduce* $2x^4+8x^3y+4xy^3+13y^4$ *to the form* $a\xi^4+6c\xi^2\eta^2+e\eta^4$.

Here $$u=(2,\ 2,\ 0,\ 1,\ 13)(x,\ y)^4.$$

$$I=2\,.\,13-4\,.\,2\,.\,1=18, \qquad J=\begin{vmatrix} 2 & 2 & 0 \\ 2 & 0 & 1 \\ 0 & 1 & 13 \end{vmatrix}=-54.$$

Let the modulus of transformation be unity, then

$$ae+3c^2=18, \quad ace-c^3=-54, \quad 2c^3-9c-27=0.$$

We may therefore take $c=3$, $ae=-9$.

Again, $$\mathbf{H}=\begin{vmatrix} 2x^2+4xy & 2x^2+y^2 \\ 2x^2+y^2 & 2xy+13y^2 \end{vmatrix};$$

therefore $$-\mathbf{H}=(4,\ -1,\ -5,\ -13,\ 1)(x,\ y)^4,$$

and $$3u-\mathbf{H}=10(x^4+2x^3y-3x^2y^2-4xy^3+4y^4)=10(x+2y)^2(x-y)^2.$$

Let $\xi=x+2y$, $(-3)\eta=x-y$, where (-3) is introduced to make the modulus unity; then $u=a\xi^4+18\xi^2\eta^2+e\eta^4$, where a, e are constants such that $ae=-9$.

To find a, put $x=1$, $y=1$, and we have $\xi=3$, $\eta=0$. Therefore $27=a\,.\,3^4$; thus $a=\frac{1}{3}$, $e=-27$ and $3u\equiv(x+2y)^4+6(x+2y)^2(x-y)^2-(x-y)^4$.

(4) **The Three Canonical Forms.** Equation (**D**) of § (3) may be written

$$4t^3-(ae+3c^2)t+ace-c^3=0,$$

the roots of which are $t_1=c$, $t_2=\frac{1}{2}(-c+\sqrt{ae})$, $t_3=\frac{1}{2}(-c-\sqrt{ae})$. ....(**G**)

Also $$\mathbf{H}=cX^4+\frac{ae-3c^2}{\sqrt{ae}}X^2Y^2+cY^4,$$

whence we can easily find that $$\mathbf{H}-t_1u=\frac{ae-9c^2}{\sqrt{ae}}X^2Y^2,$$

$$\mathbf{H}-t_2u=\tfrac{1}{2}(3c-\sqrt{ae})(X^2-Y^2)^2, \quad \mathbf{H}-t_3u=\tfrac{1}{2}(3c+\sqrt{ae})(X^2+Y^2)^2. \ldots\ldots(\mathbf{H})$$

Again, from equations (**G**), $3c+\sqrt{ae}=3t_1+t_2-t_3=-2(t_3-t_1)$.

$$3c-\sqrt{ae}=3t_1-t_2+t_3=2(t_1-t_2), \quad \text{and} \quad \sqrt{ae}=t_2-t_3,$$

Hence if $(X_1,\ Y_1)$, $(X_2,\ Y_2)$, $(X_3,\ Y_3)$ are the X, Y's of the canonical forms corresponding to t_1, t_2, t_3 respectively, then

$$\left.\begin{aligned} \mathbf{H}-t_1u&=4\frac{qr}{p}X_1^2Y_1^2=-r(X_2^2+Y_2^2)^2=q(X_3^2-Y_3^2)^2,\\ \mathbf{H}-t_2u&=r(X_1^2-Y_1^2)^2=4\frac{rp}{q}X_2^2Y_2^2=-p(X_3^2+Y_3^2)^2,\\ \mathbf{H}-t_3u&=-q(X_1^2+Y_1^2)^2=p(X_2^2-Y_2^2)^2=4\frac{pq}{r}X_3^2Y_3^2, \end{aligned}\right\} \ldots(\mathbf{K})$$

where $$p=t_2-t_3, \quad q=t_3-t_1, \quad r=t_1-t_2.$$

NOTE. The modulus of transformation from x, y to X_1, Y_1 is $1/\sqrt{p}$.

(5) **Symmetrical Resolution of the Quartic u.** *The expression*

$$w \equiv (t_2-t_3)\sqrt{(\mathbf{H}-t_1u)}+(t_3-t_1)\sqrt{(\mathbf{H}-t_2u)}+(t_1-t_2)\sqrt{(\mathbf{H}-t_3u)}$$

(where the radicals may have either sign) is the square of a linear factor of u (Cayley).

With the notation of the last section,

$$w = 2\sqrt{pqr}X_1Y_1+q\sqrt{r}(X_1^2-Y_1^2)+r\sqrt{-q}(X_1^2+Y_1^2)$$
$$=\sqrt{qr}\{(\sqrt{-r}+\sqrt{q})X_1^2+2\sqrt{p}X_1Y_1+(\sqrt{-r}-\sqrt{q})Y_1^2\}.$$

Now $$(\sqrt{p})^2-(\sqrt{-r}+\sqrt{q})(\sqrt{-r}-\sqrt{q})=p+q+r=0.$$

Therefore the expression in the brackets { } is the square of a linear function of x, y, and its square root is a factor of u, for w vanishes if $u=0$.

Ex. 1. *Prove that, whatever signs the radicals may have, the expression*

$$X_1\{\sqrt{(t_2-t_1)}+\sqrt{(t_3-t_1)}\}+Y_1\sqrt{(t_2-t_3)}$$

is a factor of u.

This follows from the preceding or directly by showing that the rationalised form of the equation

$$X_1\{\sqrt{(t_2-t_1)}+\sqrt{(t_3-t_1)}\}+Y_1\sqrt{(t_2-t_3)}=0$$

is

$$X_1^4+6\frac{c}{\sqrt{ae}}X_1^2Y_1^2+Y_1^4=0.$$

(6) **The Sextic covariant G.** (i) Referring to Ex. 2, p. 235, it will be seen that for the form $a\xi^4+6c\xi^2\eta^2+e\eta^4$,

$$\mathbf{G}=(ae-9c^2)\xi\eta(a\xi^4-e\eta^4)=\frac{ae-9c^2}{\sqrt{ae}}X_1Y_1(X_1^4-Y_1^4).$$

Or with the notation of § 4,

$$\mathbf{G}=\frac{4qr}{\sqrt{p}}X_1Y_1(X_1^2-Y_1^2)(X_1^2+Y_1^2); \quad \text{.....(L)}$$

therefore by equations (**K**) of § 4,

$$\mathbf{G}^2=-64pqrX_1^2Y_1^2X_2^2Y_2^2X_3^2Y_3^2=-4(\mathbf{H}-t_1u)(\mathbf{H}-t_2u)(\mathbf{H}-t_3u). \quad \text{(M)}$$

(ii) Again, we have $32\mathbf{G}=v_1v_2v_3$ where

$$v_1/a=(\beta+\gamma-\alpha-\delta)x^2-2(\beta\gamma-\alpha\delta)xy+\{\beta\gamma(\alpha+\delta)-\alpha\delta(\beta+\gamma)\}y^2,$$

v_2, v_3 having similar values.

Since $\mathbf{H}-t_1u$ and v_1^2 are both factors of $\mathbf{G}^2$, and the coefficient of x^4 in $\mathbf{H}-t_1u$ is $-Ha t_1$, which is equal to $-\frac{1}{16}a^2(\beta+\gamma-\alpha-\delta)^2$ (see *H.A.*, p. 191 (**L**)), it follows that

$$v_1^2=-16(\mathbf{H}-t_1u)=-64\frac{qr}{p}X_1^2Y_1^2, \quad \text{.....(N)}$$

with similar equations. Hence it follows that

$$(t_2-t_3)v_1^2+(t_3-t_1)v_2^2+(t_1-t_2)v_3^2=0. \quad \text{.....(O)}$$

Also, it follows from Cayley's Theorem in § (5), that

$$(t_2-t_3)v_1+(t_3-t_1)v_2+(t_1-t_2)v_1 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{P})$$

is the square of a linear factor of u.

Again, since $t_1+t_2+t_3=0$, it follows from (N) that

$$v_1^2+v_2^2+v_3^2=-48\mathrm{H}. \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(\mathbf{Q})$$

(iii) *The quadratics* $v_1=0$, $v_2=0$, $v_3=0$ *are mutually harmonic.*

For by § (4) these equations are equivalent to

$$X_1Y_1=0, \quad X_1^2-Y_1^2=0, \quad X_1^2+Y_1^2=0,$$

which are mutually harmonic.

EXERCISE XVIII

1. Show that a cubic u can be brought to the form ax^3+dy^3 by a linear transformation of which the modulus is 1, and then

$$\mathrm{H}=adxy, \quad \mathrm{G}=ad(ax^3-dy^3), \quad \Delta=a^2d^2.$$

Hence show that $\mathrm{G}^2+4\mathrm{H}^3=\Delta u^2$, thus obtaining another proof of Art. 8, Ex. 1.
[Δ is the resultant of $ax^2=0$, $dy^2=0$ and

$$\mathrm{G}=(-1)^3\{a(ax^3+dy^3)^2-3(ax^3+dy^3)ax^2\,.\,ax+2(ax^2)^3\}.]$$

2. For the cubics u, u', prove that

$$aa'\{(\alpha-\alpha')(\beta-\beta')(\gamma-\gamma')+(\alpha-\beta')(\beta-\gamma')(\gamma-\alpha')+(\alpha-\gamma')(\beta-\alpha')(\gamma-\beta')\}$$

is an invariant, and that it is equal to

$$3\{ad'-a'd-3(bc'-b'c)\}.$$

3. For the quartic, prove that

$$\mathrm{H}=(ac-b^2)x^4+2(ad-bc)x^3y+(ae+2bd-3c^2)x^2y^2 \\ +2(bc-ad)xy^3+(ce-d^2)y^4.$$

4. From equation (Q) on the opposite page, deduce the identity

$$\mathrm{G}^2+4\mathrm{H}^3=u^2\mathrm{H}I-u^3J.$$

5. For the quartic u, prove that

$$\frac{\partial u}{\partial x}\frac{\partial \mathrm{H}}{\partial y}-\frac{\partial u}{\partial y}\frac{\partial \mathrm{H}}{\partial x}=8\mathrm{G}.$$

[The left-hand side is a covariant, so it is only necessary to compare the leading coefficients on both sides.]

6. If the quartic u can be expressed as the sum of two fourth powers, then H is a perfect square and $J=0$.

7. For the quartic u, if $J=0$ prove that u can be brought to one of the forms X^4+Y^4 or X^3Y.

8. (i) Show that any quartic u can be brought to one of the forms

$$aX^4+6cX^2Y^2+eY^4, \quad 4bX^3Y$$

by a linear transformation of which the modulus is unity. (ii) For the first form show that $I=ae+3c^2$, $J=ace-c^3$, $\Delta=ae(ae-9c^2)^2$. (iii) Hence show that in all cases

$$\Delta=I^3-27J^2.$$

9. Find a linear substitution which will reduce the equation $x^4+12x-5=0$ to the form $y^4+fy^2+g=0$, showing that one such substitution is $x=\dfrac{by-a}{y-1}$, where a, b are the roots of $x^2-3x-2=0 (a>b)$, this reducing the equation to

$$(11-3\sqrt{17})y^4+12y^2+(11+3\sqrt{17})=0.$$

10. Using the formulae

$$v_1=\frac{u}{y}\left(\frac{1}{x-\beta\gamma}+\frac{1}{x-\gamma\gamma}-\frac{1}{x-\alpha\gamma}-\frac{1}{x-\delta\gamma}\right), \text{ etc.,}$$

prove that

$$v_2^2-v_3^2=16(t_2-t_3)u,$$

$$v_2^2+v_3^2=2a^2\{(\beta-\gamma)^2(x-\alpha y)^2(x-\delta y)^2+(\alpha-\delta)^2(x-\beta y)^2(x-\gamma y)^2\},$$

and deduce equations (O), (Q) on pages 244, 245.

11. Evaluate the determinant

$$\begin{vmatrix} \beta+\gamma-\alpha-\delta & \beta\gamma-\alpha\delta & \beta\gamma(\alpha+\delta)-\alpha\delta(\beta+\gamma) \\ \gamma+\alpha-\beta-\delta & \gamma\alpha-\beta\delta & \gamma\alpha(\beta+\delta)-\beta\delta(\gamma+\alpha) \\ \alpha+\beta-\gamma-\delta & \alpha\beta-\gamma\delta & \alpha\beta(\gamma+\delta)-\gamma\delta(\alpha+\beta) \end{vmatrix},$$

proving that it is equal to

$$-2(\beta-\gamma)(\gamma-\alpha)(\alpha-\beta)(\alpha-\delta)(\beta-\delta)(\gamma-\delta).$$

[If $v_1=a_1x^2+2b_1xy+c_1y^2$, etc., the determinant in question is equal to $-(a_1b_2c_3)$. Now v_1, v_2, v_3 are transformed into

$$8\iota\sqrt{\frac{qr}{p}}X_1Y_1,\quad 4\iota\sqrt{r}(X_1^2-Y_1^2),\quad 4\sqrt{q}(X_1^2+Y_1^2)$$

respectively by a substitution of modulus $1/\sqrt{p}$. Therefore by Ex. 21, on p. 39,

$$-(a_1b_2c_3)=(\sqrt{p})^3\,.\,2\,.\,4^3\frac{qr}{\sqrt{p}}=2\,.\,4^3pqr.]$$

CHAPTER XLIX

HOMOGRAPHIC TRANSFORMATIONS

1. Homographic Transformation of a Function of Two Variables. (1) Let a pair of variables x, y be connected with another pair X, Y by the equations

$$x=\frac{a_1X+b_1Y+c_1}{a_3X+b_3Y+c_3}, \qquad y=\frac{a_2X+b_2Y+c_2}{a_3X+b_3Y+c_3}. \quad \text{.....(A)}$$

Solving for X, Y, we find that

$$X=\frac{A_1x+A_2y+A_3}{C_1x+C_2y+C_3}, \quad Y=\frac{B_1x+B_2y+B_3}{C_1x+C_2y+C_3}, \quad \text{.....(B)}$$

where A_1, B_1, ... are the cofactors of a_1, b_1, ... in the determinant $(a_1b_2c_3)$.

The change of variables from x, y to X, Y is called a *homographic transformation*, and $(a_1b_2c_3)$ is called the determinant of transformation. It is assumed that $(a_1b_2c_3)\neq 0$, so that none of the above fractions can be of the form $0/0$.

(2) Let (x, y), (X, Y) be the coordinates of points p, P in different planes or in the same plane, the variables being connected as in § (1), then p, P are called corresponding points.

If (p_1, P_1), (p_2, P_2), ... are pairs of corresponding points, the corresponding figures $p_1p_2\ldots$, $P_1P_2\ldots$ are said to be *homographic*.

(3) If (x, y) is any point on the line $C_1x+C_2y+C_3=0$, at least one of the two, X, Y, is infinite, and we say that *the point* (X, Y) *is at infinity*. So also any point on the line $a_3X+b_3Y+c_3=0$ corresponds to a point (x, y) at infinity.

(4) It is clear that *corresponding curves are of the same degree*. In particular, *a straight line corresponds to a straight line*. Thus the line

$$lx+my+n=0$$

corresponds to the line

$$l(a_1X+b_1Y+c_1)+m(a_2X+b_2Y+c_2)+n(a_3X+b_3Y+c_3)=0.$$

In order that the last statement may be universally true, we require the following convention: *The points at infinity in any plane are to be regarded as lying on a straight line called the line at infinity in that plane.*

It then follows from § (3) that the lines

$$a_3X + b_3Y + c_3 = 0, \quad C_1x + C_2y + C_3 = 0, \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

respectively correspond to the lines at infinity in the first and second planes, and they are called the *vanishing lines.*

With this understanding, *there is a complete one-to-one correspondence between the points, and also between the straight lines in two homographic figures.*

(5) **Anharmonic Relations.**

(i) *To a pencil of four concurrent lines corresponds a pencil of four concurrent lines equi-cross with the first.*

For if the equations to the first four lines are

$$\alpha - k_1\beta = 0, \quad \alpha - k_2\beta = 0, \quad \alpha - k_3\beta = 0, \quad \alpha - k_4\beta = 0,$$

then those of the second four are

$$\alpha' - k_1\beta' = 0, \quad \alpha' - k_2\beta' = 0, \quad \alpha' - k_3\beta' = 0, \quad \alpha' - k_4\beta' = 0,$$

where $\alpha' = 0$, $\beta' = 0$ are the lines corresponding to $\alpha = 0$, $\beta = 0$. Thus (k_1k_2, k_3k_4) is a cross-ratio of each pencil, and the theorem follows.

(ii) *To a range of four collinear points corresponds a range of four collinear points equi-cross with the first.*

For if p_1, p_2, p_3, p_4 are collinear points, the corresponding points P_1, P_2, P_3, P_4 are collinear. Also, if q, Q are corresponding points, (qp_1, QP_1), etc., are pairs of corresponding lines, and, by the preceding,

$$(p_1p_2, p_3p_4) = q(p_1p_2, p_3p_4) = Q(P_1P_2, P_3P_4) = (P_1P_2, P_3P_4).$$

(6) *Two homographic figures in the same plane have three common or self-corresponding points, which are often called the* double points.

For if the figures are referred to the same axes, the common points are found by putting $X = x$, $Y = y$ in equations (A), and, in general, the resulting equations have three solutions. A special case is considered later.

(7) If two homographic figures are referred to triangles of reference in their own planes, the equations of transformation are of the form

$$x : y : z = a_1X + b_1Y + c_1Z : a_2X + b_2Y + c_2Z : a_3X + b_3Y + c_3Z. \quad \ldots\ldots\text{(D)}$$

(8) The equations of transformation involve *eight* independent constants, hence *the homographic relation is determined if we know four pairs of corresponding points or four pairs of corresponding straight lines.*

Ex. 1. *Given four pairs of corresponding points* (p_1, P_1), (p_2, P_2), *etc., it is required to find the equations of transformation.*

Let abc be the diagonal triangle of the quadrilateral $p_1p_2p_3p_4$, and let p_1, p_2 divide bc, ca respectively in the ratios $m:n$, $n:l$. Let capital letters have similar meanings for the figure $P_1P_2P_3P_4$.

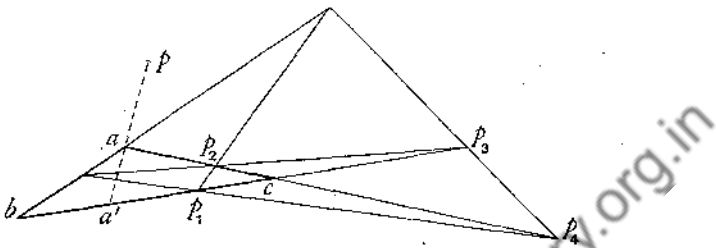


FIG. 49.

If (x, y, z), (X, Y, Z) *are the areal coordinates of corresponding points* p, P *referred to the triangles* abc, ABC, *the required equations are*

$$lx : my : nz = LX : MY : NZ.$$

For if ap meets bc in a', we have $ba'/a'c = z/y$; hence

$$a(pp_1, bc) = (a'p_1, bc) = \frac{z}{y} \Big/ \frac{m}{n} = \frac{nz}{my}.$$

Similarly $A(PP_1, BC) = NZ/MY$. Now a, A are corresponding points, being the intersections of corresponding lines: so also are b, B and c, C.

Therefore $a(pp_1, bc) = A(PP_1, BC)$ and $nz/my = NZ/MY$, etc.

Ex. 2. *Let* A, B, C *be the three common points of two homographic figures in the same plane, and let* p_1, P_1 *be a pair of corresponding points. If* ABC *is taken as the triangle of reference, the equations of transformation are*

$$x/x_1 : y/y_1 : z/z_1 = X/X_1 : Y/Y_1 : Z/Z_1,$$

where (x_1, y_1, z_1), (X_1, Y_1, Z_1) *are the coordinates of* p_1, P_1.

For if (p, P) is any pair of corresponding points, $A(pp_1, BC) = A(PP_1, BC)$, and the proof can be completed as in Ex. 1.

2. Perspective. The methods of projection and plane perspective are special cases of homographic transformation.

(1) **Projection.** Takes two planes σ, σ' meeting in the line Oy and a point V external to both planes: V is called the *vertex* and Oy the *axis* of projection.

Any line through V meets σ, σ' in *corresponding points* p, P. Any figure described by P and the corresponding figure described by P are said to be *in perspective*, and each is called the *projection* of the other.

To a straight line l in σ corresponds a straight line L in σ', which is the intersection of the plane through V and l with σ'. Thus corresponding straight lines meet on the axis Oy.

Let the planes through V parallel to σ, σ' cut σ', σ respectively in II', jj' then these lines correspond to the lines at infinity in the planes σ, σ, respectively and are the *vanishing lines*.

Let the plane through V perpendicular to Oy cut σ, σ' in Ox, OX respectively, and let (x, y), (X, Y) be the coordinates of any two corresponding points p, P referred to Ox, Oy and OX, Oy as axes. Suppose also that I, j are the points where the vanishing lines cut Ox, OX, and let $OI = a$ and $IV = b$.

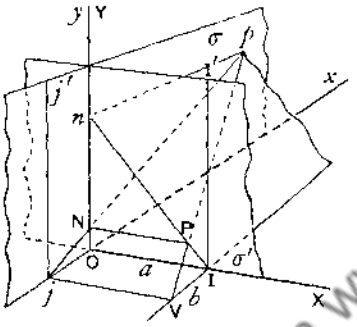


Fig. 50.

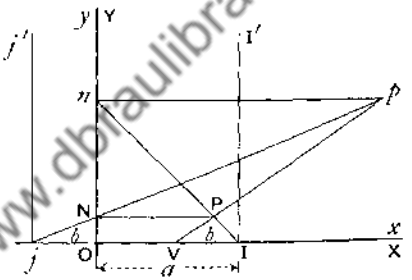


Fig. 51.

The plane through VI and p meets σ' in a line pn parallel to Ox (Fig. 50) and cuts σ' in the line In, which therefore intersects Vp in P. Hence, if PN, drawn parallel to XO, cuts Oy in N, the triangles Pnp, PIV are similar, and so are PnN, InO; therefore

$$\frac{np}{IV} = \frac{Pn}{IP} = \frac{Nn}{ON} = \frac{NP}{OI - NP}, \quad \text{and so} \quad \frac{x}{b} = \frac{y - Y}{Y} = \frac{X}{a - X}.$$

Hence the homographic relation is

$$x = \frac{bX}{a - X}, \quad y = \frac{aY}{a - X} \quad \text{or} \quad X = \frac{ax}{x + b}, \quad Y = \frac{by}{x + b}. \qquad \text{.....(A)}$$

(2) **Plane Perspective.** (i) Suppose that the plane σ (Fig. 50) rotates about Oy until it coincides with the plane σ'. One of the two ways in which this can happen is depicted in Fig. 51. The figures described by p and P are now said to be in *plane perspective*, V being the *vertex* and Oy the *axis of perspective*. As before, II' and jj' are the *vanishing lines*, their equations being $X - a = 0$ and $x + b = 0$. Also, during the rotation, V lies in the plane OxX, and when Ox, OX coincide, V is on Ox.

Given a point p of the first figure, the corresponding point P is the intersection of In and VP. The equations of transformation are the same as before. Also corresponding lines meet on the axis Oy, for their equations may be taken as $lx+my+n=0$ and $lbX+maY+n(a-X)=0$.

It follows that j, N, p are collinear, for j corresponds to the point at infinity on OX, and so PN, pj are corresponding lines and meet on the axis; this also follows from Fig. 50, for there j, N, p lie on the line where the planes xOy, jNp intersect.

(ii) *If the vertex is taken as origin and the equations to the vanishing lines are* $x=a$, $X=b$, *the homographic relation is*

$$x=\frac{aX}{X-b}, \quad y=\frac{aY}{X-b} \quad \text{or} \quad X=\frac{bx}{x-a}, \quad Y=\frac{by}{x-a}, \quad \ldots\ldots\ldots\ldots(\mathbf{B})$$

and the equation to the axis of perspective is $x=a+b$.

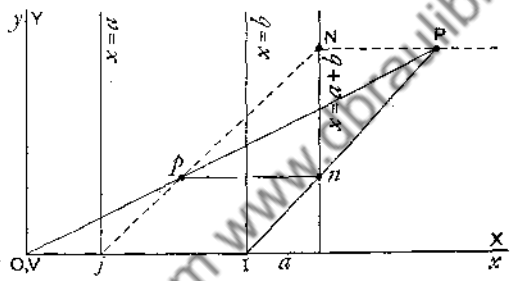


Fig. 52.

For, in Fig. 52, $\frac{x}{X}=\frac{Op}{OP}=\frac{In}{IP}=\frac{a}{X-b}$ and $\frac{x}{X}=\frac{y}{Y}$.

(iii) *The double points of the system are the vertex and every point on the axis of perspective.*

For the double points are to be found by putting $X=x$ and $Y=y$ in equations (**B**), and are given by $x(x-b)=ax$, $y(x-b)=ay$, whence $x=0$, $y=0$ or $x=a+b$, y having any value.

(iv) *Homographic figures in the same plane, which are such that the straight lines joining every pair of corresponding points pass through a fixed point, are in plane perspective.*

For, taking the fixed point as origin and $X-b=0$ as the equation to a vanishing line, it is obvious that equations (**A**) of Art. 1 must be of the form (**B**) in this section.

This statement may conveniently be taken as a *definition of plane perspective*; the fundamental property that corresponding lines meet on a fixed line following at once from equations (**B**).

(v) The relation between two figures in perspective is determined if we know:

(*a*) The vertex O, the axis and two corresponding points (which must be collinear with O).

(*b*) Or three pairs of corresponding points, (a, A), (b, B), (c, C), which must be such that the lines aA, bB, cC are concurrent.

The point of concurrence is the vertex, and the pairs of lines (bc, BC), (ca, CA), (ab, AB) meet on a line which is the axis of perspective. In the case of plane perspective, the collinearity of these points depends on Desargues' theorem. (See Ex. XIX.)

It follows that *the equations of transformation involve five independent constants.* For five conditions are required to determine the elements in (*a*) or (*b*).

(vi) In a plane perspective, suppose that the vertex O, the axis and two corresponding points q, Q are given. Let OqQ meet the axis in q', and let $\rho = (Oq, Qq')$, then *if* x_0, y_0, z_0 *are the coordinates of* O *and the equation to the axis is* $lx + my + nz = 0$, *then the equations of transformation are*

$$\frac{X}{x_0(lx+my+nz)-kx} = \frac{Y}{y_0(lx+my+nz)-ky} = \frac{Z}{z_0(lx+my+nz)-kz},$$

where $$k = \rho(lx_0 + my_0 + nz_0).$$

For let p, P be any two corresponding points, and let OpP meet the axis in p', the coordinates of p, p', P being (x, y, z), (x', y', z'), (X, Y, Z).

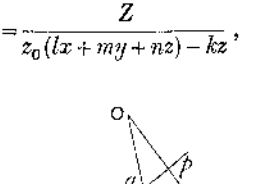


FIG. 53.

Then since pq, PQ, $p'q'$ are concurrent, $(Op, Pp') = (Oq, Qq') = \rho$; and, since O, p, P, p' are collinear, we have

$$X = \lambda x_0 + \mu x, \quad Y = \lambda y_0 + \mu y, \quad Z = \lambda z_0 + \mu z,$$

and $$x' = \lambda' x_0 + \mu' x, \quad y' = \lambda' y_0 + \mu' y, \quad z' = \lambda' z_0 + \mu' z,$$

where $$\lambda/\mu = Pp/OP \text{ and } \lambda'/\mu' = p'p/Op'.$$

Therefore $$\frac{\lambda}{\mu}\Big/\frac{\lambda'}{\mu'} = (Pp', pO) = \frac{1}{(\overline{Op}, \overline{Pp'})} = \frac{1}{\rho}.$$

Also $lx' + my' + nz' = 0$, for p' is on the axis, therefore

$$\lambda'(lx_0 + my_0 + nz_0) + \mu'(lx + my + nz) = 0.$$

Hence $$\frac{\lambda}{\mu} = -\frac{1}{\rho} \cdot \frac{lx+my+nz}{lx_0+my_0+nz_0} \text{ and } \frac{X}{\mu} = -\frac{x_0}{\rho} \cdot \frac{lx+my+nz}{lx_0+my_0+nz_0} + x,$$

with similar equations, and the result in question follows at once.

NOTE. (i) If Oq' is perpendicular to the axis and q is at infinity, with the notation of Art. 2, (2), (ii), we have $Oq'=a+b$, $OQ=b$ and $\rho=OQ/Oq'=b/(a+b)$.

(ii) Using Cartesian coordinates, if (x_0, y_0) is the vertex and $lx+my+n=0$ is the equation to the axis, the equations of transformation can be derived from the preceding by putting $z=z_0=1$.

Ex. I. *The relations connecting two figures in plane perspective may be written in the form* *

$$\frac{(l'-l)X}{l'x+my+nz}=\frac{(m'-m)Y}{lx+m'y+nz}=\frac{(n'-n)Z}{lx+my+n'z}, \quad \text{.....(C)}$$

where $lx+my+nz=0$ *is the equation to the axis and the triangle of reference ABC is chosen so that none of its sides passes through the vertex.*

If C is at the vertex, the equations are

$$\frac{X}{x}=\frac{Y}{y}=\frac{(n'-n)Z}{lx+my+n'z}. \quad \text{.....(D)}$$

This follows from equations (B) by dividing the numerators and denominators of the first, second and third fractions by x_0, y_0, z_0 respectively and writing $l-k/x_0=l'$, etc. Here it is assumed that none of x_0, y_0, z_0 is zero. In the second case $x_0=0$, $y_0=0$, etc.

3. The Circular Points at Infinity.

The equation to any circle is

$$x^2+y^2+2gx+2fy+c=0,$$

and, applying the transformation $x=bX/(a-X)$, $y=aY/(a-X)$, the resulting equation is $b^2X^2+a^2Y^2+2(bgX+afY)(a-X)+c(a-X)^2=0$.

Hence the curve corresponding to the circle meets the vanishing line $X=a$ in the points $(a, \pm ib)$, and the circle meets the line at infinity in the corresponding points, which are the same for all values of g, f, c.

Thus *all circles in a given plane meet the line at infinity in two fixed points, which lie on the lines* $y=\pm ix$ *and are called the circular points at infinity.*

4. Metrical Properties of Two Homographic Figures.

We suppose that a small letter and the corresponding capital represent corresponding points in two figures, and that the coordinates of two such points are connected by the equations

$$x=\frac{a_1X+b_1Y+c_1}{a_3X+b_3Y+c_3}, \quad y=\frac{a_2X+b_2Y+c_2}{a_3X+b_3Y+c_3}, \quad \text{.....(A)}$$

which are the same as

$$X=\frac{A_1x+A_2y+A_3}{C_1x+C_2y+C_3}, \quad Y=\frac{B_1x+B_2y+B_3}{C_1x+C_2y+C_3}, \quad \text{.....(B)}$$

where A_1, B_1, ... are the cofactors of a_1, b_1, ... in the determinant $(a_1b_2c_3)$. The coefficients in these equations are assumed to be *real* numbers.

* This matter is discussed and the result is stated wrongly in Salmon's *Higher Plane Curves*, second edition, p. 286.

(1) Let c, c' be the points at infinity in the first figure on the lines $y = \iota x$, $y = -\iota x$ respectively, and D, D' the points at infinity in the second figure on the lines $Y = \iota X$, $Y = -\iota X$ respectively.

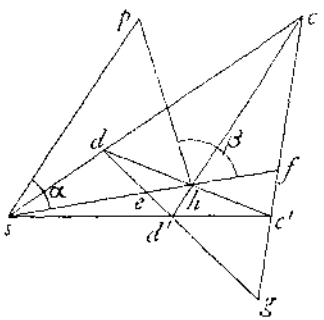


FIG. 54.

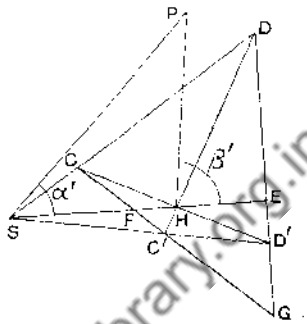


FIG. 55.

Let s, h, g be the points of intersection of cd and $c'd'$, cd' and $c'd$, cc' and dd' respectively. Let sh meet dd', cc' in e, f.

The figure thus constructed has remarkable properties:

(i) *The points s, h, S, H are real*—for c, c' are conjugate imaginary points: so also are d, d', it being assumed that the transformation is real. Hence cd, $c'd'$ and cd', $c'd$ are conjugate imaginary lines which meet in real points s, h. The corresponding points S, H are also real.

(ii) *The vanishing lines dd', CC' bisect sh, SH at right angles.* For (sh, ef) is a harmonic range and f is at infinity, therefore sh is bisected at e. Also $e(fg, cc')$ is a harmonic pencil and c, c' are the circular points at infinity, therefore eg is at right angles to ef (Ex. II, 4).

(iii) *If p, P are any two corresponding points and $\angle hsp = \alpha$, $\angle fhp = \beta$, $\angle HSP = \alpha'$, $\angle EHP = \beta'$, the angles being measured in the positive sense in each figure, then*

$$\alpha' = n\pi + \alpha, \quad \beta' = n\pi - \beta.$$

For we have

$$S(PH, DD') = s(ph, dd') = s(ph, cc'),$$

and therefore, as in Ex. II, 4,

$$\cos 2\alpha' + \iota \sin 2\alpha' = \cos 2\alpha + \iota \sin 2\alpha \quad \text{and} \quad \alpha' = n\pi + \alpha.$$

Also $$H(PS, DD') = h(ps, dd') = h(ps, c'c).$$

Now if hs, HS are turned through the angles $\pi + \beta$, $\pi + \beta'$, they will fall along hp, HP respectively, therefore

$$\cos 2\beta' + \iota \sin 2\beta' = \cos 2\beta - \iota \sin 2\beta \quad \text{and} \quad \beta' = n\pi - \beta.$$

Hence the following construction. *To find the point P corresponding to a given point p:* make angles HSL, EHM equal to α and $\pi-\beta$ respectively, then SL, HM meet in P.

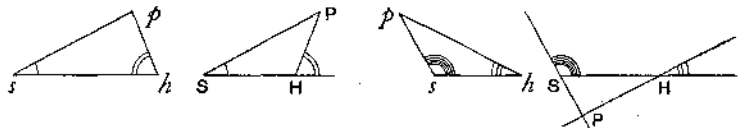


FIG. 56.

Thus, in Fig. 56, angles marked alike are equal.

Theorem (ii) is an immediate consequence of this construction, for if p is on the perpendicular bisector of sh, then P is at infinity.

(2) *To find the straight line corresponding to a given straight line.*

Let e, F be the mid-points of sh, SH. In the line sh take s', h' so that $s'e=eh'=SF$. In the line SH take S', H' so that $S'F=FH'=se$.

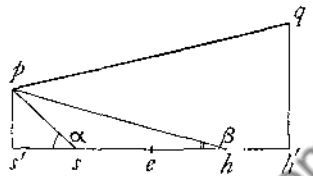


FIG. 57.

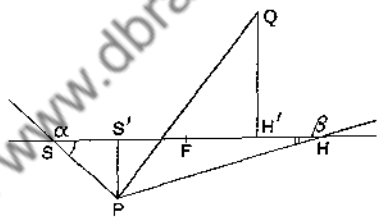


FIG. 58.

Let the given line meet the perpendiculars to sh through s', h' in p, q.

Through S', H' draw perpendiculars to SH. Along the first set off $S'P$ equal to $s'p$ and in the opposite sense. Along the second set off $H'Q$ equal to $h'q$ and in the same sense. Then PQ corresponds to pq.

For the triangles $SS'P$, $ss'p$ are congruent, and so are $S'HP$, $s'hp$; thus $\angle PSS'=\angle pss'$ and $\angle S'HP=\angle phs$. Hence P corresponds to p, and similarly it can be shown that Q corresponds to q.

It is usual to call $s'p$, $S'P$ and $h'q$, $H'Q$ the *isotropic* lines, and it follows that *they are pairs of corresponding lines.*

(3) *Any two homographic figures can be placed in perspective, and this can be done in four different ways.*

For if the second figure is placed so that S falls on s and SH is along sh or sh produced through s, the figures will be in perspective. Or if the second figure is '*turned over*' and then placed so that H falls on h and HS is along hs or hs produced through h, the figures will be in perspective.

If the figures are in the same plane and are referred to the same axes, the second figure can be placed in perspective with the first by a *translation* in which S is made to fall on s and a *rotation* about S through an angle θ such that $\tan\theta = (a_3C_2 - b_3C_1)/(a_3C_1 + b_3C_2)$.

For when the figures are in perspective, the vanishing lines are parallel.

(4) It follows that *every geometrical theorem which results from the general homographic transformation can be proved by the method of projection or plane perspective.*

Another important conclusion is that *any two quadrilaterals abcd, ABCD, can be placed in perspective.* For we can determine two homographic figures in which (a, A), (b, B), (c, C), (d, D) are pairs of corresponding points.

(5) *The coordinates of* s, h, S, H may be found as follows: In Fig. 54 at c we have $x = I$, $y = \iota I$ where $I \to \infty$; at D, $X = I$, $Y = \iota I$, and therefore at d

$$x = (a_1 + \iota b_1)/(a_3 + \iota b_3), \quad y = (a_2 + \iota b_2)/(a_3 + \iota b_3).$$

Hence the equation to cd is

$$\begin{vmatrix} x & y & 1 \\ a_1 + \iota b_1 & a_2 + \iota b_2 & a_3 + \iota b_3 \\ 1 & \iota & 0 \end{vmatrix} = 0,$$

which reduces to

$$b_3x + a_3y - a_2 - b_1 - \iota(a_3x - b_3y - a_1 + b_2) = 0.$$

The equation to $c'd'$ is obtained from this by changing the sign of ι, hence *the point* s *is given by*

$$a_3x - b_3y = a_1 - b_2, \quad b_3x + a_3y = a_2 + b_1. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(A)}$$

Similarly, *at the point* h,

$$a_3x + b_3y = a_1 + b_2, \quad b_3x - a_3y = -a_2 + b_1. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

At the point S,

$$C_1X - C_2Y = A_1 - B_2, \quad C_2X + C_1Y = B_1 + A_2. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

At the point H,

$$C_1X + C_2Y = A_1 + B_2, \quad C_2X - C_1Y = -B_1 + A_2. \quad \ldots\ldots\ldots\ldots\ldots\ldots\text{(D)}$$

EXERCISE XIX

1. If the axis of perspective is taken as the axis of y and the coordinates of the vertex are $p+q$, r, show that the equations of transformation are of the form

$$x=\frac{pX}{X-q}, \quad y=\frac{rX-qY}{X-q}.$$

2. In a plane perspective, the vertex O, the axis and two corresponding points a, A are given. If the line OaA meets the axis in a', the vertex is taken as the origin, and the equation to the axis is $lx+my+n=0$, the equations of transformation are

$$\frac{X}{x}=\frac{Y}{y}=-\frac{\rho n}{lx+my+n(1-\rho)},$$

where $\rho=(Oa, Aa')$.

3. If the equations of transformation are

$$x=aX/(X-b), \quad y=aY/(X-b),$$

show that the points s, S are at the vertex O, and that h, H are respectively the points $(2a, 0)$, $(2b, 0)$. Hence explain the constructions indicated below and verify in a more elementary way.

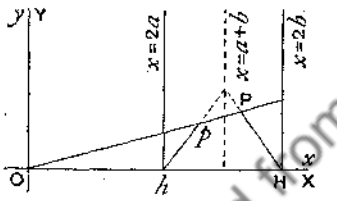


FIG. 59.

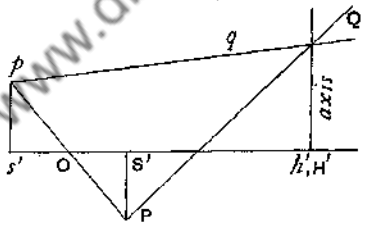


FIG. 60.

(i) Given p, to find P. In Fig. 59, $\angle hHP=\angle Hhp$.

(ii) Given a line pq, to find the corresponding line PQ. In Fig. 60,

$$s'O=OS'=b-a, \quad Oh'=OH'=b+a.$$

See Art. 4 (1) and (2).

4. In a plane perspective, the points d, d' corresponding to the circular points at infinity (D, D') are given. Consequently the vertex V is the point of intersection of dD, $d'D'$ and any line parallel to dd' may be taken as axis.

Also show that if the coordinates of d, d' are $(p, \alpha \pm i\beta)$ the coordinates of V are $(p-\beta, \alpha)$ and that the transformation is real.

5. Show that the linear transformation given by the equation

$$x'=\lambda x+x_0(lx+my+nz), \quad y'=\lambda y+y_0(lx+my+nz), \quad z'=\lambda z+z_0(lx+my+nz),$$

where λ is any number, is the general perspective transformation, with vertex at $(x_0y_0z_0)$. Deduce Desargues' Theorem.

[Prove that the joins of corresponding points pass through (x_0, y_0, z_0): then apply the equations to two triangles ABC, $A'B'C'$, taking ABC as the triangle of reference.]

6. All conics which pass through two given points (d, d') can be transformed simultaneously into circles by plane perspective. Find a transformation which will convert any conic of the system

$$ax^2+2hxy+by^2+(x-p)(\lambda x+\mu y+\nu)=0$$

into a circle, where λ, μ, ν have any values, and give the transformed equation.

[The points d, d' must correspond to D, D', the circular points at infinity. The coordinates of d, d' are $(p, \alpha\pm\iota\beta)$, where $\alpha\pm\iota\beta$ are the roots of

$$by^2+2hpy+ap^2=0,$$

and, by Ex. 4, V is the point $(p-\beta, \alpha)$.

Also we may take Oy, which is parallel to dd', as the axis of perspective.

Hence, by Ex. 1, the required transformation is

$$x=pX/(X+\beta), \quad y=(\alpha X+\beta Y)/(X+\beta),$$

where $\alpha=-ph/b$ and $\beta=\pm\sqrt{ab-h^2}\,.\,p/b$.

Also $$ax^2+2hxy+by^2=b\left\{\left(y-\frac{\alpha x}{p}\right)^2+\frac{\beta^2x^2}{p^2}\right\}=\beta^2(X^2+Y^2)/(X+\beta)^2$$

and $$x-p=-p\beta/(X+\beta),$$

hence the transformed equation is

$$\beta(X^2+Y^2)-p\{\lambda pX+\mu(\alpha X+\beta Y)+\nu(X+\beta)\}=0.$$

7. Two conics having double contact can be transformed into concentric circles by plane perspective. Taking the equations of the conics as

$$ax^2+2hxy+by^2=\lambda(x-p)^2, \quad ax^2+2hxy+by^2=\lambda'(x-p)^2,$$

find the necessary transformation and the resulting equations.

[The transformation is the same as in Ex. 6, and the transformed equations are

$$X^2+Y^2=\lambda p^2, \quad X^2+Y^2=\lambda' p^2.]$$

8. Show that the conics $ax^2+by^2=1$, $y^2=mx$ can be transformed into circles by real plane perspective, and that if a, b, m are all positive, the equations of transformation are $x=pX/(X+q)$, $y=qY/(X+q)$, where p is the negative root of $ax^2+bmx-1=0$ and $q^2=-mp$.

9. If a, b, a', b' are positive and $a>a'$, show that the conics

$$ax^2+by^2=1, \quad a'x^2-b'y^2=1$$

can be transformed into circles by real plane perspective, and that the equations of transformation are $x=pX/(X+q)$, $y=qY/(X+q)$ where

$$(b+b')p^2=(a-a')q^2=ab'+a'b.$$

10. The homographic relation for two figures in the same plane and referred to the same axes is

$$x=(4X-2Y)/5(Y+1), \quad y=(3X+16Y+5)/5(Y+1).$$

Find the coordinates of s, S, h, H and specify a displacement of the second figure which will put it in perspective with the first.

11. For areal coordinates, a circular point at infinity is given by

$$x:y:z=ae^{-\iota B}:be^{\iota A}:-c.$$

[The circular points at ∞ are given by

$$a^2yz+b^2zx+c^2xy=0, \quad x+y+z=0.]$$

12. It is required to place two given four-point figures $abcd$, $ABCD$ in perspective.

Let p, q, P, Q be the points of intersection of (ad, bc), (bd, ca), (AD, BC) respectively.

The four pairs (a, A), (b, B), (c, C), (d, D) determine homographic figures in which (p, P), (q, Q) are pairs of corresponding points. Let the vanishing line of the first figure meet bc, ca, ab in a_1, b_1, c_1; then

$$(a_1p, bc) = (\infty P, BC), \text{ and so } \frac{a_1b}{a_1c} = \frac{bp}{pc} \div \frac{BP}{PC}.$$

This determines a_1, and b_1 can be found in the same way.

On c_1a_1, a_1b_1 draw segments of circles containing angles equal to CBA, ACB respectively, and let the arcs meet in s.

Taking s as the vertex of perspective, draw $B'C'$ parallel to sa_1, so that $B'C' = BC$ and B', C' are on sb, sc respectively. Draw $C'A'$ parallel to Sb, to meet sa in A'.

Let P', Q' be the intersections of $(sp, B'C')$, $(sq', C'A')$, and let $A'P'$, $B'Q'$ meet in D'.

Then $A'B'C'D'$ is equal in all respects to $ABCD$.

For it is easy to show that if s is taken as vertex and any line parallel to $a_1b_1c_1$ as axis of perspective, the figure corresponding to $abcd$ is similar to $ABCD$.

13. Given four pairs of corresponding points (a, A), (b, B), (c, C), (d, D) of two homographic figures, it is required to find the points s, h, S, H.

The point s is that found in Ex. 12, and h is the reflection of s in the line $a_1b_1c_1$.

If the vanishing line in the second figure meets BC, CA, AB in a_1, b_1, c_1, we have $(\infty p, bc) = (a_1P, BC)$, and so $\frac{a_1B}{a_1C} = \frac{a_1c}{a_1b}$.

If segments of circles are drawn on c_1a_1, a_1b_1 to contain angles equal to cba, acb, on both sides of $a_1b_1c_1$, the arcs meet in S, H.

14. Any circle of the coaxal system with s, h as limiting points corresponds to a circle of the coaxal system with S, H as limiting points.

[A conic through c, c', d, d' (Figs. 54, 55) corresponds to a conic through C, C', D, D', and both of these are circles.]

15. In two homographic figures, there are circles in the one figure which correspond to circles in the other. Each set of circles form a coaxal system with s, h or S, H as limiting points.

Any conic in the first figure with foci at s and h corresponds to a conic with foci at S and H.

[For the lines sc, sc' correspond to SD, SD' (Figs. 54, 55), and sc, sc' touch the conic in the first figure, etc.]

MISCELLANEOUS EXERCISES

1. If (x_1, y_1, z_1), (x_2, y_2, z_2) are solutions of

$$\frac{ax+hy+gz}{x}=\frac{hx+by+fz}{y}=\frac{gx+fy+cz}{z},$$

prove that $$x_1x_2+y_1y_2+z_1z_2=0.$$

2. Show that if $x=\dfrac{n(a-b)+a}{n(a-b)+b}$, then $\dfrac{a-bx}{(1-x)^2}$ is equal to the sum of the first n terms of its expansion in ascending powers of x, a and b being unequal.

3. If a, b, c are the sides of a triangle of area Δ, prove that

$$\begin{vmatrix} (b-c)^2 & b^2 & c^2 & 1 \\ a^2 & (c-a)^2 & c^2 & 1 \\ a^2 & b^2 & (a-b)^2 & 1 \\ 1 & 1 & 1 & 0 \end{vmatrix} = -16\Delta^2.$$

4. If four positive quantities are restricted to have a sum $4c$ and a sum of squares $8c^2$, no one of them can exceed $(\sqrt{3}+1)c$.

5. If $y_1, y_2, y_3, \ldots y_n$ are n positive numbers each greater than a, connected by the single relation

$$(y_1-a)(y_2-a)\ldots(y_n-a)=b^n,$$

show that $$y_1y_2y_3\ldots y_n < (a+b)^n.$$

6. $1+x(x+1)+x^2(1+x+x^2)+\ldots$ to n terms

$$=(1-x^n)(1-x^{n+1})/((1-x)(1-x^2)).$$

7. If in the series $a_0+\dfrac{a_1}{\lfloor 1}x+\dfrac{a_2}{\lfloor 2}x^2+\ldots$ the a's are connected by the relation

$$a_n+n(n-1)a_{n-2}+n(n-1)(n-2)(n-3)a_{n-4}=0$$

for $n \geqslant 3$, show that the series is convergent when $x^2<1$.

8. Show that (i) the series whose nth term is $\dfrac{1}{n}-\dfrac{1}{2n+1}-\dfrac{1}{2n+2}$ is convergent; (ii) its sum to infinity is $\frac{3}{2}-\log 2$; and (iii) its sum to n terms differs from its sum to infinity by less than $\dfrac{3}{4n}$.

9. Show, by induction or otherwise, that the number of regions into which a plane is divided by a straight line is $(n^2+n+2)/2$, provided that no two are parallel and no three meet in a point.

10. Prove that the $\Sigma_0^\infty x^n \sinh(n+1)\alpha$ is convergent if $|x|<e^{-\alpha}$, where α is being assumed positive, and that the sum is

$$\sinh\alpha/(1-2x\cosh\alpha+x^2).$$

11. Prove that

$$\log(1+x+\tfrac{1}{2}x^2)=\Sigma_{n=1}^{n=\infty}(-1)^{n-1}\cdot\frac{1}{n}\left\{(1+i)^n+(1-i)^n\right\}\cdot\left(\frac{x}{2}\right)^n,$$

and find the coefficients of x^n, when n is of the forms $4r$, $4r+1$, $4r+2$, $4r+3$.

12. If $(1+x)^n=c_0+c_1x+c_2x^2+\ldots+c_nx^n$, prove that

$$\frac{c_0}{1^2}-\frac{c_1}{2^2}+\frac{c_2}{3^2}-\ldots+(-1)^n\frac{c_n}{(n+1)^2}=\frac{1}{n+1}\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n+1}\right).$$

13. If a_1 and b_1 are the arithmetic and harmonic means of a and b, a_2 and b_2 those of a_1 and b_1, a_3 and b_3 those of a_2 and b_2, and so on, then

$$a_n = \sqrt{(ab)}\,\frac{(\sqrt{a}+\sqrt{b})^{2n}+(\sqrt{a}-\sqrt{b})^{2n}}{(\sqrt{a}+\sqrt{b})^{2n}-(\sqrt{a}-\sqrt{b})^{2n}}.$$

14. If $p_1 = \dfrac{p_0}{1+a_0p_0}$, $p_2 = \dfrac{p_1}{1+a_1p_1}$, etc., prove that $p_n = \dfrac{p_0}{1+\lambda p_0}$, where

$$\lambda = a_0 + a_1 + \ldots + a_{n-1}.$$

15. Prove that if

$$u_2 = u_1^2 - 1, \quad u_1u_3 = u_2^2 - 1, \quad u_2u_4 = u_3^2 - 1, \quad u_3u_5 = u_4^2 - 1, \ \ldots,$$

then

$$u_1 + u_3 = u_1u_2, \quad u_2 + u_4 = u_1u_3, \quad u_3 + u_5 = u_1u_4, \quad u_4 + u_5 = u_1u_5, \ \ldots.$$

16. If $Z = \dfrac{2z-\iota}{\iota z+2}$ where $Z = X + \iota Y$, $z = x + \iota y$ and

$$-1 < X < 1, \quad Y > 0, \quad |Z| > 1,$$

show that the point z is within the area bounded by arcs of the three circles

$$x^2 + (y-2)^2 = \pm 3x, \quad x^2 + y^2 = 1,$$

each of which touches the other two.

[Find X, Y in terms of x, y. Hence show that z is outside each of the three circles and inside the circle $2x^2 + 2y^2 - 5y + 2 = 0$.]

17. If

$$u_n = 1 - \frac{n(n-1)}{\lfloor 2} + \frac{n(n-1)(n-2)(n-3)}{\lfloor 4} - \ldots,$$

$$v_n = n - \frac{n(n-1)(n-2)}{\lfloor 3} + \frac{n(n-1)(n-2)(n-3)(n-4)}{\lfloor 5} - \ldots,$$

where n is a positive integer, show that

$$u_n^2 + v_n^2 = 2^n = 2(u_nu_{n-1} + v_nv_{n-1}).$$

18. If x is large, prove that

$$\left(1+\frac{1}{x}\right)^{x+\frac{1}{2}} = e\left(1+\frac{1}{12x^2}\right) \text{ nearly.}$$

19. Prove that if u is a homogeneous polynomial in x and y of degree n, then

(i) $xu_x + yu_y = nu$.

(ii) $xu_{xx} + yu_{xy} = (n-1)u_x$.

(iii) $$\begin{vmatrix} u_{xx} & u_{xy} & u_x \\ u_{xy} & u_{yy} & u_y \\ u_x & u_y & 0 \end{vmatrix} + \frac{nu}{n-1}(u_{xx}u_{yy} - u_{xy}^2) = 0.$$

20. Show that the series $\dfrac{z^3}{\lfloor 3} - \dfrac{z^7}{\lfloor 7} + \dfrac{z^{11}}{\lfloor 11} - \ldots$ is convergent for all values of z; and that its sum is

$$\frac{1}{\sqrt{2}}(\cosh\theta\sin\theta - \sinh\theta\cos\theta) \text{ where } \theta = z/\sqrt{2}.$$

21. There are n different counters arranged in a row. Prove that the number of new arrangements which can be made by interchanging adjacent counters, no counter being moved more than once but any number of pairs being simultaneously moved, is $\dfrac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} - 1$, where $\alpha + \beta = 1$ and $\alpha\beta = -1$.

22. Find the cubic equation whose roots are α, β, γ, where

$$\alpha+\beta+\gamma=a, \quad \alpha^2+\beta^2+\gamma^2=b^2, \quad \text{and} \quad \alpha^3+\beta^3+\gamma^3=c^3.$$

If u_n denotes $\alpha^n+\beta^n+\gamma^n$, express u_n in terms of u_{n-1}, u_{n-2}, u_{n-3}, and a, b, c, and prove that u_n is the coefficient of x^n in the expansion in powers of x of

$$\frac{3-2ax+\frac{1}{2}(a^2-b^2)x^2}{1-ax+\frac{1}{2}(a^2-b^2)x^2-\frac{1}{6}(a^3-3ab^2+2c^3)x^3}.$$

23. If $b+d=a+c$, show that

$$\frac{1}{bd}+\frac{ac}{b(b+1)d(d+1)}+\ldots+\frac{a(a+1)\ldots(a+n-1)c(c+1)\ldots(c+n-1)}{b(b+1)\ldots(b+n)d(d+1)\ldots(d+n)}$$
$$=\frac{1}{bd-ac}\left[1-\frac{a(a+1)\ldots(a+n)\,.\,c(c+1)\ldots(c+n)}{b(b+1)\ldots(b+n)\,.\,d(d+1)\ldots(d+n)}\right].$$

24. If Δ_n denotes the determinant of n rows,

$$\begin{vmatrix} 2\cos\theta & 1 & 0 & 0 & \ldots \\ 1 & 2\cos\theta & 1 & 0 & \ldots \\ 0 & 1 & 2\cos\theta & 1 & \ldots \\ 0 & 0 & 1 & 2\cos\theta & \ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots \end{vmatrix},$$

show that $\Delta_m-2\cos\theta\Delta_{m-1}+\Delta_{m-2}=0$; hence prove that

$$\Delta_m=\sin(m+1)\theta/\sin\theta.$$

25. Prove that if a, b, c are positive integers, the chance that $a^2+b^2+c^2$ is divisible by 7 is $\frac{1}{7}$.

26. Prove that

$$\cosh x\cosh y=1+\frac{r^2\cosh 2a}{\underline{|2}}+\ldots+\frac{r^{2n}\cosh 2na}{\underline{|2n}}+\ldots,$$

where $\tanh a=y/x$ and $r^2=x^2-y^2$.

27. If $f(x)$ and $\phi(x)$ are polynomials with no common factor, $x-a$ is not a factor of either function, and

$$\frac{f(x)}{(x-a)^n\phi(x)}=\frac{A_1}{x-a}+\frac{A_2}{(x-a)^2}+\ldots+\frac{A_n}{(x-a)^n}+\frac{\psi(x)}{\phi(x)};$$

prove that $A_n=\dfrac{f(a)}{\phi(a)}$ and $A_{n-r}=\dfrac{1}{\underline{|r}}\left[\dfrac{d^r}{dx^r}\dfrac{f(x)}{\phi(x)}\right]_{x=a}$,

where, in the last expression, x is to be put equal to a after differentiation.

[Put $x=a$ in the equation

$$\frac{f(x)}{\phi(x)}=A_1(x-a)^{n-1}+A_2(x-a)^{n-2}+\ldots+A_n+\frac{\psi(x)}{\phi(x)}\cdot(x-a)^n.$$

Next, differentiate r times, and then put $x=a$.]

28. If $r^2=a^2+b^2+c^2$ and $\dfrac{b+ic}{r+a}=z$, prove that

$$\frac{c+ia}{r+b}=\frac{i(1-z)}{1+z} \quad \text{and} \quad \frac{a+ib}{r+c}=\frac{1+iz}{1-iz}.$$

[Show that $(r-a)(r+a)=(b+ic)(b-ic)$; hence, $z=\dfrac{b+ic}{r+a}=\dfrac{r-a}{b-ic}$, etc.]

29. If $\log n$, $\log\log n$, $\log\log\log n$, ... are denoted by $\lambda(n)$, $\lambda^2(n)$, $\lambda^3(n)$, ..., then, if we omit certain terms so that all the logarithms are real, the series

$$\Sigma\frac{1}{n\lambda(n)\{\lambda^2(n)\}^p}, \quad \Sigma\frac{1}{n\lambda(n)\lambda^2(n)\{\lambda^3(n)\}^p}, \ldots$$

are convergent if $p>1$ and divergent if $p\leqslant 1$.

[Using Cauchy's condensation test; a is any positive integer, the first series is convergent or divergent as Σv_n is convergent or divergent, where

$$v_n=\frac{a^n}{a^n\lambda(a^n)\{\lambda^2(a^n)\}^p}.$$

(i) *If* $p>1$, take $a>e$, so that $\log a>1$, and show that $v_n<1/\{n(\log n)^p\}$.

(ii) *If* $p\leqslant 1$, take $a=2$, so that $\log a<1$, and show that $v_n>1/\{n(\log n)^p\}$.

The second series can now be discussed in a similar way.]

30. If $x_1:y_1:z_1$, $x_2:y_2:z_2$, $x_3:y_3:z_3$ are three values of $x:y:z$ which satisfy the equations

$$x^3+y^3+z^3+kxyz=0 \quad \text{and} \quad lx+my+nz=0,$$

show that

$$x_1x_2x_3+y_1y_2y_3+z_1z_2z_3=0.$$

31. Prove that

$$\Sigma_{s=0}^{s=n-r}(C_s^{r+s}\,.\,C_{r+s}^n)=2^{n-r}C_r^n.$$

32. A bag contains six balls, each of which is known to be black or white, either colour being *a priori* equally likely. Two balls are drawn and found to be one black and one white: these are replaced and two others are drawn. Show that the chance of their being both black is 19/75.

33. Show that, if $a_1, a_2, \ldots a_m$ are distinct prime numbers other than unity, the number of solutions in integers (including unity) of the equation

$$x_1x_2x_3\ldots x_n=a_1a_2a_3\ldots a_m$$

is n^m.

Show also that the number of solutions in which at least one of the x's is unity is

$$\left\lfloor n\left\{\frac{(n-1)^m}{\lfloor(n-1)\rfloor\lfloor 1}-\frac{(n-2)^m}{\lfloor(n-2)\rfloor\lfloor 2}+\ldots+(-)^{n-2}\frac{1^m}{\lfloor 1\rfloor\lfloor(n-1)}\right\}\right\rfloor.$$

34. Expanding $\log(1-x^3)$ in power series in two different ways, prove that for any positive integer k,

$$\Sigma(-1)^{n-1}\frac{\lfloor n-1}{\lfloor k-n\rfloor\lfloor 2n-k}=-\frac{2}{k} \text{ or } \frac{1}{k},$$

according as $k=3p$ or $3p\pm1$, where p is an integer and the summation is taken for all values of n such that $\frac{1}{2}k\leqslant n\leqslant k$.

35. If n things are given arranged in a certain order, show that the number of sets of three things which can be formed out of these with the condition that no set shall contain any two things which were originally contiguous to each other is

$$\tfrac{1}{6}(n-2)(n-3)(n-4).$$

36. If $|z|=1$, the points representing $\sqrt{\dfrac{1+z}{1-z}}$ lie on one or other of two perpendicular straight lines.

37. Prove that, if x is real,

$$x+\frac{x^4}{\lfloor 4}+\frac{x^7}{\lfloor 7}+\ldots \text{ to } \infty = \frac{1}{3}e^x+\frac{2}{3}e^{-\frac{x}{2}}\sin\left(x\cdot\frac{\sqrt{3}}{2}-\frac{\pi}{6}\right).$$

38. Find values of N, if any exist, such that if

$$6375,\quad 8033,\quad 10106$$

are divided by N, the respective remainders are (i) in Arithmetical Progression, (ii) in Geometrical Progression.

39. In Ex. 38, the remainders in (ii), when $N=4493$, are 1882, 3540, 1120. Verify that these are in geometrical progression to a modulus 4493; and obtain a value of r less than 4493 such that

$$1120\equiv 3540r\equiv 1882r^2 \pmod{4493}.$$

40. Show that if $n=3$, $a+b+c$ is a factor of

$$\begin{vmatrix} a^n & b^n & c^n \\ a & b & c \\ 1 & 1 & 1 \end{vmatrix},$$

and that if $n>3$, $a+b+c$ is not a factor.

41. A pack of 52 cards is dealt in the usual way to 4 players. Find an expression for the number of ways in which exactly 6 cards of a particular suit may be dealt to a particular player, and show that in 4 out of every 35853 of these deals his partner would have the remaining 7 cards of the suit.

42. Find $\Sigma_{n=2}^{n=\infty}\dfrac{n^3x^{n-3}}{(n-1)(n+1)(n+2)}$, where $|x|<1$.

43. Prove that the most general solution in positive integers of the equation

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{z}$$

is given by

$$\left.\begin{aligned} x&=p(p+q)r\\ y&=q(p+q)r\\ z&=pqr \end{aligned}\right\}$$

where p, q, r are integers.

Deduce the general solution in integers of the equation

$$\frac{1}{x^2}+\frac{1}{y^2}=\frac{1}{z^2}.$$

44. Assuming that, if $0\leqslant u_n<1$ for every n, the infinite product $\Pi(1-u_n)$ converges or diverges to zero according as Σu_n converges or diverges, show that

(i) if $\Sigma_1^\infty a_n$ is a divergent series of positive terms and $A_n=a_1+a_2+\ldots+a_n$, then $\Sigma\dfrac{a_n}{A_n}$ is divergent;

(ii) if $\Sigma_1^\infty a_n$ is a convergent series of positive terms and

$$A_n'=a_n+a_{n+1}+a_{n+2}+\ldots,$$

then $\Sigma\dfrac{a_n}{A_n'}$ is divergent.

45. Find numbers represented by (i) $abccba$, (ii) $a'b'b'c'c'a'$, where a, b, ... are used as digits, each of which is a perfect square.

46. Prove that the series whose terms are the reciprocals of the numbers which can be expressed in the ordinary scale without using 0 as a digit is convergent.

[If t_n is the sum of the reciprocals of all the numbers with n digits (0 not occurring as a digit), show that $t_n < \frac{9}{10} t_{n-1}$.]

47. If n is a positive integer and

$$f_n(x) = x^n - 1 - n(x-1),$$
$$\phi_n(x) = x^n + 2x^{n-1} + 3x^{n-2} + \ldots + nx + n + 1,$$

prove that

(i) $f_n(x) = (x-1)^2 \phi_{n-2}(x)$, (ii) $\phi_n(x) = (x+1)^2 \phi_{\frac{1}{2}(n-2)}(x^2) + \frac{1}{2}n + 1$,

or $$\phi_n(x) = x(x+1)^2 \phi_{\frac{1}{2}(n-3)}(x^2) + \tfrac{1}{2}(n+1)x + n + 1,$$

according as n is even or odd.

Hence prove that

$$f_{12}(x) = \{x^2(x^4-1)\}^3 + 2(x^4-1)^2 + 3(x^2-1)^3 + 6(x-1)^2.$$

48. A bag contains 13 balls, of which 4 are white and 9 black. If a ball is drawn r times successively and replaced after each drawing, show that the chance that no two successive drawings shall have given white balls is

$$\frac{16 \cdot 12^r - (-3)^r}{15 \cdot 13^r}.$$

49. If $Z = \dfrac{z-\iota}{z+\iota}$, show that, when z lies above the real axis, Z will lie within the unit circle which has centre at the origin. How will Z move as z travels along the real axis from $-\infty$ to $+\infty$?

50. For all values of n, p_n and q_n are two positive numbers, such that $p_n = \frac{1}{2}(p_{n-1} + q_{n-1})$, and $p_n q_n = k^2$, where k is a positive constant. Show that, if p_0, q_0 are the first pair of such a sequence of numbers, and if $p_0 > q_0$, then $p_{n-1} > p_n > k > q_n > q_{n-1}$, and that if $p_n = k(1 + 2\lambda_n)$, then $\lambda_n < \lambda_0^{2n}$.

51. Show that the necessary and sufficient condition for the equation

$$x^n - ax + b = 0$$

to have more than one real root is

$$(n-1)^{n-1} a^n \geqslant n^n b^{n-1}.$$

(A double root is to count as two, and a and b are positive.)

52. The equations to three straight lines are $l_i x + m_i y + n_i = 0$, $(i = 1, 2, 3)$; and N_i is the cofactor of n_i in

$$\begin{vmatrix} l_1 & m_1 & n_1 \\ l_2 & m_2 & n_2 \\ l_3 & m_3 & n_3 \end{vmatrix}.$$

Prove that the necessary and sufficient condition for the origin to lie in one of the acute angles between the lines $i = 1, 2$ is that $(l_1 l_2 + m_1 m_2) n_1 n_2 < 0$; and that, for the origin to lie inside the triangle formed by the three lines, the necessary and sufficient conditions are that $n_1 N_1$, $n_2 N_2$, $n_3 N_3$ have the same sign.

53. If $$F(x) = \frac{1}{x} + \frac{\lfloor 1}{2x(x+1)} + \frac{\lfloor 2}{3x(x+1)(x+2)} + \ldots \text{ to } \infty,$$

prove that $$F(x) - F(x+1) = 1/x^2.$$

54. In the game of whist, the last card of the pack of 52 dealt by the dealer to himself is a trump. Show that the chance that he has t more trumps is

$$C_t^{12} \cdot C_{12-t}^{39} \div C_{12}^{51}.$$

Show also that the average number of trumps held by the dealer is $3\frac{14}{17}$.

55. To find solutions in integers of the equation

$$x^2 + y^2 - z^2 = 1,$$

(i) take any value of y such that $y^2 - 1 = \lambda\mu (\lambda > \mu)$, where λ, μ are both odd, or both even; then a solution is given by $x = \frac{1}{2}(\lambda - \mu)$, $z = \frac{1}{2}(\lambda + \mu)$.

(ii) Obtain in this way all the solutions when $y = 10$ and $y = 11$. Also obtain the solutions

$$\begin{aligned} &x = \tfrac{1}{2}k(k+1) - 2, \quad && y = 2k + 1, \quad && z = \tfrac{1}{2}k(k+1) + 2, \\ &x = k^2 + k - 1, && y = 2k + 1, && z = k^2 + k + 1, \\ &x = 2k^2 - 1, && y = 2k, && z = 2k^2. \end{aligned}$$

(iii) *Or*, take any value of z such that $z^2 + 1$ is the product of two or more primes of the form $4n + 1$, or twice such a product; then by using the identity

$$(a^2 + b^2)(p^2 + q^2) = (ap + bq)^2 + (aq - bp)^2,$$

$z^2 + 1$ can be expressed as the sum of two squares in at least one way other than $z^2 + 1^2$.

(iv) Find all the solutions when $z = 23$ and $z = 68$.

56. If $$c_{ij} = a_i b_j - a_j b_j, \quad i, j = 1, \ldots, 5,$$

show by consideration of the determinant

$$\begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ 0 & a_2 & a_3 & a_4 \\ 0 & b_2 & b_3 & b_4 \end{vmatrix},$$

or otherwise, that $$c_{12}c_{34} + c_{13}c_{42} + c_{14}c_{23} = 0.$$

Show further that, if neither c_{12} nor c_{34} is zero,

and $$c_{14}c_{15} + c_{24}c_{25} + c_{34}c_{35} = 0, \quad \text{and} \quad c_{13}c_{15} + c_{23}c_{25} + c_{43}c_{45} = 0,$$

then $$c_{15}^2 + c_{25}^2 + c_{35}^2 + c_{45}^2 = 0, \quad \text{and} \quad c_{12}c_{15} + c_{32}c_{35} + c_{42}c_{45} = 0.$$

57. The point (x, y) is transformed into (x', y') by the equations

$$x' = x \cos\alpha + y \sin\alpha + a, \quad y' = x \sin\alpha - y \cos\alpha + b.$$

Prove that in general there is just one finite line transformed into itself, viz. the line

$$(y - \tfrac{1}{2}b) \cos\tfrac{1}{2}\alpha = (x - \tfrac{1}{2}a) \sin\tfrac{1}{2}\alpha,$$

but that if $a \cos\frac{1}{2}\alpha + b \sin\frac{1}{2}\alpha = 0$, the transformation is a reflection in this line.

58. Prove that the result of eliminating x between

$$ax^2 + bx + c = 0 \quad \text{and} \quad x^5 + x^4 + x^3 + x^2 + x + 1 = 0$$

is $$(a^7 + b^7 + c^7 - 7abc(b^2 - ac)^2)(a + b + c)^{-1} = 0.$$

59. Show that

$$\frac{1}{x+1} + \frac{1}{x+2} + \ldots + \frac{1}{x+n} = \frac{n}{x+n} + \frac{n(n-1)}{2(x+n)(x+n-1)} + \frac{n(n-1)(n-2)}{3(x+n)(x+n-1)(x+n-2)} + \ldots \text{ to } n \text{ terms.}$$

60. (1) Show that if r is an odd integer

$$1^r+2^r+3^r+\ldots+n^r \text{ is divisible by } 1+2+3+\ldots+n.$$

(2) If $f(a)=1+x+x^2+\ldots+x^{a-1}$, prove that

$$f(a)\,.\,f(b)\,.\,\ldots \text{ is divisible by } f(p)\,.\,f(q)\,.\,f(r)\,.\,\ldots,$$

if $a, b \ldots$ is divisible by $p\,.\,q\,.\,r\,.\,\ldots$; where $a, b \ldots$ are integers and $p, q, r \ldots$ are primes; the number of factors in the product $a\,.\,b \ldots$ being not necessarily the same as that in the product $p\,.\,q\,.\,r\,.\,\ldots$.

61. Express as the product of prime factors: 1110111, 1112111, 1113111*, 1115111*, 1119111, 1001011, 1010011*, 9135683*, 9135689**, 123454321*.

[For the numbers marked * try $\sqrt{N}$ method, and for those marked ** use $\sqrt{8N}$.]

62. If $a_1, a_2, \ldots a_n$ are positive and

$$a_1+a_2+\ldots+a_n \leqslant 1,$$

prove that

$$\frac{1}{a_1}+\frac{1}{a_2}+\ldots+\frac{1}{a_n} \geqslant n^2;$$

and that if x is greater than any of the numbers $a_1, a_2, \ldots a_n$, then

$$\frac{1}{x-a_1}+\frac{1}{x-a_2}+\ldots+\frac{1}{x-a_n} \geqslant \frac{n}{x-\frac{1}{n}(a_1+a_2+\ldots+a_n)}.$$

63. Two queens are placed at random on a chess board; prove that the chance they cannot take one another is $\frac{2\,3}{3\,6}$.

64. Show that the relation independent of λ, which is satisfied by the roots of

$$az^2+bz+c+\lambda(a'z^2+b'z+c')=0,$$

is

$$\left(z_1-\frac{\beta}{\gamma}\right)\left(z_2-\frac{\beta}{\gamma}\right)=\frac{\beta^2-\gamma\alpha}{\gamma^2},$$

where z_1, z_2 are the roots, and $\alpha=bc'-b'c, \quad \beta=ca'-c'a, \quad \gamma=ab'-a'b$.

Deduce that, if a, b, c, a', b', c' are real numbers, the roots are real for all real values of λ, provided that $\beta^2-\gamma\alpha$ is negative; but that when $\beta^2-\gamma\alpha$ is positive, there are real values of λ for which the roots are imaginary, and that the points representing them in the Argand diagram lie on the circle

$$\left(x-\frac{\beta}{\gamma}\right)^2+y^2=\frac{\beta^2-\gamma\alpha}{\gamma^2}.$$

65. If the roots of $t^2-2t+2=0$ are α, β, show that

$$\frac{(x+\alpha)^n-(x+\beta)^n}{\alpha-\beta}=\frac{\sin n\phi}{\sin^n\phi} \quad \text{where} \quad \cot\phi=x+1.$$

66. Prove that if x is the nth root of a, the error involved in taking x for the $(n+q)$th root of a is

$$\frac{qx\log_e x}{n+q}\left\{1-\frac{q\log_e x}{2(n+q)}\right\} \text{ approx.},$$

where $(q\log_e x)/(n+q)$ is small.

67. If $x=\dfrac{a_1}{1+}\dfrac{a_2}{1+}\cdots\dfrac{a_n}{1+x}$ and $y=\dfrac{a_n}{1+}\cdots\dfrac{a_2}{1+}\dfrac{a_1}{1+y}$, and these fractions are assumed to be convergent, prove that

$$q_{n-1}x^2+(q_n-p_{n-1})x=p_n, \quad \text{and} \quad q_{n-1}(1+y)^2-(q_n-p_{n-1})(1+y)=p_n,$$

where p_r/q_r is the rth convergent of x.

Hence deduce that $x(1+y)=p_n/q_{n-1}$.

68. Prove that if $u_n\to L$ when $n\to\infty$, then

$$\lim_{n\to\infty}\frac{1^r u_1+2^r u_2+3^r u_3+\ldots+n^r u_n}{n^{r+1}}=\frac{L}{r+1};$$

and that, if Σu_n is a convergent series of positive decreasing terms, then

$$\lim_{n\to\infty}\frac{1^r u_1+2^r u_2+3^r u_3+\ldots+n^r u_n}{n^r}=0, \ r \text{ being positive.}$$

69. If $\sin^{-1}2=\alpha+\iota\beta$, where α, β are real, show that

$$\alpha=2n\pi+\frac{\pi}{2} \quad \text{and} \quad \beta=\log(2\pm\sqrt{3}),$$

where n is an integer.

70. Find to the nearest half-inch the length of the longest rectangular strip of carpet, one yard wide, that can be put down in a rectangular room 8 yards long and 6 yards wide.

[If the length is x yards, prove that $x^4-102x^2+192x-99=0$; show that this equation has two imaginary roots, one negative root, and one positive root between 9 and 10, and find the latter to 3 decimal places.]

71. Show that the equation whose roots are

$$\alpha+\beta, \quad \omega\alpha+\omega^4\beta, \quad \omega^2\alpha+\omega^3\beta, \quad \omega^4\alpha+\omega\beta, \quad \omega^3\alpha+\omega^2\beta,$$

where $\omega=\cos 2\pi/5+\iota\sin 2\pi/5$, is

$$x^5-5\alpha\beta x^3+5\alpha^2\beta^2 x-(\alpha^5+\beta^5)=0.$$

Deduce that the quintic,

$$a_0x^5+5a_1x^4+10a_2x^3+10a_3x^2+5a_4x+a_5=0,$$

can be completely solved if its coefficients satisfy the relations:

$$a_0^2a_3-3a_0a_1a_2+2a_1^3=0,$$

and

$$4(a_0a_2-a_1)^2=a_0^3a_4-4a_0^2a_1a_3+6a_0a_1^2a_2-3a_1^4.$$

[Remove the second term and equate coefficients.]

72. Discuss completely, when z is real or complex, the convergence of

$$\Sigma\left(\frac{nz}{n+1}\right)^n.$$

73. If $\alpha, \beta, \gamma, \ldots$ are the roots of

$$x^n-p_1x^{n-1}+p_2x^{n-2}-\ldots+(-1)^n p_n=0,$$

show that

(i) If $n=3$, $\Pi_4(\sqrt{\alpha}\pm\sqrt{\beta}\pm\sqrt{\gamma})=p_1^2-4p_2$.

(ii) If $n=4$, $\Pi_8(\sqrt{\alpha}\pm\sqrt{\beta}\pm\sqrt{\gamma}\pm\sqrt{\delta})=(p_1^2-4p_2)^2-2^8p_4$.

(iii) If $n=5$, $\Pi_{16}(\sqrt{\alpha}\pm\sqrt{\beta}\pm\sqrt{\gamma}\pm\sqrt{\delta}\pm\sqrt{\epsilon})$
$=\{(p_1^2-4p_2)^2-2^8p_4\}^2-2^{11}(p_1^2-4p_1p_2+8p_3)p_5$.

(The suffix denotes the number of factors.)

74. If a, b, c are complex numbers ($a \neq 0$, $bc \neq 1$), show that, by the transformation

$$Z = a\frac{bz+1}{z+c},$$

circles in the z plane are transformed into circles and straight lines in the w plane.

Find the condition that the interior of $|z|=1$ should be transformed into the interior of $|Z|=1$.

75. Find the chance that in a well-shuffled pack of 52 cards two kings are contiguous.

76. ABC is a triangle in which the lengths of BC, CA, AB are respectively 4, 2, 3 units. A circle is drawn with centre A and 1 unit radius. If r, r' are the distances of any point on the circle from B, C respectively, show that the values of r^2 at the points P, P' where $r+r'$ is a minimum or a maximum, and at Q, Q' where $r'-r$ or $r-r'$ have their greatest values, are the roots of

$$4x^4 - 155x^3 + 2116x^2 - 11865x + 23040 = 0.$$

Find the roots of this equation to 5 places of decimals. Also show that the corresponding values of r' are given by

$$(r')^2 = r^2(r^2-13)^2/(r^4-19^2+72)^2.$$

Draw a diagram amd mark the points P, P', Q, Q'.

77. Show that

$$\frac{1}{a+}\,\frac{1}{b+}\,\frac{1}{c+}\,\frac{1}{a+}\,\frac{1}{b+}\,\frac{1}{c+} \ \ldots \text{ to } 3n \text{ terms}$$

is equal to

$$\frac{bc+1}{abc+a+c+}\,\frac{1}{(abc+a+b+c)+}\,\frac{1}{(abc+a+b+c)+} \ \ldots \text{ to } n \text{ terms.}$$

78. By considering the auxiliary function $f(x) - \lambda g(x)$, prove that, if $g'(x)$ does not vanish,

$$\frac{f(b)-f(a)}{g(b)-g(a)} = \frac{f'(\xi)}{g'(\xi)}$$

for some value of ξ between a and b.

Also show that, for another ξ,

$$\text{(ii)} \quad \frac{f(\xi)-f(a)}{g(b)-g(\xi)} = \frac{f'(\xi)}{g'(\xi)},$$

by considering the function $[f(x)-f(a)][g(b)-g(x)]$.

79. If x_1, y_1 is the simplest solution in positive integers of the equation $x^2 - Ny^2 = 1$, where N is an integer which is not a perfect square, and if x_r, y_r is the solution obtained in the usual manner by raising $x_1 + y_1\sqrt{N}$ to the rth power, show that

$$x_{np+q}\, y_{np-p+q} - y_{np+q}\, x_{np-p+q}$$

is independent of the value of n; p, q and n being integers.

80. Show that $\Sigma n r^{n^2}$ and $\Sigma n^2 r^{n^2}$ are convergent if $0 < r < 1$.

81. Show that if

$$f_0(x) = 1 + \frac{x^3}{3!} + \frac{x^6}{6!} + \dots,$$

$$f_1(x) = x + \frac{x^4}{4!} + \frac{x^7}{7!} + \dots,$$

$$f_2(x) = \frac{x^2}{2!} + \frac{x^5}{5!} + \frac{x^8}{8!} + \dots,$$

then $$f_0(x+y) = f_0(x)f_0(y) + f_1(x)f_2(y) + f_2(x)f_1(y).$$

82. Find in determinant form the discriminant of the equation

$$ax^4 + 4bx^3 + 6cx^2 + 4dx + e = 0,$$

and express the double root (when there is one) as a rational function of the coefficients.

83. If $x + iy = \tan \frac{1}{2}(u + iv)$, show that

$$x^2 + y^2 = 1 - 2x \cot u = -1 + 2y \coth v;$$

and that u is the angle between the lines joining the point (x, y) to the points $(0, \pm 1)$.

84. From a bag containing n balls, each equally likely to be white or black, a ball is drawn which turns out to be white; this is replaced and another ball is drawn which also turns out to be white. If the second ball is replaced and another ball is drawn, prove that the chance that this is a black ball is

$$\tfrac{1}{2}(n-1)/(2n+1).$$

85. (1) Sum to infinity the series whose nth term is $\dfrac{n^2 - n - 4}{(n+1)^2(n+2)^2}$.

(2) Show that the limiting value of

$$\frac{1}{2^{2n}(2^2-1)} + \frac{1}{3^{2n}(3^2-1)} + \dots + \frac{1}{n^{2n}(n^2-1)},$$

when n is infinite, is zero; and that the series

$$\sum_{q=1}^{q=n} \sum_{p=2}^{p=n} \frac{1}{p^{2q}}$$ is convergent and equal to $\frac{3}{4}$ when n is infinite.

86. Find all the solutions of $x^3 + 1 \equiv 0 \pmod{p}$ when p is a prime of the form $3b^2 + 1$.

87. If $\alpha_1, \alpha_2, \dots \alpha_n$ are the roots of $x^n + nax - b = 0$, show that

$$(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \dots (\alpha_1 - \alpha_n) = n(\alpha_1^{n-1} + a).$$

Form the equation whose roots are $\alpha_1^{n-1}, \alpha_2^{n-1}, \dots \alpha_n^{n-1}$, and show that the product of the squared differences of the roots of the first equation is

$$(-1)^{\frac{1}{2}(n^2-n+2)} n^n \{(n-1)^{n-1}a^n + b^{n-1}\}.$$

88. If

$$u_n = 1 - \frac{n(n-1)}{\lfloor 2} + \frac{n(n-1)(n-2)(n-3)}{\lfloor 4} - \dots,$$

$$v_n = n - \frac{n(n-1)(n-2)}{\lfloor 3} + \frac{n(n-1)(n-2)(n-3)(n-4)}{\lfloor 5} - \dots,$$

where n is a positive integer, show that

$$u_n = u_{n-1} + v_{n-1}, \quad v_n = u_{n-1} - v_{n-1} \quad \text{and} \quad u_n = 1 + v_1 + v_2 + \dots + v_{n-1}.$$

89. If n is a positive integer,

$$1-\frac{n^2}{n+1}+\frac{n^2(n^2-1)}{(n+1)(n+2)}-\frac{n^2(n^2-1)(n^2-2)}{(n+1)(n+2)(n+3)}$$
$$+\frac{n^2(n^2-1)(n^2-2)(n^2-3)}{(n+1)(n+2)(n+3)(n+4)}-\ldots=\frac{1}{n+1}.$$

90. If $F=\dfrac{a_1}{b_1+}\dfrac{a_2}{b_2+}\dfrac{a_3}{b_3+}\ldots$ and $F_n\equiv\dfrac{p_n}{q_n}$ is the nth convergent, then

$$(F-F_{n-1})q_{n-1}\frac{\partial F}{\partial a_n}=(F-F_{n-2})q_{n-2}\frac{\partial F}{\partial b_n}.$$

91. In the sequence

$$\frac{1}{1},\ \frac{1}{2},\ \frac{1}{3},\ \frac{2}{3},\ \ldots,\ \frac{1}{m},\ \frac{2}{m},\ \frac{3}{m},\ \ldots,\ \frac{m-1}{m},\ \ldots,$$

prove that the nth fraction is a/b, where b is the greatest integer in

$$\tfrac{3}{2}+\tfrac{1}{2}\sqrt{8n-15},\quad \text{where } n>1,$$

and $a=n-\frac{1}{2}b^2+\frac{3}{2}b-2$.

92. If z, z' are complex, show that

$$|\tfrac{1}{2}(z+z')|>|\sqrt{zz'}|,$$

provided that the origin lies inside the rectangular hyperbola whose foci are represented by z, z'.

93. Prove that

$$\frac{1}{1-}\,\frac{1}{3-}\,\frac{4}{5-}\ldots\frac{n^2}{2n+1}=1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n+1}.$$

94. Show, without using the trigonometrical or the exponential functions, that if y_1 and y_2 are functions of x, such that

$$y_1''=-y_1,\quad y_1(0)=0,\quad y_1'(0)=1,$$
$$y_2''=-y_2,\quad y_2(0)=1,\quad y_2'(0)=0,$$

then $y_1'=y_2,\quad y_2'=-y_1,\quad$ and $\quad y_1^2+y_2^2=1,$

and $$y_1(a+b)=y_1(a)y_2(b)+y_2(a)y_1(b).$$

95. If

$$x=\frac{1}{a+}\,\frac{1}{b+}\,\frac{1}{c+}\,\frac{1}{a+}\,\frac{1}{b+}\,\frac{1}{c+}\ldots,$$
$$y=\frac{1}{c+}\,\frac{1}{b+}\,\frac{1}{a+}\,\frac{1}{c+}\,\frac{1}{b+}\,\frac{1}{a+}\ldots,$$

show that

$$xy=\frac{q}{(p^2+2q)-}\,\frac{q^2}{(p^2+2q)-}\,\frac{q^2}{(p^2+2q)-}\ldots,$$

where $p=abc+a+c-b,\quad q=(ab+1)(bc+1)$. [See Ex. 77.]

96. Show that there are no two square numbers of which the sum and difference are both squares.

[If $x^2+y^2=p^2$ and $x^2-y^2=q^2$, prove that x, p, q are odd, $y=2mn$, and $x^2=(m^2)^2+(2n^2)^2$: hence $x=r^2+s^2$, $m^2=r^2-s^2$, $n^2=rs$, and r, s, $r+s$, $r-s$, are all squares, with $r+s<x^2+y^2$: and so on indefinitely.]

97. Deduce from Ex. 96, or use a similar method to prove, the following theorems enunciated by Fermat.

(i) The sum or difference of two fourth powers cannot be either a square or twice a square, trivial cases excepted.

(ii) No triangular number, $\frac{1}{2}n(n+1)$, except unity, is a fourth power.

(iii) The area of a primitive triangle, i.e. one whose sides can be expressed by rational numbers, cannot be expressed as the square of a rational number.

98. Prove that, if n is a positive integer,

$$\lfloor n = \Pi_{\nu=1}^{\infty}\left(1+\frac{1}{\nu}\right)^n \Big/ \Pi_{\nu=1}^{\infty}\left(1+\frac{n}{\nu}\right).$$

[Use $\lfloor n / \lfloor r-1 = r(r+1)\ldots(r+n-1)/(n+1)(n+2)\ldots(n+r-1)$.]

99. A person, A, subscribed to a football pool. In all there were 50,000 subscribers at 1s. each; and the whole proceeds were to be divided equally (after deducting 15 per cent.) among those subscribers who correctly forecast three games resulting in draws from amongst 54 games to be played on a certain Saturday. A found from the Sunday newspaper that he had succeeded in selecting three draws; and that 15 matches had resulted in draws.

What is A's expectation after seeing the paper?

100. Show that $$\frac{F(x+h)+F(x-h)-2F(x)}{h^2} = F''(x+\theta h),$$

where θ is some number between -1 and 1.

101. If x, y, z are positive integers such that

$$x^3+xy+y^2=z^2,$$

show that $x/(p^2-q^2)=y/(2pq+q^2)=z/(p^2+pq+q^2)$, where p, q are positive integers and $p>q$.

If p is prime to q, show that

$$p^2-q^2, \quad 2pq+q^2 \quad \text{and} \quad p^2+pq+q^2$$

have no common factor except 3 and that 3 is a common factor only when $p \equiv q \pmod 3$.

102. In an equation $x^n+ax^{n-1}+bx^{n-2}+\ldots+k=0$ all the coefficients except a are fixed. How many values of a will in general cause the equation to have equal roots?

103. Considering only real functions, prove from first principles that, k being a fixed positive integer,

(i) If $f(n)\to a$, then $\{f(n)\}^k \to a^k$.

(ii) If $\{f(n)\}^k \to b\,(>0)$, then $f(n)\to b^{1/k}$.

Hence show that, provided $a>0$, (i) is true for all positive rational values of k.

104. Show that $$\frac{1}{1+}\,\frac{1}{3+}\,\frac{1}{5+}\cdots = \frac{e^2-1}{e^2+1}.$$

Hence find the fraction with denominator less than 200 which is nearest to $(e^2-1)/(e^2+1)$ or $\tanh 1$.

105. Find eight solutions in positive integers of the equation

$$2x^2-6xy+3y^2-4x+8y+17=0.$$

Find also the general solution in integers of $x^2=97y+22$.

106. If $f(x)$ is positive for all positive values of x, and continually decreases as x increases, show that

$$\tfrac{1}{2}f(1)+\int_1^n f(x)\,dx<\Sigma_1^n f(x)<f(1)+\int_1^n fx\,dx.$$

Deduce an approximation to the sum of the first million terms of the series

$$\text{(i) } 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\ldots, \quad \text{(ii) } 1+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\frac{1}{\sqrt{4}}+\ldots.$$

107. $x_1, x_2, \ldots, x_n$; $\alpha_1, \alpha_2, \ldots, \alpha_n$ are two systems of positive numbers with the same sum. Show that, the α's being individually fixed and the x's variable,

$$\frac{x_1^p}{\alpha_1^{p-1}}+\frac{x_2^p}{\alpha_2^{p-1}}+\ldots+\frac{x_n^p}{\alpha_n^{p-1}},$$

where p (not necessarily integral) is greater than 1, is least when

$$x_1=\alpha_1, \quad x_2=\alpha_2, \ldots, \quad x_n=\alpha_n,$$

so that

$$\frac{x_1^p}{\alpha_1^{p-1}}+\frac{x_2^p}{\alpha_2^{p-1}}+\ldots+\frac{x_n^p}{\alpha_n^{p-1}}\geqslant\alpha_1+\alpha_2+\ldots+\alpha_n.$$

Deduce that, if $a_1, a_2, \ldots, a_n$ are any positive numbers whatsoever, then

$$\frac{a_1^p}{\alpha_1^{p-1}}+\frac{a_2^p}{\alpha_2^{p-1}}+\ldots+\frac{a_n^p}{\alpha_n^{p-1}}\geqslant\frac{(a_1+a_2+\ldots+a_n)^p}{(\alpha_1+\alpha_2+\ldots+\alpha_n)^{p-1}}.$$

By taking $a_n=A_nB_n$, show that with a suitable choice of α_n the above gives

$$\Sigma A_nB_n\leqslant(\Sigma A_n{}^p)^{\frac{1}{p}}(\Sigma B_n{}^q)^{\frac{1}{q}},$$

where q is determined by the relation

$$\frac{1}{p}+\frac{1}{q}=1.$$

108. Prove that $\sin\pi/14$ is a root of

$$8y^3-4y^2-4y+1=0,$$

and express the other roots as trigonometrical functions.

109. Prove that if n is a positive integer, the solution of

$$x+\tfrac{1}{2}(x+y-1)(x+y-2)=n$$

in positive integral values of x, y is possible in one and only one way.

110. Prove by considerations connected with limits of indetermination that, if $-1<\lambda<1$ and $a_{n+1}+\lambda a_n\to a$ as $n\to\infty$, then $a_n\to a/(1+\lambda)$.

Prove also that if $\lambda=-1$, $a_n\to\infty$, and if $\lambda=1$, a_n may tend to $\frac{1}{2}a$ or oscillate.

111. If 2, 3, 5, ..., p, ..., are all the prime numbers in ascending order and $f(n)$ denotes $1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}$, prove that

$$f(p)<\left\{\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\ldots\left(1-\frac{1}{p}\right)\right\}^{-1},$$

and show that the infinite series $\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{p}+\ldots$ is divergent.

Prove that the sum of the reciprocals of all numbers which have no *repeated* prime factor is divergent, but that the sum of the reciprocals of all numbers which have no *unrepeated* prime factor is convergent.

112. If $(a+ib)^{c+id}$ is real, and principal values only are considered,

$$(a+ib)^{c+id} = \sqrt[2]{(a^2+b^2)^{c}e^{-d\alpha}},$$

113. Show that the congruence $x^p \equiv a \pmod{2^n}$, where a is odd, has exactly one solution if p is an odd prime. Find the number of solutions when $p=2$.

114. Show that the number 7 is a quadratic non-residue of all primes of the forms $28k \pm 5$, $28k \pm 11$, $28k \pm 13$, and a quadratic residue of all other primes.

115. If an event happens at random on an average once in time a, the chance of its not happening in a given period b is $e^{-\frac{b}{a}}$.

116. Two men, A and B, play a game, and the winner plays C; then the winner of the second game plays the remaining player; and so on. Any player is considered to have won when he has beaten the other two. If in each game it is an even chance which player wins, show that C's chance of winning is $\frac{2}{7}$.

117. Players P_1, P_2, P_3, ... P_m, of equal skill, play a game consecutively in pairs as P_1P_2, P_2P_3, P_3P_4, ... $P_{m-1}P_m$, P_mP_1, ..., and any player who wins two consecutive games wins the match. Prove that

(i) the chance that the match is won at the rth game is $\frac{r-1}{2^r}$.

(ii) If p_r is the chance that P_r wins the match, then

$$p_r = \left\{\frac{m}{(2^m-1)^2} - \frac{r-1}{2^m-1}\right\} \cdot 2^{m-r},$$

also $$p_{r+1} = p_r - \tfrac{1}{2}p_{r-1} \quad \text{if} \quad r < m,$$

and $$p_1 = p_m - \tfrac{1}{2}p_{m-1}.$$

(iii) Verify that $p_1+p_2+p_3+\ldots+p_m=1$, and show that when $m=3, 4, 5,$ the values of $p_1, p_2, p_3 \ldots$ are as below.

m	p_1,	p_2,	p_3,	p_4,	p_5
3	12,	20,	17	—	$\div 7^2$
4	32,	76,	68,	49	$\div 15^2$
5	80,	288,	268,	196,	$129 \div 31^2$

118. If $u_n = 6u_{n-1} - 4u_{n-2}$, and $u_0=3$, $u_1=14$, find u_n.
Also show that the integral part of $(3+\sqrt{5})^n+1$ is divisible by 2^n.

119. Prove that $\frac{n}{m} + \frac{n-1}{m-1} + \ldots + \frac{1}{m-n+1} < \frac{n(n+1)}{2m-n+1}$, and deduce that, if m and n are positive integers, $m > n$,

$$C_n^m > \left[\frac{2m-n+1}{n+1}\right]^n.$$

120. Two vessels, A and B, are of equal capacity. A is full of water, B half-full of wine. B is filled up from A, and then A from B, the contents being well stirred each time. This double operation is performed n times. Prove that the proportion of water to wine in A is then

$$2+(\tfrac{1}{4})^n \text{ to } 1-(\tfrac{1}{4})^n.$$

121. Prove that the rationalized equivalent of the equation

$$(\beta-\gamma)\sqrt{(x-\alpha)(y-\alpha)} + (\gamma-\alpha)\sqrt{(x-\beta)(y-\beta)} + (\alpha-\beta)\sqrt{(x-\gamma)(y-\gamma)} = 0$$

is $(\beta-\gamma)^2(\gamma-\alpha)^2(\alpha-\beta)^2(x-y)^2=0$.

ANSWERS

EXERCISE I

PAGE

4. 5. $(z-1)/(z-2)=3(Z-1)/(Z-2)$.

EXERCISE III

36. 1. $a=-1$, $b=-2$, $A=4$, $B=3$, $A'=3$, $B'=-2$.

EXERCISE IV

55. 1. (i) $1-\sqrt{2}<x<1+\sqrt{2}$; (ii) $-\frac{1}{2}<x<\frac{1}{2}$; (iii) $-1<x<1$.
2. $1/(1-x)(1-y)$.

56. 6. $|x|<1$, $|x+y|<1$; sum $=(1-x-y)^{-1}$.
9. (iv) 0·10516.

EXERCISE VIII

101. 7. (1, 1), (2, 4), (ω, ω^2), (ω^2, ω).

8. $x=1-\frac{1}{5}(\sqrt{6}+1)(1-\iota\sqrt{3})$, $y=1+\dfrac{\sqrt{2}}{5}(\sqrt{6}+1)(\iota+\sqrt{3})$,

$x=1+\frac{1}{5}(\sqrt{6}-1)(1-\iota\sqrt{3})$, $y=1+\dfrac{\sqrt{2}}{5}(\sqrt{6}-1)(\iota+\sqrt{3})$,

and two other solutions by writing $-\iota$ for ι.

102. 14. $(\pm1, \mp1, \pm2)$, $(\pm\frac{1}{3}, \pm\frac{2}{3}, \mp\frac{2}{3})$. 16. $(-1, 1)$, $(-1, 3)$, $(\frac{8}{3}, \frac{8}{3})$.
17. (1, 2). 18. $(-\frac{10}{9}, -\frac{10}{9}, -\frac{10}{9})$, $(2, -\frac{1}{3}, -5)$, $(-\frac{1}{3}, -5, 2)$, $(-5, 2, -\frac{1}{3})$.

EXERCISE IX

117. 1. (i) 1/6; (ii) 7/9. 2. (i) 1/4; (ii) 2/3. 3. 1/2.
4. 216/19. 5. 3/11. 6. 108/109.

118. 10. 13.

EXERCISE X

135. 2. (50, 7), (48, 7), (15, 4). 3. (261, 25); 218/125.
5. (i) (2, 1), (50, 31); (ii) (3, 2), (29, 18); (iii) (5, 2), (12, 5).
6. (25, 1), (623, 25); (7775, 312); $(25+21)/18$ gives one period.
8. (i) $x=\frac{1}{2}(a^2-a+2)$, $y=\frac{1}{2}(a-1)$; (ii) $x=\frac{1}{2}(a^2+a+2)$, $y=\frac{1}{2}(a+1)$.

EXERCISE XI

PAGE

151. 1. $\pm 20, \pm 31, \pm 16$. 2. $\pm 38, \pm 25, \pm 42$.
3. $\pm 28, \pm 57, \pm 47, \pm 71, \pm 38$. 4. $\pm 19, \pm 30, \pm 27, \pm 52, \pm 77$.
5. $\pm 20, \pm 91, \pm 37$. 6. $\pm 71, \pm 66, \pm 83$.
7. $\pm 889, \pm 623, \pm 569, \pm 631$. 8. $\pm 2641, \pm 1973, \pm 245, \pm 4917$.

152. 9. ± 23. 10. $\pm 7, \pm 15$. 11. $\pm 14, \pm 41$.
12. $\pm 17, \pm 37$. 13. $\pm 73, \pm 101$.
14. $\pm 41, \pm 151, \pm 201, \pm 311$. 15. $\pm 32, \pm 45, \pm 241, \pm 318$.
17. $8+73t, \ -9+73t$. 18. $3+71t, \ -16+71t$.
19. $4+85t, \ -13+85t, \ -16+85t, \ -13+85t$.
20. $x=29t+2, \ y=174t^2+23t+1$; $x=29t+3, \ y=174t^2+35t+2$.
21. $x=31t-3, \ y=217t^2-53t+3$; $x=31t+9, \ y=217t^2+115t+15$.
22. $\pm 120, \pm 130$. 23. $\pm 7, \pm 8$.
30. $x=13t\pm 6, \ y=13t^2\pm 12t+1$; (6, 1), (7, 2), (19, 26), (20, 29).
31. $x=23t\pm 6, \ y=23t^2\pm 12t+1$; (6, 1), (17, 12), (29, 36), (40, 69).
32. $x=97t\pm 33, \ y=97t^2\pm 66t+11$; (33, 11), (64, 42), (130, 174), (161, 267).
33. $x=3u, \ y=3v-5$; (12, 1), (30, 37), (33, 46).
34. $x=7u, \ y=7v-3$; (14, 4), (28, 32), (35, 53).
36. $143k^2\pm 54k+5, \ 143k^2\pm 76k+10$; (27, 5), (38, 10), (105, 77), (116, 94).
37. $x=153k\pm 25, \ y=153k^2\pm 50k+4$;
$x=153k\pm 43, \ y=153k^2\pm 86k+12$.
38. $x=79t\pm 27, \ y=79t^2\pm 40t+9$. 39. $x=83t\pm 20, \ y=83t^2\pm 40t+5$.

EXERCISE XII

166. 1. (i) (17, 11), (23, 7); (ii) (5, 13), (17, 7);
(iii) (17, 19), (35, 1); (iv) (43, 1), (37, 7).
3. (19, 4), (59, 16), (851, 236), (2971, 824).
4. (i) (377, 70); (ii) (387, 59). 5. (1, 1), (13, 5).
6. (7, 1), (35, 13). 7. (15, 2), (78, 29). 8. (7, 1), (31, 7).
9. (20, 3), (1177, 270). 10. (7, 1), (119, 21).
11. (8, 1), (17, 4). 12. (27, 5), (699, 149).

167. 15. (i) (2, 3), (1, 2); (ii) (10, 4), (5, 1);
(iii) (3, 36), (4, 13), (5, 7), (8, 1); (iv) (5, 3);
(v) (3, 2), (4, 2); (vi) (5, 2), (5, 1);
(vii) (2, 9), (2, 1); (viii) (1, 3).
16. (i) (5, 10), (84, 219); (ii) (9, 2), (72, 12).

EXERCISE XIII

172. 2. (i) 6, 8, 23; (ii) 49. 3. 10, 16, 18, 37.
4. (i) 7; (ii) 4, 6, 9; (iii) 2, 10, 19; (iv) $\pm 21, \pm 23$. 5. 2, 34.

EXERCISE XIV

PAGE

185. 2. (v) $X=2x^6+x^5+4x^4-x^3+4x^2+x+2$, $Y=x^5+x^3+x$.

3. $X=2x^9+x^7+5x^6+7x^5+4x^4+7x^3+5x^2+x+2$.
$Y=x^7+x^6+x^5+2x^4+x^3+x^2+x$.

EXERCISE XV

195. 1. 17^2+16^2.

2. (i) $3161=56^2+5^2=44^2+35^2=29\,.\,109$;
(ii) $6109=78^2+5^2=75^2+22^2=41\,.\,149$;
(iii) $28013=163^2+38^2=157^2+58^2=109\,.\,257$.

3. (8, 11), (12, 17). 9. 51^2+20^2, $43^2+2\,.\,24^2$, $63^2-2\,.\,22^2$, $2\,.\,85^2-107^2$.

11. $23^2+18^2+15^2+5^2$. 12. $91^2+41^2+6^2+3^2$.

13. $81^2+42^2+41^2+1^2$.

14. (27, 5, 4), (25, 12, 1), (25, 9, 8), (24, 13, 5), (23, 15, 4), (17, 16, 15), (20, 17, 9), (20, 19, 3).

16. $23\,.\,89$. 18. $5\,.\,397\,.\,2113$.

20. Residues, 3, -22, -31, 41; factors, 61, 491. 22. 59, 509.

EXERCISE XVI

211. 3. (i) Converges; (ii) oscillates; (iii) converges; (iv) converges when a, b, c, d are positive.

MISCELLANEOUS

262. 22. $x^3-ax^2+\frac{1}{2}(a^2-b^2)x-\frac{1}{6}(a^3-3ab^2+2c^3)=0$.
$u_n-au_{n-1}+\frac{1}{2}(a^2-b^2)u_{n-2}-\frac{1}{6}(a^3-3ab^2+2c^3)u_{n-3}=0$.

264. 38. (i) 83 or 415; (ii) 23. 39. 508.

42. $(1-x)^{-1}-\left[\frac{1}{6x}+\frac{1}{2x^2}-\frac{8}{3x^4}\right]\log(1-x)+\frac{31}{36x}+\frac{5}{6x^2}+\frac{8}{3x^3}$,

43. u^4-v^4, $2uv(u^2+v^2)$, $2uv(u^2-v^2)$.

45. (i) 698896; (ii) 511225.

265. 49. Round circumference of unit circle.

266. 55. (ii) $x=49, 15, 1$; $y=50, 18, 1$: $x=29, 13, 7, 1$; $y=31, 17, 13, 11$.
(iv) $x=23, 19$; $y=1, 13$: $x=68, 65, 64, 55$; $y=1, 20, 23, 40$.

267. 61. $3\,.\,37\,.\,73\,.\,137$; $7\,.\,11^2\,.\,13\,.\,101$; $3^2\,.\,337\,.\,367$; $1051\,.\,1061$; $3\,.\,7^2\,.\,23\,.\,331$; $11\,.\,17\,.\,53\,.\,101$; $31^2\,.\,1051$; $2003\,.\,4561$; $2027\,.\,4507$; $41^2\,.\,271^2$.

268. 70. 9 yds. 2 in. (9·056).

72. $0<z<1$, convergent; $-1<z<0$, convergent; $z=1$, divergent; $z=-1$, oscillates.
$|z|>1$, divergent; $|z|<1$, absolutely convergent.
$|z|=1$, convergent but not absolutely convergent.

PAGE

269. 74. $|a|=1$, $|b|=|c|$, $|ab|>1$.

75. $\frac{1201}{5525}$.

76. 6·76032, 4·51605, 13·55035, 13·92318.

270. 82.
$$\begin{vmatrix} ac-b^2 & ad-bc & ae-bd \\ ad-bc & ae-c^2 & be-cd \\ ae-bd & be-cd & ce-d^2 \end{vmatrix}=0.$$

The double root is given by $(2HI-3aJ)(ax+b)+GI=0$.

85. (i) 0. 86. $3b^2$, $1+\frac{3}{2}b(b\pm1)$, mod $(3b^2+1)$.

272. 99. 46s. 4d. 102. n. 104. $\frac{115}{151}$.

105. (6, 5), (11, 5), (9, 11), (26, 11), (34, 51), (121, 51), (334, 151), (46, 151).

273. 106. $14\frac{1}{2}$; 2000, roughly.

274. 113. See p. 143.

118. $u_n=\frac{1}{2}(3+\sqrt{5})^n+\frac{1}{2}(3-\sqrt{5})^n$; the integral part of $(3+\sqrt{5})^n+1=2u_n$.

INDEX

The numbers refer to pages.

Printed in Great Britain by
Lowe and Brydone (Printers) Limited, London, N.W.10