Three Field Theory

Four Galois Theory

Five Ring Theory

Six Classical Ideal Theory

From "Elements of Abstract Algebra"
by Allan Clark
Wadsworth Publishing 1971
reprinted by Dover Books 1984

Introduction

Classical algebra was the art of resolving equations. Modern algebra, the subject of this book, appears to be a different science entirely, hardly concerned with equations at all. Yet the study of abstract structure which characterizes modern algebra developed quite naturally out of the systematic investigation of equations of higher degree. What is more, the modern abstraction is needed to bring the classical theory of equations to a final perfect form.

The main part of this text presents the elements of abstract algebra in a concise, systematic, and deductive framework. Here we shall trace in a leisurely, historical, and heuristic fashion the genesis of modern algebra from its classical origins.

The word *algebra* comes from an Arabic word meaning "reduction" or "restoration." It first appeared in the title of a book by Muhammad ibn Musa al-Khwarizmi about the year 825 A.D. The renown of this work, which gave complete rules for solving quadratic equations, led to use of the word algebra for the whole science of equations. Even the author's name lives on in the word *algorithm* (a rule for reckoning) derived from it. Up to this point the theory of equations had been a collection of isolated cases and special methods. The work of al-Khwarizmi was the first attempt to give it form and unity.

The next major advance came in 1545 with the publication of *Artis Magnae* *sive de Regulis Algebraicis* by Hieronymo Cardano (1501–1576). Cardano's book, usually called the *Ars Magna*, or "The Grand Art," gave the complete solution of equations of the third and fourth degree. Exactly how much credit for these discoveries is due to Cardano himself we cannot be certain. The solution of the quartic is due to Ludovico Ferrari (1522–1565), Cardano's student, and the solution of the cubic was based in part upon earlier work of Scipione del Ferro (1465?–1526). The claim of Niccolo Fontana (1500?–1557), better known as Tartaglia ("the stammerer"), that he gave Cardano the cubic under a pledge of secrecy, further complicates the issue. The bitter feud between Cardano and Tartaglia obscured the true primacy of del Ferro.

A solution of the cubic equation leading to Cardano's formula is quite simple to give and motivates what follows. The method we shall use is due to Hudde, about 1650. Before we start, however, it is necessary to recall that *every complex number has precisely three cube roots*. For example, the complex number $1 = 1 + 0i$ has the three cube roots, 1 (itself), $\omega = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$, and $\omega^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$. In general, if z is any one of the cube roots of a complex number w, then the other two are ωz and $\omega^2 z$.

For simplicity we shall consider only a special form of the cubic equation,

$$x^3 + qx - r = 0. \tag{1}$$

(However, the general cubic equation may always be reduced to one of this form without difficulty.) First we substitute $u + v$ for x to obtain a new equation,

$$(u^3 + 3u^2v + 3uv^2 + v^3) + q(u + v) - r = 0, \tag{2}$$

which we rewrite as

$$u^3 + v^3 + (3uv + q)(u + v) - r = 0. \tag{3}$$

Since we have substituted two variables, u and v, in place of the one variable x, we are free to require that $3uv + q = 0$, or in other words, that $v = -q/3u$. We use this to eliminate v from (3), and after simplification we obtain,

$$u^6 - ru^3 - \frac{q^3}{27} = 0. \tag{4}$$

This last equation is called the *resolvent equation* of the cubic (1). We may view it as a quadratic equation in u^3 and solve it by the usual method to obtain

$$u^3 = \frac{r}{2} \pm \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}. \tag{5}$$

Of course a complete solution of the two equations embodied in (5) gives six values of u—three cube roots for each choice of sign. These six values of u are the roots of the sixth-degree resolvent (4). We observe however that if u is a cube root of $(r/2) + \sqrt{(r^2/4) + (q^3/27)}$, then $v = -q/3u$ is a cube root of $(r/2) - \sqrt{(r^2/4) + (q^3/27)}$. Consequently the six roots of (4) may be conveniently designated as u, ωu, $\omega^2 u$ and v, ωv, $\omega^2 v$, where $uv = -q/3$. Thus the three roots of the original equation are

$$\alpha_1 = u + v, \qquad \alpha_2 = \omega u + \omega^2 v, \qquad \alpha_3 = \omega^2 u + \omega v, \tag{6}$$

where

$$u^3 = \frac{r}{2} + \sqrt{\frac{r^2}{4} + \frac{q^3}{27}} \quad \text{and} \quad v = \frac{-q}{3u}.$$

In other words, the roots of the original cubic equation (1) are given by the *formula of Cardano*,

$$\alpha = \sqrt[3]{\frac{r}{2} + \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}} + \sqrt[3]{\frac{r}{2} - \sqrt{\frac{r^2}{4} + \frac{q^3}{27}}},$$

in which the cube roots are varied so that their product is always $-q/3$.

For our purposes we do not need to understand fully this complete solution of the cubic equation—only the general pattern is of interest here. The important fact is that the roots of the cubic equation can be expressed in terms of the roots of a resolvent equation which we know how to solve. The same fact is true of the general equation of the fourth degree.

For a long time mathematicians tried to find a solution of the general quintic, or fifth-degree, equation without success. No method was found to carry them beyond the writings of Cardano on the cubic and quartic. Consequently they turned their attention to other aspects of the theory of equations, proving theorems about the distribution of roots and finding methods of approximating roots. In short, the theory of equations became analytic.

One result of this approach was the discovery of the *fundamental theorem of algebra* by D'Alembert in 1746. The fundamental theorem states that every algebraic equation of degree n has n roots. It implies, for example, that the equation $x^n - 1 = 0$ has n roots—the so-called *nth roots of unity*—from which it follows that every complex number has precisely n nth roots. D'Alembert's proof of the fundamental theorem was incorrect (Gauss gave the first correct proof in 1799) but this was not recognized for many years, during which the theorem was popularly known as "D'Alembert's theorem."

D'Alembert's discovery made it clear that the question confronting algebraists was not the existence of solutions of the general quintic equation, but whether or not the roots of such an equation could be expressed in terms of its coefficients by means of formulas like those of Cardano, involving only the extraction of roots and the rational operations of addition, subtraction, multiplication, and division.

In a new attempt to resolve this question Joseph Louis Lagrange (1736–1813) undertook a complete restudy of all the known methods of solving cubic and quartic equations, the results of which he published in 1770 under the title *Réflexions sur la résolution algébrique des equations.* Lagrange observed that the roots of the resolvent equation of the cubic (4) can be expressed in terms of the roots $\alpha_1, \alpha_2, \alpha_3$ of the original equation (1) in a completely symmetric fashion. Specifically,

$$\begin{aligned} v &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3), & u &= \tfrac{1}{3}(\alpha_1 + \omega\alpha_3 + \omega^2\alpha_2), \\ \omega v &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_1 + \omega^2\alpha_2), & \omega u &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_1 + \omega^2\alpha_3), \\ \omega^2 v &= \tfrac{1}{3}(\alpha_2 + \omega\alpha_3 + \omega^2\alpha_1), & \omega^2 u &= \tfrac{1}{3}(\alpha_3 + \omega\alpha_2 + \omega^2\alpha_1). \end{aligned} \tag{7}$$

All these expressions may be obtained from any one of them by permuting the occurrences of $\alpha_1, \alpha_2, \alpha_3$ in all six possible ways.

Lagrange's observation was important for several reasons. We obtained the resolvent of the cubic by making the substitution $x = u + v$. Although this works quite nicely, there is no particular rhyme nor reason to it—it is definitely *ad hoc.* However Lagrange's observation shows how we might have constructed the resolvent on general principles and suggests a method for constructing resolvents of equations of higher degrees. Furthermore it shows that the original equation is solvable in radicals if and only if the resolvent equation is.

To be explicit let us consider a quartic equation,

$$x^4 - px^3 + qx^2 - rx + s = 0, \tag{8}$$

and suppose that the roots are the unknown complex numbers $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Without giving all the details we shall indicate how to construct the resolvent equation. First we recall that the fourth roots of unity are the complex numbers $1, i, i^2, i^3$, where $i = \sqrt{-1}$ and $i^2 = -1$, $i^3 = -i$. Then the roots of the resolvent are the twenty-four complex numbers

$$u_{ijkl} = \tfrac{1}{4}(\alpha_i + i\alpha_j + i^2\alpha_k + i^3\alpha_l), \tag{9}$$

where the indices i, j, k, l are the numbers 1, 2, 3, 4 arranged in some order. Therefore the resolvent equation is the product of the twenty-four distinct factors $(x - u_{ijkl})$. That is, we may write the resolvent equation in the form

$$\phi(x) = \prod_{ijkl} (x - u_{ijkl}) = 0. \tag{10}$$

Thus the resolvent of the quartic has degree 24, and it would seem hopeless to solve. It turns out, however, that every exponent of x in $\phi(x)$ is divisible by 4, and consequently $\phi(x) = 0$ may be viewed as a sixth-degree equation in x^4. What is more, this sixth-degree equation can be reduced to the product of two cubic equations (in a way we cannot make explicit here). Since cubics can be solved, a solution of the quartic can be obtained by a specific formula in radicals. (Such a formula is so unwieldy that it is more useful and understandable simply to describe the process for obtaining solutions.)

For quintic, or fifth-degree, equations Lagrange's theory yields a resolvent equation of degree 120, which is a 24th-degree equation in x^5. Lagrange was convinced that his approach, which revealed the similarities in the resolution of cubics and quartics, represented the true metaphysics of the theory of equations. The difficulty of the computations prevented Lagrange from testing whether his techniques could produce a formula for resolving the quintic in radicals. Moreover, with his new insights, Lagrange could foresee the point at which the process might break down, and he gave equal weight to the impossibility of such a formula.

A short time afterward, Paolo Ruffini (1765–1822) published a proof of the unsolvability of quintic equations in radicals. Ruffini's argument, given in his two-volume *Teoria generale delle equazioni* of 1799, was correct in essence, but was not, in actual fact, a proof. A complete and correct proof was given by Niels Henrik Abel (1802–1829) in 1826 in a small book published at his own expense. The brilliant work of Abel closed the door on a problem which had excited and frustrated the best mathematical minds for almost three centuries.

There remained one final step. Some equations of higher degree are clearly solvable in radicals even though they cannot be factored. Abel's theorem raised the question: which equations are solvable in radicals and which are not? The genius Évariste Galois (1811–1832) gave a complete answer to this question in 1832. Galois associated to each algebraic equation a system of permutations of its roots, which he called a *group.* He was able to show equivalence of the solvability of an equation in radicals, with a property of its group. Thus he made important discoveries in the theory of groups as well as the theory of equations. Unfortunately Galois' brief and tragic life ended in a foolish duel before his work was understood. His theory perfected the ideas of Lagrange, Ruffini, and Abel and remains one of the stunning achievements of modern mathematical thought.

At this point we can only leave as a mystery the beautiful relation Galois discovered between the theory of equations and the theory of groups—a mystery resolved by the deep study of both theories undertaken in the text.

We can, however, gain some insight into modern abstraction by a short and informal discussion of groups. To take an example near at hand, we shall consider the group of permutations of the roots $\alpha_1, \alpha_2, \alpha_3$ of the cubic equation—which happens to be the Galois group of this equation in general. This group consists of six operations, A, B, C, D, E, and I, specified as follows:

A leaves α_1 fixed and interchanges the roots α_2 and α_3 wherever they occur.
B leaves α_2 fixed and interchanges α_1 and α_3.
C interchanges α_1 and α_2, leaving α_3 fixed.
D replaces α_1 by α_2 at each occurrence, α_2 by α_3, and α_3 by α_1.
E replaces α_1 by α_3, α_3 by α_2, and α_2 by α_1.
I is the identity operation, which makes no change at all.

For example, the result of applying the operation A to v, as expressed in (7), is u. We indicate this by writing

$$A(v) = u.$$

Similarly, the result of applying the operation E to v is ωv, or in other words, $E(v) = \omega v$. Of course, by definition, $I(v) = v$. It is easy to verify that by applying the six operations A, B, C, D, E, and I to v, we obtain all six of the expressions in (7) for the roots of the resolvent equation.

These operations have the property that if any two of them are applied successively, the result is the same as if one of the others had been applied once. For example, suppose we apply the operation A to v, obtaining u, and then apply the operation D to u, obtaining ωu. The result is the same as if we had applied the operation C directly to v. We can express this in symbols by

$$D(A(v)) = C(v).$$

In fact this remains true no matter what we put in place of v. That is, the result of first applying the operation A and then applying D is the same as applying the operation C. We sum this up in the simple equation: $DA = C$. There are many other relations of this sort among these operations. For example, we may compute the result of the composite operation EB on any function $f(\alpha_1, \alpha_2, \alpha_3)$ as follows:

$$B(f(\alpha_1, \alpha_2, \alpha_3)) = f(\alpha_3, \alpha_2, \alpha_1),$$
$$EB(f(\alpha_1, \alpha_2, \alpha_3)) = E(f(\alpha_3, \alpha_2, \alpha_1)) = f(\alpha_2, \alpha_1, \alpha_3) = C(f(\alpha_1, \alpha_2, \alpha_3)).$$

Thus $EB = C$. The thirty-six relations of this type can be given conveniently in a table. We put the result of the composite operation XY in the X row and the Y column.

We observe now that composition of the operations A, B, C, D, E, and I has the following properties.

(1) For any three operations X, Y, and Z, we have

$$X(YZ) = (XY)Z.$$

In other words, the result of first performing the operation YZ and then the operation X is the same as the result of first performing the operation Z and then the operation XY. For example, from Table 1 we see that $AB = D$ and $BC = D$, and therefore

Table 1

	A	*B*	*C*	*D*	*E*	*I*
A	*I*	*D*	*E*	*B*	*C*	*A*
B	*E*	*I*	*D*	*C*	*A*	*B*
C	*D*	*E*	*I*	*A*	*B*	*C*
D	*C*	*A*	*B*	*E*	*I*	*D*
E	*B*	*C*	*A*	*I*	*D*	*E*
I	*A*	*B*	*C*	*D*	*E*	*I*

$$A(BC) = AD = B = DC = (AB)C.$$

Thus we have verified the equation above for the special case where $X = A$, $Y = B$, and $Z = C$. This property of the composition of the operations is called *associativity*. To verify associativity completely from Table 1 we would have to make 216 checks like the one above.

(2) For any operation X we have

$$XI = X = IX.$$

In other words, the composition of any operation X with the identity operation I always gives X again. This property is easily checked by examining the last row and the last column of Table 1.

(3) For any operation X there is precisely one operation Y such that

$$XY = I = YX.$$

In other words, whatever the operation X does to the roots $\alpha_1, \alpha_2, \alpha_3$, Y does just the opposite. We call Y the inverse of X and denote it by X^{-1}. It is easy to see from Table 1 that

$$A^{-1} = A, \quad B^{-1} = B, \quad C^{-1} = C, \quad D^{-1} = E, \quad E^{-1} = D, \quad I^{-1} = I.$$

Whenever we have a set of operations and a rule for composing them that satisfies these three properties, we say that the operations form a *group*.

Once we know that a set of operations with a particular rule for composing them is a group, we can analyze properties of these operations and their composition without regard to the manner in which they are defined or the context in which they arose. This simplifies the situation by eliminating irrelevant details, and gives the work generality.

To clarify this process of abstraction, let us consider another group of operations defined in a completely different way. Again we shall have six operations, but this time we shall call them by the Greek letters α, β, γ, δ, ε, and ι. These will operate on the rational numbers (except 0 and 1) by the following rules:

$$\alpha(x) = \frac{1}{x}, \qquad \delta(x) = \frac{1}{1-x},$$

$$\beta(x) = 1 - x, \qquad \varepsilon(x) = \frac{x-1}{x},$$

$$\gamma(x) = \frac{x}{x-1}, \qquad \iota(x) = x,$$

where x is any rational number except 0 or 1. We may compose these operations and the result will always be one of the other operations. For example, we have that $\delta\alpha = \gamma$, since

$$\delta(\alpha(x)) = \delta\left(\frac{1}{x}\right) = \frac{1}{1-(1/x)} = \frac{x}{x-1} = \gamma(x).$$

Again, we may make a table of all thirty-six compositions of these six operations.

Table 2

	α	β	γ	δ	ε	ι
α	ι	δ	ε	β	γ	α
β	ε	ι	δ	γ	α	β
γ	δ	ε	ι	α	β	γ
δ	γ	α	β	ε	ι	δ
ε	β	γ	α	ι	δ	ε
ι	α	β	γ	δ	ε	ι

It is immediately apparent that Table 2 has a strong resemblance to Table 1. For example, every occurrence of A in the first table corresponds to an occurrence of α in the second. Similarly the letters B and β occur in the same positions in each table. In fact Table 1 may be transformed into Table 2 by making the substitutions:

$$A \to \alpha, \quad B \to \beta, \quad C \to \gamma, \quad D \to \delta, \quad E \to \varepsilon, \quad I \to \iota.$$

In other words, these two groups have the same structure *as groups* even though the individual operations are defined in quite different ways. To put it another way, all the facts which depend solely upon the way operations are composed will be the same for both groups. In such a case two groups are said to be *isomorphic*. Group theory studies the properties of groups which remain unchanged in passing from one group to another isomorphic with it.

Group theory was called the "theory of substitutions" until 1854 when the English mathematician Arthur Cayley (1821–1895) introduced the concept of *abstract group*. The convenience and power of the abstract approach to group theory was evident by the end of the nineteenth century. Subsequent abstractions, such as *field* and *ring*, have also proved to be powerful concepts. The success of abstract thinking in algebra has been so enormous that the terms *modern algebra* and *abstract algebra* are synonymous.

Abstraction is simply the process of separating form from content. We abstract whenever we pass from a particular instance to the general case. Even the simplest mathematics, ordinary arithmetic, is an abstraction from physical reality. In modern mathematics we abstract from previous mathematical experience and reach a new and higher plane of abstraction. Indeed, each mathematical generation abstracts from the work of preceding ones, continually distilling and concentrating the essence of old thought into new and more perfect forms. The rewards are great. Not only does abstraction greatly enhance our understanding, it also dramatically increases the applications of mathematics to practical life. Even such an apparently recondite subject as group theory has applications in crystallography and quantum mechanics. Over centuries modern algebra has grown into a large body of abstract knowledge worthy of study both for its intrinsic fascination and extrinsic application.