TEXT TWO

THE THEORY OF EQUATIONS

History shows the necessity for the invention of new numbers in the orderly progress of civilisation and in the evolution of mathematics. We must review briefly the growth of the number system in the light of the theory of equations and see why **the complex number system** need not be enlarged further. Suppose we decide that we want all polynomial equations to have roots. Now let us imagine that we have no numbers in our possession except **the natural numbers.** Then a simple linear equation like $2x=3$ has no root. In order to remedy this condition, we invent **fractions.** But a simple linear equation, like $x+5=2$ has no root even among the fractions. Hence we invent **negative numbers.** A simple quadratic equation like $x^2=2$ has no root among all the (positive and negative) **rational numbers,** therefore we invent the **irrational numbers** which together with the rational numbers complete the system of **real numbers.**

However, a simple quadratic equation like $x^2=-1$ has no root among all the real numbers, hence, we invent **the pure imaginary numbers.** But a simple quadratic equation like $x^2+2x+4=0$ has no roots among either the real or pure imaginary numbers; therefore we invent **the complex numbers.** The story of $\sqrt{-1}$ the imaginary unit, and of $x+yi$, the complex number, originated in the logical development of algebraic theory. The word "imaginary" reflects the elusive nature of the concept for distinguished mathematicians who lived centuries ago. Early consideration of the square root of a negative number brought unvarying rejection. It seemd obvious that a negative number is not a square, and hence it was concluded that such square roots had no meaning. This attitude prevailed for a long time.

G. Cardano (1545) is credited with some progress in introducing complex numbers in his solution of the cubic equation, even though he regarded them as "fictitious". He is credited also with the first use of the square root of a negative number in solving the now-famous problem, "Divide 10 into two parts such that the product ... is 40", which Cardano first says is "manifestly impossible"; but then he goes on to say, in a properly advanturous spirit, "Nevertheless, we will operate". Thus he found $5+\sqrt{15}$ and $5-\sqrt{-15}$ and showed that they did indeed have the sum of 10 and a product of 40. Cardano concludes by saying that these quantities are "truly sophisticated" and that to continue working with them is "as subtle as it is useless". Cardano did not use the symbol $\sqrt{-15}$, his designation was "$R_x{\cdot}m$", that is, "radix minus", for the square root of a negative number. R. Descartes (1637) contributed the terms "real" and "imaginary". L. Euler (1748) used "i" for $\sqrt{-1}$ and C. F. Gauss (1832) introduced the term "complex number". He made significant contributions to the understanding of complex numbers through graphical representation and defined complex numbers as ordered pairs of real numbers for which $(a, b)\cdot(c, d)=(ac-bd, ad+bc)$, and so forth.

Now, we may well expect that there may be some equation of degree 3 or higher which has no roots, even in the entire system of complex numbers. That this is not the case was known to **C. F. Gaüss,** who proved in 1799 the following theorem, the truth of which had long been expected: **Every algebraic equation of degree n with coefficients in the complex number system has a root (and hence n roots) among the com-**

plex numbers. Later Gauss published three more proofs of the theorem. It was he who called it "**Fundamental Theorem of Algebra**". Much of the work on complex number theory is Gauss's. He was one of the first to represent complex numbers as points in a plane. Actually, Gauss gave four proofs for the theorem, the last when he was seventy; in the first three proofs he assumes the coefficients of the polynomial equation are real, but in the fourth proof the coefficients are any complex numbers. We can be sure now that for the purpose of solving polynomial equations we do not need to extend the number system any further.

Algebraic Formulas for the Roots

The general linear equation can be written in the form $ax+b=0$ $(a\neq 0)$, hence the formula for its roots is $x=\frac{-b}{a}$ The mathematician's desire for several results makes it natural to ask the following question: Can we get similar formulas giving the roots as algebraic expressions in terms of the coefficients for the general equation of any degree? For the general quadratic and cubic equations and equation of degree four such formulas, as we have already seen, were obtained in the XVI c. The next task was naturally to obtain similar formulas for the general equation of degree five: $ax^5+bx^4+cx^3+dx^2+ex+f=0$. Attempts to find such formulas were made from the XVI c. until early in the XIX c. without success. The reason for this failure became evident (in 1824) when **N. H. Abel** and **E. Galois** (in 1831) proved that it is not possible to write the roots of the general equation of degree higher than **four** as algebraic expressions in terms of the coefficients. You may be tempted to ask: "How can you boldly assert that it is impossible to find such formulas? Perhaps some day some genius will discover them. All things are possible. Are you sure you don't mean simply that no one has found them yet?" The answer is that we do not merely mean that no one has found them yet; we mean that no one will ever find them because it is impossible for such formulas to exist. Notice that we have not said that the general equation of degree **five** cannot be solved. In fact, it can be solved by other means, but its roots cannot be given as algebraic expressions in the coefficients. However, the roots of some **particular** equations of degree five or more can be obtained. For example, if in the fifth degree equation above, we restrict ourselves to the particular case where $b=c=d=e=0$ $a\neq 0$, that is, to equations of the form $ax^5+f=0$, then we can clearly express one root as $x=\sqrt[5]{-f/a}$ which is an algebraic expression. Therefore a natural question to raise is: **Given a definite polynomial equation of degree five or more, how can we tell whether or not its roots are expressible as algebraic expressions in its coefficients?** This question was settled by E. Galois.

Before describing the momentous work of Abel and Galois, we must note some of the events immediately preceding and directly influencing the remarkable achievements of these gifted young mathematicians both of whom died in their twenties. In 1770 **Euler** devised a new method for solving the quartic equation but his optimistic hope that some similar method could solve the general polynomial equation was ill-fated. In the same year **Lagrange** considered the problem of solving the general polynomial equation by comparing the known solutions of quadratic, cubic and quartic equations and noting that in each of these three cases a certain reduction transformed the equation to one of the lower degree; but, unhappily, when Lagrange tried this "reduction" on a quintic equation, the degree of the resulting equation was increased rather than decreased. Although Lagrange did not succeed in his main objective, his attack on the problem made use of **permutations of the roots of the equations;** and he discovered the key to the theory of permutation groups, including the property mentioned earlier and now called Lagrange's theorem.

Both **Abel** and Galois built on Lagrange's work. It is not surprising that Abel approached the general problem of trying to solve the polynomial equation of degree n by trying to solve the general quintic equation. In fact, he thought he had succeeded and the "solution" was sent to a leading mathematician, but while waiting for a reply, Abel fortunately discovered his mistake and this misadvanture caused him to wonder **whether a general algebraic solution was indeed possible.** Although Abel succeeded in showing that for n greater than four the general polynomial equation could not be solved algebraically, he did not claim to have completely achieved the objective he set for himself: 1) to find all the equations of any degree which are solvable algebraically; 2) to determine whether a given equation is or is not solvable algebraically.

It was fortunate that Abel's proof, in which he used permutation groups to some extent, received early publication. This proof caught the imagination of **Galois** who gave complete answers to the questions proposed by Abel. Galois showed that every equation could be associated with a characteristic group and that the properties of this group could be used to determine whether the equation could be solved by radicals. In 1831 Galois stated his criterion: **A polynomial equation is solvable if and only if its group, over the coefficient field, is solvable.** The concepts associated with this result was usually characterized as Galois's theory. In his work he used the idea of isomorphic groups, and was the first to demonstrate the importance of invariant (or normal) subgroups and factor groups. **The term "group" is due to Galois.** The work of Galois was quite original in character and was not well understood at the time because of the sketchy expositions which he presented. Galois's mathematical abilities were not appreciated by his teachers, and in fact he received no recognition for his work while he lived. Although Galois's accomplishments were mathematical landmarks of the greatest significance and originality, they did not immediately make their full impact on his contemporaries because these men were slow to understand, appreciate, and publish Galois's work. However, what is now called **the Galois theory of equations** is studied everywhere by advanced students of mathematics.

Abel was not yet 27 when he died leaving behind a wealth of highly original work which stimulated mathematical research for many years after. Galois was killed in a duel at the age of less than 21. Abel and Galois proved in entirely different ways that **there cannot be any general formulas for solving polynomial equations of degree higher than four.** At least there can be no formulas which give the solutions in terms of the coefficients and which involve only addition, subtraction, multiplication, division and the extraction of roots.

Read the text. Reproduce orally the historical development of algebraic structures and explain why many different branches of modern mathematics are all interrelated by virtue of the "group" structures.

TEXT THREE

FIELDS, RINGS, GROUPS

The concept of a "field" was used by both Abel and Galois at an intuitive, subformal level in their work on polynomial equations. In algebra the word " field" is used to describe a structure that closely resembles ordinary arithmetic. The operations of addition, subtraction, multiplication and division occur in a field and are much like the corresponding operations in arithmetic. **The set of real numbers, under ordinary addition and multiplication, is the most familiar example of a field.** There exists a large variety of fields in algebra. In ordinary algebra in which the letters represent real numbers, the field axioms are assumed. One of the most interesting field properties usually assumed in ordinary algebra (actually it is not an axiom but a theorem) is the "nonexistence of zero divisors". This is used in solving quadratic equation by the factoring method and guarantees that if a product like $(x-2)(x-3)$ is zero, at least one of the factors must be zero. In 1871 **R. Dedekind** gave a concrete formulation and the earliest expositions of the theory of fields. One of the greatest accomplishments of the XIX c. in mathematics is expressed in the statement that the real number system is a **"complete ordered field".**

More formally the word "field" means a mathematical system in which addition and multiplication can be carried out in a way that satisfies the familiar rules, namely (1) the commutative law of addition and multiplication, (2) the associative law of addition and multiplication, (3) the distributive law. Furthermore, a field must contain a zero element 0, characterized by the property, that $x+0=x$ for any element x. It contains a unit element, 1, that has the property that $1\times x=x$. For any given element x there exists another element $-x$ such that $-x+x=0$. Finally, for any elements x $(x\neq 0)$ a field must contain an element $1/x$ such that $x(1/x)=1$. **Thus, a field is a structure (exemplified by e. g., the rational numbers) whose elements can be added, subtracted, multiplied and divided under the familiar rules of arithmetic.**

Considering now the second word, a field is **"ordered"** if the sizes of its elements can be compared. The shorthand symbol used to denote this property is the sign $>$, meaning "greater than". This symbol must obey its own set of rules, (1) the trichotomy law: for any two elements x and y, exactly one of the following three relations is true, $x>y$, $x=y$, or $y>x$; (2) the transitivity law: if $x>y$ and $y>z$ then $x>z$; (3) the law of addition: if $x>y$, then $x+z>y+z$; (4) the law of multiplication: if $x>y$ and $z>0$, then $xz>yz$.

Finally, what do we mean by the word "complete" in describing the system of real numbers as a "complete ordered field"? This has to do with the problem raised by a number such as $\sqrt{2}$. Practically speaking, $\sqrt{2}$ is given by a sequence of rational numbers such as 1, 1.4, 1.41, 1.414 ... that provide better and better approximation to it. Squaring these numbers yields a sequence of numbers that are getting closer and closer to 2. So, we think of $\sqrt{2}$ as a "limiting value" of such a sequence of approximation. An ordered field is called "complete" if, corresponding to any regular sequence of elements, there is an element of the field that the sequence approaches as a limiting value. This is "the law of completenss", the final axiomatic requirement for the real-number system.

In a field as we have just seen, we can add, subtract, multiply and divide (except that division by 0 is barred). Not all algebraic structures have as comprehensive a list of operations. In a **Ring,** for example, we can add, subtract and multiply but not necessarily divide. A familiar example of a **Ring is the whole numbers, both positive and negative.** Even more restricted than a ring is the concept of a **group,** with the existence in it of only one operation, which can be thought of as a kind of **generalized multiplication.** The idea of a group is one which pervades the whole of modern mathematics both pure and applied. The theory of groups, a central concern of contemporary mathematics, has evolved through a progression of abstractions. **A group is one of the simplest and the most important algebraic structures of consequence.** Group theory traces its origin back to a problem that has fascinated mathematicians since the Middle Ages: the solution of algebraic equations of degree greater than two by algebraic processes. In the particular form of the study of symmetry, group theory can claim to have its origin in prehistoric times. Nowadays, group theory is developed in an abstract way so that it can be applied in many different circumstances but many of those applications still concern symmetry.

Some of the components of the group concept (i. e., those essential properties that were later abstracted and formulated as axioms) and also of the field concept, were recognized as early as 1650 B. C. when the Egyptians showed a curious awareness that something was involved in assuming that $ab=ba$. The Egyptians also freely used the distributive law, namely, $a(b+c)=ab+ac$, but without any comment. The Babylonians (c. 1700 B. C.) also used the commutative and distributive laws. These laws were tacitly assumed in their rhetorical algebra when, in effect they used such formulas as $(a+b)^2=a^2+2ab+b^2$. Looking at Greek mathematics, we see that Euclid was more aware of the explicit nature of the distributive law, declaring in his Proposition 1: $a(b+c+d)=ab+ac+ad$. Somewhat later Diophantus exhibited interesting insights regarding multiplicative inverses and the unity element. One may perhaps claim that the concept of a **cyclic group** is prehistoric in the sense that the Ancients measured a circle by using equal divisions of its circumference, or that the 24-hour clocks of the Babylonians and Egyptians were (implicitly) examples of finite additive groups with 24 used as a zero element and Euclid's work contains at the implicit level what is classified now as algebraic number theory and group theory.

The group concept was not recognized as explicitly as were some of its axioms, but even so it was implicitly sensed and used before Abel and Galois brought it into focus and before **Cayley (1854)** defined a general abstract group. During the two hundred years from Viète to Abel and Galois, in the work of some great mathematicians an implicit grasp of the group concept was already to be found. During **the seventeenth century** it was clear to those working with the nth roots of unity that these n elements formed a multiplicative cyclic group and that the primitive nth roots could be used as generators of the group. The use of group theory at the subformal level — and a striking one — is found in **Euler's** proof (1760—1761) of a generalization of Fermat's "little theorem". Euler was actually using an idea later formulated by **Lagrange** (1770) and now known as Lagrange's theorem, which says that the number of elements in the first-column subgroup divides the number of elements in the whole table. Lagrange gave the idea an explicit and general formulation and showed that the number of elements in a symmetric group is divisible by the number of elements in any subgroup (which is, of course, a permutation group). Hence his result was valid for non-Abelian permutation groups as well as for Abelian groups.