"The Classical Problems --
from Archimedes to Galois"

by

Evelyn Vivian Mills

M.A. Thesis, Univ. of Manitoba

1995

Bibliography

Monographs on Modern Mathematics -- edited by J. W. A. Young

Mathematical Essays and Recreations -- Hermann Schubert

Klein's Famous Problems of Elementary Geometry -- Felix Klein

Greek Mathematics. Vol. 1 -- T. L. Heath

History of Greek Mathematics -- J. Gow

What is Mathematics -- Courrant and Robbins

Modern Algebra -- Birkhoff and MacLane

On Squaring the Circle -- Hobson

A Budget of Paradoxes -- Augustus De Morgan

Elementary Theory of Equations -- L. E. Dickson

Galois and the Theory of Groups -- Lillian R. Lieber

Mathematical Recreations and Essays -- W. W. R. Ball

The Elements of Euclid -- I. Todhunter

History of Mathematics -- F. Cojori

Men of Mathematics -- Bell

Introduction to Theory of Equations -- L. E. Dickson

Theory and Application of Finite Groups -- Miller, Blichfeldt and Dickson

Index

A. Historical

1. Squaring of the Circle

(a) Calculating value of

Rhina Papyrus

Anagaxorus

Sophists -- Antiphon and Bryson

Hippocrates

Archimedes

Ptolemy

Oriental mathematicians

(b) Constructions

Archimedes

Dinostratus -- quadratrix

Kochansky

(c) Post Renaissance

Wallis

Newton

Gregory

Machin

Chinese and Japanese

2. Duplication of the Cube

Origin of Problem

Hippocrates -- two mean proportionals

Archytas

Eudoxus

Menaechmus -- Conics

Plato

Eratosthenes

Nicomedes

Apollonius

3. Trisection of an Angle

Earliest Solution -- Author unknown

Nicomedes -- conchoid

Quadratrix of Hippias

Archimedes

Conics employed

Descartes

Modern attempt

4. To Describe Regular Polygons

Figures of 3, 4, 6, 8, 12, and multiples of these

Figure of 17 sides and equations belonging thereto

Pentagon

Impossibility of describing regular heptagon -- Gauss

5. Solution of Equations by radicals

Rhind Papyrus and other very early work

Hindus -- negative and irrational roots

Arabians

Scipio Ferro -- Cubic

Tartaglia -- Cardau -- cubic

Lodovico Ferrari -- biquadratic

Gauss -- A root for every algebraic equation

Descartes -- rule of signs

Horner -- solution of a fifth degree equation

B. Modern Approach

1. Galois Theory

Domain

Substitution

Abstract group

Symmetric group

Cyclic group

Subgroup

Alternating group

Transposition

Transform

Invariant subgroup

Group of an equation

Galois function

Galois resolvent

Properties of Group "A" and "B"

Quotient Group

Solvable groups

Sufficient and necessary conditions for solvability of an equation

Jordan's theorem

Fifth degree equations not in general solvable

Solution of a certain fifth degree equation

2. Inscription of Regular Polygons

Criterion of constructibility

Quadratic solved by means of ruler and compasses

Equation $x^{2^k+1} - 1 = 0$ has constructible roots

Figure with 2^l sides constructible

Galois theory applied

3. Trisection of an Angle

Impossible for the angle 120°

Group theory applied

4. Duplication of the Cube

$x^3 - 2 = 0$ irreducible in rational field

Indirect proof of impossibility of constructibility

Galois theory applied

5. Irrationality of π

If e^x irrational, then π cannot be rational

Transcendental numbers exist

Constructibility and analytic statement

Transcendence of e

Transcendence of π

Impossibility of squaring the circle

Part A

In attempting a summary of the work done on the Classical Problems (i.e. Squaring the Circle, Duplication of the Cube, Trisection of the Angle, Construction of Regular Polygons and the Solving of Equations of degree higher than the fourth -- and especially the solving of fifth degree equations) I am going to trace out an historical account of the attempts toward solution of each problem, leaving to the latter part the proofs of the impossibility of each. We shall see a number of most instructive examples of great things arising out of impossibility, since from these "unsuccessful" attempts, extending over more than two thousand years, have, within the last one hundred and fifty years, come some of the central and most characteristic developments of modern mathematics. A study of these efforts brings us then, at the end and in certain fields, to the threshold of mathematics in the present century. It is also of interest for the surprising relations which it reveals between apparently unrelated questions.

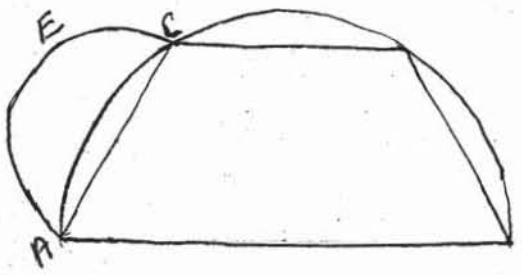
The first problem I shall approach is the squaring of the circle. In modern notation this problem may be described as the attempt to find an exact value for π in the formula for the area of a circle of radius r, $A = \pi r^2$. There are here two distinct problems. Firstly there is the practical problem of finding the value of π with sufficient accuracy to satisfy the technological needs of the time. This the Greeks had certainly done by the time of Archimedes or even before; his value of 3 1/7 being accurate to 4 parts in 10,000 still suffices for all but very refined measurements, and he is reported to have obtained considerably better values than this. Secondly there is the theor-

etical problem of constructing a line of length π times a given line using straight edge and compass alone. We shall be concerned chiefly with the history of this theoretical problem, which though apparently simple, has occupied the efforts of many great men until it was finally shown to be impossible about sixty three years ago; and it has occupied the efforts of many lesser men both before and after it was shown to be impossible.

The earliest recorded value of π is found in the Rhind Papyrus (in the British Museum) copied about 1700 B.C. by the Egyptian Scribe Ahmes. The Egyptians being so highly practical probably obtained their value for the relation between the diameter and area of a circle by trial, and it is amazingly accurate: the area of the circle is equal to the area of the square whose side is the diameter diminished by 1/9 i.e. $A = \left(\frac{8}{9} d\right)^2$. This would give for π the value $\frac{256}{81} = 3.1604$ (in place of the exact value 3.14159.....) a tremendous improvement on the Babylonian, also on the Hebraic value of 3. (See 1 Kings Vll, 23) used in Solomon's building of the Temple. This reference "ten cubits from one brim to the other: it was round all about,..... and a line of thirty cubits did compass it about" reminds us that squaring the circle, that is, finding the side of a square whose area is equal to that of the given circle, and the rectification of the circle, which is the laying off of a line equal in length to the circumference, being given the radius, are one and the same problem, both depending on the ratio which later came to be called π.

Anaxagoras (born about 500 B.C.) is the earliest name we have in connection with this problem, and he did not offer any solution. He was trying to find an <u>exact</u> relation between the

radius and the area. The Sophists Antiphon and Bryson and their contemporary Hippocrates have left the results of their efforts. Antiphon introduced the "Method of Exhaustion" by which a square or an equilateral triangle is inscribed in a circle, then a figure with twice as many sides, continuing the process until the polygon and circle differed by as little as one pleased. Antiphon was really the only ancient who considered the circle to be a polygon of an infinite number of sides, though Bryson's work differed little except that he introduced circumscribed as well as inscribed polygons, and finally took the mean of the two values. The area of squares equal to the outer and inner polygons could be found, as also could the area of their mean. Simplicius and Eudemus pointed out that the circle and the polygon cannot be equal, if the principle that magnitudes are divisible without limit is true. Hippocrates (about 430 B.C. a Pythagorean) attempted the squaring of the circle by means of lunulae or menisci, which depends on the proposition Euclid Xll (2) that the areas of two circles are to each other as the squares on their diameters. I have shown the diagram but have not included his reasoning here as Hippocrates himself did not claim to have been successful in the problem. His work on lunes is memorable however because the earliest specimens in existence of reasoned geometric proofs are contained therein.



Amongst all the varies subjects that Archimedes (287 - 212 B.C.) studied, quadrature and cubature were his chief hobbies, and the process he favored most was by Exhaustion. He obtained

the result that $3\ 1/7 < \pi < 3\ 10/71$ by a lengthy proof. (See Appendix 1) He is credited with a still more accurate measurement, 3.141596, the account of which has been lost, but the first one must have pleased Archimedes himself, as, according to Heath, he was more interested in a value which could be used in daily life than in one of theoretical interest only. Archimedes' methods were used for a thousand years to calculate π to ever increasing places of decimals.

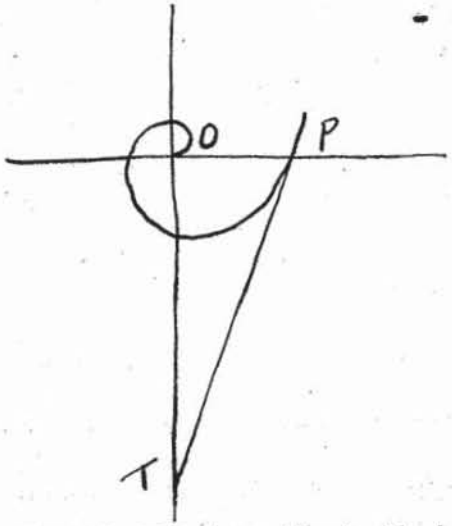
Ptolemy (of Alexandria, around 139 B.C.) from the relation of chords of a circle calculated the value $3^{\circ}\ 8'\ 30''$ which is 3.1416, as is easily verified. This is the mean between the Archimedean values of 3 1/7 and 3 10/71.

Oriental mathematicians also worked on this problem. Their most noteworthy results are the following. The Hindu, Aryabhatta (500 A.D.) obtained the value 3.1416, while Brahmagupta nearly a century later gave π as $\sqrt{10}$ which was the most commonly used value in Mediaeval times. Bhâskara with the correct relation $a_{2n} = \sqrt{2 - \sqrt{4 - a_n^2}}$ between sides of an n-sided and a 2n-sided inscribed polygon arrived at 3.1416. The Chinese astronomer Tsu Ch'ungchih (born 430 A.D.) found the values 22/7 and 355/113. The Chinese are represented again in the work of a later period.

It is interesting to note that the great Leonardo de Vinci attempted this problem, but arrived nowhere with it.

Besides calculating the value of π, the ancients tried to demonstrate that constructions could be given which would accomplish the squaring of the circle. The first noteworthy one is Archimedes' spiral which has the equation $\rho = a\theta$.

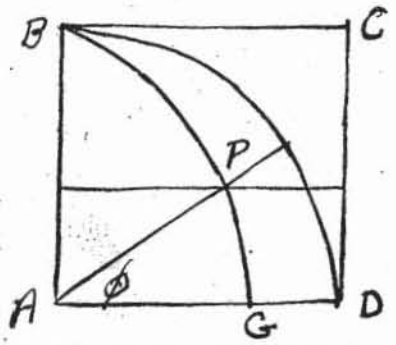
From O, a line is drawn perpendicular



to the radius vector after one complete turn and this perpendicular meets the tangent drawn from P. Then OT will be the circumference of the circle with radius OP, but I can not find full details of what Archimedes offered as proof, though Gow indicates that it is linked up with his method of Exhaustion. Heath gives the following: Assuming OT = $\frac{\rho^2}{a}$ (Proved by Archimedes!) and having the equation $\rho = a\theta$, it can be seen that after one complete revolution $\rho = 2\pi a = OP$

$$\therefore OT = \frac{\rho^2}{a} = \rho \cdot \frac{\rho}{a} = \rho \cdot \frac{2\pi a}{a} = 2\pi\rho = 2\pi \cdot OP$$

Dinostratus applied the quadratrix (invented by Hippias of Elis about 430 B.C. who may also have used it in this problem) to the quadrature of the circle. The quadratrix is described



thus: given a square, ABCD, suppose that a radius of the circle moves uniformly about A from AB to the position AD and that in the same time the line BC moves uniformly parallel to itself from the position BC to the position AD. The intersection of these two moving lines will determine a point and the locus of this point is the quadratrix. The application of the quadratrix to the rectification of the circle presents a difficulty, recognized by the ancients, in that it requires us to know the position of G, the point where the quadratrix intersects AD. (In the final position, both lines, radius and line parallel to BC co-incide and so cannot actually intersect).

Let AD be the X axis and AB the Y axis

For the point P, the ordinate y is proportional to the angle ϕ,

and when $y = 1, \phi = \frac{\pi}{2} \quad \therefore \phi = \frac{\pi}{2} y$

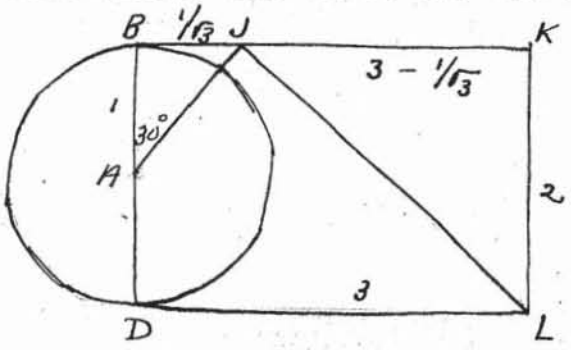
but $\phi = \tan^{-1} \frac{y}{x} \quad \therefore \frac{y}{x} = \tan \frac{\pi}{2} y$

$\therefore x = \frac{y}{\tan \frac{\pi}{2} y}$ which meets the X axis at $x = \lim_{y \to 0} \frac{y}{\tan \frac{\pi}{2} y} =$

$$\lim_{y \to 0} \frac{y}{\frac{\pi}{2} y + \frac{(\frac{\pi}{2} y)^3}{3} + \ldots} = \frac{2}{\pi}$$

When $\frac{2}{\pi}$ is known, π can easily be found. Now, each of these ingenious constructions may be said to rectify the circle. However it is the classical problem of constructing a line of length π with straight edge and compass alone, that we are considering, (and will eventually show to be impossible), so that neither of the above, nor the helix which is supposed to have been used by Apollonius, are acceptable solutions, since they require more elaborate mechanical devices for their construction.

I find the simple, though admittedly only approximate solutions below quite interesting. The first one was given by Kochansky in 1685



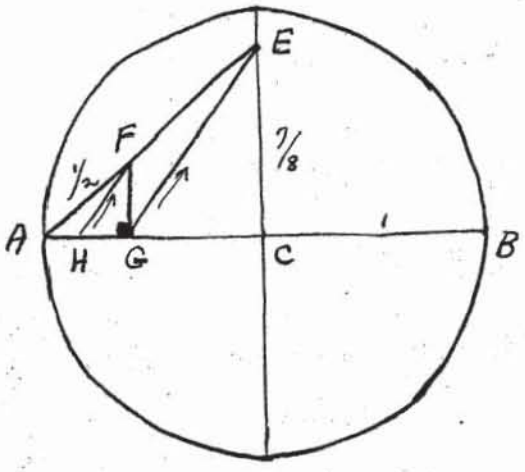
A circle of radius 1, having DL and BK tangents of length 3 is drawn. The angle BAJ is constructed to be 30° and JL is joined.

Then $JL = \sqrt{\left(3 - \frac{1}{\sqrt{3}}\right)^2 + 4} = \sqrt{\frac{40}{3} - \sqrt{12}} = 3.141533$

Then the square is readily constructed having area practically the same as the circle.

Another, invented by Grunert uses $\pi = 355/113 = 3 + \frac{4^2}{7^2 + 8^2} =$

3.14159292.... in place of 3.14159265.....



Let circle have radius 1, and refer to diagram.

$AE = \sqrt{1 + \frac{49}{64}} = \sqrt{\frac{113}{8}}$

$\frac{AG}{1} = \frac{\frac{1}{2}}{\sqrt{\frac{113}{8}}} \quad \therefore \quad AG = \frac{4}{\sqrt{113}}$

$\frac{AH}{AG} = \frac{\frac{1}{2}}{\sqrt{\frac{113}{8}}} \quad \therefore \quad \frac{AH}{\frac{4}{\sqrt{113}}} = \frac{\frac{1}{2}}{\sqrt{\frac{113}{8}}}$

$\therefore AH = \frac{16}{113}$

$\therefore 3 + AH$ gives $3 + \frac{16}{113} = \frac{355}{113}$, the semi-circumference.

Amazing advances followed the attacks of the great mathematicians of the eighteenth century on this, and related problems. John Wallis (1716-1703) had effected the quadrature of curves whose ordinates are any integral powers of $(1 - x^2)$ i.e. $y = (1 - x^2)^n$ where n is integral. Following this by the study of $y = (1 - x^2)^0$ and $y = (1 - x^2)$, he attempted to find $y = (1 - x^2)^{\frac{1}{2}}$ by interpolation, which brought this device into prominence. Consideration of the difficulties that Wallis met led Newton to the discovery of the Binomial Theorem. Another new development came about in the invention of the theory of continued fractions due to Lord Brouncker's studies of Wallis' work. Lord Brouncker obtained the first infinite series for the area between an equilateral hyperbola and its asymptotes, and Nicolaus Mercator arrived at the logarithmic series. But the most startling result of the study of quadrature was Newton's invention of the method of

fluxions (the calculus) and also to the foundation of the theory of limits. And it was through his detailed study of the quadrature of curves that Leibnitz became acquainted with higher mathematics.

After the invention of calculus all methods of determining π depended on Analysis. Gregory (who was the first to try to prove the problem impossible) used the series $a = t - \frac{t^3}{3r^2} + \frac{t^5}{5r^4} - \cdots$ where a = length of arc, t = length of tangent and r = radius of circle. This is now written in the form

$\tan^{-1} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \cdots\cdots\cdots (-1 \leq x \leq 1)$.

During the next hundred years many series and relations were discovered by which π could be evaluated to ever increasing numbers of places. Many used Machin's formula $\frac{\pi}{4} = 4 \tan^{-1}\frac{1}{5} - \tan^{-1}\frac{1}{239}$ (I do not find how Machin came upon this -- probably by trial -- at least it is easily verified). By expanding this series π was found to 100, and later to 707 places of decimals -- the latter achievement by W. Shanks in 1874. "One can ascribe this feat to a sportsmanlike interest in making a record, since no application could ever require such accuracy." says Klein in his Elementary Mathematics from an advanced Viewpoint.

Remarkable work along this line was accomplished by both Chinese and Japanese scientists but their methods were likely inspired by the teachings of the European missionary Pierre Jartoux. In Europe more and more students were becoming convinced that π was not the root of any algebraic equation. Neither was any practical purpose served by evaluating π to hundreds of places. The fact that, using 10 decimal places, the circum-

ference of the Earth can be computed to within a fraction of an inch illustrates the futility of seeking still closer approximations to its value.

The problem of squaring the circle, or of finding a rational value for π had not been done and mathematicians turned their whole attention to attempting to prove the non-algebraic nature of π. On the other hand many men without training still kept presenting solutions, as is evidenced in the pages and pages De Morgan in his "A Bundle of Paradoxes" devotes to defending himself from attacks for not accepting their work. Even yet, the attempt goes on. I came across a book in the Library (University of Manitoba) entitled "The Circle squared beyond Refutation" by Carl Theodore Heisel -- acknowledging Carl Theodore Faber -- first edition 1931. This author "published several thousand of these books at considerable expense to himself and distributed them <u>free</u> to libraries, colleges and scientists throughout the United States and Foreign Countries, to promulgate the new truth and to leave the world better off because he lived." He does not claim to be a renouned mathematician but offers as credentials that he is a <u>successful</u> businessman (and a 33° Mason) and publishes his picture to support his statements (this last inference is clearly made). Quoting further we find "Although the Royal Society of England, over a hundred years ago, declared that the circle could not be squared, thousands of students and scholars all over the world are continually studying and figuring to find the true and exact ratio between the diameter and the circumference of the circle, which they know from the very nature of things, must exist, or they would not devote their time to the study."

The value for π which Heisel offers is 3 13/81, derived from the diameter being in ratio 9:8 to the side of the square of equal area. He admits that this value was stated in the Rhind papyrus, but claims to have found it independently before the discovery of the Papyrus. I could find no proof in his book other than the bald statement of fact, and certain measurements of lines on diagrams. I tested only one of these and it was not exact. The book consists largely of the reviling of professional mathematicians "who hesitate to acknowledge anything new.....for fear of losing their positions."

The problem of the Duplication of the Cube is one of the most ancient of all. It seems to have originated almost immediately after the discovery that a square, double the size of a given one, can be described, using the diagonal as a side. No doubt, the priest of the Oracle at Delos who ordered an Altar built twice the size of the existing one, well knew what he was saying and that the pestilence from which the people sought deliverance would have time to run itself out before the completion of the Altar -- though Plato, whose help they asked, interpreted the task set by the god as proof that he wished to shame the Greeks for their neglect of geometry.

For a time the problem was attacked as one in solid geometry -- but Hippocrates observed that the problem was identical with that of finding two mean proportionals between two given numbers. Let a be the side of the original cube, then find two mean proportionals x and y between a and 2a.

i.e. $a : x = x : y = y : 2a$

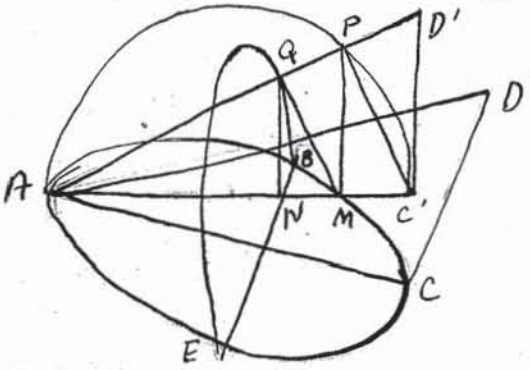
$$ay = x^2 \quad \therefore \quad y = \frac{x^2}{a}$$

$$\text{also } 2ax = y^2$$

$$\therefore 2ax = \frac{x^4}{a^2} \qquad \therefore 2a^3 = x^3$$

and x is the required length. After this the problem was always considered as one in plane geometry. It should be noted here that this seems to have been the introduction of the method of geometrical reduction and the "reductio ad absurdum" procedure.

The one worth while attempt in three dimensions is that of Archytas (428 - 347 B.C.). It is to determine the intersection of the three surfaces of revolution -- the right cone, the cylinder, and the anchor ring; having its inner diameter nil.



Let AC and AB be the two lengths between which we wish to find the two mean proportionals. Draw a semicircle AC but in a plane perpendicular to the circle ABC and let this semicircle revolve about an axis through A (thus generating the tore with inner diameter zero). Then construct a right cylinder on the circle ABC as base, which will cut the tore in some curve. Finally let CD, the tangent to the circle at C meet AB produced at D and let the triangle ADC revolve about AC as axis, generating the surface of a right cone and the point B describing a semicircle BQE in a plane perpendicular to ABC, and with its diameter BE at right angles to AC. The surface of the cone will cut across the curve of the intersection of cylinder and tore in some point

P, in which position AC′ cuts the circle ABC at M; and AM is the side of the required cube, when AC = 2AB.

Since both semicircles EQB and APC′ are perpendicular to the plane, their line of intersection QN will be perpendicular to BE.

$\therefore QN^2 = BN.NE = AN.NM$

$\therefore \angle AQM = 90^\circ$

$\therefore MQ \parallel PC$

$\therefore$ C A : AP = AP : AM = AM : AQ

i.e. AC : AP = AP : AM = AM : AB

or AB, AM, AP, AC are in continued proportion

In analytical geometry, using A as origin and AC as X axis

(1) $x^2+y^2+z^2 = \frac{a^2}{b^2}x^2$ (cone)

(2) $x^2+y^2 = ax$ (cylinder)

(3) $x^2+y^2+z^2 = a\sqrt{x^2+y^2}$ (tore)

where AC = a, and AB = b

From (1) and (2) $x^2+y^2+z^2 = \frac{(x^2+y^2)^2}{b^2}$ and combining this with (3)

$$\frac{a}{\sqrt{x^2+y^2+z^2}} = \frac{\sqrt{x^2+y^2+z^2}}{\sqrt{x^2+y^2}} = \frac{\sqrt{x^2+y^2}}{b}$$

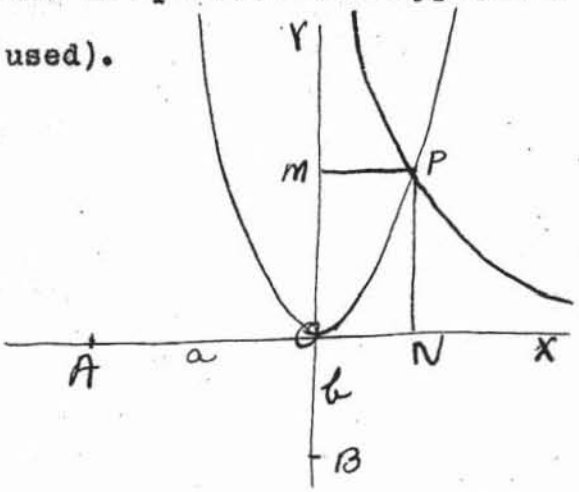
or AC : AP = AP : AM = AM : AB.

Eudoxus, a pupil of Archytas, apparently claimed to have solved the problem but there are no trustworthy records of any original contribution to this problem on his part. It seems that he used Archytas method, only projecting the curves onto the plane, obtaining the curve known as the Kampyle of Eudoxus.

Menaechmus' solution appeals to me as the most interesting one of all, in its simplicity and in the fact that it led to the discovery of conics, the theory of which soon raised geometry to the greatest height which it was to reach during ancient times. (Heath credits Menaechmus rather than Euclid with the dictum "There is no royal road to geometry.")

Using the proportion a : x = x : y = y : b, he observes that $x^2 = ay$, $y^2 = bx$ and $xy = ab$. The intersection of any two of these will give the value of x corresponding to any given value of a and b. In giving the detail of the solution, I shall

use the parabola and hyperbola (though two parabolae could be used).



Construct a parabola with b as latus rectum and OY as principal axis, so that its equation is $x^2 = by$ and the hyperbola such that the rectangle formed by the perpendiculars drawn to the asymptotes has an area ab i.e. $xy = ab$. The point of intersection P gives PN and PM, the required means for

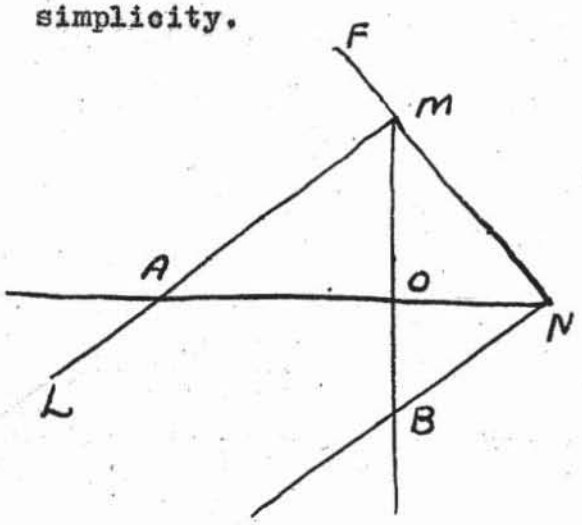
$$AO : PN = PN : PM = PM : OB$$

$$\therefore \frac{AO}{PN} = \frac{PM}{OB} \text{ which is } xy = ab$$

and $\frac{PN}{PM} = \frac{PM}{OB}$ which is $x^2 = by$

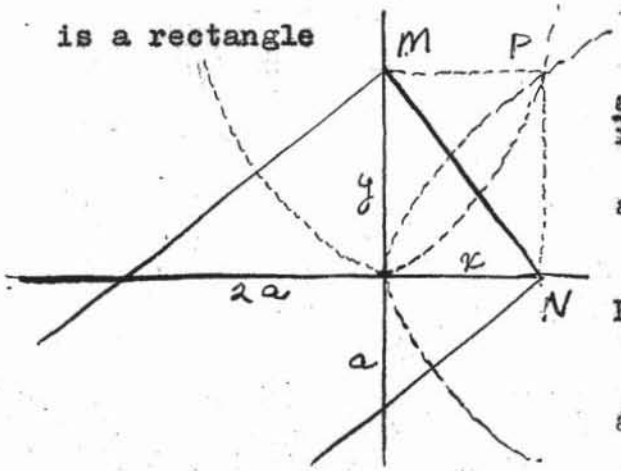
If $a = 1$, and $b = 2$, then a cube with side PN will have double the volume of one with side OB.

A purely mechanical device is sometimes ascribed to Plato (429 - 348 B.C.) though there is doubt concerning this as Plato definitely scorned mechanical solutions. If his, some suggest that he wished to ridicule the inventors of such, by its extreme simplicity.



OA is twice OB and is placed perpendicular to OB. FNB is a rigid wooden angle of 90° and ML is a sliding bar always remaining parallel to BN. The arm BN is placed passing through B and with

the right angle on OA produced. Then ML is slid along until both the right angle FMA has its vertex on OB produced and ML passes through A. This would no doubt require many trials, the position of BN being adjusted each time. Finally ON and OM are the two mean proportionals between OB and OA, which is easily seen from the three similar triangles of the figure. One recognizes from the analytical statement that this is essentially the intersection of two parabolae (Menaechmus' method) since OMPN is a rectangle



$\frac{a}{x} = \frac{x}{y}$ $\therefore x^2 = ay$

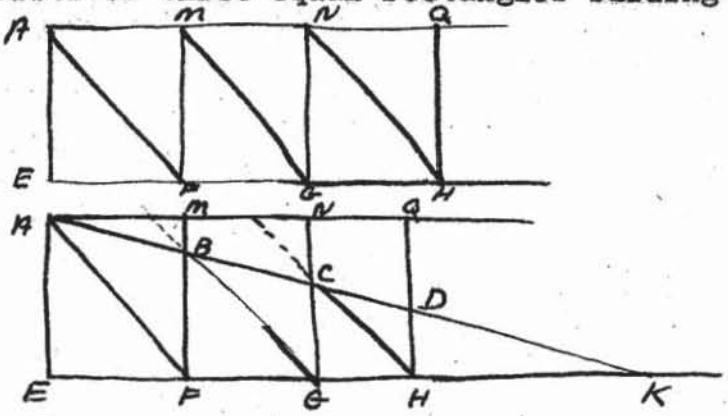
also $\frac{x}{y} = \frac{y}{2a}$ $\therefore y^2 = 2ax$

Hence $\frac{x^4}{a^2} = 2ax$

and $x^3 = 2a^3$

where x is one co-ordinate of the point of intersection of the two curves.

More readily done is Eratosthenes'(275-194? B.C.) solution. It consists of three equal rectangles sliding along a common base EH.



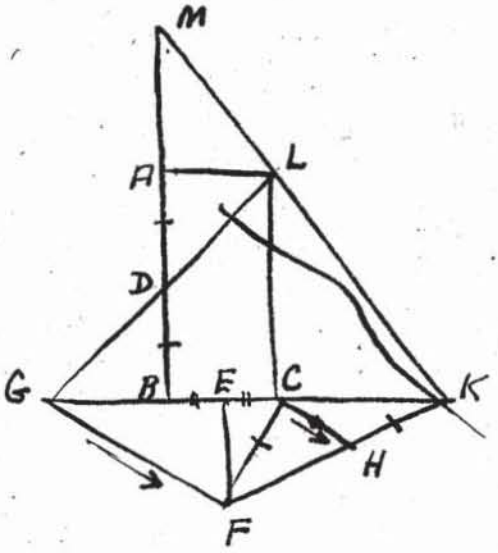
Let AE and DH be the given lengths between which it is required to find the two mean proportionals. Slide one rectangle under the other until the straight line joining A and D passes through

the intersections of MF and NG with the diagonals. Let it meet EH produced in K. Triangles DHK, CGK, BFK and AEK are similar; also the triangles CHK, BGK and AFK.

$$\therefore \frac{DH}{CG} = \frac{HK}{GK} = \frac{CK}{BK} = \frac{CG}{BF} = \frac{GK}{FK} = \frac{BK}{AK} = \frac{BF}{AE}$$

$$\therefore \frac{DH}{CG} = \frac{CG}{BF} = \frac{BF}{AE}$$ and CG is the side of the cube which will have double the volume of one with side DH. No wonder Eratosthenes was pleased with his "mesolabium" or "mean finder", even though it did not usher in any new curves to add to the sum of geometric knowledge.

Nicomedes (about 150 B.C.) however, derided Eratosthenes' effort as being impracticable(!) as well as ungeometrical. His own, by means of the Conchoid is as follows:



BC and AB are the two given lengths. Complete the rectangle and bisect AB at D and BC at E. Join LD and produce to G on CB produced. Draw EF perpendicular to BC and of such a length that FC = AD. Join FG. Draw CH parallel to FG, having it of such a length that HK = AD where FHK is a straight line. Join KL and produce to M on BA produced.

Proof: $EK = BK - BE$

$$\therefore EK^2 = BK^2 - 2BE.BK + BE^2$$
$$= BK\,(BK - 2BE) + BE^2$$
$$= BK\,(CK) + BE^2$$
$$\therefore EK^2 = BK.CK + CE^2 \text{ (BC bisected at E)}$$

$$\therefore EK^2 + EF^2 = BK.CK + CE^2 + EF^2$$

$$\therefore FK^2 = BK.CK + CF^2 \quad \ldots\ldots\ldots(1)$$

and using $MD = MA + AD$ we get

$$MD^2 = BM.MA + DA^2 \quad \ldots\ldots\ldots(2)$$

From the similar triangles MAL and LCK

$$\frac{MA}{LC} = \frac{AL}{CK}$$

$$\therefore \frac{MA}{AB} = \frac{BC}{CK}$$

$$\therefore \frac{MA}{\frac{1}{2}AB} = \frac{2BC}{CK}$$

$$\therefore \frac{MA}{AD} = \frac{GC}{CK} \quad (GB = AL = BC)$$

$$\therefore \frac{MA}{AD} = \frac{FH}{HK}$$

and $$\frac{MA}{AD} + 1 = \frac{FH}{HK} + 1$$

$$\therefore \frac{MD}{AD} = \frac{FK}{HK}$$

and $$\frac{MD}{AD} = \frac{FK}{AD}$$

$$\therefore MD = FK$$

From (1) and (2)

$$BM.MA + DA^2 = BK.CK + CF^2$$

$$\therefore BM.MA = BK.CK \text{ (since } DA = CF$$

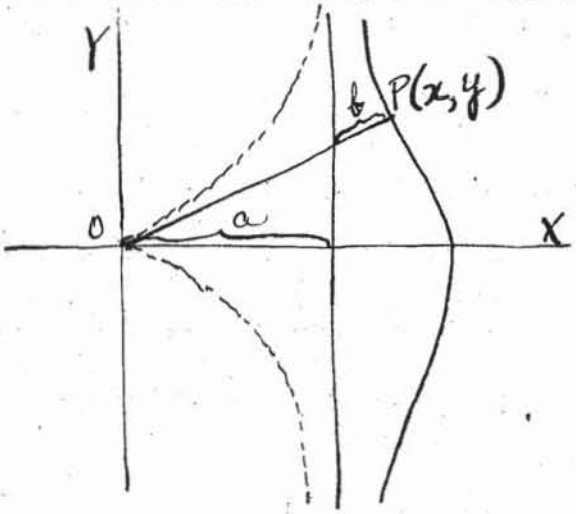
$$\therefore \frac{CK}{MA} = \frac{BM}{BK}$$

$$= \frac{LC}{CK} = \frac{MA}{AL}$$

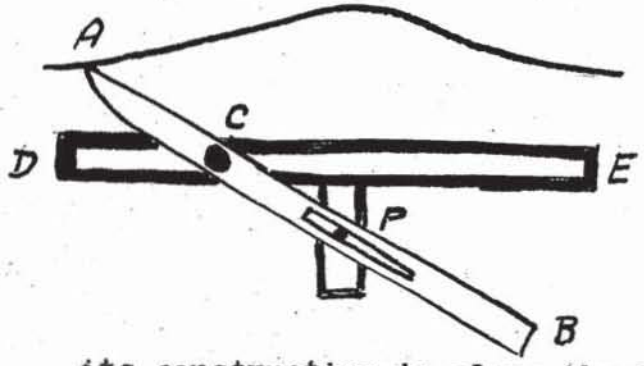
i.e. $$\frac{LC}{CK} = \frac{CK}{MA} = \frac{MA}{AL} \quad \text{or} \quad \frac{AB}{CK} = \frac{CK}{MA} = \frac{MA}{BC}$$

and if AB is twice BC, then MA is the side of a cube having the volume $2(BC)^3$. Nicomedes was able to find the point K in the

diagram by means of the Conchoid which he defined as a curve such that the straight line joining any point on it with a given point is cut by a given straight line so that the segment between the curve and the given straight line is of given length.

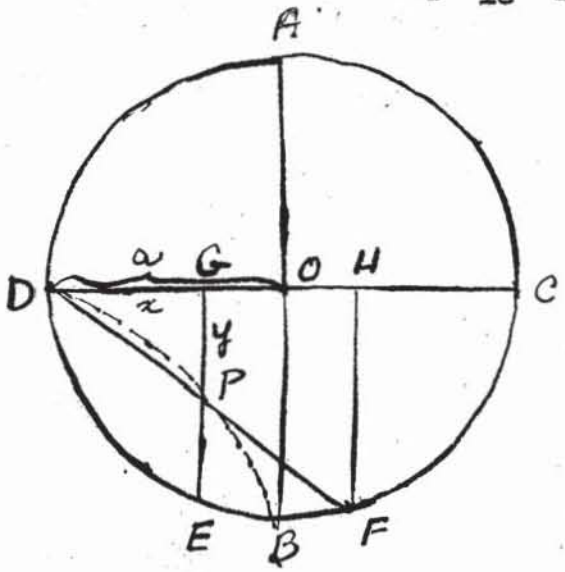


In cartesians (where O is the given point, a - the given distance from given point to given straight line, and b - the given length) we have $\frac{r}{x} = \frac{b}{x - a}$ (from similar triangles), whence $r^2(x - a)^2 = b^2x^2$ and $(x^2 + y^2)(x - a)^2 - b^2x^2 = 0$. The curve is shown by the dotted line when b is negative. Its polar equation is $r = b + a \sec \theta$. Nicomedes invented an instrument for drawing the curve to accompany his solution. The arm AB can move horizontally along DE, the pivot C keeping the distance AC constant, the point P being the pole.



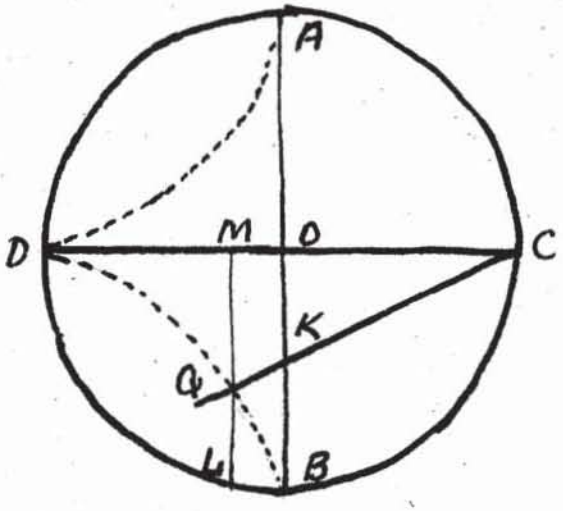
Another solution was presented by Apollonius (247 - 222 B.C.) but its construction is along the lines of this last one, though it leads to the equations of the conic as in Menaechmus work.

Diocles (also about 150 B.C.) must also be mentioned. His construction first required the invention of the Cissoid.



AB and CD are diameters of the circle perpendicular to each other and G and H are points equidistant from the centre. GE and HF are perpendiculars to DC. Join FD and the cissoid is the locus of points of intersection of DF and GE for all positions of G (and of H). In the cissoid EG = FH and DG = HC so that $\frac{CG}{GE} = \frac{DH}{HF}$ and $\frac{CG}{GE} = \frac{GE}{DG}$ (from the semicircle DEG); also $\frac{DG}{GP} = \frac{DH}{HF}$ (from similar triangles)

$\therefore \frac{CE}{GE} = \frac{GE}{DG} = \frac{DG}{GP}$ and the cissoid gives two mean proportionals between GP and CG.



K is taken on OB so that $\frac{OK}{OC} = \frac{b}{a}$ (here $\frac{1}{2}$). Join CK and produce it to cut the cissoid in Q. Through Q draw the ordinate LM.

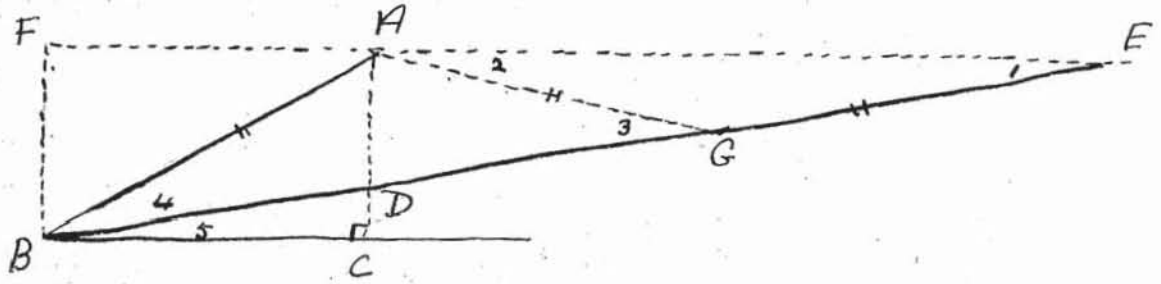
Then $\frac{OK}{OC} = \frac{MQ}{MC} = \frac{1}{2}$ (from triangles KOC and MQC), and $\frac{MQ}{MD} = \frac{MD}{LM} = \frac{LM}{CM}$ by the properties of the cissoid and DM is the side of the cube which shall have twice the volume of the one with the side MQ. The cartesian equation of the cissoid, using D as origin and DC as axis of X is obtained from $\frac{GP}{DG} = \frac{DG}{GE} = \frac{GE}{CG}$

$\therefore \frac{y}{x} = \frac{x}{\sqrt{x(2a - x)}} = \frac{\sqrt{x(2a - x)}}{2a - x}$ where DC = 2a

$\therefore y(2a - x) = x\sqrt{x(2a - x)}$ and by squaring $y^2(2a - x) = x^3$.

In all these "solutions", it must be noted that in no case has the problem been solved -- and these Greek scholars knew it had not. In Eratosthenes' work, and in the one attributed to Plato, it is frankly admitted that one must resort to trial which is highly ungeometric. There is Plato's criticism that "the good of geometry is set aside and destroyed for we again reduce it to the world of sense, instead of elevating and imbuing it with the eternal and incorporeal images of thought, even as it is employed by God, for which reason He always is God." In other "solutions", use is made of curves that can not be constructed by means of compasses and straight edge. Actually, the drawing of the conchoid, cissoid, and conics is essentially done by trial so that for all the tremendous efforts and ingeniousness of the ancients, the accomplishment was as far away as ever. Yet in the very failure, much was added to the store of mathematical knowledge that would have been delayed many centuries, had a satisfactory solution been obtained.

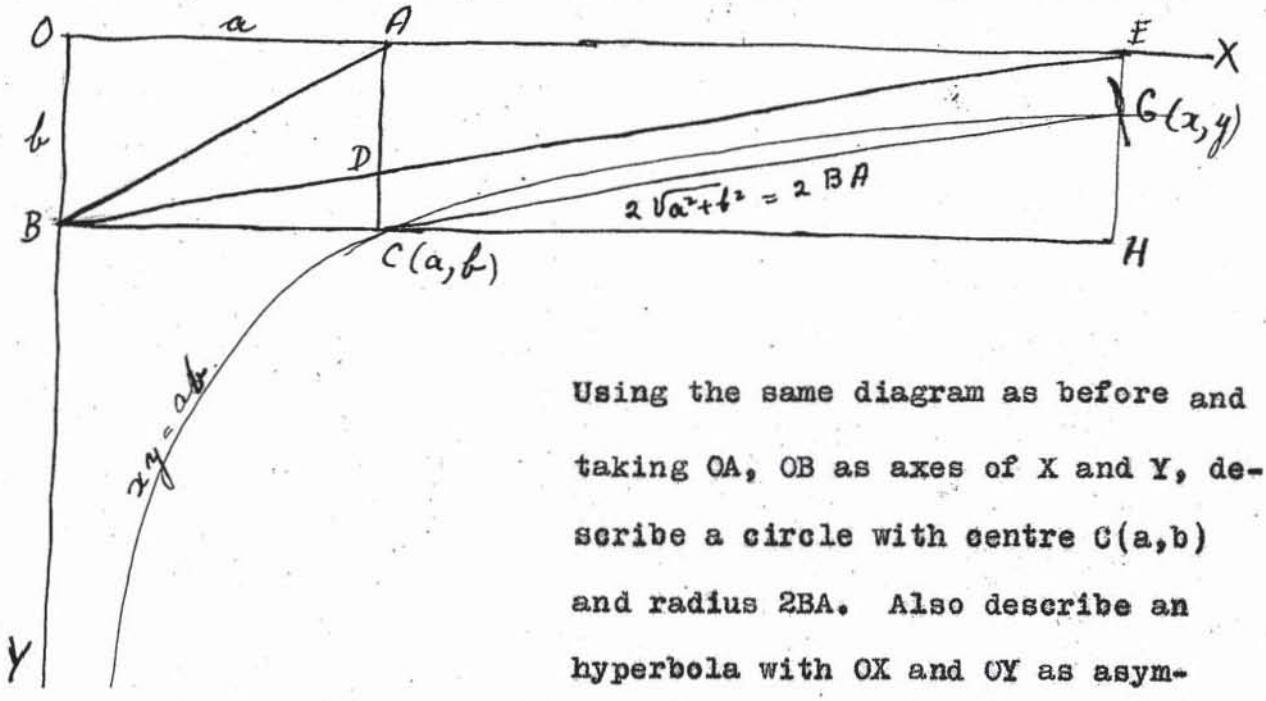
Attention was probably focused on the problem of trisecting an angle, in the course of attempting to construct a regular polygon of nine sides (which will be considered later). One of the earliest solutions, whose author is unknown is as follows:



Let ABC be the given angle to be trisected. Complete the rectangle ACBF and produce FA to such a point E that when BE is joined, DE

will be twice BA in length. Join AG where G is mid point of DE and it is seen that AG will also equal BA since ADE is a right angled triangle. Then $\angle 1 = \angle 2$, and $\angle 3 = 2(\angle 1)$

$\therefore \angle 4 = 2(\angle 1)$ $\therefore \angle 4 = 2(\angle 5)$ since $\angle 1 = \angle 5$ (exterior-interior) $\therefore$ the angle ABC is three times the angle DBC. Of course, the difficulty here is to be able to find the point E, a difficulty which can only be overcome with the help of conics.



Using the same diagram as before and taking OA, OB as axes of X and Y, describe a circle with centre C(a,b) and radius 2BA. Also describe an hyperbola with OX and OY as asymptotes i.e. the hyperbola $xy = ab$. Draw EG perpendicular to OX and join BE and this line trisects the angle. It is necessary to prove that DE = CG = 2BA and then the proof of trisection given above, applies. Since $xy = ab$, then $\frac{x}{a} = \frac{y}{b}$ $\therefore \frac{x}{x-a} = \frac{b}{b-y}$

or $\frac{BH}{CH} = \frac{EH}{GH}$ in the triangle BEH.

$\therefore$ CG is parallel to BE and DCGE is a parallelogram

$\therefore$ DE = CG

Analytically, the above solution is expressed thus. The hyperbola $xy = ab$ and the circle $(x-a)^2 + (y-b)^2 = 4(a^2+b^2)$

intersect. The equation of the circle may be expressed

$(x + a)(x - 3a) = (y + b)(3b - y)$ or $\frac{3b - y}{x - 3a} = \frac{x + a}{y + b}$

and $\frac{x + a}{y + b} = \frac{a}{y}$ since $\frac{x}{b} = \frac{a}{y}$ from $xy = ab$

$\therefore \frac{3b - y}{x - 3a} = \frac{a}{y}$ $\therefore y(3b - y) = a(x - 3a)$

$\therefore y(3b - y) = a(\frac{ab}{y} - 3a)$ (since $xy = ab$)

$\therefore a^2(b - 3y) = y^2(3b - y)$

i.e. $y^3 - 3by^2 - 3a^2y + a^2b = 0$

Now $\tan ABC = \frac{b}{a}$; and let $\tan DBC = \frac{DC}{a} = \frac{y}{a}$ and let $\frac{y}{a} = t$.

Then $y = at$ and we have $a^3t^3 - 3a^2bt^2 - 3a^3t + a^2b = 0$

or $at^3 - 3bt^2 - 3at + b = 0$ which factors into

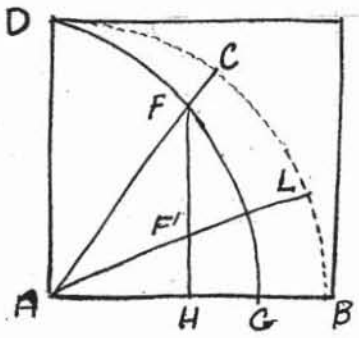
$a(t^3 - 3t) + b(1 - 3t^2) = 0$ or $b(1 - 3t^2) = a(3t - t^3)$

$\therefore \frac{b}{a} = \frac{3t - t^3}{1 - 3t^2} = \tan ABC$

$\therefore t = \tan(1/3\ ABC)$ from the trigonometric relation for multiple angles, so that the trisection of the angle is the same thing as solving a cubic equation.

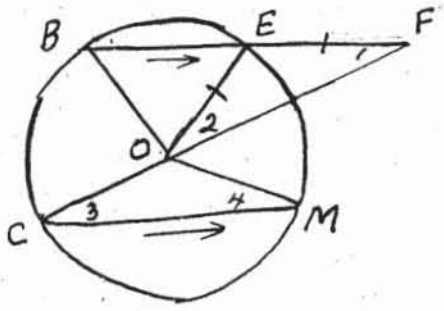
Nicomedes' curve, the conchoid, (discussed earlier) can be used for the trisection problem also, and actually, when used, is another means of finding the points D and E in the first diagram in this section. Here B would be the given point, AC the given straight line, and 2AB the constant length required by the conchoid.

Another curve, that has been described before, is the quadratix of Hippias. (see -- the squaring of the circle.) This curve can be used, not only to trisect an angle, but also to divide it into any number of equal parts.



DFG is the quadratix and CAB the given angle which intersects the quadratix at F. Draw FH perpendicular to AB and divide it in the ratio 1 : 2 (or in any given ratio). Join AF'L and LAB is one third of the given angle as is easily seen from the properties of the quadratix.

Archimedes solution of this problem is interesting (as far as it goes) because of its simplicity.



The angle BOC is to be trisected. From B, a chord of the circle with centre O and radius OB, is drawn and produced until it meets CO produced at F, <u>care being taken that EF equals the radius of the circle</u>. Join EO and the angle EOF is one third of the angle BOC. Draw CM parallel to BE and join OM. Angles 1 and 2 are equal, also angles 3 and 4 and $\angle 1 = \angle 3$ (interior-alternate).

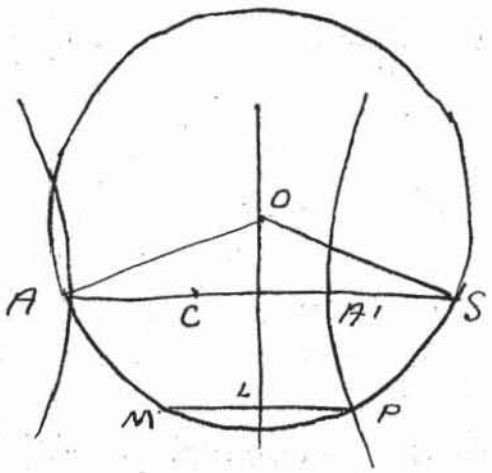
But angle FOM $= \angle 3 + \angle 4$

$\therefore \quad = 2(\angle 3)$

$\therefore \quad = 2(\angle 2)$

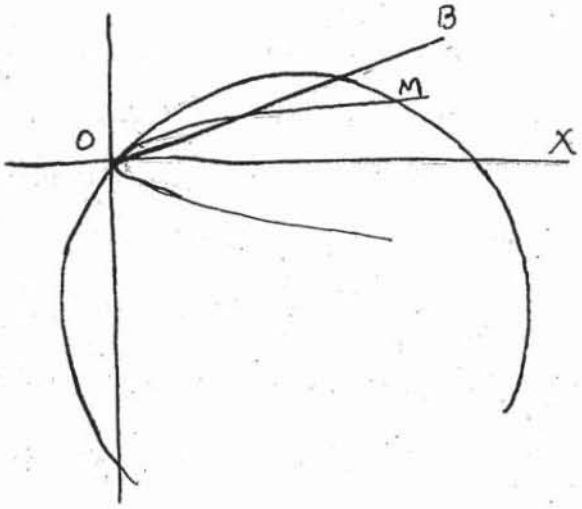
$\therefore$ angle EOM has been trisected . Since the chords BE and CM were parallel, the arcs BC and EM are equal, and hence angle BOC is equal to the angle EOM and angle EOF is one third of angle BOC.

Returning to solutions making direct use of conics, this one is found recorded by the historian Pappus -- but the name of its author is lost. Draw a hyperbola with e = 2, having centre C and vertices A and A' and with CA' produced to S so that A'S = CA'.



On AS describe a segment to contain the given angle and let the right bisector of AS cut the segment in O. With O as centre and radius OA describe a circle to cut the hyperbola in P. Then the angle SOP is one third the angle SOA. From the definition of the hyperbola $\frac{SP}{LP} = 2$, as it is readily established that S is the focus and OL the directrix of the conic. Therefore the arc SP = the arc PM and the angle SOP = angle POM; but angle POM = $2 \angle$ POL and as SOL is one half the given angle, then angle SOP is one third of given angle SOA. This contains one of the very few references to focus and directrix of conics to be found in Greek Mathematics. Too, we may note that this is essentially the same solution as the best one offered by Newton (1642 - 1727) and, in a form that differs only slightly, by Clairaut.

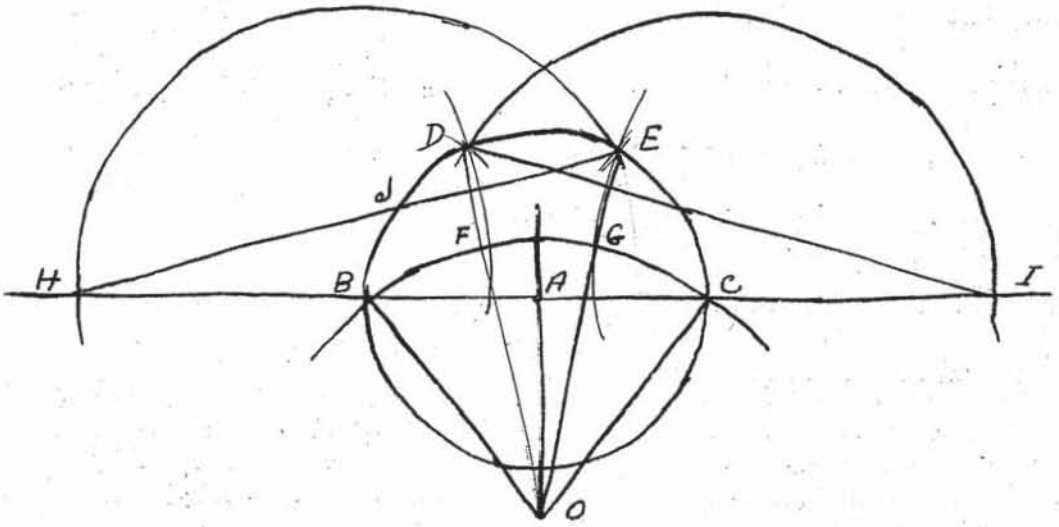
An ingenious construction worked out by Descartes leads to a cubic equation. With the curves $y^2 = \frac{1}{4}x$ and $x^2 + y^2 - \frac{13}{4}x + 4ay = 0$, where a = Sin 3A and 3A is the angle to be trisected, he finds the points of intersection, other than the origin



BOX = 3A is the angle whose sine is a. Substituting for x we get $4y^3 - 3y - a = 0$ or $4y^3 - 3y - \text{Sin}3A = 0$ which is similar to a well known equation and has as its smallest positive root $y = \text{Sin A}$. So, constructing

the angle whose sine is this value of y, we have trisected the angle.

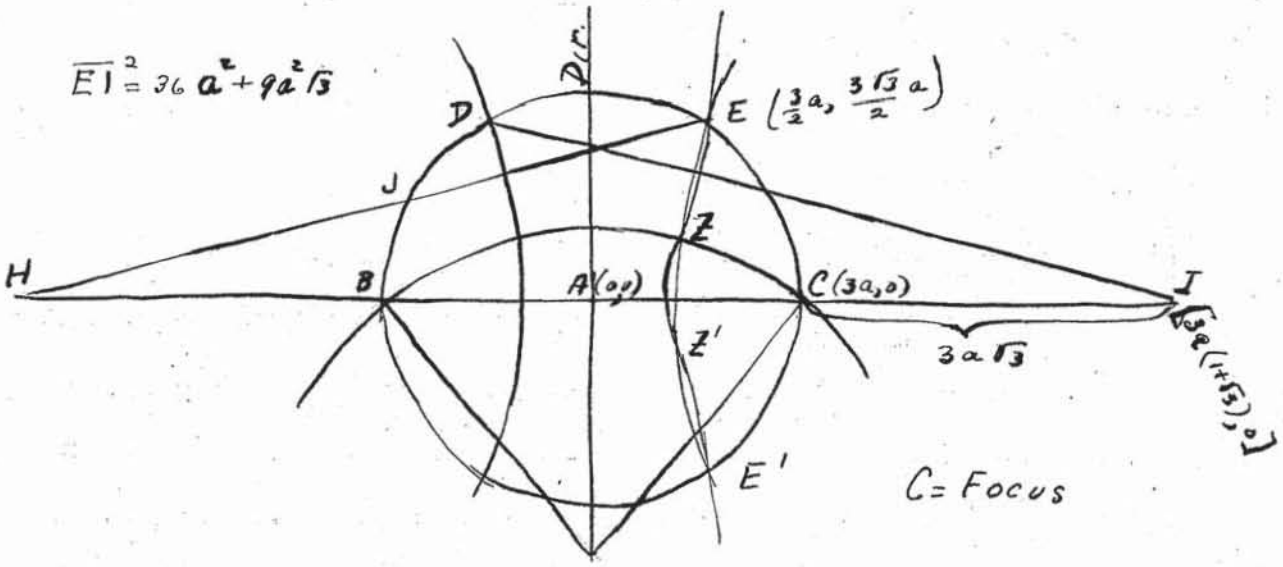
I am indebted to Dr. C. Mark for an interesting communication from Mr. L. J. Seaman to Prof. S. Beatty of the University of Toronto, in which Mr. Seaman offers Prof. Beatty a partnership (and a share in the royalties) for handling the "propaganda" for his "solution of a problem considered insolvable for 2500 years." He had it copyrighted in the United States in 1931. It is as follows. The Arc BFGC bounds the given angle. Describe a circle



with the chord BC as diameter and on this circle locate the points D and E such that the chords BD and EC are each equal to the radius. With B as centre and BE as radius, describe an arc cutting CB produced at H and similarly an arc with C as centre, cutting BC produced at I. Bisect the arc BD at J and join EJH. (It <u>is</u> readily proved that EJH are co-linear as Mr. Seaman suggests although I do not know why he introduces J at all). With centre H and radius HD describe an arc cutting the arc BC at F. Similarly with centre I and radius EI, cut the arc BC at G. Join FO, and GO, and the angle BOC is trisected -- so Mr. Seamsn says.

The arcs DF and EG depend only on BC and are supposed to work for any position of O on AO (that is, for any size of angle

on the segment BC). Actually the trisection is accomplished for angles of two different magnitudes, but not for others. The hyperbola with e = 2 really would trisect any angle, and it can be drawn once BC is given and would go through E (or D).



The circle and hyperbola cannot intersect in more than four points, of which two are E and E′. The other two Z and Z′ lie between these. The construction works for these points only though it is very close for its whole length.

Letting AC = 3a, the distance CJ = CI is found to be $3a\sqrt{3}$ (from the right angled triangle BEC) and the distance EI is $\sqrt{36a^2 + 9a^2\sqrt{3}}$, by using the law of cosines. The circle with centre I $(3a\,(1+\sqrt{3}), 0)$ and radius $\sqrt{36a^2 + 9a^2\sqrt{3}}$ is

$x^2 + y^2 - 2(1+\sqrt{3})3ax + \sqrt{3} \cdot 9a^2 = 0.$

The equation of the hyperbola with e = 2, focus at C(3a,o) and directrix x = o is $3x^2 - y^2 + 6ax - 9a^2 = 0$

These intersect where $4x^2 - 2\sqrt{3} \cdot 3ax + (\sqrt{3} - 1)\,9a^2 = 0$

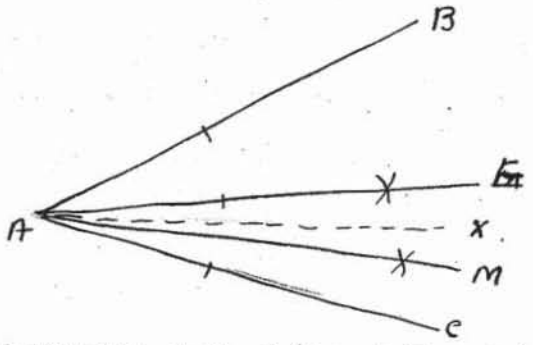
or $(2x - 3a)(2x - (\sqrt{3} - 1)\,3a) = 0$

$\therefore x = \frac{3a}{2}$ (i.e. at E and E′)

and $x = (\sqrt{3} - 1)\frac{3a}{2}$ (i.e. at Z and Z′)

Thus, the Seaman construction trisects an angle of 90°, at E and also an angle of about 72°.

It is supposed that the real problem spurring on the Greeks, to try to discover how to trisect an angle was that of describing a regular polygon of nine sides. It had been easy to construct figures of three, four, five, six and eight sides. A heptagon seemed too difficult -- as well it might -- and they concentrated on the attempt to describe a nonagon, or to divide an angle of 360°, into nine equal parts, which would achieve their goal for them. The quadratrix could be used for this purpose, as stated previously, but this construction was not acceptable here either, because the aim was to find a means of obtaining a nonagon with ruler and compasses -- one that would lead to ideal results. Also it is quite likely that they were able to arrive at good approximations by which constructions could be worked out practically such as: BAC is bisected. Then CAE is bisected, then MAE, until the bisecting lines can no longer be distinguished, and to all intents and purposes XAC is an angle one third the size of BAC.



This is actually the sum of the infinite G.P. $1/2 - 1/4 + 1/8 - 1/16 \ldots\ldots\ldots = 1/2 \div (1 + 1/2) = 1/3$. But of course one can only approach, not achieve, this limit.

The Greeks readily drew figures of ten, twelve, and sixteen sides, and all multiples by two of any of these, besides the ones mentioned earlier, but not until the time of Gauss (1777 - 1855) was it guessed that a 17 sided figure was constructible. The figure and description is given as Gauss worked it out at the age

of 17 years but its proof necessitates some consideration of methods of solving the reciprocal equation by periods, as discovered by Gauss.

Solve $x^{17} - 1 = 0$ (i.e. find $\sqrt[17]{1}$ which will give the terminals of the sides of the inscribed polygon of 17 sides, in a circle of radius 1). Dividing both sides by $x - 1$, we get

$x^{16} + x^{15} + x^{14} + \ldots\ldots\ldots\ldots x + 1 = 0.$

To divide this into suitable periods, we seek an integer g such that the 16 roots can be arranged in such an order that each root is the gth power of the preceding one. This integer g is found by trial. That such an integer exists is proved in the theory of numbers and the proof is found in the appendix. Two is unsuitable, but $g = 3$ is successful so that the roots are $r, r^3, r^9, r^{10}, r^{13}, r^5, r^{15}, r^{11}, r^{16}, r^{14}, r^8, r^7, r^4, r^{12}, r^2, r^6$, after noting that $r^{27} = r^{17}(r^{10}) = 1(r^{10}) = r^{10}$ and the like. Taking alternate terms we form the two periods

$y_1 = r + r^9 + r^{13} + r^{15} + r^{16} + r^8 + r^4 + r^2$

$y_2 = r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6$

Then $y_1 + y_2$ = the sum of the roots of $x^{16} + x^{15} + x^{14} + \ldots\ldots x + 1 = 0$

$\therefore y_1 + y_2 = -1.$

By multiplying out $y_1 y_2$ we have 64 partial products, in the whole of which each root is repeated four times $\therefore y_1 y_2 = -4$ so that y_1 and y_2 satisfy the quadratic equation $y^2 + y - 4 = 0$.....(1)

Again, using alternate terms of y_1, we have the two periods

$z_1 = r + r^{13} + r^{16} + r^4$

$z_2 = r^9 + r^{15} + r^8 + r^2$ and the alternate terms of y_2 give

$w_1 = r^3 + r^5 + r^{14} + r^{12}$

$w_2 = r^{10} + r^{11} + r^7 + r^6$

or simply $z_1 + z_2 = y_1$

$w_1 + w_2 = y_2$

Multiplying out $z_1 z_2$ term by term, we get the sum of all the sixteen roots $\therefore z_1 z_2 = -1$ and similarly $w_1 w_2 = -1$

$\therefore z_1$ and z_2 satisfy $z^2 - y_1 z - 1 = 0$.....(2)

and w_1 and w_2 satisfy $w^2 - y_2 w - 1 = 0$.....(3)

Taking alternate terms in z_1 we have $v_1 = r + r^{16}$

$v_2 = r^{13} + r^4$

Here $v_1 + v_2 = z_1$ and $v_1 v_2 = r^{14} + r^{12} + r^5 + r^3$

$= w_1$, so that v_1 and v_2 are the roots of $v^2 - z_1 v + w_1 = 0$.....(4) and finally since $r + r^{16} = v_1$ and $r\, r^{16} = r^{17} = 1$, r and r^{16} will be the roots of

$t^2 - v_1 t + 1 = 0$.....(5)

Thus, to find the values of the roots, nothing more difficult than the solving of quadratic equations is needed.

By De Moivre's theorem, each of the 17th roots of unity is given by $r = \cos \frac{2n\pi}{17} + i \sin \frac{2n\pi}{17}$

where $n = 1,2,3,.....17$

$r = \cos \frac{2\pi}{17} + i \sin \frac{2\pi}{17}$

$r^{16} = \cos \frac{2\pi}{17} - i \sin \frac{2\pi}{17}$ [since $\cos \frac{32\pi}{17} = \cos \frac{2\pi}{17}$ and $\sin \frac{32\pi}{17} = -\sin \frac{2\pi}{17}$] $\therefore r + r^{16} = 2 \cos \frac{2\pi}{17} = v_1$

Similarly $r^{13} + r^4 = 2 \cos \frac{8\pi}{17} = v_2$

$\therefore z_1 = 2 \cos \frac{2\pi}{17} + 2 \cos \frac{8\pi}{17}$ which is bound to be positive, for while $\cos \frac{8\pi}{17}$ is negative, it is not as large numerically as $\cos \frac{2\pi}{17}$. Likewise $w_1 = r^3 + r^{14} + r^5 + r^{12}$

$= 2\cos\frac{6\pi}{17} + 2\cos\frac{10\pi}{17}$ which is also positive, and

$$y_2 = (r^3 + r^{14}) + (r^7 + r^{10}) + (r^5 + r^{12}) + (r^6 + r^{11})$$

$$= 2\cos\frac{6\pi}{17} + 2\cos\frac{14\pi}{17} + 2\cos\frac{10\pi}{17} + 2\cos\frac{12\pi}{17}.$$

Each of the last three terms is negative, and the second is greater than the first, so that the whole expression for y_2 is negative.

Going back to equation (1), i.e. $y^2 + y - 4 = 0$ we see that the product of the roots is negative $\therefore$ y_1 is positive and y_2 is negative.

Solving equation (1) $y = \frac{-1 \pm \sqrt{1+16}}{2}$

$\therefore$ $y_1 = \frac{1}{2}(\sqrt{17} - 1)$ and $y_2 = \frac{1}{2}(-\sqrt{17} - 1)$.

Solving equation (2), i.e. $z^2 - y_1 z - 1 = 0$ we have

$$z_1 = \frac{y_1 + \sqrt{y_1^2 + 4}}{2}$$

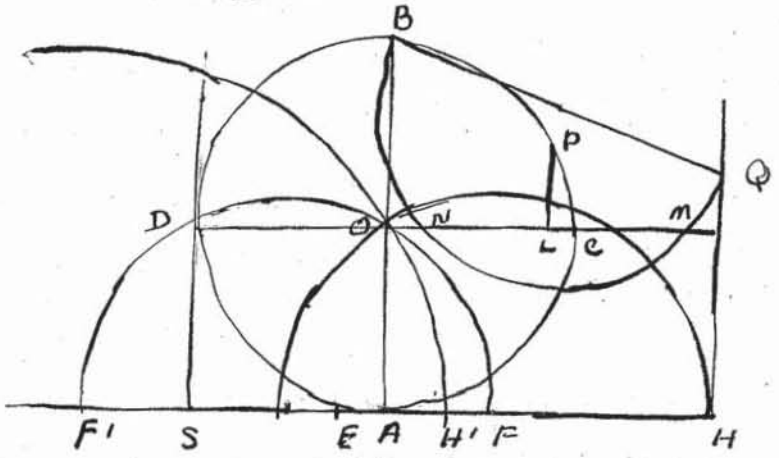
$$= \tfrac{1}{2}y_1 + \sqrt{1 + \tfrac{1}{4}y_1^2}$$

and by solving equation (3) or $w^2 - y_2 w - 1 = 0$, we have

$$w_1 = \frac{y_2 + \sqrt{y_2^2 + 4}}{2} = \tfrac{1}{2}y_2 + \sqrt{1 + \tfrac{1}{4}y_2^2}.$$

The co-efficients for equation (4) are now known, so it can be solved, and then equations (5) which will give the values of two roots of the original equation. A different choice of signs would lead to a different pair of answers. The construction for an inscribed regular polygon of seventeen sides is as follows:

In a circle of radius unity, draw two diameters AB and CD at right angles to each other, and draw tangents AS and DS. Find E so that $AE = \frac{1}{4}AS$ (by means of two besections.) Describe a circle with centre E and radius $OE = \frac{1}{4}\sqrt{17}$, to cut AS at F and F'.



Then $AF = EF - EA = OE - \frac{1}{4} = \frac{1}{4}\sqrt{17} - \frac{1}{4} = \frac{1}{2}y_1$, where $y = \frac{1}{2}(\sqrt{17} - 1)$

$AF' = EF' + EA = OE + \frac{1}{4} = \frac{1}{4}\sqrt{17} + \frac{1}{4} = -\frac{1}{2}y_2$, where $y = \frac{1}{2}(-\sqrt{17} - 1)$

(y_1 and y_2, thus having the same values as in the foregoing reciprocal equation).

$OF = \sqrt{OA^2 + AF^2} = \sqrt{1 + \frac{1}{4}y_1^2}$

$OF' = \sqrt{OA^2 + AF'^2} = \sqrt{1 + \frac{1}{4}y_2^2}$.

Let the circle with centre F and radius FO cut AS at H, and the circle with centre F' and radius F'O cut AS at H.

Then $AH = AF + FH = AF + OF = \frac{1}{2}y_1 + \sqrt{1 + \frac{1}{4}y_1^2}$

and it is seen that this is z_1 in the work above. Also

$AH' = F'H' - F'A = OF' - AF' = \sqrt{1 + \frac{1}{4}y_2^2} + \frac{1}{2}y_2$ and this is clearly w_1. The lengths $AH = z_1$ and $AH' = w_1$ are the co-efficients of v in equation (4). The next step is to find the roots of the equation with these co-efficients. Draw HTQ parallel to OA and intersecting DC produced, in T and having $TQ = AH'$. Using B (o,1) to Q (z_1, w_1) (where OB, OT are the axes) as diameter, describe a circle cutting OT in N and M, and we have ON, OM the roots of equation (4). The larger root v, was previously shown to be $2\cos\frac{2\pi}{17}$. Bisect OM at L to get the value of $\cos\frac{2\pi}{17}$, and erect the perpendicular LP. The angle POL is $\frac{2\pi}{17}$, therefore

the chord CP is one side of the required regular polygon.

The construction of the regular pentagon (while known by other methods, to the Greeks) can be carried out in the same way.

Solve $x^5 - 1 = 0$. First divide by $x - 1$ getting $x^4 + x^3 + x^2 + x + 1 = 0$. For this $g = 2$, so that r, r^2, r^4, r^3 are the roots. Take alternate roots as periods $y_1 = r + r^4$

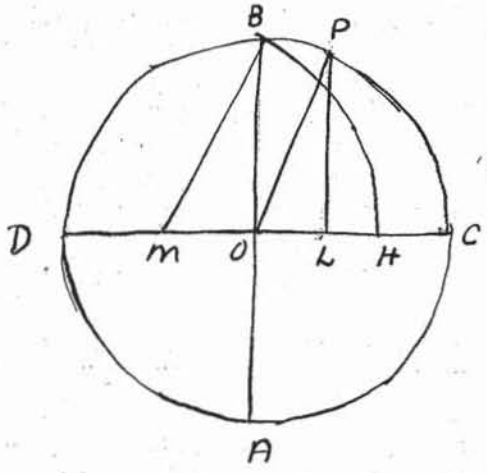
$$y_2 = r^2 + r^3.$$

Since $y_1 + y_2 = -1$, and by multiplying y_1 and y_2 $= (r + r^4)(r^2 + r^3)$ $= r^3 + r^4 + r + r^2 = -1$, we have the equation $y^2 + y - 1 = 0$...(1) whose roots are $\frac{-1 \pm \sqrt{5}}{2}$.

$$r + r^4 = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5} + \cos \frac{2\pi}{5} - i \sin \frac{2}{5}$$

$$= 2 \cos \frac{2\pi}{5} \text{ which is positive}$$

$\therefore r + r^4 = \frac{-1+\sqrt{5}}{2}$.



With circle of radius 1, take M as mid-point of OD. Then $BM^2 = OB^2 + OM^2$

$$= 1 + \tfrac{1}{4}$$

$\therefore BM = \frac{\sqrt{5}}{2}$.

With centre M and radius MB, describe an arc cutting OC at H. Bisect OH at L and erect the perpendicular LP.

$OH = MH - OM = BM - OM = \frac{\sqrt{5}}{2} - \frac{1}{2} = y$,

$\therefore OH = 2 \cos \frac{2\pi}{5}$ $\therefore OL = \cos \frac{2\pi}{5}$

$\therefore$ the angle $POC = \frac{2\pi}{5}$ and the chord CP is one side of the inscribed pentagon.

Gauss established the impossibility of describing a regular heptagon. Proceeding along similar lines,

$z^7 - 1 = (z - 1)(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) = 0$

let $x = z + \frac{1}{z}$ and the second factor becomes $x^3 + x^2 - 2x - 1 = 0$ which is irreducible. If reducible it would have a factor $x - \frac{p}{q}$ where p and q have no common factor and $\frac{p}{q}$ would have to be a factor of -1. But by trial neither 1 nor -1 is a root of $x^3 + x^2 - 2x - 1 = 0$ and hence the equation is irreducible, and has no constructible root, constructible, that is, by ruler and compass, being a result in definite accord with the work of yet more modern investigators.

A regular polygon of 257 sides has been constructed, but until modern times, it was not known that only relatively few regular polygons could be inscribed in a circle.

The story of the solution of algebraic equations is a long one, that of a growth that proceeded slowly. Back in the Rhind Papyrus, we find the earliest recorded equation in "heap, its seventh, its whole, it makes 19" which we would write $\frac{x}{7} + x = 19$. The quadratic equation was studied by Diophantus, the only Greek who wrote anything whatever on Algebra, though there likely were many others who used the knowledge that the Egyptians had had. It is surprising that while he could multiply two negative numbers, he did not recognize negative roots of an equation; he did not admit two roots even when both were positive, evidently being satisfied in having obtained one -- and of course he did not solve the equation when the roots were irrational, although the Pythagoreans had known of the existence of irrational numbers. Diophantus used symbols for the unknown, and for equality and minus. He

changed a tremendous number of problems to equations and solved them. As has been noted earlier many geometric constructions which needed the intersection of two lines actually give a practical method of solving equations (most frequently they were cubics). The second book of Euclid is on quadratic equations. I quote proposition XI to illustrate "To divide a given straight line into two parts so that the rectangle contained by the whole and one of the parts may be equal to the square on the other part."

Both negative and irrational roots were well known to the Hindus who on the whole made much greater progress in Algebra than the Greeks had done -- though undoubtedly they knew and used such knowledge as the Greeks had possessed. The writings of the Hindus did not reach the western world directly but through the hands of the Arabians, of whom the most important writer was Mohammed Ben Musa who records the general solution of the quadratic in much the form we use it today. Still he only admitted the two roots when both were positive. Other Arabian mathematicians were Alkarchi and Omar Alkhayyami who classified cubic equations by means of their geometric constructions but there was no attempt at a general solution of equations of the third degree.

The Arabian writings were brought to Italy in the thirteenth century by Leonardo of Pisa and there interesting solutions were found. Scipio Ferro solved the cubic equation in the form $x^3 + mx = n$ but his methods are not known, a result of the fad in those times of keeping findings secret. This matter of secrecy reminds us of the bitter quarrel between Tartaglia and Cardan, as to who originated the general solution of the cubic. It is generally believed that Tartaglia was the author and that he devised

rules for the solution of the various forms of cubics included under the classification made by the Arabians. The solution of the general cubic equation $x^3 + bx^2 + cx + d = 0$ can be made to depend upon the solution of $y^3 + py + q = 0$ by using the substitution $x = y - \frac{b}{3}$, obtaining $y^3 + (c - \frac{b^2}{3})y + d - \frac{bc}{3} + \frac{2b^3}{27} = 0$

and if we set $c - \frac{b^2}{3} = p$ and $d - \frac{bc}{3} + \frac{2b^3}{27} = q$ we have

$y^3 + py + q = 0$, the reduced cubic equation. In this put $y = z - \frac{p}{3z}$ and obtain $z^3 - \frac{p}{27z^3} + q = 0$ whence we get

$$z^6 + qz^3 - \frac{p^3}{27} = 0.$$

Solving this as a quadratic equation for z^3, we have

$$z^3 = \frac{-q \pm \sqrt{q^2 + \frac{4p^2}{27}}}{2} = \frac{-q \pm 2\sqrt{\left(\frac{q}{2}\right)^2 + \frac{p^3}{27}}}{2}$$

$$= -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \frac{p^3}{27}},$$

Then write this as $z^3 = -\frac{q}{2} \pm \sqrt{R}$ where $R = \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$.

From the theory of complex numbers it is possible to find the cube root of any complex number (including real numbers), using $(\cos\theta + i \sin\theta)^3 = \cos 3\theta + i \sin 3\theta$, and having found one cube root, the other two are obtained by multiplying the known root by $\omega = -\frac{1}{2} + \sqrt{3}\, i$ and by $\omega^2 = -\frac{1}{2} - \sqrt{3}\, i$.

Since $(-\frac{q}{2} + \sqrt{R})(-\frac{q}{2} - \sqrt{R}) = \frac{q^2}{4} - R$

$= \frac{q^2}{4} - \left[\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2\right] = \left(\frac{-p}{3}\right)^3$ we can find particular cube roots

$$A = \sqrt[3]{-\frac{q}{2} + \sqrt{R}}, \qquad B = \sqrt[3]{-\frac{q}{2} - \sqrt{R}}$$

such that $AB = -\frac{p}{3}$.

Therefore we have six values of z, i.e. A, ωA, $\omega^2 A$, B, ωB, $\omega^2 B$, which can be paired thus AB, $\omega A(\omega^2 B)$ and $\omega^2 A(\omega B)$ each pair having a product $-\frac{p}{3}$, so that for any one of the six values of z, there is another paired with it that $z = -\frac{p}{3z}$. Originally we put $y = z - \frac{p}{3z}$ so the values of y are the sums of the values of z in any of the above pairs, i.e. $y_1 = A + B$, $y_2 = \omega A + \omega^2 B$, $y_3 = \omega^2 A + \omega B$, which are now known as Cardan's formulae for the roots of the reduced cubic. They were published in his Ars Magna 1545. Cardan definitely was aware of negative roots but did not like them, calling them fictitious. If the roots of a cubic equation are all real and distinct A and B of Cardan's formulae require the finding of cube roots of imaginary quantities for R turns out to be negative.

Since $(y_1 - y_2) = A - \omega A + B - \omega^2 B = (1 - \omega)(A - \omega^2 B)$

as $\omega^3 = 1$ and $(y_1 - y_3) = A - \omega^2 A + B - \omega B = -\omega^2(1 - \omega)(A - \omega B)$

also $(y_2 - y_3) = \omega A - \omega^2 A + \omega^2 B - \omega B = \omega(1 - \omega)(A - B)$

The product of these three $(y_1 - y_2)(y_1 - y_3)(y_2 - y_3)$

$= -\omega^3(1 - \omega)^3 (A - \omega^2 B)(A - \omega B)(A - B)$

$= -1\left[3(\omega^2 - \omega)\right]\left[A^3 - B^3\right]$ noting $\omega^2 + \omega + 1 = 0$

$= -1\,(3)(\sqrt{3}\,i)(2\sqrt{R}) = 6\sqrt{3}\sqrt{R}\,i.$

The product of the squares of the differences of the roots of any equation is called the discriminant $\triangle$ of the equation

$\therefore \triangle = (y_1 - y_2)^2 (y_1 - y_3)^2 (y_2 - y_3)^2 = (6\sqrt{3}\sqrt{R}\,i)^2 = -108R.$

This is obviously positive if the roots are real and distinct

$\therefore$ R must be negative.

It is called the "irreducible case" when R is negative; and this case is treated as follows. The equation is handled as

above to the point of finding $A = \sqrt[3]{-\frac{1}{2}q+\sqrt{R}}$ and $B = \sqrt[3]{-\frac{1}{2}q-\sqrt{R}}$

Then instead of what followed there, find r and θ so that

$-\frac{1}{2}q+\sqrt{R} = r(\cos\theta + i\sin\theta)$ i.e. $-\frac{1}{2}q = r\cos\theta$

and $\sqrt{R} = r\,i\sin\theta$ or $R = -r^2\sin^2\theta$.

Since $r^2 = r^2(\cos^2\theta + \sin^2\theta)$

$= r(\cos\theta + i\sin\theta)\, r(\cos\theta - i\sin\theta)$

$= (-\frac{1}{2}q+\sqrt{R})(-\frac{1}{2}q-\sqrt{R}) = \frac{1}{4}q^2 - R$

$= -\frac{p^3}{27}$ as explained previously.

$r = \sqrt{-\frac{p^3}{27}}$ (R being negative means that $-\frac{p^3}{27}$ is positive and

$\cos\theta = -\frac{1}{2}q \Big/ \sqrt{-\frac{p^3}{27}}$. As R is negative $-\frac{p^3}{27} > \frac{1}{4}q^2$

or $\sqrt{-\frac{p^3}{27}} > -\frac{q^2}{2}$ $\therefore$ $\cos\theta < 1$ and can be found from a table

of cosines. Similarly $-\frac{1}{2}q - \sqrt{R} = r(\cos\theta + i\sin\theta)$ so that

the cube roots of $-\frac{q}{2}+\sqrt{R}$ and $-\frac{q}{2}-\sqrt{R}$ are

$\sqrt{-\frac{p}{3}}\left[\cos\frac{\theta + m360^\circ}{3} \pm i\sin\frac{\theta + m360^\circ}{3}\right]$ $(m = 0, 1, 2)$ and for

each value of m, the product of these two numbers is $-\frac{p}{3}$ and

therefore, their sum $2\sqrt{-\frac{p}{3}}\cos\frac{\theta + m360^\circ}{3}$ for the three values of

m, gives the three real roots of the cubic. A purely algebraic

method of finding the cube root of the imaginary numbers entailed

in this, fails. There is a solution for the cubic with real

distinct roots (the other cases offer no especial difficulty)

making even greater use of trigonometry that is due to Vieta.

He used $\cos 3x = 4\cos^3 x - 3\cos x$ or putting $z = \cos x$

$$z^3 - \frac{3}{4}z - \frac{1}{4}\cos 3x = 0$$

Compare this with $y^3 + py + q = 0$ after putting $y = nz$

i.e. $n^3z^3 + pnz + q = 0$ or $z^3 + \frac{pz}{n^2} + \frac{q}{n^3} = 0$ from which

$n = \sqrt{\frac{4p}{-3}}$ and $\cos 3x$ is $\frac{-q/2}{\sqrt{\frac{-p^3}{27}}}$.

Then cos 3x can be found from a table of cosines. The three values of z (= cos x) are cos x, cos $(x + 120^\circ)$ and cos $(x + 240^\circ)$ from which the values of y are easily written off. Vieta also solved equations by a method of approximation that was definitely the forerunner of Horner's method. Thus in $x^2 + 14x = 7929$, taking 80 for the approximate root, and placing $x = 80 + b$, we get

$(80 + b)^2 + 14(80 + b) = 7929$

or $174\,b + b^2 = 409$.

Since 174 b is much greater than b^2, put $174\,b = 409$ and get $b = 2$. Hence the second approximation to the root is 82. Put $x = 82 + c$, then $(82 + c)^2 + 14(82 + c) = 7929$

or $178\,c + c^2 = 57$ and continue the process as far as desired.

About this time we find negative roots for equations completely accepted. Stevin is the first to record his definite approval.

Naturally the equation of the fourth degree next claimed the attention of mathematicians. Cardan seems to have tried to find a solution, but where he failed, a pupil of his, Lodovico Ferrari, succeeded, using a transformation to make both sides of the equation a perfect square, a new unknown quantity being introduced which is itself determined by an equation of the third degree. To solve $x^4 + bx^3 + cx^2 + dx + e = 0$ write it in the equivalent form $(x^2 + \frac{1}{2}bx)^2 = (\frac{1}{4}b^2 - c)x^2 - dx - e$

By adding $(x^2 + \frac{1}{2}bx)y + \frac{1}{4}y^2$ to both sides we have

$(x^2 + \frac{1}{2}bx + \frac{1}{2}y)^2 = (\frac{1}{4}b^2 - c + y)x^2 + (\frac{1}{2}by - d)x + \frac{1}{4}y^2 - e$

The first member is a perfect square and the second member can be made so, by choosing a suitable value y_1 of y.

Let $b^2 - 4c + 4y_1 = t \quad (\text{with } t \neq 0)$

Then $\frac{1}{4}t^2x^2 + (\frac{1}{2}by_1 - d)x + \frac{1}{4}y_1^2 - e = \left(\frac{\frac{1}{2}tx + \frac{1}{2}by_1 - d}{t}\right)^2$

$\therefore \frac{1}{4}y_1^2 - e = \left(\frac{\frac{1}{2}by_1 - d}{t}\right)^2$

i.e. $\frac{1}{4}y_1^2 - e = \frac{(\frac{1}{2}by_1 - d)}{b^2 - 4c + 4y_1}$

$\therefore y_1^3 - cy_1^2 + \frac{1}{4}b^2y_1^2 - eb^2 + 4ec - 4ey_1 = \frac{1}{4}by_1^2 - bdy_1 + d^2$

or $y_1^3 - cy_1^2 + (bd - 4e)y_1 - eb^2 + 4ec - d^2 = 0$

which is a cubic and can be solved for y_1.

Now $x^2 + \frac{1}{2}bx + \frac{1}{2}y_1 = \pm\left(\frac{1}{2}tx + \frac{\frac{1}{2}by_1 - d}{t}\right)$

$\therefore x^2 + \frac{1}{2}(b - t)x + \frac{1}{2}y_1 - \frac{\frac{1}{2}by_1 - d}{t} = 0$

and $x^2 + \frac{1}{2}(b + t)x + \frac{1}{2}y_1 - \frac{\frac{1}{2}by_1 - d}{t} = 0$

From each of the above quadratic equations, two values of x can be found.

The equation of the third degree, and that of the fourth having been successfully solved, men were encouraged to try to find a similar solution for the equation of the fifth degree. Descartes, Euler and Lagrange all contributed much to the knowledge of Algebra through their unsuccessful efforts; for example, Descartes Rule of Signs" is still the handiest means of locating real roots. Lagrange undertook to review the work of all his predecessors and showed that their results belonged to one uniform principle, which consists in reducing the given equation to that of one of lower degree whose roots are linear functions of the

roots of the given equation and of the roots of unity. He showed too that the quintic could not be so reduced, the equation on which its solution depended being of sixth degree. But there began to be suspicions that equations of higher degree were impossible of solution, and other lines to the approach to the study of the equations were being followed. We have Gauss' proof that every algebraic equation of degree n, with complex co-efficients has n roots. For this Gauss needed imaginary numbers which had been used, though scarcely admitted, from the time of Cardan onwards. Euler in 1748 set up the relation $e^{ix} = \cos x + i \sin x$, by which time complex numbers were quite well established. Gauss' proof that every equation has a root is, briefly, this:

Given the polynomial

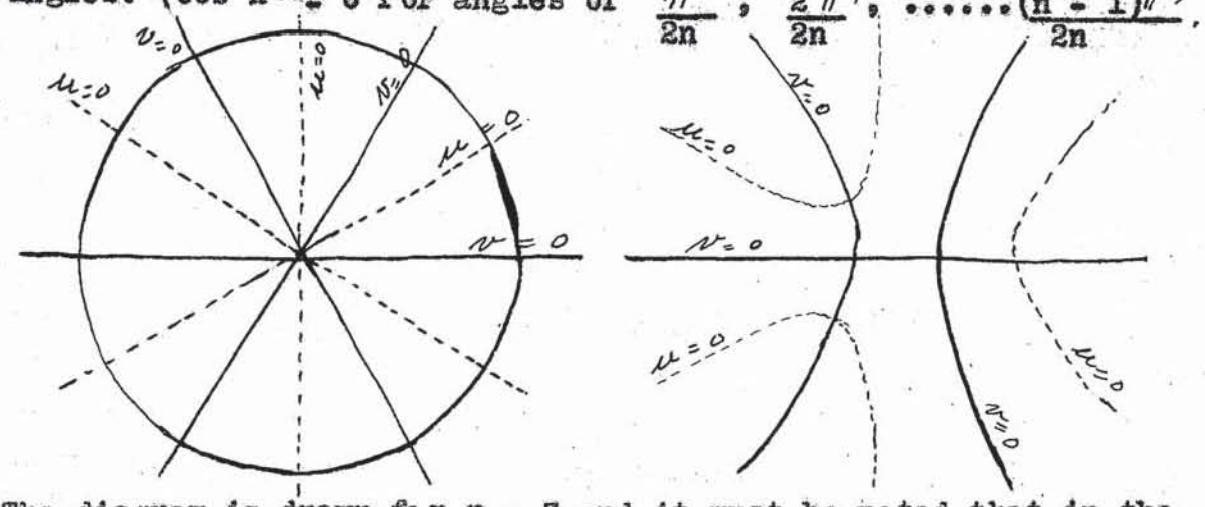
$f(z) = z^n + a_1 z^{n-1} + \ldots\ldots\ldots a_n$, we may write

$f(x + iy) = u(x,y) + iv(x,y)$ where u and v are real polynomials in the variables x and y. We are to show that there are real numbers x and y for which $u(x,y) = 0$ and $v(x,y) = 0$, in the XY plane and therefore they must have one point in common, and for that point $f(x + iy) = 0$ would be true; i.e. that point would be a root of $f(z) = 0$. If we use the trigonometric form of z: $z = r(\cos\theta + i \sin\theta)$, it follows by De Moinre's theorem that $z^n = r^n(\cos n\theta + i \sin n\theta)$. If r, the absolute value of z, be taken very large, the limit

$$\frac{f(z)}{z^n} = 1 + \frac{a_1}{z^1} + \frac{a_2}{z^2} + \ldots\ldots\ldots\ldots\frac{a_n}{z^n} = 1$$

or f(z) approaches z^n asymptotically. Therefore u and v approach $r^n \cos n\theta$ and $r^n \sin n\theta$ in the same way, so that the course of the curves $u = 0$ and $v = 0$ can be found from

$\cos n\theta = 0$ and $\sin n\theta = 0$. The curve $\sin n\theta = 0$ consists of n straight lines which go through the origin and meet the X axis at angles of $0, \frac{\pi}{n}, \frac{2\pi}{n}, \ldots\ldots\frac{(n-1)\pi}{n}$. Whereas $\cos n\theta = 0$ consists of n lines through the origin which bisect the former angles. ($\cos n\theta = 0$ for angles of $\frac{\pi}{2n}, \frac{2\pi}{2n}, \ldots\ldots\frac{(n-1)\pi}{2n}$.



The diagram is drawn for $n = 3$ and it must be noted that in the central part of the figure the true curves $u = 0$ and $v = 0$ can be essentially different from straight lines (indicated in the second diagram) -- but as stated before, if r is very large, the values approach these straight lines.

Drawing a circle with O as centre and very large value of r for radius, it is obvious that the branches u and v outside the circle alternate so that it is graphically clear that these branches must cross one another inside the circle. This establishes the fact that a point exists for which $u = 0$ and $v = 0$ are both true and therefore that there is a point for which $f(x + iy) = 0$ or $f(z) = 0$ is true or that $f(z) = 0$ has a root. If one such root is found, we can divide out a linear factor which reduces the degree of the equation by one, and repeat the argument n times: thus an equation of nth degree has n roots. This explanation which is given by Felix Klein is somewhat briefer

than Gauss' original one but is essentially the same.

In 1631 Harriot had discovered the composition of an equation as the product of factors and the relations between the roots and the co-efficients of an equation. This was an important milestone, since it showed that any integral root must be a factor of the absolute term, but is naturally of no avail if the equations has no integral root.

Knowing that all equations of nth degree have n complex roots, and despairing of finding a general method by which roots could always be found exactly, mathematicians concerned themselves with the problem of finding the roots of an equation to any required degree of accuracy, developing and improving Vieta's early methods. First the roots must be roughly located. Descartes "Rule of Signs" gave (at least to within an even integer) the number of positive roots and the number of negative roots. Rolle, Sturm, Fourier and Budan worked out excellent methods of isolating the roots. The equation can then be solved by methods advances by Newton, by Horner, by Graffe, and one using continued fractions by Bernoulli, and one also by Euler, though Lagrange showed that this was essentially the same as Newton's. I shall give here, the details of only Horner's method, by using it to solve the equation $x^5 + x^4 - 12x^3 + 27x + 27 = 0$ for the root which exists between 1 and 2. A root does exist for f(1) is positive and f(2) is negative and since f(x) is continuous, at least one value of $f(x) = 0$ must lie between 1 and 2. We shall use the transformed equation with root = p where $x = 1 + p$ i.e. $p = x - 1$, and our equation is the same as $(x - 1)^5 + 6(x - 1)^4 + 2(x - 1)^3 - 32(x - 1)^2 - 24(x - 1) + 32 = 0$

or $p^5 + 6p^4 + 2p^3 - 32p^2 - 24p + 32 = 0$

The co-efficients of this may be found thus, from the co-efficients of the given equation

1	1	-12	-12	27	27	1
	1	2	-10	-22	5	
1	2	-10	-22	5	32	
	1	3	- 7	-29		
1	3	- 7	-29	-24		
	1	4	- 3			
1	4	- 3	-32			
	1	5				
1	5	2				
	1					
1	6					

By trial the root of this is found to lie between .7 and .8 so finding a second transformed equation as before from the equation

$p^5 + 6p^4 + 2p^3 - 32p^2 - 24p + 32 = 0$

1	6	2	-32	-24	32	.7
	.7	4.69	4.683	-19.1219	-30.18533	
1	6.7	6.69	-27.317	-43.1219	1.81467	
	.7	5.18	8.309	-13.3056		
1	7.4	11.87	-19.008	-56.4275		
	.7	5.67	12.278			
1	8.1	17.54	- 6.730			
	.7	6.16				
1	8.8	23.70				
	.7					
1	9.5					

We now can form the equation $y^5 + 9.5y^4 + 23.7y^3 - 6.73y^2 - 56.4275y + 1.81467 = 0$ whose roots are 1.7 less than the roots of the original equation. The value of y in this last equation is very small so the two most important terms are $-56.4275\,y + 1.81467$ which are approximately equal to zero, from which $y = .03216$. The next divisor therefore would be .03 but a fairly accurate value is found by stopping at this point and taking $x = 1.7 + .03216$ or 1.73216. This process can be used to find any and all real roots of an equation, and is quite satisfactory from a practical point of view. It is however readily seen that this method entails "trial" and does not lead to formulae by which the roots of a fifth degree equation can be expressed -- as is the case with equations of lower degree. A way around had been found but the problem had not been solved and no further progress was made till the time of Abel and Gauss.

Part B

In modern times it has been proved that it is impossible to solve the general fifth degree equation -- that is, that no root exists in any number field made up from the rational operations on integers. To set forth clearly what is meant by field, it is first necessary to define "Domain". An integral domain is any set of elements for which the operations of addition and subtraction are defined with the following properties:

(a) each pair of elements a and b in the domain determine uniquely a sum $a + b$ and a product ab for which the distributive law $\left[a(b + c) = ab + ac\right]$, the associative laws $\left[a + (b + c) = (a + b) + c \text{ and } a(bc) = (ab)c\right]$ and the commutative laws $\left[a + b = b + a \text{ and } ab = ba\right]$ hold.

(b) the domain must contain the elements zero and unity to act as indentities for addition and multiplication

(c) For each a in the domain there is an element $-a$.

(d) the cancellation law for multiplication holds.

Obviously the set of all integers forms a domain, and the set of all integers with some surd adjoined also forms a domain as $a + b\sqrt{7}$. It can be easily seen that this satisfies the four postulates above. Now a Field is an integral domain which also contains an inverse a^{-1} for each element a (not zero). That is, division by any element except zero is possible in a field though not in a domain. The field must be decided upon before it is possible to decide whether a given equation is solvable. For example $2x - 5 = 0$ is solvable easily if the field is one in which x represents a number of dollars, but if x represents a number of

people, no answer is possible. The field in which we seek the answers to the fifth degree equation is that formed from the integers by the rational operations, addition, subtraction, multiplication and division, and the extracting of a root of unity a finite number of times.

Note that an algebraic expression may be reducible (that is in factorable) or irreducible depending upon the field used. A polynomial in one variable x with co-efficients in the field is said to be reducible if it can be expressed as a product of polynomials, neither being a constant, each having co-efficients in the field. For example x^2+1 is irreducible in the field of real numbers, but factors into $(x + i)(x - i)$ in the field which contains the imaginary element i. This further illustrates the necessity for specifying the field of operations.

The operation by which a set of elements $x_1, x_2, x_3, \ldots x_n$, is changed into a set of elements $x_a, x_b, x_c, \ldots x_l$ is called a substitution. To each of the indices a, b, c,.....l there corresponds one and one only of 1, 2, 3, ...n. This we call a one-one correspondence or an isomorphism. A substitution may be written $s = x_1\ x_2\ x_3 \ldots$

$x_2\ x_3\ x_4 \ldots$

or s = (1 2 3 .....) either of which means x_1 is replaced by x_2 and so on. We define the "product" of two substitutions, s_1 and s_2, as the substitution obtained by first performing s_1 and afterwards performing s_2. For example (123), meaning that x_1 is replaced by x_2, x_2 by x_3 and x_3 by x_1, multiplied by (12) may be written as (123)(12) and is equal to (23). It must be noted

that the product of two substitutions is not commutative. The product (12)(123) is (13).

An abstract group is a system composed of a set of elements (a, b, c,.....n) and the "multiplication" operation, and having the properties (i) that the product of any two and the square of each are elements of the system, (ii) that the associative law holds, (iii) that the system contains an identity element I, (by which any element is replaced by itself) and (iv) that it contain an inverse for every element of the set (this allows that the product of two elements forms the product I). The abstract group definition can be applied to a wide variety of systems: for instance, the elements may be the rotations of a regular hexagon through an angle of 60°, or through multiples of 60°; but what is important here is that a set of substitutions may form a group (said to be of order m if it contains m elements). We shall consider only groups of substitutions in the following. The group of substitutions I, (123), (132), (12), (13), (23) is of order six. It consists of the 3! possible substitutions on 3 letters, and is known as the symmetric group of order six. Similarly the symmetric group of order n! consists of the n! substitutions on n letters.

If group is such that all its elements are powers of some one element (other than the identity) it is known as a cyclic group. That is, if s is a substitution of order n, the substitutions $I, s, s^2, \ldots\ldots s^{n-1}$ form a cyclic group generated by the substitution s. Further, a group is "regular" if each element is changed into every other element, and into itself, once and once only by all the substitutions of the group.

The group I, (123), (132) is both regular and cyclic, [(123), $(123)^2$ = (132), $(123)^3$ = 1 and x_1, x_2, x_3 becomes x_1, x_2, x_3 by I, and x_2, x_3, x_1 by (123) and x_3, x_1, x_2 by (132)]. This group I, (123), (132) which is of order three is a subgroup of the symmetric group of order six, since it is contained in the latter but in itself satisfies all the requirements of the definition of a group. Actually a group may be considered as a subgroup of itself, but since we are usually only interested in a subgroup which is smaller than the whole, such a subgroup is called a "proper subgroup". I and (12) form a proper subgroup of the symmetric group of order six, as also do I, (123), and (132). The order of a subgroup is a factor of the order of the group, for, given a group G with n elements in it and a subgroup H containing r elements, then r is a factor of n. If a_1, a_2, a_3 .....a_r are the elements of H, and if b_1 is some element of G but not of H, then the products a_1b_1, a_2b_1, a_3b_1 .....a_rb_1 will all be in G but not in H from the definition of a group. If G is not exhausted, choose some other element b_2 of G (but not of H, nor of a_1b_1, a_2b_1, ... a_rb_1,) and multiply the terms of H by it, obtaining a_1b_2, a_2b_2, a_3b_2.....a_rb_2 which again will all be in G but neither in H, nor in the previous subgroup. Repeating this, the elements of G all become used, and may be displayed as follows:

a_1, a_2, a_3 .....a_r

a_1b_1, a_2b_1, a_3b_1 .....a_rb_1

a_1b_2, a_2b_2, a_3b_2 .....a_rb_2

etc.

so that the whole number n is a multiple of the number of elements in the first row. Thus the order of the subgroup is a factor of

the order of the group. The result of dividing the order of the group by the order of the subgroup is the "index" of the subgroup under the group.

The alternating group is the full number of even substitutions on n letters, where by an even substitution is meant one that can be decomposed into an even number of transpositions of two letters. The alternating function is

$$P = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)\ldots\ldots\ldots\ldots(x_1 - x_n)$$
$$(x_2 - x_3)(x_2 - x_4)\ldots\ldots\ldots\ldots(x_2 - x_n)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(x_{n-1} - x_n)$$

An exchange or transposition of two numbers changes the sign of the function P, as using (12), the first factor is changed in sign, while those in the rest of that line are interchanged with factors in the line below, so that the product is not further altered. Similarly, for any odd number of transpositions the sign of P is changed. An even number of transpositions makes no change in the product. The symmetric group is of order n! Half of these substitutions are odd. It contains at least one odd substitution (a transposition t), therefore all of its even substitutions multiplied by t give distinct and odd substitutions, and there are at least as many odd substitutions as even ones. Again, the product of its odd substitutions by t give distinct and even substitutions, so that there are at least as many even substitutions as odd. Hence half of the substitutions of the symmetric group are even. These are the substitutions which make up the alternating group on n letters. Its order, therefore, is $\frac{1}{2}n!$. The alternating

group is a subgroup of index 2 in the symmetric group.

The "transform" of one element by another is the result obtained by multiplying any given element, on the right by some other element and on the left by the inverse of the latter. Thus $g^{-1}Hg$ is the transform of H by g, where g^{-1} indicates the inverse of g. Thus the transform of (12) by (123) is the product (132) (12) (123), [(132) being the inverse of (123), since (132)(123) = I]. The result of the transform of (12) by (123) is seen to be (23). A subgroup is called "invariant" if it contains exactly the same elements, though perhaps in different arrangement, when all the elements of the subgroup are transformed by all the elements of the original group; that is, if it is transformed into itself by all the substitutions of the group. The identity is an invariant substitution of every group. It may be observed that the function $\psi = x_1x_2 + x_3x_4$ is invariant under the following G_8 = I, (12)(34), (13)(24), (14)(23), (13), (24), (1234) and (1432). Any other of the substitutions on four letters changes ψ into some other function, say $\psi_2 = x_1x_3 + x_2x_4$ which is obtained using (23), not in G_8. or stated otherwise: any of G_{24} transformed by a member of G_8 gives a result found in G_8, for example (13) [(12)(34)] (13), or (12)(34) transformed by (13), gives (1432). A function such as $\psi_2 = x_1x_3 + x_2x_4$ which is obtained from ψ by substitutions of the group G_{24} not found in the subgroup G_8 is said to be conjugate to ψ. If the subgroup is of index 3 under G, there will be three distinct conjugate values of the function being considered and all the substitutions of the group G will be divided into three subgroups, which are called a set of conjugate subgroups of G. If these conjugate

subgroups are all identical, the subgroup is said to be self-conjugate or invariant. The symmetric group of order six contains no invariant subgroup except the identity. The maximal invariant proper subgroup (that is a proper self-conjugate subgroup, not contained in a larger self conjugate subgroup of G) is the most important one for our purposes. If we have a succession of maximal invariant proper subgroups each contained within the preceding one, say G, H, K ..... where K is a subgroup of H, and H of G, and if a is the index of H under G, and if b is the index of K under H, etc, then a, b .....are known as the composition factors of the group G. If all the composition factors of the group G are prime numbers, G is called a "solvable group", but before dealing with a solvable group I shall consider the group of an equation. (Not until page , however will it be possible to define the group of an equation.)

In the first place, every equation has associated with it a definite group which will differ, in most cases, for different fields. Let us take the equation $ax^3 + bx^2 + cx + d = 0$, of the third degree which has been proved to have three roots. We will assume the roots to be distinct, for if they are not, f(x) and its derivative $f'(x)$ would have a common divisor g(x), not a constant, and we could treat the equation $f(x)/g(x) = 0$ as having no multiple root. In all that follows, therefore, we will consider the roots of the equation to be distinct. In the case in hand, let the roots be x_1, x_2 and x_3. If we take some function of these roots, say $x_1 x_2 + x_3$ and replace the x's by each other in as many ways as possible, we shall find there are 3! possible substitutions $\left[1, (12), (13), (23), (123), (132)\right]$ and

if we had taken some function of all the roots of an equation of the nth degree, there would be n! substitutions. Some of these substitutions alter the value of the function and some do not, as in the case above, of the cubic equation and the function $x_1 x_2 + x_3$, the substitution (12) does not alter the value of the function while (13) does. Futhermore, a certain substitution may change one function of the roots and yet not change another, as (12) would change $x_1 - x_2$ but not $x_1 + x_2$.

Suppose that for the equation of the nth degree, we take this function of the roots: $V_1 = m_1 x_1 + m_2 x_2 + m_3 x_3 + \ldots\ldots\ldots\ldots m_n x_n$ (this is the Galois function of the roots), then the m's can be so chosen that every possible substitution of the x's does alter the expression; hence it has n! different values which are represented by $V_1, V_2, \ldots\ldots V_{n!}$. To show that it is possible to choose such m's, give to m_1 any integral value, say 0, and to m_2 any different integral value, say 1. Looking at the equations $V_1 = V_2$ [where V_2 is obtained from V_1 by a substitution such as (213)] we find that certain values of m_3 are determined if $V_1 = V_2$ contains m_3 but not m_i $(i > 3)$ i.e. if $V_1 = V_2$, then $x_2 + m_3 x_3 = x_1 + m_3 x_2$

or if $m_3 = \dfrac{x_1 - x_2}{x_3 - x_2}$. Any

value of m_3 except this will make $V_1 \neq V_2$. There will be other values to be avoided, at each later stage, -- ones which will make $V_1 = V_4$ or $V_2 = V_4$ for instance, but there is an infinite choice of values that make V_1, V_2, V_3 all different. Next we give to m_4 an integral value different from the values of m_4 determined by the relations $V_1 = V_3$ involving m_4 but not m_i $(i > 4)$ and so on.

Using the n! Galois functions we form the expression

$P(y) = (y - V_1)(y - V_2)(y - V_3)\ldots\ldots\ldots\ldots\ldots(y - V_{n!})$

where y is a variable. Let $s_1 = 1, s_2, s_3 \ldots\ldots s_{n!}$ be the substitutions used to form V_i from V_1. If $s_j s_k = s_i$ (a group of substitutions) and we apply s_j to V_1, getting V_{s_j}, and follow this by s_k, we get V_{s_i}. With k fixed and the values 1, a, ...n! for j, i will take the same values in some new order so that s simply permutes $V_1, V_{s_2}\ldots\ldots\ldots V_{s_{n!}}$ amongst themselves. Thus the elementary symmetric functions of V_s' found in P(y) are symmetric functions of $x_1, x_2, x_3 \ldots\ldots\ldots x_n$, and hence they are integral rational functions of the co-efficients of the original equation in x. They are also of course, integral rational functions of the m's. Thus the co-efficients of the various powers of y in P(y) are quantities in the field F under consideration. If P(y) is reducible in F, let G(y) be that factor, itself irreducible in F, for which $G(V_1) = 0$. If P(y) is irreducible in F then $G(y) = P(y)$. The equation $G(y) = (y - V_1)(y - V_2) \ldots\ldots (y - V_k) = 0$ is called a Galois resolvent of the given equation for the field F. The Galois resolvent again is different for different fields. The equation $x^3 + x^2 + x + 1 = 0$ which is known to have the roots $x_1 = -i, x_2 = i, x_3 = -1$ illustrates this.

$V_1 = m_1x_1 + m_2x_2 + m_3x_3$ with $m_1 = 0$, $m_2 = 1$, and $m_3 = -1$ gives

$V_1 = x_2 - x_3 = 1 + i$

$V_2 = x_3 - x_1 = -1 + i$

$V_3 = x_1 - x_2 = -2i$

$V_4 = x_3 - x_2 = -1 - i$

$V_5 = x_1 - x_3 = 1 - i$

$V_6 = x_2 - x_1 = 2i$

$P(y) = (y - V_1)(y - V_2)(y - V_3)(y - V_4)(y - V_5)(y - V_6)$

$= (y - \overline{1 + i})(y - \overline{-1 + i})(y + 2i)(y + 1 + i)(y - 1 + i)(y - 2i)$

$= (y - 1 - i)(y - 1 + i)(y + 2i)(y - 2i)(y + 1 - i)(y + 1 + i)$

$= (y^2 - 2y + 2)(y^2 + 4)(y^2 + 2y + 2)$.

The irreducible part of this that contains $(y - V_1)$ is

$G(y) = y^2 - 2y + 2$ or $(y - V_1)(y - V_5)$

if the field is the real numbers but if the field is that with complex numbers, then $G(y) = y - 1 - i$ or $y - V_1$. In order to show that the substitutions of the x's which change the V's into one another form a group of the given equation for the given field, it is necessary to prove the following theorem which I am taking from "Modern Algebraic Theories" by L. E. Dickson.

"Let $\phi(x_1, \ldots\ldots\ldots x_n)$ be any polynomial, with co-efficients in a field F, in the roots x_i of an equation with co-efficients in F. Let s be any substitution on the roots and let it replace ϕ by ϕ_s and V_1 by V_s where V_1 is the n! valued Galois function with integral co-efficients. Then $\phi_s = \frac{\lambda(V_s)}{P'(V_s)}$ where λ is a polynomial with co-efficients in F while P' is the derivative of the polynomial.

$P(y) = (y - V_1)(y - V_2) \ldots\ldots\ldots\ldots\ldots\ldots (y - V_{n!})$ whose co-efficients belong to F whence $P'(V_s) \neq 0$. Thus ϕ_s is the same rational function $\rho(V_s)$ of V_s that $\phi \equiv \phi_1$ is of V_1." If $s_j s_k = s_i$, then s_k replaces ϕ_{s_j} by ϕ_{s_i}. Thus s_k permutes $\phi_1, \ldots\ldots\ldots \phi_{n!}$ in the same manner that it permutes $V_1, \ldots\ldots\ldots V_{s_{n!}}$. Hence the terms of

$$\lambda(y) = \phi_1 \frac{P(y)}{y - V_1} + \phi_{s_2} \frac{P(y)}{y - V_2} + \ldots\ldots\ldots\ldots\ldots\ldots \phi_{s_{n!}} \frac{P(y)}{y - V_{s_{n!}}}$$

are merely permuted amongst themselves by any substitution on $x_1, x_2, \ldots\ldots\ldots x_n$. Thus the co-efficients of $\lambda(y)$ are rational

integral symmetric functions of $x_1, x_2, \ldots\ldots x_n$ with co-efficients in the field F, and hence are equal to quantities in F. Taking $y = V_s$, we obtain $\lambda(V_s) = \phi_s P'(V_s)$ since all the fractions $\phi_i \frac{P(y)}{y - V_i}$ will have the factor $y - V_s = 0$ except $\phi_s \frac{P(y)}{y - V_s}$ which equals $\phi_s P'(V_s)$ when V_s has been substituted for y.

$$\therefore \lambda(V_s) = \phi_s P'(V_s)$$

$$\therefore \phi_s = \frac{\lambda(V_s)}{P'(V_s)}.$$

Now let the roots of the Galois resolvent $G(y) = 0$ of degree g be $V_1, V_a, V_b \ldots\ldots\ldots V_p$ where 1, a, b.....p indicate the substitutions by which the different V's are obtained from V_1. Then 1, a, b .....p form a group G(the group of the given equation for the given field). We must show that the product of any two of them is equal to one of them.

Let $V_r = \frac{\lambda(V_1)}{P'(V_1)}$ where $V_r = \phi$ in the foregoing. Then $V_{rs} = (V_r)_s = \frac{\lambda(V_s)}{P'(V_s)}$.

We suppose V_r is one of the roots of $G(y) = 0$, then the equation $G\left(\frac{\lambda(y)}{P'(y)}\right) = 0$ is satisfied when $y = V_1$. Multiply by the gth power of $P'(y)$ and we obtain a polynomial $H(y)$ which vanishes for $y = V_1$. Since $G(y) = 0$ is irreducible, any root V_s of $G(y) = 0$ is a root of $H(y) = 0$, and since $P'(V_s)$ is not zero, we may divide $H(V_s)$ by the gth power of $P'(V_s)$ and get $0 = G\left(\frac{\lambda(V_s)}{P'(V_s)}\right) = G(V_{rs})$ hence V_{rs} is one of the roots of $G(y) = 0$.

Returning to the illustration $x^3 + x^2 + x + 1 = 0$, for which $G(y) = 0$ or $(y - V_1)(y - V_5) = 0$ had roots V_1 and V_5 in the field of real numbers, the group is $\{I, (x_1, x_5)\}$, but in the field of

complex numbers for which $G(y) = 0$ or $y - V_1 = 0$, the group is the identity.

Two very important properties of the group G of a given equation follow. The first is

A. "If a rational function, with co-efficients in the field F, of the roots of an equation with co-efficients in F remains unaltered in value by all the substitutions of the group G of the equation for F, it is equal to a quantity in F".

A rational function of the roots of the equation may be expressed in the form $\frac{\phi}{\psi}$ where, as in the theorem on page 53 $\phi \equiv \phi_1 = \frac{\lambda(V_1)}{P'(V_1)}$, and when we express $\psi \equiv \psi_1$ in the form $\frac{\mu(V_1)}{P'(V_1)}$. In ψ_s we must restrict the co-efficients of the polynomial μ so that $\psi_1 \neq 0$. If s is any substitution of the group of substitutions 1, a, b, ...p, then $\psi_s \neq 0$, for if V_s is a root of $\mu(y) = 0$, then so is V_1, in virtue of the irreducibility of the Galois resolvent $G(y) = 0$. Hence $\frac{\phi_s}{\psi_s} = \frac{\lambda(V_s)}{\mu(V_s)}$ $(s = 1, a, b, \ldots p)$ are defined for each substitution s of the Group G.

Suppose that $\frac{\phi}{\psi}$ is unaltered in value by all these substitutions, then

$$\frac{\phi}{\psi} = \frac{\lambda(V_1)}{\mu(V_1)}$$

$$\frac{\phi}{\psi} = \frac{\lambda(V_a)}{\mu(V_a)}$$

$$\vdots \qquad\qquad \vdots$$

$$\frac{\phi}{\psi} = \frac{\lambda(V_p)}{\mu(V_p)}$$

Therefore $(g)\left(\frac{\phi}{\psi}\right) = \frac{\lambda(V_1)}{\mu(V_1)} + \frac{\lambda(V_a)}{\mu(V_a)} + \cdots\cdots\cdots\cdots + \frac{\lambda(V_p)}{\mu(V_p)}$

or $\frac{\phi}{\psi} = \frac{1}{g}\left\{\frac{\lambda(V_1)}{\mu(V_1)} + \frac{\lambda(V_a)}{\mu(V_a)} + \cdots\cdots\cdots\cdots + \frac{\lambda(V_p)}{\mu(V_p)}\right\}$

the second member of which is a rational symmetric function with co-efficients in F of the roots $V_1, V_a, \ldots\ldots\ldots V_p$ of $G(y) = 0$ therefore it equals a rational function of the co-efficients of G and hence is a quantity in F, and therefore $\frac{\phi}{\psi}$ is in F and property A is proved.

The Second of these properties is the converse:

B. "If a rational function of the roots with co-efficients in F is equal to a quantity in F, it remains unaltered in value by all the substitutions of G." To prove this, let $\frac{\phi}{\psi} = r$ where r is in F. Then $\frac{\lambda(y)}{\mu(y)} - r = 0$ is satisfied by $y = V_1$, and so $\lambda(y) - r\mu(y) = 0$ for every root V_s of the resolvent equation $G(y) = 0$. Therefore $r = \frac{\lambda(V_s)}{\mu(V_s)} = \frac{\phi_s}{\psi_s}$ where $s = 1, a, b \ldots\ldots p$ so that $\frac{\phi}{\psi}$ is unaltered by all the substitutions of G.

To illustrate properties A and B with the equation $x^3 + x^2 + x + 1 = 0$, let us use the function $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$. This expression equals $\sqrt{18bcd - 4b^3d + b^2c^2 - 4c^3 - 27d^2}$ for any cubic equation $x^3 + bx^2 + cx + d = 0$ and is relatively easily found. For our equation, this is $\sqrt{-16}$. This equals a quantity in the field of complex numbers and so, by property B, remains unaltered by all the substitutions of the group of the equation for the complex field. If we try all the substitutions I, (12), (13), (23), (123), (132) we find that only three of them, i.e. 1, (123), and (132) leave the function unaltered, hence the group for the complex field is no greater than I, (123), (132) but might be only the identity I. Try another function of the roots, say x_1. The equation under consideration

has one rational root $X_1 = -1$, and two complex roots, so that the substitutions (123) and (132) alter the function X_1, and therefore by property B, again, (123) and (132) are not in the group for the complex field, which thus consists of I alone. In the field of real numbers however, the group is seen to be I, (23), on working with the same functions. In general, adjoining further elements such as i in this case, reduces the group of the equation.

It is interesting to note that it is immaterial which of a number of functions of the roots is used to determine the group of the equation. First, if property A holds for a group $H = 1, r, \ldots\ldots\ldots m$, the co-efficients of $\phi(y) = (y - V_1)(y - V_r) \ldots\ldots\ldots\ldots (y - V_m)$ being symmetric functions of $V_1, V_r \ldots\ldots\ldots V_m$ are not altered by the substitutions of H and therefore are equal to quantities in F. The equation $\phi(y) = 0$ has one root V_1 of the irreducible equation $G(y) = 0$, therefore it has all the roots $V_1, V_a, V_b \ldots\ldots\ldots V_p$ of $G(y) = 0$, so we see that $G = 1, a, b, \ldots\ldots\ldots p$ occur amongst the substitutions $1, r, \ldots\ldots\ldots m$ of H and G is a subgroup of H.

Again, let $K = 1, p, \ldots\ldots\ldots t$ be a group for which property B is true. The Galois function $G(V_1)$ is equal to zero in F and is unaltered in value by the substitutions of K, therefore $G(V_1) = G(V_p) = \ldots\ldots\ldots\ldots\ldots = G(V_t) = 0$ and $V_1, V_p, \ldots\ldots, V_t$ occur amongst the roots of $G(y) = 0$ and K is a subgroup of G. The two properties evidently hold simultaneously if $H = K = G$ and the group of the equation is unique. The functions by which it can be determined are said to belong to the group.

If a given function belongs to a subgroup H of index μ, there are μ conjugate functions. There are μ substitutions belong-

ing to the group which will carry the given function into each of its conjugates. For example, the function $\psi_1 = x_1 x_2 + x_3 x_4$ belongs to the subgroup $H_1 = G_8$ and $\psi_2 = x_1 x_3 + x_2 x_4$ and $\psi_3 = x_1 x_4 + x_2 x_3$ belong to the subgroups H_2 and H_3. ψ_2 can be obtained from ψ_1 by the substitution (234) and ψ_3 from ψ_1 by the substitution (243). The set of substitutions such that to any substitution of the group on the letters $x_1, x_2, \ldots\ldots\ldots x_n$, there corresponds one definite substitution on the letters of one of the conjugates is called the group Γ. In the example above, it is $\Gamma = [I, (234), (243)]$

If H is an invariant subgroup of G of prime index, the group Γ is a transitive group of order n on n letters and therefore is a regular group. A group is said to be transitive if, for each element of the group, we can find substitutions in the group which replace this element by each of the other elements in the group. The group $G_3 = [I, (123), (132)]$ is a transitive group of order three on three letters, for I replaces x_1 by x_1, (123) replaces x_1 by x_2, (132) replaces x_1 by x_3 etcetera. The symmetric group on n letters is transitive but is not regular if $n > 2$. Let H be the subgroup containing all the substitutions of G that leave one element x_1 unaltered. Since the group is transitive, there will be a substitution s_2 say, which carries x_1 into x_2. This substitution, applied to all the substitutions in H must give a new set of substitutions, H_{s_2} having exactly as many members as H each of which is different from all the members of H. This process can be continued till we have

$G = H + H_{s_2} + H_{s_3} + \ldots\ldots\ldots\ldots + H_{s_{n-1}}$ where the number of elements is nx. It is readily seen that every substitution of the group is in one of the H_{s_i} so that the order of the group is divisible

by n.

Further if an equation is irreducible in a field F, its group for F will be transitive, and conversely. Suppose that the group G for $f(x) = 0$, irreducible in F, is intransitive and contains substitutions replacing x_1 by $x_1, x_2, \ldots\ldots x_m$, but none replacing x_1 by the later terms $x_{m+1} \ldots\ldots\ldots\ldots x_n$. Consider some one substitution s of G replacing x_i by x_j $(i \leq m)$. G contains a substitution t replacing x_1 by x_i and therefore a substitution ts replacing x_1 by x_j with $j \leq m$ and the $x_1, x_2, \ldots\ldots\ldots x_m$ are simply permuted amongst themselves by s, and any symmetric function of $x_1, x_2, \ldots\ldots x_m$ is unaltered. Therefore, by property A, the co-efficients of x in $g(x) = (x - x_1)(x - x_2) \ldots\ldots\ldots (x - x_m)$ are in F and f(x) is seen to have the factor g(x), and it is established that if the group is intransitive, the equation is reducible. Conversely, let G be transitive and f(x) be reducible in F. Then f(x) has some factor g(x) of degree m $(m < n)$ such that $g(x) = 0$ has the root x_1 and since g(x) is equal to zero (in F) it is, by property B, unaltered in value by every substitution of G. Since G is transitive, x_1 can be replaced by any x_i giving $g(x_i) = 0$ for all $i \leq n$, in contradiction to our assumption that $m < n$. To illustrate, I will find the group of the equation $x^3 - 3x + 1 = 0$ for the field of rational numbers. The equation is irreducible in this field, because if it had been reducible, it would have had to have at least one linear factor, and neither of the two possibilities $x+1$ and $x - 1$ are factors. The function $\psi = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ is the square root of the discriminant of the equation and is equal to ± 9 (in the rational

field) but only to either +9 or to -9. Any transposition of x_1, x_2, x_3 changes ψ into $-\psi$ and so alters ψ and therefore the transposition is not in G, by property B. That is (12), (13), and (23) are not in the group which therefore consists of $\{I, (123), (132)\}$. Thus we have a transitive group as the group of the irreducible equation $x^3 - 3x + 1 = 0$.

One other expression that will be used later is "quotient group". If H is an invariant subgroup of G, of index μ, the quotient group is designated G/H. It is of order μ, which is the result of dividing the order of G by the order of H. As an example, we consider as above $\psi = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$, which belongs to G_3 [i.e. is unchanged under the substitutions of $G_3 = \{1, (123), (132)\}$] and which takes a second value $\psi_2 = -\psi$ under G_6; then G_6/G_3 is the group $\Gamma = \{I, (\psi, \psi_2)\}$. Further, a simple group is one which has no invariant subgroup except itself and the identity. Otherwise, it is composite. It is seen that a quotient group is simple, since in the operation G/H, the subgroup H must be invariant or self conjugate and if Γ had a subgroup other than the identity, then the substitutions of the subgroup of Γ applied to H would give different results from those of the substitutions of Γ not contained in the subgroup of Γ, contrary to the hypotheses that H is invariant. And now we are ready to attack the statement that "a group is called solvable if its factors of composition are all prime, otherwise insolvable."

The solution of an equation with the group G for any given field can be reduced to the solution of a series of equations, each having a simple regular group for the field obtained by adjoining to the field of the previous one a root of one of the

earlier equations of the series; or in other words, if G is a solvable group, each auxiliary equation has a regular cyclic group of prime order. If we begin with the group G of the given equation for the given field, we can find a series G, H, K, ..., I, such that each is a maximal invariant subgroup of the preceding one, and ending with the identity group. If ν is the index of H under G, and we construct a rational function ψ of the roots with co-efficients in the field and such that ψ belongs to the subgroup H of G, then ψ will be a root of an equation of degree ν whose group Γ is simply isomorphic (i.e. there is a one-to-one correspondence between products) with the simple quotient group G/H. Enlarge the field by the adjunction of the root ψ and the group will be reduced to the subgroup H. This process is continued until the identity group is reached. The field then contains all the roots of the equation, for any one root, say x_1, is unchanged by the substitution of the group, namely I, and, by property A, is in the field. If in each case the index is prime, each auxiliary equation will be of prime degree.

It is now necessary to show that any equation with a regular cyclic group of prime order p is solvable by radicals, when the field contains an imaginary pth root of unity, ρ. Let x_0, x_1, x_2, ..., x_{p-1} be the roots of the given equation and let the group be generated by the substitution

$s = (x_0, x_1, x_2, \ldots\ldots, x_{p-1})$. Construct the function

$$r_i = x_0 + \rho^i x_1 + \rho^{2i} x_2 + \rho^{3i} x_3 + \ldots\ldots\ldots\ldots + \rho^{(p-1)i} x_{p-1}$$

with co-efficients in the given field. The substitution s replaces r_i by $\rho^{-i} r_i$ $\left[\text{i.e. } (r_i)_s = x_1 + \rho^i x_2 + \rho^{2i} x_3 + \ldots\ldots\ldots + \rho^{(p-1)} x_p \right.$

$\left. = x_1 + \rho^i x_2 + \rho^{2i} x_3 + \ldots\ldots\ldots + \rho^{-i} x_0 \right]$.

Let $v_i = (r_i)^p$. Then v_i is unaltered by s for v_i becomes $(\rho^{-i} r v_i)^p = (r_i)^p$ and v_i is therefore in the given field so r_i is one of the pth roots $\sqrt[p]{v_i}$ of a quantity in the field. The given function is as follows for $i = 1, 2, \ldots\ldots\ldots, p-1$

$$r_0 = x_0 + x_1 + x_2 + x_3 + \ldots\ldots\ldots + x_{p-1} = c$$

$$r_1 = x_0 + \rho x_1 + \rho^2 x_2 + \rho^3 x_3 + \ldots\ldots\ldots + \rho^{p-1} x_{p-1} = \sqrt[p]{v_1}$$

$$r_2 = x_0 + \rho^2 x_1 + \rho^4 x_2 + \rho^6 x_3 + \ldots\ldots\ldots + \rho^{2(p-1)} x_{p-1} = \sqrt[p]{v_2}$$

$$r_3 = x_0 + \rho^3 x_1 + \rho^6 x_2 + \rho^9 x_3 + \ldots\ldots\ldots + \rho^{3(p-1)} x_{p-1} = \sqrt[p]{v_3}$$

$$\vdots$$

$$r_{p-1} = x_0 + \rho^{p-1} x_1 + \rho^{2(p-1)} x_2 + \rho^{3(p-1)} x_3 + \ldots\ldots + \rho^{(p-1)^2} x_{p-1} = \sqrt[p]{v_{p-1}}$$

Multiplying these equations by $1, \rho^{-1}, \rho^{-2}, \ldots\ldots, \rho^{-(p-1)}$ we get

$$r_0 = x_0 + x_1 + x_2 + x_3 + \ldots\ldots\ldots + x_{p-1} = c$$

$$\rho^{-1} r_1 = \rho^{-1} x_0 + x_1 + \rho x_2 + \rho^2 x_3 + \ldots\ldots\ldots + \rho^{p-2} x_{p-1} = \rho^{-1} \sqrt[p]{v_1}$$

$$\rho^{-2} r_2 = \rho^{-2} x_0 + x_1 + \rho^2 x_2 + \rho^4 x_3 + \ldots\ldots\ldots + \rho^{2(p-2)} x_{p-1} = \rho^{-2} \sqrt[p]{v_2}$$

$$\rho^{-3} r_3 = \rho^{-3} x_0 + x_1 + \rho^3 x_2 + \rho^6 x_3 + \ldots\ldots\ldots + \rho^{3(p-2)} x_{p-1} = \rho^{-3} \sqrt[p]{v_3}$$

$$\vdots$$

$$\rho^{-(p-1)} r_{p-1} = \rho^{-(p-1)} x_0 + x_1 + \rho^{(p-1)} x_2 + \ldots\ldots\ldots + \rho^{(p-1)(p-2)} x_{p-1} = \rho^{-(p-1)} \sqrt[p]{v_{p-1}}$$

Summing these, the result is

$$x_0 (1 + \rho^{-1} + \rho^{-2} + \rho^{-3} + \ldots\ldots\ldots + \rho^{-(p-1)}) + p x_1 +$$
$$x_2 (1 + \rho + \rho^2 + \rho^3 + \ldots\ldots\ldots + \rho^{(p-1)}) +$$
$$x_3 (1 + \rho^2 + \rho^4 + \rho^6 + \ldots\ldots\ldots + \rho^{2(p-1)}) + \ldots\ldots\ldots +$$
$$x_{p-1} (1 + \rho^{p-2} + \rho^{2(p-2)} + \ldots\ldots\ldots + \rho^{(p-2)(p-1)}) =$$
$$c + \rho^{-1} \sqrt[p]{v_1} + \rho^{-2} \sqrt[p]{v_2} + \ldots\ldots\ldots + \rho^{-(p-1)} \sqrt[p]{v_{p-1}}.$$

Since, from the theory of numbers, $1 + \rho^t + \rho^{2t} + \ldots\ldots\ldots + \rho^{(p-1)t} = 0$ when p is a prime, for $t = 1, 2, \ldots\ldots, p-1$, then the above result becomes $px_1 = c + \rho^{-1} \sqrt[p]{v_1} + \rho^{-2} \sqrt[p]{v_2} + \ldots\ldots + \rho^{-(p-1)} \sqrt[p]{v_{p-1}}$.

or $x_1 = \frac{1}{p}\left\{c + \rho^{-1}\sqrt[p]{V_1} + \rho^{-2}\sqrt[p]{V_2} + \rho^{-3}\sqrt[p]{V_3} + \cdots\cdots + \rho^{-(p-1)}\sqrt[p]{V_{p-1}}\right\}$

$x_1, x_2, \ldots\ldots, x_{p-1}$ can be found similarly by multiplying the expressions for $r_0, r_1, r_2 \ldots\ldots\ldots r_{p-1}$ by $1, \rho^{-j}, \rho^{-2j}, \rho^{-3j}, \ldots$ $\ldots\rho^{-(p-1)j}$ where j has the values 2, 3, $\ldots\ldots$p - 1 instead of 1 as in the case worked out to find the value of x_1.

$\therefore x_j = \frac{1}{p}\left\{c + \rho^{-j}\sqrt[p]{V_1} + \rho^{-2j}\sqrt[p]{V_2} + \cdots\cdots + \rho^{-(p-1)j}\sqrt[p]{V_{p-1}}\right\}$

As the x's are distinct by hypothesis, the V's are not all zero. Some certain r_i is not zero, and let us consider it as r_1. The substitution s then determines the other roots. We have thus obtained expressions in terms of radicals for the roots of an equation with a regular cyclic group of prime order, but it must be noted that the work just given definitely requires that one be able to find the pth roots of unity, which is done by solving the cyclotomic equation $x^{p-1} + x^{p-2} + x^{p-3} + \cdots\cdots\cdots + x + 1 = 0$ where p is an odd prime. This equation is irreducible, for if it were not, suppose that it had factors $f(x) = \phi(x)\cdot\psi(x)$. Let $x = 1$, then $f(x) = p = \phi(1)\cdot\psi(1)$ and as p is prime, either $\phi(1)$ or $\psi(1)$, say $\psi(1)$ must be ± 1. All the roots $\rho, \rho^2, \rho^3 \ldots$ $\ldots\ldots\ldots\rho^{p-1}$ of f(x) satisfy $\phi(x)\cdot\psi(x) = 0$, therefore $\phi(x)$ vanishes for at least one of these values.

$\therefore \phi(\rho)\cdot\phi(\rho^2)\cdot\phi(\rho^3)\ldots\ldots\ldots\ldots\ldots\cdot\phi(\rho^{p-1}) = 0$

or a function

$P(x) = \phi(x)\cdot\phi(x^2)\cdot\phi(x^3)\ldots\ldots\ldots\ldots\cdot\phi(x^{p-1}) = 0$

for any one of the roots of $f(x) = 0$. Hence $P(x) \equiv f(x).q(x)$. Again letting $x = 1$, we get $P(1) = \left[\phi(1)\right]^{p-1} = (\pm 1) = p.q(1)$, which is impossible, therefore the cyclotomic equation is irreducible in the field of rational numbers.

Returning to the problem of solving

$x^{p-1} + x^{p-2} + x^{p-3} + \ldots\ldots + x + 1 = 0$ which is obtained from $x^p - 1 = 0$ by dividing by $x - 1 = 0$, we use the fact from the theory of numbers that there exists a number g such that the roots $\rho, \rho^2, \rho^3, \ldots\ldots, \rho^{p-1}$ may be arranged in the order $\rho, \rho^g, \rho^{g^2}, \rho^{g^3}, \ldots\ldots, \rho^{g^{p-2}}$ because the integers $1, g, g^2, g^3, \ldots\ldots g^{p-2}$ when divided by p give the numbers 1, 2, 3, ...p - 1 in some order. If $x_1 = \rho$, $x_2 = \rho^g$ $x_3 = \rho^{g^2}$, $x_4 = \rho^{g^3}, \ldots\ldots, x_{p-1} = \rho^{g^{p-1}}$ then $x_2 = x_1^g$, $x_3 = x_2^g$, $x_4 = x_3^g, \ldots\ldots, x_{p-1} = x_{p-2}^g$ and since $g^{p-1} \equiv 1 \pmod p$, $x_p = (x_{p-1})^g =$ will equal x_1.

Consider any substitution s of the group of the cyclotomic equation $s = \begin{pmatrix} x_1, & x_2, & x_3, \ldots\ldots, & x_{p-1} \\ x_a, & x_b, & x_c, \ldots\ldots & x_l \end{pmatrix}$

we have $x_2 = x_1^g$ $\therefore$ $x_b = x_a^g$. (By property B, if a rational function of the roots equals a number in the field, it remains unaltered in value by all the substitutions of the group) and $x_c = x_b^g, \ldots\ldots, x_a = x_l^g$.

But, likewise from the fact that $x_i = x_{i-1}^g$ above, $x_{a+1} = x_a^g$ and therefore $x_b = x_{a+1}$ (both equal to x_a^g)

$x_c = x_{b+1}, \ldots\ldots, x_a = x_{l+1}$ and obviously $b \equiv a + 1$, $c \equiv b + 1 \equiv a + 2 \pmod{p - 1}$ so the substitution may be written

$$s = \begin{pmatrix} x_1, & x_2, & x_3, & x_4, \ldots\ldots, & x_{p-1} \\ x_a, & x_{a+1}, & x_{a+2}, & x_{a+3}, \ldots\ldots, & x_{a+p-2} \end{pmatrix}$$

where x_{k+p-1} is replaced by x_k since $k + p - 1 \equiv p \pmod{p - 1}$. It is therefore seen that the substitution s is the a - 1 power of $(x_1\ x_2\ x_3 \ldots\ldots x_{p-1})$ as can be readily verified by putting a = 3, say, in the substitution s just given. s was any substitution of the group G, therefore G is a subgroup, not necessarily a

proper subgroup, of the cyclic group generated by (x_1 x_2 x_3 ..... x_{p-1}). The cyclotomic equation being irreducible, G will be transitive and therefore we can say that if p is an odd prime, the group, for the field of rational numbers, of the cyclotomic equation whose roots are the pth roots of unity, is a regular cyclic group of order p - 1. Too, one of the pth roots of unity can always be found, and the others are successive powers of the one root.

An equation having a regular cyclic group of prime order p for any field F is solvable by radicals relatively to that field. Let C(x) = 0 be an equation having a regular cyclic group. Adjoin to F an imaginary pth root of unity ϵ . When any element, not in a given field (not obtainable from elements in the field by addition, subtraction, multiplication or division) is adjoined to the field, the field is enlarged, as any sum, difference, product or quotient of this new element with itself or the original elements will be in the field. When the field has been enlarged by the adjunction of ϵ , the group of C(x) = 0 is either the original cyclic group or the identity group. Since the order was prime, there is no other possibility. If the group of C(x) =0 is cyclic, C(x) = 0 is solvable in (F, ϵ) as was shown on page 61 . If the group of C(x) = 0 is the identity group, the roots are in (F, ϵ) and so can be found from the quantities in F by rational operations and root extractions, the index of each root extraction being a prime divisor of p - 1 which is the order of the cyclotomic group of the cyclotomic equation for the pth roots of unity.

This completes the sufficient condition for the solvability of an equation. If its group is cyclic, it can be solved, whether

the group is of prime order, or not. If it is not of prime order then it will have factors of composition which are the prime factors of its order and it will end in a cyclic group of prime order. Also if the group of the equation has a series of factors of composition, such that each subgroup is of prime index and ending in the identity group, it is solvable. In the latter case, there is a series of auxiliary equations, each of prime degree, which will have regular cyclic groups of prime order, and hence each is solvable. These roots are adjoined to the field and the next auxiliary equation is solved, until the field containing the roots of the given equation is reached.

The next task is to show that it is a necessary condition, that for an equation to be solvable by radicals, its group must be a solvable group; that is, that its group must be a regular cyclic group or have a series of prime composition factors leading to the identity. By hypothesis, the roots $x_1, x_2, \ldots\ldots, x_n$ must be able to be found by rational operations and root extractions from the quantities in the field $F = (F, k_1, k_2, k_3, \ldots\ldots\ldots k_m)$, where $k_1, k_2, k_3, \ldots\ldots\ldots, k_m$ are the roots of the m auxiliary equations. If ψ is a rational function, of the roots of the equation, that belongs to the subgroup H of G of index u, then ψ is the root of an equation of degree u with co-efficients in F whose group is isomorphic with the quotient group G/H. Let k_1 be the root ψ. Similarly $k_2, k_3, \ldots\ldots\ldots, k_m$ are the roots of the other auxiliary equations. The index of each root extraction may be assumed to be prime for otherwise, it can be considered as two or more extractions of prime index performed in succession. If $\xi, \eta, \ldots\ldots, \psi$ stand for the radicals in the expressions for $x_1, x_2, \ldots\ldots, x_n$

the procedure may be set forth by the series of binomial equations

(1) $\xi^{\lambda} = L, \quad \eta^{\mu} = M, \ldots\ldots\ldots, \psi^{\alpha} = S$

where L is a rational function of $k_1, k_2, \ldots\ldots, k_m$; M is a rational function of $\xi, k_1, k_2, \ldots\ldots, k_m$ and so on, with S a rational function of $(\ldots\ldots\ldots\ldots\eta, \xi, k_1, k_2, \ldots\ldots, k_m)$. Hence consider a binomial equation of prime degree p,

(2) $x^p - A = 0$ where A is in the field F. Let ϵ be an imaginary pth root of unity. If one root r of (2) belongs to the field $F' = (F, \epsilon)$, then all the other roots $\epsilon r, \epsilon^2 r, \ldots\ldots\ldots, \epsilon^{p-1} r$ belong to F' and the group of (2) for F' is the identity. On the other hand, if A is not the pth power of a quantity in F', (2) will not be reducible. Here the roots can be denoted $x_2 = \epsilon x_1$, $x_3 = \epsilon x_2, \ldots\ldots, x_p = \epsilon x_{p-1}, x_1 = \epsilon x_p$. By reasoning like that on the cyclotomic equation, it is found that the group of (2) for F' is a subgroup of the cyclic group generated by $(x_1 x_2 \ldots\ldots x_p)$ but (2) being irreducible, its group is transitive and therefore of order $\geq p$ and so it is the regular cyclic group of order p. Thus the binomial equations (1) are equivalent to a series of equations of prime degrees, each with a regular cyclic group,

$\phi(y; k_1, k_2 \ldots\ldots, k_m) = 0$ for field $F(k_1, k_2, \ldots\ldots\ldots, k_m)$

$\psi(z; y, k_1, k_2, \ldots\ldots, k_m) = 0$ for field (y, F)

$\ldots\ldots\ldots\ldots$

$\theta(w; \ldots\ldots z, y, k_1, k_2, \ldots\ldots, k_m) = 0$ for field $(\ldots\ldots z, y, F)$

Solve the first of these and adjoin its root tothe field and use for the field of the succeeding one. In this way, the field containing each root of the given equation is finally reached. The group of this equation with respect to this field is therefore the identity group.

Due to Galois (1811 - 1832) is the theorem that, by each of these adjunctions, the group of the proposed equation is either not reduced at all or else is reduced to an invariant subgroup of prime index. I have been unable to find Galois' proof of this, so must be content with deducing it from Jordan's theorem which follows.

"Let the group G_1, for a field F, of an algebraic equation $f_1(x) = 0$ be reduced to G_1' by the adjunction of all of the roots of a second equation $f_2(x) = 0$, and let the group G_2 for F of the second equation be reduced to G_2' by the adjunction of all of the roots of the first equation. Then G_1' and G_2' are invariant subgroups of G_1 and G_2 respectively, of equal indices, and the quotient groups G_1/G_1' and G_2/G_2' are simply isomorphic."

There does exist a rational function ψ_1 (with co-efficients in F) of the roots $\xi_1, \ldots\ldots, \xi_n$ of the first equation, such that ψ_1 belongs to the subgroup G_1', which is the subgroup to which the group of the equation $f_1(x) = 0$ was reduced by the adjunction of the roots $\eta_1, \eta_2, \ldots\ldots, \eta_m$ of the second equation. Therefore, by property A, ψ_1 lies in the enlarged field.

$\therefore$ (3) $\psi(\xi_1, \xi_2, \ldots\ldots, \xi_n) = \phi_1(\eta_1, \eta_2, \ldots\ldots, \eta_m)$ where ϕ is a rational function with co-efficients in F. Let the numerically distinct values which ψ_1 can assume under the substitution G_1 on the roots $\xi_1, \xi_2, \ldots\ldots, \xi_n$ be denoted by $\psi_1, \psi_2, \ldots\ldots, \psi_k$ Then G_1' is of index k under G_1. These k expressions ψ are the roots of an irreducible equation in F. Similarly for the l quantities ϕ where $\phi_1, \phi_2, \ldots\ldots, \phi_l$ are all the distinct numerical values which ϕ_1 can take under the substitutions (on $\eta_1, \eta_2, \ldots\ldots, \eta_m$) of G_2. From (3) we see that these two equations have a common root $\psi_1 = \phi_1$, and whenever two irreducible equations have one common root, they are identical, so that the roots of one correspond in

some order with the roots of the other, and therefore $k = 1$.

If s_i is a substitution of G_1 which replaces ψ_1 by ψ_i, then the group G_1' of ψ is transformed by s_i into the group of ψ_i of the same order as G_1'. Since ψ_i equals a certain ϕ, it is in the field $F' = (F, \eta_1, \eta_2, \ldots\ldots, \eta_m)$ and so is unaltered by the substitutions of the group G_1' of $f_1(x) = 0$ by property B. Hence the group to which ψ_i belongs has all the substitutions of G_1', and is of the same order and therefore is identical with G_1', and hence G_1' is invariant in G_1. Thus the group for F of the irreducible equation satisfied by ψ_1 is the quotient group G_1/G_1'.

Now let H_2 be the subgroup of G_2 to which $\phi(\eta_1, \eta_2, \ldots\ldots, \eta_m)$ belongs. It is of index k, since ϕ_1 is a root of an equation of degree $l = k$ that is irreducible in F. By the adjunction of ϕ_1 (or of ψ_1 by (3) the group G_2 of $f_2(x) = 0$ is reduced to H_2 and perhaps to a subgroup of H_2 if all the roots of the equation $f_1(x) = 0$ be adjoined as well as ψ_1 (which is a rational function of those roots) but this last is the subgroup G_2'; hence it is equal to, or contained in H_2. Now we have the result that if a group of $f_1(x) = 0$ reduces to a subgroup, of index k, on adjoining all the roots of $f_2(x) = 0$, then the group of $f_2(x) = 0$ reduces to a subgroup of index k_1, where $k_1 \geq k$, when all the roots of $f_1(x) = 0$ are adjoined. If in the foregoing result f_1 and f_2 are interchanged, it will read: if the group of $f_2(x) = 0$ reduces to a subgroup of index k_1 on adjoining all the roots of $f_1(x) = 0$, then the group of $f_1(x) = 0$ reduces to a subgroup of index k_2 where $k_2 \geq k$, but k_2 is seen to be the original k.

$\therefore\ k = k_2 \geq k_1 \geq k$ and this means that $k_1 = k_2$. Hence, as before, the subgroup G_2' is invariant in G_2. Therefore the irreducible equation in F which is satisfied by ϕ_1 has the quotient group G_2/G_2'

as its group. But the two irreducible equations were identical and so the group G_1/G_1' and G_2/G_2' must either be identical or simply isomorphic;--and now, --

Galois' theorem:--

"By the adjunction of any one root of an equation $f_2(x) = 0$ whose group for F is a regular cyclic group of prime order p, the group for F of the equation $f_1(x) = 0$ either is not reduced at all, or else is reduced to an invariant subgroup of index p." Note that if one root of $f_2(x) = 0$, which has a regular cyclic group, is adjoined, then all the roots are adjoined, for all the others are rationally expressible in terms of one. The order of the group for $f_2(x) = 0$ being prime in this case, it can be reduced only to the identity, if at all, by the adjunction of roots of $f_1(x) = 0$ and so the invariant subgroup is of prime index. If $f_1(x) = 0$ has its group reduced, it will have to be to an invariant subgroup of the same index (by Jordan's theorem) and therefore prime.

Altogether, the extraction of roots is done from binomial equations which have the identity group or a regular cyclic group of prime index. The adjunction of the roots of these binomial equations form a series of subgroups G, H, K .....and each reduction is of prime index. Hence the law that the group is solvable if and only if it is cyclic, or has a series of prime composition factors, ending in the identity, which is the only substitution leaving all the roots unchanged. For each reduction of prime index in the order of the subgroups, there is an auxiliary equation of prime degree to be solved. Thus we see that an equation is solvable if, and only if, its group for the field determined by the co-efficients is a solvable group. We are now in a

position to establish the theorem (concerning the solution of algebraic equations of degree greater than four) to which all the preceding considerations in Part B have been directed.

The general equation of degree $n > 4$ is not solvable by radicals

The group of any equation, for the field determined by its co-efficients and any constants finite in number, is the symmetric group which is of order n!, as can be readily seen from the Galois resolvent $\psi = (r - V_1)(r - V_2) \ldots\ldots\ldots\ldots (r - V_{n!})$, where the V's have been shown to be quantities in the field determined by the co-efficients. When an invariant subgroup exists, (which is self conjugate) the transform of any substitution of this subgroup is within the subgroup. Since any substitution transforms a product of k transpositions into a product of k transpositions and therefore an even substitution into an even substitution, it is seen that the substitutions of the alternating group are transposed into even substitutions of the same alternating group and hence, the latter group is self conjugate or invariant. The factors of composition for the symmetric group on n quantities are 2 and $\frac{1}{2}n!$ for the series G, H, I but $\frac{1}{2}n!$ is not prime and hence the group, and therefore the equation, is not, in general, solvable. Consider the groups for the cubic, quartic and quintic equations. Let P_n stand for the symmetric group of order n! on n letters. Let A_n stand for the alternating group of order $\frac{1}{2}n!$ on n letters. Let $5 \times (123)$ mean 5 operations of the type (123), etc. Then $P_3 \equiv I + 3 \times (12) + 2 \times (123)$ is of order six.

$A_3 \equiv I + 2 \times (123)$ is an invariant subgroup of order three and index two, which has I as its only invariant subgroup and this is of index three, so the composition factors are 2 and

3 which are primes.

Again $P_4 \equiv I + 6 \times (12) + 8 \times (123) + 6 \times (1234) + 3 \times (12)(34)$ is of order twenty four.

$A_4 \equiv I + 8 \times (123) + 3 \times (12)(34)$ is an invariant subgroup of order twelve (not a prime) and index two. This has $I + 3 \times (12)(34)$ as an invariant subgroup of order 4 and index three, since, for example $[(123)]^{-1}(12)(34)[123] \equiv (14)(23)$ etc. This in turn has $I + (12)(34)$ as an invariant subgroup of order two and index two, since for example $[(13)(24)]^{-1}(12)(34)[(13)(24)] \equiv (12)(34)$ and finally there is I as a maximal invariant subgroup of index two. Thus the factors of composition are 2, 3, 2, 2 which are primes.

Also $P_5 \equiv I + 10 \times (12) + 20 \times (123) + 30 \times (1234) + 24 \times (12345) + 15 \times (12)(34) + 20 \times (123)(45)$ is of order one hundred and twenty.

$A_5 \equiv I + 20 \times (123) + 24(12345) + 15 \times (12)(34)$ is of order sixty and index two. Now are there any invariant subgroups of A_5? A_4 is a subgroup, but it is not invariant, since for example $[(12)(35)]^{-1}(123)[(12)(35)] \equiv (152)$. Suppose, however, that such a subgroup K exists, and consider one of its substitutions, k. The subgroup K must contain the transform of k by any substitution e of P_5. Now if k contains five letters say (12345) the choice of $e = (1234)$ gives $[(1234)]^{-1}(12345)[(1234)] = (2341)$ which is not in K which is a subgroup of A_5, for it is not in A_5. If k is of the type (12)(34), the choice of $e = (12)$ gives $[(12)]^{-1}(12)(34)[(12)] \equiv (12)$, again not in K. If k is of the type (123), the choice of $e = (12)$ gives $[(12)]^{-1}(123)[(12)] \equiv (21)$ not in K, the subgroup of A_5. Thus k has been shown to be no substitution of A (except I)

so no subgroup K of A exists. Hence the group P has subgroup A with subgroup I, only, and the composition factors are 2 and 60 (not a prime). The fifth degree equation, therefore, is not, in general, solvable.

Some classes of equations of the fifth degree can be solved. For example the equation $y^5 + 5y^3 + 5y + 2 = 0$. This may be simplified as in Cardan's solution of the cubic by setting $y = z - \frac{1}{z}$, resulting in $z^5 - \frac{1}{z^5} + 2 = 0$ or $z^{10} + 2z^5 - 1 = 0$. Treating this as a quadratic we have $z^5 = -1 \pm \sqrt{2}$ and hence $z = \sqrt[5]{-1+\sqrt{2}}$ and $z = \sqrt[5]{-1-\sqrt{2}}$. Let $A = \sqrt[5]{-1+\sqrt{2}}$ and $B = \sqrt[5]{-1-\sqrt{2}}$ where A denotes a definite one of the fifth roots $\sqrt[5]{-1+\sqrt{2}}$. The others are then $\epsilon\sqrt[5]{-1+\sqrt{2}}$, $\epsilon^2\sqrt[5]{-1+\sqrt{2}}$, $\epsilon^3\sqrt[5]{-1+\sqrt{2}}$, and $\epsilon^4\sqrt[5]{-1+\sqrt{2}}$ where ϵ is an imaginary fifth root of unity. These may be written A, ϵA, ϵ^2A, ϵ^3A and ϵ^4A, and similarly we obtain B, ϵB, ϵ^2B, ϵ^3B and ϵ^4B.

Since $(-1+\sqrt{2})(-1-\sqrt{2}) = -1$, a particular fifth root $\sqrt[5]{-1+\sqrt{2}}$ may be chosen to pair with a certain $\sqrt[5]{-1-\sqrt{2}}$ so that the product is -1. Thus A and B, ϵA and ϵ^4B, ϵ^2A and ϵ^3B, ϵ^3A and ϵ^2B also ϵ^4A and ϵB may be paired. Since z_1 and z_6 give a product -1, then $z_1 = \frac{-1}{z_6}$ and similarly for the other pairs of roots of $z^{10} + 2z^5 - 1 = 0$. Now y was equal to $z - \frac{1}{z}$, so that the values of y will be

$$y_1 = A + B$$

$$y_2 = \epsilon A + \epsilon^4 B$$

$$y_3 = \epsilon^2 A + \epsilon^3 B$$

$$y_4 = \epsilon^3 A + \epsilon^2 B$$

$$y_5 = \epsilon^4 A + \epsilon B$$

which are the roots of the given equation, showing that this part-

icular fifth degree equation has been solvable.

The next task is to show that this is consistent with the results of Group Theory. It is solvable because it has a regular cyclic group of order five. Referring to the function $x_0 + \rho^i x_1 + \rho^{2i} x_2 + \cdots\cdots + \rho^{(p-1)i} x_{p-1} = r_i$ which was used in establishing the fact that a regular cyclic group of prime order was solvable.

$$
\begin{array}{l|l}
i = 0 & y_1 + y_2 + y_3 + y_4 + y_5 = 0 \\
i = 1 & y_1 + \epsilon y_2 + \epsilon^2 y_3 + \epsilon^3 y_4 + \epsilon^4 y_5 = 5B \\
i = 2 & y_1 + \epsilon^2 y_2 + \epsilon^4 y_3 + \epsilon^6 y_4 + \epsilon^8 y_5 = 0 \\
i = 3 & y_1 + \epsilon^3 y_2 + \epsilon^6 y_3 + \epsilon^9 y_4 + \epsilon^{12} y_5 = 0 \\
i = 4 & y_1 + \epsilon^4 y_2 + \epsilon^8 y_3 + \epsilon^{12} y_4 + \epsilon^{16} y_5 = 5A
\end{array}
$$

(The results 0, 5B, 0, 0, 5A are found by multiplying the known values of y_1, y_2, y_3, y_4, y_5 by the powers of ϵ indicated, and adding). The substitutions s, s^2, s^3, s^4, s^5 where $s = (12345)$ which are the same as (12345), (13524), (14253), (15432) and I, applied to the functions above leave the quantities still in the field determined by A, B and ϵ. Summing the quantities given above $5y_1 = 5B + 5A$ or $y_1 = A + B$ and y_2, y_3, y_4, y_5 are found after the cyclic substitutions are applied.

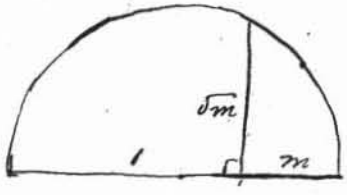
The fact, now established, that one problem may be impossible leads us to consider the others. Is it possible for example to inscribe a regular polygon of any number of sides within a circle? As shown in an earlier section, polygons of three, four, five, six, eight, ten and seventeen sides have been constructed, besides certain multiples -- for example; a 34-sided figure is readily obtained from a seventeen sided figure. Are all others possible -- or can the various polygons be classified as to which are constructible and which are not? The first stip is to establish the criterion

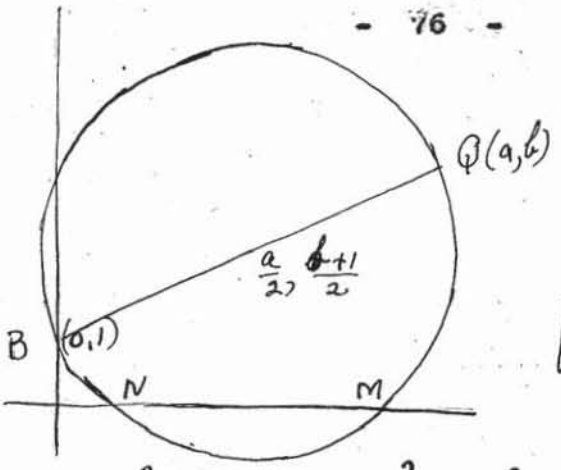
that " a proposed construction is possible by ruler and compass if, and only if, the numbers which define analytically the desired geometric elements can be derived from those defining the given elements by a finite number of rational operations, and square roots taken a finite number of times." The foregoing is a necessary condition, for if two straight lines intersect, their point of intersection is rationally expressible in terms of the co-efficients in the equations of the straight lines. If a circle $(x - d)^2 + (y - e)^2 = r^2$ and a straight line $y = mx + b$ intersect, the value $mx + b$ can be substituted for y and a quadratic equation in x results, which leads to nothing more complicated than a square root. The intersection of two circles is similar, for it is easy to obtain, by subtraction, the equation of their common chord, a straight line, and the task then resolves into the intersection of a circle and a straight line as above.

The criterion quoted gives also a sufficient condition, for the rational operations of addition and subtraction can be accomplished with a ruler, as also multiplication and division with parallel lines.

As shown, $p = ab$ since $\frac{a}{1} = \frac{p}{b}$.

Division is similar. The construction of a square root requires the compass. To find the square root of m, lay off the length m and 1 in the same straight line and use $m + 1$ as diameter. The perpendicular from the circle to the diameter at the end of m is $\sqrt{m}$ in length. Thus any construction whose algebraic expression is a quadratic equation is possible. To construct the roots of $ax^2 + bx + c = 0$, plot the points





B(0,1) and Q(a,b) and on BQ as diameter describe a circle. Its centre is $\frac{a}{2}$, $\frac{b+1}{2}$ and radius

$$\sqrt{\left(\frac{a}{2}-0\right)^2+\left(\frac{b+1}{2}-1\right)^2}=\sqrt{\left(\frac{a}{2}\right)^2+\left(\frac{b-1}{2}\right)^2}$$

Thus the equation of the circle is

$$\left(x-\frac{a}{2}\right)^2+\left(y-\frac{b+1}{2}\right)^2=\left(\frac{a}{2}\right)^2+\left(\frac{b-1}{2}\right)^2$$

At M and N, $y = 0$, hence

$$\left(x-\frac{a}{2}\right)^2+\left(-\frac{b+1}{2}\right)^2=\left(\frac{a}{2}\right)^2+\left(\frac{b-1}{2}\right)^2$$

or $$x^2-ax+\frac{a^2}{4}+\frac{b^2+2b+1}{4}=\frac{a^2}{4}+\frac{b^2-2b+1}{4}$$

or $x^2 - ax + b = 0$ and ON and OM give the values of x for which this is true. The construction of the roots of a quadratic equation was used earlier, as part Gauss' construction of the 17 sided regular polygon -- see page 29.

If to the domain of rational numbers we adjoin a quadratic surd, $(a + \sqrt{b})$, the domain also obviously includes its conjugate since an equation with rational co-efficients that has $x = a + \sqrt{b}$ for one root, also has $x = a - \sqrt{b}$ for a root; $(x - a - \sqrt{b})(x - a + \sqrt{b}) = 0$ is $x^2 - 2ax + a^2 - b = 0$. And if there are more quadratic surds in one root, it will be possible to find more conjugates to the value of the root. Thus, if the root has n distinct radicals, there will be 2^n conjugate expressions $x_1, x_2, x_3, \ldots\ldots x_{2^n}$ The equation $f(x) = (x - x_1)(x - x_2)\ldots\ldots\ldots(x - x_{2^n}) = 0$ will have only rational co-efficients, as the factors may be combined in pairs to reduce the number of surds by one, and these results combined in pairs again. The equation is of degree 2^n and is irreducible in the field of rational numbers, or is an exact power

of an equation $\phi(x)$ of lower degree, l, where l is the lowest degree possible, which is satisfied by one of the roots x_1. Divide $f(x)$ by $\phi(x)$ and let the quotient be $f_1(x)$ i.e. $f(x) = \phi(x) \cdot f_1(x) + r(x)$ [$f_1(x)$ and $\phi(x)$ are integral functions with co-efficients in the field.] Since $f(x_1) = 0$ and $\phi(x_1) = 0$ then $r(x_1) = 0$. If it is not identically zero, then it is an equation having the root x_1 of degree lower than l, and therefore contrary to hypothesis. $\therefore r(x) = 0$ identically and $f(x) = \phi(x) \cdot f_1(x)$. The same process repeated can give $f(x) = \phi(x)^k$. Therefore the degree of $f(x) = lk$, but it was previously shown to be of degree 2^n so that l is a factor of 2^n and hence, a power of 2. Therefore the unique equation of lowest degree with co-efficients in the field of rational numbers which is satisfied by a function x_1 derived from numbers of the field by a finite number of rational operations and extractions of square roots is of degree a power of 2. With this, it can be deduced that a construction is not possible with ruler and compasses if any one of the numbers which define analytically the required geometric elements satisfies an irreducible equation in the given field which is of degree other than a power of 2. Thus the inscription of a regular polygon of n sides in a circle of radius 1 is possible only when the nth roots of unity satisfy an equation $x^{2^h+1} - 1 = 0$ where h is a positive integer. We use the form $r = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ for the roots of unity. We can divide both sides of the equation $x^{2^h+1} - 1 = 0$ by $x - 1$, obtaining the irreducible equation $x^{2^h} + x^{2^h-1} + \ldots\ldots\ldots\ldots + x + 1 = 0$ which is of the degree required above. But, if h has an odd factor f [$h = fk$], then $2^h + 1$ or $2^{fk} + 1$ has the factor $2^k + 1$ and $2^h + 1$ is not a prime number. This case is considered later. Meantime if the power $2^h + 1$ is

a prime, h must have no odd factor, therefore the power must be of the form $2^{2^t} + 1$ which shown us why figures with three, five and seventeen sides can be inscribed, as can also figures of 257 and 65537 sides.

If the number of sides, n, is not a prime, but a composite number it is easy to construct a polygon having n sides, if $n = ab$ where a and b are primes of the form $2^{2^t} + 1$. First a polygon of a sides is constructed which subtends an angle of $\frac{2\pi}{a}$ at the centre, and then in a similar manner, a polygon of b sides, subtending an angle of $\frac{2\pi}{b}$. For the primes a and b there exist integers c and d for which $ca + db = 1$ and hence

$d.\frac{2\pi}{a} + c.\frac{2\pi}{b} = \frac{2\pi(ca + db)}{ab} = \frac{2\pi}{ab}$ which is the angle required at the centre to subtend each side of a regular polygon of ab sides. The process can be continued for any number of prime factors of the required form so long as they occur only to the first power.

Lastly, to investigate the construction of a polygon of p^s sides where p is a prime. From De Moivre's theorem, the equation $x^{p^s} - 1 = 0$ which has the complex root $\rho = \cos\frac{2\pi}{p^s} + i\sin\frac{2\pi}{p^s}$ ...(1)

and has the factor $x^{p^{s-1}} - 1 = 0$ since the complex root (1) is not a root of the latter $\therefore \frac{x^{p^s} - 1}{x^{p^{s-1}} - 1} = x^{p^{s-1}(p-1)} + x^{p^{s-1}(p-2)} + \ldots\ldots + 1 = 0$ ...(2)

has the root (1). This is an irreducible equation as can be established by a proof, almost the same as that for the cyclotomic equation, which can be deduced from the above if $s = 1$. For the proof, replace $\rho, \rho^2, \ldots\ldots\rho^{p-1}$ by $\rho, \rho^a, \rho^b, \ldots\ldots\rho^l$ where l, a, b .....l denote positive integers less than p^s and not divisible by p, where ρ is a primitive p^sth root of unity $(\rho, \rho^a, \rho^b, \ldots\ldots\rho^l)$ are all the primitive p^sth roots of

unity). From the theory of numbers, there exists a primitive root g of p^s (p an odd prime) i.e. an integer g such that 1, g, g^2, g^3, ... $g^{p^{s-1}(p-1)}$ when divided by p^s give in some order the integers 1, a, b .....1. Thus the roots of (2) are $\rho, \rho^g, \rho^{g^2}, \ldots \rho^{g^{p^{s-1}(p-1)}}$. These roots can be constructed with ruler and compasses if $p^{s-1}(p-1)$ is a prime which is not true if $s > 1$. Thus a regular polygon can be constructed if the number of sides is $n = 2^l p.q.r....t$ where p, q, r.....t are primes of the form $2^{2^t} + 1$. The factor 2^l really represents l bisections of angles formed from n = p.q.r.....t sides. This truth was arrived at by Gauss, but proof of only part of it was published by him.

In group theory this is explained briefly as follows. If the roots of the equation are not expressed in rational numbers, then the adjunction of a square root to the field will either not reduce the group at all or will reduce it to a subgroup of index 2. Hence the equations to be solved $x^{2^{2^t}+1} - 1 = 0$ when divided by x - 1, giving $x^{2^{2^t}} + x^{2^{2^t}-1} + \ldots\ldots\ldots + 1 = 0$ will be solvable in the field only if the subgroups can be dropped successively by the index 2, till the subgroup containing only the identity is reached which will be possible with no other prime number of sides than one of the form $2^{2^t} + 1$ or compounds made up of different factors of this form. This applies also to equation (2) and so the roots can not be expressed in rational numbers and square roots (i.e. constructed) unless $p^{s-1}(p-1)$ is a power of 2, which it cannot be for $s > 1$. Thus it is clearly and conclusively shown by the Galois' theorem that a regular figure of seven, or of nine sides cannot be constructed by ruler and compass. Note the construction of the 17 sided figure shows the use made of auxiliary quadratic

equations -- equations of index 2 of group theory.

It was shown earlier that the roots of a quadratic equation could readily be constructed with straight edge and compasses. This is not possible for a cubic equation, in general, as the roots lie in a field not made available from the rational field by the adjunction of square roots. If the cubic equation has a linear factor, the situation will be quite simple, but if the equation is irreducible, it is not possible. Some cubic equations such as $x^3 - 1 = 0$ have constructible roots as was proved by Gauss, since the power 3 is of the form $2^{2^t} + 1$ (for $t = 0$) but this, as was stated above, follows from its having a linear factor in the field of rational numbers.

The problem of the trisection of an angle is possible for certain angles, for example 90°, but is not, in general, possible. It will suffice if we show it to be impossible in one case and the standard one used for demonstrating this is the angle 120°. From trigometry $\text{Cos } 3A = 4 \text{ Cos}^3 A - 3 \text{ Cos } A$

$\therefore \text{Cos } 120^\circ = 4 \text{ Cos}^3 40^\circ - 3 \text{ Cos } 40^\circ$.

Let $\text{Cos } 40^\circ = y$, and noting that $\text{Cos } 120^\circ = -\frac{1}{2}$ we have

$$-\frac{1}{2} = 4y^3 - 3y \quad \text{or} \quad 8y^3 - 6y + 1 = 0.$$

Let $2y = x$. Then $x^3 - 3x + 1 = 0$ describes the trisecting of an angle of 120°, for if x, and hence y or $\text{Cos } 40^\circ$ can be constructed it will be easy to construct a right-angled triangle having y for base and 1 for hypotenuse, and the required angle would be found. But it is impossible to solve $x^3 - 3x + 1 = 0$, that is to get any constructible root for it has no linear factor. Incidentally another proof for the impossibility of trisection of this angle follows from the fact that it is impossible to construct a regular

polygon of 9 sides.

Treating the equation under group theory, the maximum number of substitutions on the three roots is six, namely 1, (12), (13), (23), (123), (132). The function $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ for this equation is $\pm\sqrt{-4c^3 - 27d^2} = \pm\sqrt{108 - 27} = \pm\sqrt{81} = \pm 9$ which is in the rational field; and so this function must be unchanged by all the substitutions of the group which must therefore consist of 1, (123), (132). But the adjunction of a quadratic surd cannot reduce this group to the identity because it is of index 3, and so would need a cubic surd which is not constructible with ruler and compasses. In this way, we may use the Galois' theory to show that the ancients could not have succeeded in their attempts to trisect any angle.

Doubling the cube had just as much reason to be baffling. The analytical representation of the problem is $x^3 = 2$ or $x^3 - 2 = 0$. It is irreducible in the field of rational numbers for it has no linear factor as can be proved by assuming the root $\frac{a}{b}$, a and b having no common factor;-an assumption that leads to a contradiction. An indirect proof of the impossibility of finding a constructible root of $x^3 - 2 = 0$ is as follows. Assume such a root exists, though it is not in the rational field but in some extension of the rational field made by adjunction of quadratic surds. Let it be written in the form $x = p + q\sqrt{w}$ where p, q and w belong to some field F_{k-1} (k being the least positive integer denoting the necessary extensions), but $\sqrt{w}$ does not belong to the field F_{k-1} but to F_k. Since x is in the field F_k, so is x^3 and also $x^3 - 2$, and therefore we have $x^3 - 2 = a + b\sqrt{w}$ (a and b in F_{k-1}).

$\therefore (p + q\sqrt{w})^3 - 2 = a + b\sqrt{w}$ $\left[x = p + q\sqrt{w}\right]$

or $p^3 + 3p^2q\sqrt{w} + 3pq^2w + q^3w\sqrt{w} - 2 = a + b\sqrt{w}$.

Equating the rational parts and the irrational, gives

$a = p^3 + 3pq^2w - 2$

$b = wpq^2 + q^3w$.

If $x = p + q\sqrt{w}$ is a root of an equation with rational co-efficients, it is known that $x = p - q\sqrt{w}$ must also be a root.

Then $(p - q\sqrt{w})^3 - 2$

$= p^3 - 3p^2q\sqrt{w} + 3pq^2w - q^3w\sqrt{w} - 2$

$= p^3 + 3pq^2w - 2 - (3p^2q + q^3w)\sqrt{w}$.

$= a - b\sqrt{w}$

But $x = p + q\sqrt{w}$ was a root of $x^3 - 2 = 0$ which means that $a + b\sqrt{w} = 0$ and this cannot be true unless both a and $b = 0$, for if $b \neq 0$, then $\sqrt{w} = -\frac{a}{b}$ and $\sqrt{w}$ would be in the field F_k, in which a and b lie, contrary to the assumption. Then $(p - q\sqrt{w})^3 - 2 = a - b\sqrt{w} = 0$ and $p - q\sqrt{w}$ is shown to be a second root of this equation and both of these roots are real and lie in the field F_k. This is impossible for De Moivre's work on roots of unity (and also of any rational number) shows that only one root can be real, the other two being imaginary.

$r_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$ (imaginary)

$r_2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}$ (imaginary)

$r_3 = \cos\frac{6\pi}{3} + i\sin\frac{6\pi}{3}$ (real)

Hence the assumption that a solution of $x^3 - 2 = 0$ lies in some quadratic field F_k has led to a contradiction and therefore is wrong.

This however is much more simply proved by means of the Galois' theorem. The equation $x^3 - 2 = 0$ has substitutions in its group for the field of rational numbers [1, (12), (13), (23), (123), (132)]. The only invariant subgroup of this is [1, (123), (132)] which is of index 2 under the original group and this can be reached only by the adjunction of a root of an equation whose group is a regular cyclic group of order 2, that is by a quadratic surd. But the group is now of order 3, and this can not be solved without the use of a cube root which can not be constructed with straight edge and compasses. It must be observed how elegantly the Galois theorem lays the ghost of four of the problems upon which mathematicians of all ages have been defeated. (Though tomorrow some naive person will bring forth still another "solution" of one of them.)

There remains the record of the attempts, and final success in proving the irrationality of π. The first investigation of any importance was that of J. H. Lambert in 1761. By considering $e^x = 1 + \frac{x}{1} + \frac{x^2}{\lfloor 2} + \frac{x^3}{\lfloor 3} + \ldots\ldots\ldots\ldots$ he showed that if x is a rational number, not zero, e^x can not be rational; also, if x is a rational number different from zero, tan x cannot be a rational number since $\tan x = x + \frac{x^3}{3} + \frac{x^5}{5} + \frac{x^7}{7} + \ldots\ldots\ldots$

Then if $x = \frac{\pi}{4}$, $\tan x = 1$. $\therefore \frac{\pi}{4}$ and also π cannot be rational.

That η cannot be the root of any algebraic equation with rational co-efficients was definitely proved by Louiville in 1840. Liouville Let x be a real root of the algebraic equation $ax^n + bx^{n-1} + cx^{n-2} + \ldots\ldots = 0$ with co-efficients all integers. If this equation has any equal roots, they can be removed, so consider it as having

all roots unequal, and let them be $x, x_1, x_2, x_3, \ldots\ldots, x_{n-1}$.

If $\frac{p}{q}$ be any rational fraction then

$$a\left(\frac{p}{q}\right)^n + b\left(\frac{p}{q}\right)^{n-1} + c\left(\frac{p}{q}\right)^{n-2} + \ldots\ldots\ldots\ldots$$

$$= a\left(\frac{p}{q} - x\right)\left(\frac{p}{q} - x_1\right)\left(\frac{p}{q} - x_2\right)\ldots\ldots\ldots\ldots\left(\frac{p}{q} - x_{n-1}\right)$$

or $\frac{1}{q^n}\left(ap^n + bp^{n-1}q + cp^{n-2}q^2 + \ldots\ldots\ldots\ldots\right)$

$$= a\left(\frac{p}{q} - x\right)\left(\frac{p}{q} - x_1\right)\left(\frac{p}{q} - x_2\right)\ldots\ldots\ldots\left(\frac{p}{q} - x_{n-1}\right)$$

$$\therefore \frac{p}{q} - x = \frac{ap^n + bp^{n-1}q + cp^{n-2}q^2 \ldots\ldots\ldots}{q^n(a)\left(\frac{p}{q} - x_1\right)\left(\frac{p}{q} - x_2\right)\ldots\ldots\ldots\left(\frac{p}{q} - x_{n-1}\right)}.$$

If we have a series of rational fractions converging to x as a limit, but none of them equal to x, and if $\frac{p}{q}$ be one of these fractions

$$\left(\frac{p}{q} - x_1\right)\left(\frac{p}{q} - x_2\right)\left(\frac{p}{q} - x_3\right)\ldots\ldots\ldots\left(\frac{p}{q} - x_{n-1}\right)$$

approximates to the fixed number $(x - x_1)(x - x_2)(x - x_3)\ldots\ldots\ldots(x - x_{n-1})$. We may therefore suppose for all fractions $\frac{p}{q}$, that $a\left(\frac{p}{q} - x_1\right)\left(\frac{p}{q} - x_2\right)\ldots\ldots\ldots\left(\frac{p}{q} - x_{n-1}\right)$ is numerically less than some fixed positive number A. Also $ap^n + bp^{n-1}q + \ldots\ldots\ldots$ is an integer numerically ≥ 1.

$\therefore \left|\frac{p}{q} - x\right| > \frac{1}{Aq^n}$ which must hold for all the fractions of the sequence, from and after some fixed element of the sequence for a fixed number A. If however, a number x can be defined such that no matter how far we go in the sequence and no matter how A be chosen, there exist fractions belonging to the sequence for which $\left|\frac{p}{q} - x\right| < \frac{1}{Aq^n}$, it may be concluded that x cannot be a root of an equation of degree n with integral co-efficients, and if we can show this to be the case for all values of n, we can conclude that x cannot be a root of any algebraic equation with

rational co-efficients. Consider a number

$x = \frac{k_1}{r^{1!}} + \frac{k_2}{r^{2!}} + \frac{k_3}{r^{3!}} + \cdots\cdots\cdots + \frac{k_m}{r^{m!}} \cdots\cdots\cdots$ where k_1, k_2, ...k_m .....are all integers less than the integer r, and do not all vanish after some fixed value of m, Then let

$\frac{p}{q} = \frac{k_1}{r^{1!}} + \frac{k_2}{r^{2!}} + \frac{k_3}{r^{3!}} + \cdots\cdots\cdots + \frac{k_m}{r^{m!}}$ and we have $\frac{p}{q}$ continually approaching x as m is increased i.e.

$$x - \frac{p}{q} = \frac{k_{m+1}}{r^{(m+1)!}} + \frac{k_{m+2}}{r^{(m+2)!}} + \cdots\cdots\cdots\cdots\cdots$$

$$< r\left[\frac{1}{r^{(m+1)!}} + \frac{1}{r^{(m+2)!}} + \cdots\cdots\cdots\cdots\right] \text{ since all k's} < r.$$

$$< \frac{2r}{q^{m+1}} \left[\begin{array}{l} r^{m!} = q \\ r^{(m+1)!} = (r^{m!})^{m+1} = q^{m+1} \end{array}\right]$$

Therefore no matter what values A and n have, if m and therefore q, is large enough, we have $\frac{2r}{q^{m+1}} < \frac{1}{Aq^n}$ thus the former relation $\left|\frac{p}{q} - x\right| > \frac{1}{Aq^n}$ is not satisfied for all the fractions $\frac{p}{q}$. The numbers x so defined are therefore transcendental. (Transcendental numbers are those which cannot be a root of an equation of any degree whatever where the co-efficients are rational numbers.) The above does not answer our question but does prove the existence of transcendental numbers.

In constructions with ruler and compass, points in the plane are determined by the intersection of two straight lines, the intersection of a circle and a straight line, or by the intersection of two circles, all of which can be represented by equations. In the above three cases, the straight lines can be determined by a pair of points whose co-ordinates are known, and the circles by their centres and one point on the circumference. The co-ordinates of the points of intersection are found by solving the pair of

equations that describe the lines, and these operations are either rational or involve the taking of the square root, in case one or both of the lines are circles as was stated before in connection with polygons. The co-ordinate x, of a new point may be written $x = a + b\sqrt{B} + b'\sqrt{B'} + \ldots\ldots\ldots$ or $x - a - b'\sqrt{B'} - \ldots\ldots\ldots = b\sqrt{B}$ and squaring both sides $(x - a - b'\sqrt{B'} - \ldots\ldots\ldots)^2 = b^2B$ so that one surd is eliminated and all may be, by successive applications of the same process, and a final equation results which is of degree that is some power of 2 and its co-efficients will be rational functions of the co-ordinates of the points. Whether such an equation can exist is sufficient information to determine whether the problem corresponding to it can be performed by Euclidean methods or not. Thus, if we can show that π is a transcendental number, we shall have shown that there is no possibility of constructing with ruler and compass, a line π times a given line; that is, we shall have shown the impossibility of squaring or rectifying the circle with ruler and compass.

It is necessary to prove the transcendence of e before proving that of π. The proof for e, as follows, is based on Professor D. E. Smith's account of Enrique's work (1907). To prove that e is a transcendental number means that it must be shown that e is not a root of any algebraic equation with rational co-efficients, that is, that it is impossible to have a general equation of the form $C_0 + C_1 e + C_2 e^2 + \ldots\ldots\ldots C_n e^n = 0$ where n is any positive integer and $C_0, C_1, C_2 \ldots\ldots\ldots C_n$ are rational numbers including 0. (C_0 and $C_n \neq 0$ since this would change the degree of the equation.) It is necessary to consider the function $f(x) = a_1 x + a_2 x^2 + \ldots\ldots + a_n x^n$, ...(1) the a's being rational,

and also $f(x) = \frac{x^{p-1}\left[(x-1)(x-2)\ldots\ldots\ldots(x-m)\right]^p}{(p-1)!}$ .....(2)

$\therefore\ a_1x + a_2x^2 + \ldots\ldots\ldots + a_nx^n = \frac{x^{p-1}\left[(x-1)(x-2)\ldots\ldots\ldots(x-m)\right]^p}{(p-1)!}$

from which we see that $n = p(m+1) - 1$ and that a_{p-1} is the first co-efficient that is not zero. Also we must consider the function $F(x) = f'(x) + f''(x) + \ldots\ldots\ldots + f^n(x)$. The proof depends largely upon the following three lemmas -- the proofs of which will be found in the Appendix to this theses.

$f^{(n)}(x)$
station

Lemma I. If $f(x) = a_1x + a_2x^2 + \ldots\ldots\ldots + a_nx^n$ and if S_n denotes the sum of the first n terms of the series e^x, so that $S_1 = 1$, $S_2 = 1 + x$, $S_3 = 1 + x + \frac{x^2}{2!}$ then F(x) becomes

$1!\,a_1S_1 + 2!\,a_2S_2 + 3!\,a_3S_3 + \ldots\ldots\ldots + n!\,a_nS_n$

Also $F(o) = 1!\,a_1 + 2!\,a_2 + 3!\,a_3 + \ldots\ldots\ldots + n!\,a_n$.

Lemma II. Again using (2) if p is any prime number, n any positive integer and $C_o, C_1, C_2, \ldots\ldots\ldots, C_m$ any integers, then $C_oF(o) + C_1F(1) + \ldots\ldots\ldots + C_mF(m) = C_o(m!)^p + pQ$ where Q is some integer depending upon the value of the C's and p.

Lemma III. Again using

$f(x) = a_1x + a_2x^2 + \ldots\ldots\ldots + a_nx^n = \frac{x^{p-1}\left[(x-1)(x-2)\ldots\ldots(x-m)\right]^p}{(p-1)!}$

and letting $A_1 = |a_1|$, $A_2 = |a_2|$ etc. and $X = |x|$ then

$A_1X + A_2X^2 + \ldots\ldots\ldots + A_nX^n = \frac{X^{p-1}\left[(X+1)(X+2)\ldots\ldots\ldots(X+m)\right]^p}{(p-1)!}$

In the required proof starting with $e^x = 1 + \frac{x}{1} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots\ldots\ldots\frac{x^n}{n!}$ (which is convergent for all values of x) and letting

$S_1 = 1$, $S_2 = 1 + \frac{x}{1}$, $S_3 = 1 + \frac{x}{1} + \frac{x^2}{2!}$, $S_n = 1 + \frac{x}{1} + \frac{x^2}{2!} + \ldots\ldots + \frac{x^n}{n!}$

as before, and multiplying the expansion of e^x successively by $1!, 2!, \ldots\ldots\ldots n!$ and putting

$$U_1 = x + \frac{x^2}{2} + \frac{x^3}{2.3} + \cdots\cdots\cdots$$

$$U_2 = x^2 + \frac{x^3}{3} + \frac{x^4}{3.4} + \cdots\cdots\cdots$$

$$\vdots$$

$$U_n = x^n + \frac{x^{n+1}}{n+1} + \frac{x^{n+2}}{(n+1)(n+2)} + \cdots\cdots\cdots$$

we have

$$1!\, e^x = 1!S_1 + x + \frac{x^2}{2} + \frac{x^3}{2.3} + \cdots\cdots\cdots = 1!S_1 + U_1$$

$$2!\, e^x = 2!S_2 + x^2 + \frac{x^3}{3} + \frac{x^4}{3.4} + \cdots\cdots\cdots = 2!S_2 + U_2$$

$$\vdots$$

$$n!\, e^x = n!S_n + x^n + \frac{x^{n+1}}{n+1} + \frac{x^{n+2}}{(n+1)(n+2)} + \cdots\cdots\cdots = n!S_n + U_n.$$

If we multiply both members of these last equations by $a_1, a_2, a_3, \cdots\cdots, a_n$ and add, we shall have

$$(1!a_1 + 2!a_2 + \cdots\cdots + n!a_n)e^x = (1!S_1a_1 + 2!S_2a_2 + \cdots\cdots n!S_na_n) + (a_1U_1 + a_2U_2 + \cdots\cdots + a_nU_n)$$

but Lemma I states that

$$F(x) = 1!S_1a_1 + 2!S_2a_2 + \cdots\cdots + n!S_na_n.$$

also $F(o) = 1!a_1 + 2!a_2 + \cdots\cdots + n!a_n$.

$\therefore F(o)e^x = F(x) + a_1U_1 + a_2U_2 + \cdots\cdots + a_nU_n.$

$\therefore F(o)e^x = F(x) + \psi(x)$ which is an expression for e^x which depends upon $F(x)$ and hence depends upon the choice of p in (2).

Now recall that the essential point of the problem is to prove that it is impossible that $C_o + C_1e + C_2e^2 + \cdots\cdots + C_me^m = 0$.

Take $F(o)e^x = F(x) + \psi(x)$ and substitute 1, 2, 3, $\cdots\cdots$, m for x and multiply by $C_o, C_1, C_2, \cdots\cdots$ and C_m, then add

$$F(o)e^oC_o = CF(o) + C_o\psi(o)$$

$F(0)e\,C_1 = C_1F(1) + C_1\psi(1)$

$F(0)e^2C_2 = C_2F(2) + C_2\psi(2)$

$\vdots$

$F(0)e^m C_m = C_mF(m) + C_m\psi(m)$;

that is

$F(0)\left[C_0 + eC_1 + e^2C_2 + \cdots\cdots + e^mC_m\right] = C_0F(0) + C_1F(1) + C_2F(2) + \cdots\cdots + C_mF(m) + C_0\psi(0) + C_1\psi(1) + C_2\psi(2) + \cdots + C_m\psi(m)$.

Now supposing that $C_0 + C_1e + C_2e^2 + \cdots\cdots + C_me^m = 0$ were possible we should have $0 = \left[C_0(m!)^p + pQ\right] + \left[C_0\psi(0) + C_1\psi(1) + \cdots\cdots + C_m\psi(m)\right]$ by Lemma II.

To show that this is impossible, we shall first show that $C_0(m!)^p + pQ$ is greater than, or equal to one, and that $C_0\psi(0) + C_1\psi(1) + C_2\psi(2) + \cdots\cdots + C_m\psi(m)$ is less than one.

To investigate the first part, take p a prime greater than m and not a factor of C_0, then $C_0(m!)^p$ is not divisible by p, and since C_0 is not zero, there results the fact that $C_0(m!)^p + pQ$ has an absolute value ≥ 1 since it is an integer (all the numbers C_0, m, and Q are integers, previously stated.)

To show the second part $C_0\psi(0) + C_1\psi(1) + \cdots\cdots + C_m\psi(m)$ to be less than 1, note that $\psi(x) = a_1U_1 + A_2U_2 + \cdots\cdots + a_nU_n$ and

$|\psi(x)| < A_1|U_1| + A_2|U_2| + \cdots\cdots + A_n|U_n| \cdots\cdots\cdots (a)$

$U_n = x^n\left[1 + \frac{x}{n+1} + \frac{x^2}{(n+1)(n+2)} + \cdots\cdots\cdots\right]$

Let $X = |x|$, so

$|U_n| \leq X^n\left[1 + \frac{X}{n+1} + \frac{X^2}{(n+1)(n+2)} + \cdots\cdots\cdots\right]$

$\therefore |U_n| < X^n\left[1 + \frac{X}{1!} + \frac{X^2}{2!} + \cdots\cdots\cdots\right]$

$\therefore |U_n| < X^n e^X$

$\therefore |\psi(x)| < e^X\left[A_1X + A_2X^2 + \cdots\cdots + A_nX^n\right]$

from Lemma III

$$|\psi(x)| < e^{X}.\frac{X^{p-1}\left[(X+1)(X+2)\ldots\ldots\ldots\ldots(X+m)\right]^{p}}{(p-1)!}$$

$$< e^{X}(X+1)(X+2)\ldots\ldots\ldots(X+m)\left[\frac{X(X+1)(X+2)\ldots\ldots(X+m)}{(p-1)!}\right]^{p-}$$

For any fixed value of X, we can take for p a value so large that $\left[\frac{X(X+1)(X+2)\ldots\ldots\ldots(X+m)}{(p-1)!}\right]^{p-1}$ shall be as small as we please, since it is similar to $\frac{y^{n}}{n!}$. The expression therefore approaches zero as p increases.

$\therefore |\psi(0)|, |\psi(1)|, |\psi(2)|, \ldots\ldots\ldots |\psi(m)|$

can all be made as small as we please by taking p sufficiently large, hence $C_0\psi(0) + C_1\psi(1) + \ldots\ldots\ldots + C_m\psi(m)$ can certainly be made less than unity

$\therefore \left[C_0(m!)^{p} + pQ\right] + \left[C_0\psi(0) + C_1\psi(1) + \ldots\ldots + C_m\psi(m)\right]$

cannot equal zero, since it is something ≥ 1 + something < 1, therefore the supposition $C_0 + C_1 e + C_2 e^{2} + \ldots\ldots\ldots C_m e^{m} = 0$ must be wrong. Therefore e cannot be the root of an algebraic equation.

Finally, to establish the transcendence of π. This depends upon the following three truths already established

$F(0)e^{x} = F(x) + \psi(x)$.

$$|\psi(x)| < e^{X}\frac{X^{p-1}\left[(X+1)(X+2)\ldots\ldots\ldots(X+m)\right]^{p}}{(p-1)!}$$

and $1 + e^{i\pi} = 0$ (see appendix).

If we assume π to be an algebraic number, then $i\pi$ is an algebraic number and therefore is the root of an algebraic equation with rational co-efficients. Let the roots of this equation be $y_1, y_2, y_3 \ldots\ldots\ldots y_m$, and amongst these, $i\pi$ must be found. Therefore since $1 + e^{i\pi} = 0$, we have

$(1 + e^{y_1})(1 + e^{y_2})\ldots\ldots\ldots(1 + e^{y_m}) = 0$

Therefore, on multiplying we have

$$1 + (e^{y_1} + e^{y_2} + \ldots\ldots + e^{y_m}) + (e^{y_1+y_2} + \ldots\ldots e^{y_1+y_m} + \ldots\ldots + e^{y_{m-1}+y_m}) + \ldots\ldots\ldots + (e^{y_1+y_2+\ldots\ldots y_m}) = 0 \ldots\ldots \text{equation (3)}$$

The proof of the transcendence of π consists in showing the last equation to be impossible. The symmetric functions of the quantities $y_1, y_2, \ldots\ldots, y_m$ are rational numbers and are the roots of an algebraic equation. Let $\phi(x) = 0$ represent this equation. The symmetric functions of the quantities $y_1 + y_2, y_1 + y_3, \ldots\ldots, y_{m-1} + y_m$ are also symmetric functions of y_K and therefore rational numbers, and so are roots of a second algebraic equation $\phi_1(x) = 0$ and so on until we have $y_1 + y_2 + \ldots\ldots + y_m$ the root of an algebraic equation $\phi_{m-1}(x) = 0 \therefore \phi(x).\ \phi_1(x).\ \phi_2(x)\ldots\ldots\ldots\phi_{m-1}(x)$ is an integral function of x which becomes zero as soon as x becomes equal to one of the numbers $y_1, y_2, \ldots\ldots, y_m, y_1 + y_2, y_1 + y_3, \ldots\ldots, y_{m-1} + y_m, \ldots\ldots, y_1 + y_2 + \ldots\ldots + y_m$. Some of these numbers, say N of them, may be equal to zero. If we place $\phi(x).\ \phi_1(x) \ldots\ldots\ldots \phi_{m-1}(x) = 0$ and suppress the factor x^N we have an equation $\theta(x) = 0$ which we may consider as being reduced to a form having integral co-efficients. Since the zero roots have just been suppressed, $\theta(0)$ cannot equal zero, hence $\theta(x)$ may be written $\theta(x) = ax^m + a_1x^{m-1} + \ldots\ldots + a_m = 0$ where $a, a_1, \ldots\ldots, a_m$ are integral and a and a_m are not zero and a is positive. This may be transformed by multiplying by a^{m-1} and putting z for ax, into an equation with integral co-efficients of the form $\theta(z) = z^m + b_1z^{m-1} + \ldots\ldots + b_m = 0$ where the co-efficient of the highest power is unity. Let the roots of the equation $\theta(x)$ be $x_1, x_2, x_3, \ldots\ldots\ldots$, these repres-

enting the numbers amongst $y_1, y_2, \ldots\ldots, y_m, y_1 + y_2, y_1 + y_3 \ldots\ldots, y_{m-1} + y_m, \ldots\ldots\ldots, y_1 + y_2 + \ldots\ldots + y_m$ that are not equal to zero. It is seen from equation (3) that they must satisfy the equation $K + e^{\gamma_1} + e^{\gamma_2} + e^{\gamma_3} + \ldots\ldots\ldots = 0$

Now, note the earlier relation $F(0)e^{\gamma} = F(x) + \psi(x)$. If we put x for the numbers $x_1, x_2, x_3 \ldots\ldots\ldots$ and add the results we have

$F(0)e^{\gamma_1} + F(0)e^{\gamma_2} + F(0)e^{\gamma_3} + \ldots\ldots = F(x_1) + F(x_2) + F(x_3) \ldots\ldots + \psi(x_1) + \psi(x_2) + \psi(x_3) + \ldots\ldots$ or

$F(0)\left[e^{\gamma_1} + e^{\gamma_2} + e^{\gamma_3} + \ldots\ldots\ldots\right] = F(x_1) + F(x_2) + F(x_3) + \ldots\ldots\ldots + \psi(x_1) + \psi(x_2) + \psi(x_3) \ldots\ldots\ldots$

$\therefore F(0)[-K] = F(x_1) + F(x_2) + F(x_3) + \ldots\ldots\ldots + \psi(x_1) + \psi(x_2) + \psi(x_3) + \ldots\ldots\ldots$ or

$KF(0) + F(x_1) + F(x_2) + F(x_3) + \ldots\ldots\ldots + \psi(x_1) + \psi(x_2) + \psi(x_3) + \ldots\ldots\ldots = 0$

Hermite ? If this can be proved impossible, the, clearly, the one hypotheses, that is, that π be an algebraic number, must be incorrect. This will be done in two steps: first, proving $KF(0) + F(x_1) + F(x_2) + \ldots\ldots\ldots$ to be integral and not = 0, and second, proving the other part $\psi(x_1) + \psi(x_2) + \psi(x_3) \ldots\ldots\ldots < 1$; thus the two parts could not possibly equal zero

absolute values

Consider $f(x) = \dfrac{Z^{p-1}[\theta_1(Z)]^p}{(p-1)!} = \dfrac{a^{mp-1}x^{p-1}[\theta(x)]^p}{(p-1)!}$ where p is a prime. (Note $Z = ax$, $\theta(x) = ax^m + a_1x^{m-1} + \ldots\ldots + a_m = 0$ and $\theta_1(Z) = Z^m + b_1Z^{m-1} + \ldots\ldots\ldots + b_m = 0$.) Arrange according to ascending powers of Z, thus

$[\theta_1(Z)]^p = A_0 + A_1Z + A_2Z^2 + \ldots\ldots$

$= A_0 + A_1ax + A_2a^2x^2 + \ldots\ldots\ldots$ where the A's are

integral and $A_0 = b_m^p$. Therefore

$$f(x) = \frac{A_0 a^{p-1} x^{p-1} + A_1 a^p x^p + A_2 a^{p+1} x^{p+1} + \cdots\cdots\cdots}{(p-1)!}$$

Taking derivatives of this and letting $x = 0$, we have

$$f(0) = 0,\ f'(0) = 0,\ \cdots\cdots, f^{p-2}(0) = 0$$

$$f^{p-1}(0) = \frac{(p-1)!\, A_0 a^{p-1}}{(p-1)!} = b_m^p a^{p-1}$$

$$f^p(0) = \frac{p!\, A_1 a^p}{(p-1)!} = p A_1 a^p$$

$$f^{p+1}(0) = p(p+1) A_2 a^{p+1}$$

If p, which is a prime, is chosen larger than the greatest number a, b_m, K, then $f^{p-1}(0)$ is not divisible by p while all the other derived functions are either 0, or are divisible by p.

$\left[f^{p-1}(0) = b_m a^{p-1} \right.$ and $a^{p-1} \equiv 1(p)$ (see appendix.)$\left.\right]$ Therefore $F(0)$ which is $f'(0) + f''(0) + \cdots\cdots$ is an integer not divisible by p. Therefore $K.F(0)$ is also an integer not divisible by p. Going back to $f(x) = \frac{z^{p-1}[\theta_1(z)]^p}{(p-1)!}$, we may arrange it according to ascending powers of $(z - z_K)$ where z_K is one of the roots.

$$f(x) = \frac{(z - z_K)^p B_1(z_K) + (z - z_K)^{p+1} B_2(z_K) + \cdots\cdots\cdots}{(p-1)!}$$

$$= \frac{a^p (x - x_K)^p B_1(z_K) + a^{p+1}(x - x_K) B_2(z_K) + \cdots\cdots\cdots}{(p-1)!}$$

since $z = ax$ and $B_1(z_K)$, $B_2(z_K)$ etc. are integral functions of z_K with rational co-efficients. Hence taking derivatives and letting $x = x_K$ we have $f(x_K) = 0$, $f'(x_K) = 0$, $\cdots\cdots, f^{p-1}(x_K) = 0$,

$$f^p(x_K) = \frac{(p!)\, a^p B_1(z_K)}{(p-1)!} = p a^p B_1(z_K)$$

$f^{p+1}(x_K) = p(p+1) a^{p+1} B_2(z'_K)$ but recalling that

$F(x) = f'(x) + f''(x) + \cdots\cdots\cdots + f^n(x)$

$F(x_K) = f'(x) + f''(x) + \cdots\cdots\cdots + f^p(x_K) + f^{p+1}(x_K) + \cdots\cdots$

$\ldots\ldots + f^{n}(x)$

$= 0 + 0 + \ldots\ldots + p\,a^{p}B_1(\xi_k) + p(p-1)a^{p+1}B_2(\xi_k) + \ldots\ldots$

$=$ an integral multiple of p

$\therefore F(x_1) + F(x_2) + F(x_3) + \ldots\ldots\ldots\ldots =$ an integral multiple of p since each one of $F(x_1)$, $F(x_2)$ etc. is.

Therefore $K.F(0) + F(x_1) + F(x_2) + F(x_3) + \ldots\ldots\ldots$ consists of two parts, one of which $K.F(0)$, is an integer not divisible by p, and the other $F(x_1) + F(x_2) + F(x_3) + \ldots\ldots\ldots$, which is an integer divisible by p, so their sum must be an integer not divisible by p.

The second step in our undertaking is to prove that $|\psi(x_1) + \psi(x_2) + \psi(x_3) + \ldots\ldots + \psi(x_m)| < 1$. (This proof, I received from Dr. C. Mark.)

Consider again $f(x) = \dfrac{a^{mp-1}\,x^{p-1}\,[\theta(x)]^{p}}{(p-1)!}$ with

$\theta(x) = ax^{m} + a_1x^{m-1} + \ldots\ldots\ldots + a_m$

$= a(x - x_1)(x - x_2)\ldots\ldots\ldots\ldots(x - x_m)$

then $f(x) = \dfrac{a^{(m+1)p-1}\,x^{p-1}\,[(x - x_1)(x - x_2)\ldots\ldots\ldots(x - x_m)]^{p}}{(p-1)!}$

Assume $f(x) = b_1x + b_2x^{2} + \ldots\ldots\ldots + b_nx^{n}$ where $n = (m+1)p - 1$ and taking $A = |a|$, $X = |x|$, $X_i = |x_i|$, $(i = 1, 2, \ldots\ldots m)$ and $B_i = |b_i|$, it follows, as in the proof of Lemma III, that

$B_1X + B_2X^{2} + \ldots\ldots\ldots + B_mX^{m} =$

$$\frac{A^{(m+1)p-1}\,X^{p-1}\,[(X + X_1)(X + X_2)\ldots\ldots\ldots(X + X_m)]^{p}}{(p-1)!}$$

for any value of p.

To consider now $|\psi(x_1) + \psi(x_2) + \ldots\ldots\ldots + \psi(x_m)|$, first note that $\psi(x) = b_1U_1 + b_2U_2 + \ldots\ldots\ldots + b_nU_n$ where U_i is the quantity

$$x^{i} + \frac{x^{i+1}}{i+1} + \frac{x^{i+2}}{(i+1)(i+2)} + \ldots\ldots\ldots$$

and we have already proved that $|U_n| < X^n e^X$ or $|U_i| < X^i e^X$.

Further $|\psi(x)| \leq B_1|U_1| + B_2|U_2| + \cdots\cdots + B_n|U_n|$ equation (4)

$$= e^X \left\{B_1 X + B_2 X^2 + B_3 X^3 + \cdots\cdots + B_m X^m\right\}$$

$$= e^X \left\{\frac{A^{(m+1)p-1} X^{p-1} \left[(X + X_1)(X + X_2) \cdots\cdots (X + X_m)\right]^p}{(p-1)!}\right.$$

$$= e^X A^m (X + X_1)(X + X_2) \cdots\cdots (X + X_m) \cdot \frac{A^{m+1} X \left[(X + X_1)(X + X_2) \cdots\cdots (X + X_m)\right]^{p-1}}{(p-1)!}$$

For any number X, p can be chosen so large that this expression can be made as small as we please. Then taking x in turn equal to $x_1, x_2, x_3, \ldots\ldots$ we can make each one as small as we please

$\therefore \psi(x_1) + \psi(x_2) + \cdots\cdots + \psi(x_m)$ can be made < 1 or since $\Sigma|\psi(x_i)|$ can be < 1 and since $-\Sigma|\psi(x_i)| \leq \Sigma\psi(x_i) \leq |\psi(x_i)|$ we have $\Sigma\psi(x_i)$ between -1 and 1. Hence $KF(0) + F(x_1) + F(x_2) + \cdots\cdots + \psi(x_1) + \psi(x_2) + \cdots\cdots = 0$ is impossible since the left member has been proved equal to an integer not zero, plus a quantity less than one.

Therefore it is not possible to have a function $\phi(x) \cdot \phi_1(x) \cdot \phi_2(x) \cdots\cdots$ which could be equal to zero when x is equal to one of the numbers $y_1, y_2, \ldots\ldots, y_m$, $y_1 + y_2, y_1 + y_3, \ldots\ldots, y_{m-1} + y_m, \ldots\ldots, y_1 + y_2 + y_3 + \cdots\cdots y_m$. Therefore it is impossible to find an equation $(1 + e^{y_1})(1 + e^{y_2}) \cdots\cdots (1 + e^{y_m}) = 0$ where the y's are algebraic numbers.

Since $1 + e^{i\pi}$ is $= 0$, $i\pi$ and hence π must be a transcendental number. That is π satisfies no algebraic equation with rational co-efficients and therefore cannot be constructed with ruler and compasses.

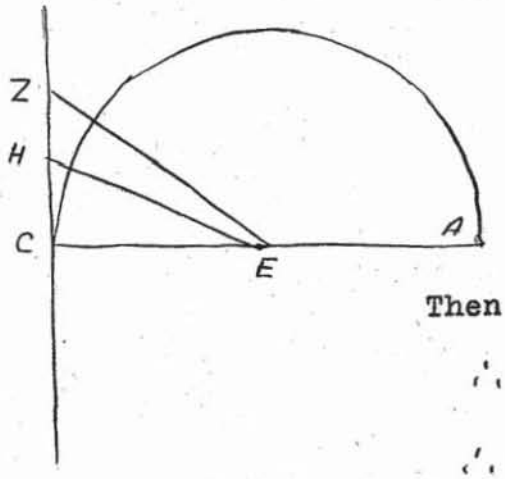
In this was, in quite recent times (the first proof of the

transcendence of π was given in (1882) one of the very early and famous mathematical problems was finally solved -- if to be shown incapable of solution may be spoken of as itself a solution. With respect to both the attaining of this solution, and the reader who reaches this point (if there be one), it may be appropriate to again recall Augustus De Morgan's famous dictum: The quality of the human mind which must impress us in its infinite patience.

Appendix 1

Archimedes Proof that $3\ 1/7 < \pi < 3\ 10/71$

(According to J. Gow "History of Greek Mathematics)



Let the circle have diameter AC with centre E. Let ZEC be one third of a right angle with Z lying on the tangent at C.

Then $EZ = 2ZC$

$\therefore EC^2 = 3ZC^2$

$\therefore \frac{EC}{ZC} = \frac{\sqrt{3}}{1} > \frac{265}{153}$

and $\frac{EC}{ZC} = \frac{2}{1} = \frac{306}{153}$

Draw EH, bisecting the angle ZEC

Then $\frac{ZE}{EC} = \frac{ZH}{HC}$

and $\frac{ZE}{ZH} = \frac{EC}{HC}$

$\therefore \frac{ZE + EC}{ZH + HC} = \frac{EC}{HC}$

$\therefore \frac{ZE + EC}{ZC} = \frac{EC}{HC}$

$\therefore \frac{265}{153} + \frac{306}{153} < \frac{CE}{HC}$

i.e. $\frac{CE}{HC} > \frac{571}{153}$

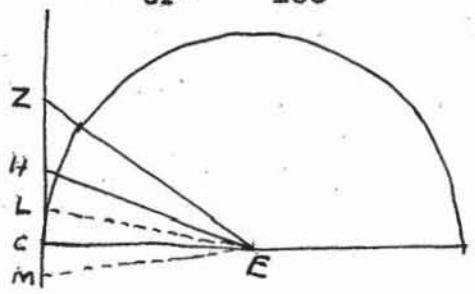
$\frac{CE^2}{HC^2} > \frac{326041}{23409}$

$\frac{CE^2 + HC^2}{HC^2} > \frac{326041 + 23409}{23409}$

$\frac{EH^2}{HC^2} > \frac{349450}{23409}$

and $\frac{EH}{HC} < \frac{591\ 1/8}{153}$

Again bisect the angle HEC by the line EP. On the same principle, $\frac{EC}{CP} > \frac{1162\ 1/8}{153}$, Proceed by further bisections until the angle LEC that is 1/48 of a right angle is reached for which



$$\frac{EC}{LC} > \frac{4673\ \frac{1}{2}}{153}$$

At E, make the angle CEM = LEC

The angle LEM = 1/24 of a right angle and the line LM is a side of a polygon of 96 sides circumscribed about the triangle

$$\frac{AC}{LM} = \frac{4673\ \frac{1}{2}}{153} \quad \left[\frac{AC}{LM} = \frac{2EC}{2LC} = \frac{4673\ \frac{1}{2}}{153}\right]$$

$$\therefore \frac{AC}{\text{perimeter of 96 sided polygon}} = \frac{4673\frac{1}{2}}{14688}$$

or $$\frac{\text{perimeter}}{AC} = \frac{14688}{4673\ \frac{1}{2}}$$

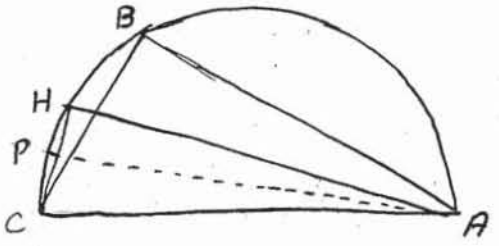
$$= \frac{3(4673\ \frac{1}{2}) + 667\ \frac{1}{2}}{4673\ \frac{1}{2}}$$

$$< \frac{3(4673\ \frac{1}{2}) + 1/7(4673\ \frac{1}{2})}{4673\ \frac{1}{2}}$$

$$< 3\ 1/7$$

Much more then, is the circumference of the circle less than 3 1/7 times the diameter.

Secondly, take a circle with diameter AC, and make the angle BAC equal one third of a right angle



Then $\frac{AB}{BC} < \frac{1351}{780} \left[\frac{AB}{BC} = \sqrt{\frac{3}{1}}\right]$

But $\frac{AC}{BC} = \frac{1560}{780} \left[\text{i.e. } \frac{2}{1}\right]$

Bisect the angle BAC by HA. The triangles HCZ and HCA are equiangular and therefore $\frac{AH}{HC} = \frac{CH}{HZ} = \frac{AC}{CZ}$

But $\frac{AC}{CZ} = \frac{CA + AB}{BC} \quad \left[\text{since } \frac{CA}{AB} = \frac{CZ}{BZ}\right]$

$$\therefore \frac{CA + AB}{BC} = \frac{AH}{HC}$$

$$\therefore \frac{CA + AB}{BC} < \frac{2911}{780} \quad \left[\text{i.e. } \frac{1351}{780} + \frac{1560}{780}\right]$$

$$\therefore \frac{AH^2}{HC^2} < \frac{8473921}{608400}$$

and $$\frac{AC^2}{HC^2} < \frac{9082321}{608400}$$

Bisect the angle CAH by AP and following the same procedure, we obtain the result that the ratio of

$$\frac{\text{the perimeter of inscribed polygon of 96 sides}}{AC} > \frac{6336}{2017\frac{1}{4}} > 3\ 10/71$$

Much more then, is the circumference of the circle greater than 3 10/71 times the diameter.

Appendix II

If g is a primitive root of p, the numbers $g, g^2, g^3, \ldots\ldots, g^{p-1}$ are distinct (mod.p) and have the residues 1, 2, 3, ..., p - 1 in some order.

Proof. Suppose $g^h \equiv g^k \pmod p$

where $p - 1 \geqq h > k \geqq 1$.

Then $g^{h-k} \equiv 1 \pmod p$

But $p - 1 > h - k \geqq 1$ and hence there is a contradiction to the hypothesis that g is a primitive root.

$\therefore g^h$ is not $\equiv g^k$

$\therefore g, g^2, \ldots\ldots, g^{p-1}$ all have different residues, and therefore the residues 1, 2, 3, ..., p - 1 in some order.

For small value of p, g is found by trial.

For p = 5, try g = 2

$2 \equiv 2;\ 2^2 \equiv 4;\ 2^3 \equiv 3;\ 2^4 \equiv 1$ (all mod 5)

Appendix 111

If a and p be prime to each other and p is any prime then $a^{p-1} \equiv 1 \pmod{p}$

Let $r_1, r_2, r_3, \ldots\ldots\ldots, r_{p-1}, r_p \equiv 0$, be the residues, modulus p, then $ar_1, ar_2, ar_3, \ldots\ldots\ldots ar_{p-1}$ will be congruent to $r_1, r_2, r_3, \ldots\ldots\ldots, r_{p-1}$, though perhaps not in that order.

That is
$$\left.\begin{aligned} ar_1 &\equiv r_{J_1} \\ ar_2 &\equiv r_{J_2} \\ &\ldots\ldots\ldots\ldots \\ ar_{p-1} &\equiv r_{J_{p-1}} \end{aligned}\right\} \pmod{p}$$

Multiplying, the congruences we have

$$a^{p-1} r_1 r_2 \ldots\ldots\ldots r_{p-1} \equiv r_{J_1} r_{J_2} \ldots\ldots\ldots\ldots r_{J_{p-1}} \equiv P$$

or $a^{p-1} P \equiv P \pmod{p}$

Divide both sides by P

Then $a^{p-1} \equiv 1 \pmod{p}$

Appendix IV

Let $f(x)$ and $g(x)$ be polynomials with co-efficients in a field F and let $f(x)$ be irreducible in F. If one root α of $f(x) = 0$ satisfies $g(x) = 0$, then $f(x)$ is a divisor of $g(x)$.

α is a root of $f(x) = 0$ and of $g(x) = 0$, therefore $x - \alpha$ is a factor both of $f(x)$ and of $g(x)$ and also of their greatest common divisor $t(x)$, and so $t(x)$ is not a constant. The co-efficients of $t(x)$ lie in the field F. Let $f(x)/g(x) = a(x)$ with remainder $r(x)$ or $f(x) = g(x)\,[a(x)] + r(x)$, where $r(x)$ is of degree less than $g(x)$; similarly, when $g(x)$ is divided by $r(x)$ let the quotient be $b(x)$ and remainder $s(x)$, so that $g(x) = r(x)\,[b(x)] + s(x)$

Proceeding thus, let

$$f(x) = g(x) \cdot a(x) + r(x)$$

$$g(x) = r(x) \cdot b(x) + s(x)$$

$$r(x) = s(x) \cdot c(x) + t(x)$$

$$s(x) = t(x) \cdot d(x)$$

Since $a(x)$, $r(x)$, $b(x)$.....were obtained by rational operations their co-efficients are in the field F. $t(x)$ is seen to be a divisor of $s(x)$, $r(x)$, $g(x)$ and $f(x)$ and is the greatest common divisor.

$r(x) = f(x) - g(x) \cdot a(x)$ and $s(x) = g(x)\,[1 + a(x) \cdot b(x)] - f(x) \cdot b(x)$ and $t(x) = f(x)\,[1 + b(x) \cdot c(x)] - g(x)\,[a(x) + c(x) + a(x) \cdot b(x) \cdot c(x)]$

which shows the greatest common divisor to have its co-efficients in the field F.

The quotient of $f(x)$ by $t(x)$ is a constant independent of x since otherwise $f(x)$ would be reducible $\therefore f(x) = c.t(x)$. But $t(x)$ divides $g(x)$ $\therefore f(x)$ divides $g(x)$.

Appendix V

To find the value of e^{x} - Using Maclauren's formula.

$$f(x) = f(0) + f'(0).x + f''(0).\frac{x^2}{1.2} + f'''(0).\frac{x^3}{1.2.3} + \cdots\cdots$$

we have

$$e^{x} = e^{0} + e^{0}.x + e^{0}.\frac{x^2}{1.2} + e^{0}\frac{x^3}{1.2.3} + \cdots\cdots\cdots$$

$$= 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\cdots$$

Appendix VI

To find the value of tan x - Again using Maclaurin's formula,

$$\tan x = \tan 0 + \sec^2(0)\, x + 2 \sec^2 0.\tan 0.\, \frac{x^2}{1.2} +$$

$$(4 \sec^3 0.\tan^2 0 + 2 \sec^4 0)\, \frac{x^3}{1.2.3} + \cdots\cdots\cdots$$

$$= x + \frac{x^3}{3} + \cdots\cdots\cdots$$

or

$$\tan x = x + \frac{x^3}{3} + \frac{x^5}{5} + \frac{x^7}{7} + \cdots\cdots\cdots$$

Appendix V11

To prove that $e^{i\pi} + 1 = 0$

$$e^{ix} = 1 + \frac{ix}{1} - \frac{x^2}{2!} - \frac{ix^3}{3!} + \cdots\cdots$$

$$i \sin x = ix - \frac{ix^3}{3!} + \frac{ix^5}{5!} - \cdots\cdots$$

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots\cdots$$

both being found from Maclaurin's formula

$$\therefore e^{ix} = \cos x + i \sin x$$

$$\therefore e^{i\pi} = \cos \pi + i \sin \pi = -1$$

$$\therefore e^{i\pi} + 1 = 0$$

Appendix VIII

Proof of Lemma I

If $f(x) = a_1 x + a_2 x^2 + a_3 x^3 + \ldots\ldots + a_n x^n$ and if we let

$S_1 = 1$, $S_2 = 1 + \frac{x}{1}$,

$S_3 = 1 + \frac{x}{1!} + \frac{x^2}{2!}$, $\ldots\ldots\ldots$, $S_n = 1 + \frac{x}{1} + \ldots\ldots + \frac{x^{n-1}}{(n-1)!}$

then $f'(x) + f''(x) + f'''(x) + \ldots\ldots + f^n(x) =$

$$1!\, S_1 a_1 + 2!\, S_2 a_2 + \ldots\ldots + n!\, S_n a_n .$$

Write $f(x)$ as $1!\, a_1 \frac{x}{1!} + 2!\, \frac{a_2 x^2}{2!} + 3!\, \frac{a_3 x^3}{3!} + \ldots\ldots + n!\, a_n \frac{x^{n-1}}{n!}$.

Then $f'(x) = 1!a_1 + 2!a_2 \frac{x}{1!} + 3!a_3 \frac{x^2}{2!} + \ldots\ldots + n!a_n \frac{x^{n-1}}{(n-1)!}$.

$f''(x) = 2!a_2 + 3!a_3 \frac{x}{1!} + 4!a_4 \frac{x^2}{2!} + \ldots\ldots\ldots + n!a_n \frac{x^{n-2}}{(n-2)!}$

$f^n(x) = n!a_n$

$\therefore f'(x) + f''(x) + f'''(x) + \ldots\ldots + f^n(x)$

$= 1!a_1 + 2!\, a_2 \left(1 + \frac{x}{1!}\right) + 3!a_3 \left(1 + \frac{x}{1!} + \frac{x^2}{2!}\right) + \ldots\ldots\ldots$

$\ldots\ldots + n!a_n \left(1 + \frac{x}{1!} + \ldots\ldots\ldots + \frac{x^n}{n!}\right)$

$= 1!a_1 S_1 + 2!a_2 S_2 + 3!a_3 S_3 + \ldots\ldots + n!a_n S_n$

or $1!S_1 a_1 + 2!S_2 a_2 + 3!S_3 a_3 + \ldots\ldots\ldots + n!S_n a_n$.

Proof of Lemma II

If $f(x) = \dfrac{x^{p-1}\left[(x-1)(x-2)\ldots\ldots\ldots(x-m)\right]^p}{(p-1)!}$

and $F(x) = f'(x) + f''(x) + \ldots\ldots\ldots + f^n(x)$ where p is any prime number and n is any positive integer and the C's are any integers, then $C_0 F(0) + C_1 F(1) + C_2 F(2) + \ldots\ldots + C_m F(m) = C_0 (m!)^p + pQ$ where Q is some integer depending on the value of the C's and p.

Arranging $f(x)$ in ascending powers of x

$$f(x) = \frac{B_{p-1}\, x^{p-1} + B_p x^p + \ldots\ldots + B_{p(m+1)-1}\, x^{p(m+1)-1}}{(p-1)!}$$

B_{p-1}, B_p, $\ldots\ldots\ldots B_{p(m+1)-1}$ are all integers and B_{p-1} is the product

$\left[(-1)(-2)(-3)\ldots\ldots\ldots(-m)\right]^p = \pm (m!)^p$. Taking derivatives so as to determine F(0), F(1), ..., F(m) the results are

$f'(0) = 0,\ f''(0) = 0,\ \ldots\ldots, f^{p-2}(0) = 0,$

$f^{p-1}(0) = B_{p-1}$, $f^p(0) = pB_p, \ldots\ldots, f^n(0) = p(p+1)\ldots\ldots\ldots nB_n$.

$\therefore F(0) = B_{p-1} + pB_p + \ldots\ldots + \left[p(p+1)\ldots\ldots\ldots nB_n\right]$

$= \pm (m!)^p + pB_p + \ldots\ldots + \left[p(p+1)\ldots\ldots nB_n\right]$

$\therefore C_0F(0) = C_0(m!)^p +$ a multiple of p. Also taking derivates of f(x) in the form

$$f(x) = \frac{x^{p-1}\left[(x-1)(x-2)\ldots\ldots\ldots(x-m)\right]^p}{(p-1)!}$$

$$f'(x) = \frac{(p-1)x^{p-2}\left[(x-1)(x-2)\ldots\ldots\ldots(x-m)\right]^p}{(p-1)!} + \frac{x^{p-1}\cdot\frac{d\left[(x-1)(x-2)\ldots\ldots\ldots(x-m)\right]^p}{dx}}{(p-1)!}$$

$\therefore f'(1) = 0$, and all derivatives will be either zero, or multiples of p when 1 is substituted for x.

F(1) which is $= f'(1) + f''(1) + f'''(1) + \ldots\ldots$ and also $C_1F(1)$ will be a multiple of p.

Similarly $C_2F(2)$ is a multiple of p and so on to $C_mF(m)$, also a multiple of p.

$\therefore C_0F(0) + C_1F(1) + C_2F(2) + \ldots\ldots + C_mF(m) = C_0(m!)^p + pQ$

Proof of Lemma III

If $f(x) = a_1x + a_2x^2 + a_3x^3 + \ldots\ldots + a_nx^n$

$$= \frac{x^{p-1}\left[(x-1)(x-2)(x-3)\ldots\ldots\ldots(x-m)\right]^p}{(p-1)!}$$

and if $A_1 = |a_1|$, $A_2 = |a_2|$, ..., $A_n = |a_n|$ and $X = |x|$

then $A_1X + A_2X^2 + \ldots\ldots + A_nX^n = \frac{X^{p-1}\left[(X+1)(X+2)\ldots\ldots\ldots(X+m)\right]^p}{(p-1)!}$

The second form of f(x) is obviously an expression with alternating signs. If a certain set of binomial factors, all with plus signs be multiplied -- and then a second set, identical, only that all

have minus signs, the results are the same except that in the latter case the signs are alternately plus and minus i.e. $x^{p-1}\left[(x-1)(x-2)\ldots\ldots\ldots(x-m)\right]^p$ could differ from $x^{p-1}\left[(x+1)(x+2)\ldots\ldots\ldots(x+m)\right]^p$ only in having alternate signs different, which proves the theorem.