Introduction

How to understand the numbers we encountered in secondary school, and equations involving them: this is our point of departure in studying Galois theory.

No two people have identical experiences in secondary school, to be sure; I would venture, however, that we all encountered numbers such as $1/7$, $\sqrt{2}$, $\sqrt[3]{-5}$, $\sqrt[4]{20}$, and $11 + 13/\sqrt{17}$. Now to begin a proper mathematical study of these numbers, we should consider what these numbers have in common – and which numbers we should exclude from our study. After all, a mathematical discipline proceeds by studying a little bit of mathematical reality quite closely, widening the field of vision only later.

A moment's reflection reveals that each of our numbers bears a certain relationship to rational numbers. Each is either a rational number, a root of a rational number, or some combination – using addition, subtraction, multiplication, and division – of rational numbers and roots of integral degree. Having made this observation, we might choose to take the plunge and restrict ourselves to arithmetic combinations of rational numbers and their roots, a set which would appear easy to manipulate.

Before rushing headlong into definitions and theorems, however, we should step back and contemplate whether we are comfortable with what it is that we are representing by the symbols above. For instance, what exactly do we mean by the symbol $\sqrt[3]{-5}$? *A priori*, all that we know of the number is that its cube is -5. An excellent question to ask at this point is whether or not such a number actually exists, and any answer to this question will depend, in some measure, on what we mean by the word *number*.

For the moment, let us simply ask whether or not there is, at least, some *complex number* such that its cube is -5. Our answer then is yes because, by the Fundamental Theorem of Algebra, inside the complex numbers exist roots of every polynomial (in one variable) with complex number coefficients. Hence there exists a complex number which is a root of $X^3 + 5$. Stated another way, there must be a complex number that is a solution to the equation $X^3 = -5$. We may agree, therefore, that when we think of a number, we will think of an element of the complex numbers.

We are not done, however, exploring what we mean by $\sqrt[3]{-5}$. After all, when we write $\sqrt[3]{-5}$ we are expressing only that we mean *some* root of the polynomial $X^3 + 5$, and there may exist several solutions – three, in fact. Our symbol $\sqrt[3]{-5}$, therefore, does not uniquely define a number. With this observation we face one of the dangerous subtleties in the naming of things.

To address this ambiguity, we now make a pact that when we write down a symbol for a number, we agree to specify that number as precisely as we can. Since there are three third roots of -5, we should provide another distinguishing characteristic of the number to indicate which of the three we mean. One distinguishing characteristic, for instance, is a complex approximation to the number. Only at the very end of the book, in section 35, will this pact expire, and adventurers there will have to decide amid the sound and fury of a grand generalization whether, in fact, what we signify there with our new definitions is nothing – or, somehow, everything.

Returning to our consideration of the numbers of secondary school, observe that we have isolated an important property of these numbers: they are not only complex numbers but also solutions to polynomial equations. It turns out that to think of rational numbers and their roots as part of a larger system of roots of polynomials is to give our work a more natural context. (We will return specifically to rational numbers and their roots in section 34, where we discuss solvability by radicals.)

Now we might choose to study the full set of numbers that are roots of polynomials, say polynomials with any complex coefficients whatsoever. Such a system, however, would cast the net extremely far out, since any complex number would be such a number. After all, if c is a complex number, it is certainly a root of the polynomial $X - c$. While the study of the arithmetic of the entire set of complex numbers is certainly compelling, we would quickly be caught short by the fact that there are complex numbers that we grasp very differently from those in our initial list.

Notice that, apart from rational numbers, we are able to express most complex numbers only by their *properties*. Furthermore, the nature of these properties typically dictates the way in which we study them. Even leaving aside the question of existence for numbers defined only by properties, we surely do not grasp such numbers or their

CAMBRIDGE

Cambridge University Press
978-0-521-54499-3 - Exploratory Galois Theory
John Swallow
Excerpt
More information

“values” in the same sense as we grasp rational numbers, and the properties that complex numbers have may be quite varied.

For instance, we are familiar with the idea that i is a certain solution to the polynomial equation $X^2 = -1$, while π, on the other hand, is the ratio of the circumference of a circle to its diameter. It takes some work to associate a nongeometric property with π, such as, for instance, to see π as an infinite sum. Now to understand numbers defined by properties, we must look for ways to understand the connections between their properties. We have an enormous advantage with i, it turns out, since i is a root of polynomial with rational coefficients, and the fact that π is *not* the root of a polynomial with rational coefficients – in other words, the fact that π is *transcendental* – means that the methods of studying i are very likely not going to be especially useful in studying π.

In approaching Galois theory, we choose, then, to consider only those numbers that are roots of polynomials with *rational number* coefficients. Each of the numbers suggested at the beginning of this section satisfies this stronger criterion: $1/7$ is a root of $7X - 1$; $\sqrt{2}$ is a root of $X^2 - 2$; $\sqrt[3]{-5}$ is a root of $X^3 + 5$; $\sqrt[4]{20}$ is a root of $X^4 - 20$, and $11 + 13/\sqrt{17}$ is a root of $X^2 - 22X + (1888/17)$. We call a root of a polynomial with rational coefficients an *algebraic number*.

Now that we have settled on a precise context for the numbers we wish to study, a context that is neither too narrow nor too broad, we turn to determining which equations involving algebraic numbers are valid. Immediately we ask whether one algebraic number may be expressed in terms of another. For instance, if ω is a nonreal third root of 1 – that is, a nonreal solution of $X^3 - 1 = 0$ – then we observe with interest that the other nonreal third root is ω^2, and, even further, that the three third roots are arithmetically related: $1 + \omega + \omega^2 = 0$. These observations cause us to wonder if there might be a *reduced form* of an expression involving algebraic numbers, so that by finding a unique reduced form we might decide if two sides of a purported equation are in fact equal. For instance, if we could reduce $2 + \omega^3$ and $4 + \omega + \omega^2$ to reduced forms, we might then notice that each is equal to 3.

These same observations will later lead us to ask whether this coincidence – that an expression involving one root of a polynomial is equal to another root of the same polynomial – is frequent or rare. Along the way we will consider the set of all expressions involving a particular root of a polynomial, calling this set a *field extension*, and we will wonder if the field extensions determined by two different roots of the same polynomial are somehow similar. Perhaps, under the right additional hypotheses, they are even isomorphic. In answering these questions, we will appreciate a group, the group of automorphisms of a field extension, that has been visible for only the past two centuries. The answers will also embrace an elegant correspondence between subsets of algebraic numbers and subgroups of Galois groups, a correspondence used to great effect by mathematicians today.

This text tells what is really only the first episode in the story of the algebraic numbers. We will review in the first chapter some preliminaries, and in the second chapter we will begin a close study of algebraic numbers. Moving into the third chapter, we will question what relationships exist among the many algebraic numbers, the polynomials of which they are roots, and the field extensions that they generate. The fourth chapter will show you how to consider more than one algebraic number at the same time, developing quite a bit of theory about isomorphisms, and then the fifth chapter will reveal the Galois correspondence. Along the way, pay particular attention to exercises marked with an asterisk, for they are referred to in the text, either beforehand or afterwards. Finally, for the adventurous who seek mathematical applications of the glorious correspondence, we offer several classical topics in the last chapter. Enjoy!

CHAPTER ONE

Preliminaries

This chapter briefly reviews some of the basic results and notation from a first course in abstract algebra that we need in our exposition of algebraic numbers and Galois theory. We also introduce a few functions from *Maple* and *Mathematica* that may assist the reader in exploring some of the material.

In this text, $\mathbb{N}$ denotes the integers greater than 0, and, given a field K, K^* denotes the multiplicative group of nonzero elements of K.

1. Polynomials, Polynomial Rings, Factorization, and Roots in $\mathbb{C}$

Definition 1.1 (Polynomial, Polynomial Ring). Let K be a field. The *polynomial ring* $K[X]$ *over* K is the set of formal sums

$$\left\{ \sum_{i=0}^{n} a_i X^i \;\middle|\; a_i \in K,\ n \in \mathbb{N} \cup \{0\},\ a_n \neq 0 \right\} \cup \{0\}.$$

Elements of $K[X]$ are called *polynomials over* K. Under the usual polynomial addition and multiplication, $K[X]$ is a commutative ring. The polynomial 0 is the additive identity, and the polynomial 1 is the multiplicative identity.

We usually denote polynomials by letters, but when we wish to indicate the underlying variable, we parenthesize the variable and append the expression to the name, as in $p(X)$.

A useful notion of the size of a nonzero polynomial over a field K is its degree.

Definition 1.2 (Degree of a Polynomial). Let K be a field and $p = p(X) = \sum_{i=0}^{n} a_i X^i$ a nonzero polynomial with $a_n \neq 0$. The *degree* $\deg(p)$ is n, the greatest power of X with nonzero coefficient in p.

The degree is therefore a function

$$\deg\colon K[X] \setminus \{0\} \to \mathbb{N} \cup \{0\} = \{0, 1, 2, \ldots\}$$

satisfying $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$ and $\deg(fg) = \deg(f) + \deg(g)$ for $f, g \in K[X]$.

The degree of a polynomial p is 0 if and only if it is a nonzero element of K; hence $\deg(p) = 0 \Leftrightarrow p \in K^* \subset K[X]$. We call such polynomials, together with the polynomial 0, *constants.*

The analogy between polynomials and integers is one of the most fruitful in algebra, and in the following definitions and propositions we proceed to develop this analogy.

Definition 1.3 (Polynomial Factor, Reducible Polynomial). Let K be a field and $p \in K[X]$ a nonconstant polynomial. We say that p *factors over* K, or is *reducible over* K, if $p = fg$ for nonconstant polynomials $f, g \in K[X]$. Otherwise, p is *irreducible over* K.

We may omit the indication "over K" if the context makes its mention redundant. Note that we are uninterested in the case in which $p = fg$ with f or g an element of K since every $p \in K[X]$ may be so expressed: $p = (1/k)(kp)$ for any $k \in K^*$. We may multiply a nonzero polynomial p by an element of K in order to "normalize" it by changing the coefficient of its highest-order term to 1, just as for any nonzero integer we may always choose an element of $\{+1, -1\}$ by which to multiply the integer in order that the result is positive.

Definition 1.4 (Monic, Leading Coefficient). Let K be a field. A nonzero polynomial

$$0 \neq p = p(X) = \sum_{i=0}^{n} a_i X^i \in K[X]$$

is *monic* if its *leading coefficient* a_n is 1.

As with integers, we may divide one polynomial by another to produce a unique quotient and remainder.

Theorem 1.5 (Division Algorithm). *Let K be a field and $f, g \in K[X]$ polynomials with $f \neq 0$. Then we may constructively* divide *f into g so that there exist a unique* quotient polynomial *$q \in K[X]$ and a unique* remainder polynomial *$r \in K[X]$ such that*

- *$g = qf + r$ and*
- *either* $\deg r < \deg f$ *or* $r = 0$.

Proof. The algorithm follows by analogy the standard procedure for long division of integers, where in place of a decomposition of an integer into a sum of powers of 10, with coefficients ranging from 0 to 9, we decompose the polynomial into a sum of powers of X, with coefficients in K.

First we give a procedure that produces a q and r in $K[X]$ satisfying $g = qf + r$. If $g = 0$, then let $q = 0$ and $r = 0$. Otherwise, suppose

$$f = \sum_{i=0}^{\deg f} f_i X^i, \quad f_i \in K, \qquad g = \sum_{i=0}^{\deg g} g_i X^i, \quad g_i \in K.$$

If $\deg f > \deg g$, then let $q = 0$ and $r = g$, and we are done. Otherwise, we will find

$$q = \sum_{i=0}^{\deg(g)-\deg(f)} q_i X^i$$

with the $q_i \in K$ determined, one at a time, as follows.

Let $n = \deg(g) - \deg(f)$, and set q_n, the highest-order coefficient of q, to be the quotient of the highest-order coefficients of g and f, so that

$$q_n = g_{\deg g}/f_{\deg f}.$$

Then the polynomials g and $(q_n X^n) f$ agree in highest-order terms, and hence their difference,

$$d_n = g - (q_n X^n) f,$$

has degree no greater than $\deg(g) - 1$. If $n = 0$, then $\deg d_n < \deg f$ and we may stop after setting $r = d_n$.

Otherwise, we begin an induction on the coefficients of q. At each step, we define the coefficient q_{n-i} in such a way that $g - (q_n X^n + \cdots + q_{n-i} X^{n-i}) f$ has degree at most $\deg(g) - (i + 1)$. Clearly we have established the base case $i = 0$. Now assume that the induction is true for $i < n$.

Write d_{n-i} as

$$d_{n-i} = \sum_{j=0}^{\deg(g)-(i+1)} d_{n-i,j} X^j, \qquad d_{n-i,j} \in K$$

and set $q_{n-(i+1)}$ to be the quotient of certain coefficients of d_{n-i} and f:

$$q_{n-(i+1)} = d_{n-i,\deg(g)-(i+1)}/f_{\deg f}.$$

One checks that g and $(q_n X^n + \cdots + q_{n-(i+1)} X^{n-(i+1)}) f$ have identical coefficients for the terms with $X^{\deg(g)}, X^{\deg(g)-1}, \ldots, X^{\deg(g)-(i+1)}$. As a result, the difference

$$d_{n-(i+1)} = g - \left(\sum_{j=n-(i+1)}^{n} q_j X^j \right) f$$

has degree no greater than $\deg(g) - (i+2)$. Hence we have shown that the inductive statement is true for $i+1$. By the principle of mathematical induction, it is true for all $0 \le i \le n$ and we have defined a polynomial q.

By the induction property, $g - qf$ has degree no greater than $\deg(g) - (n+1) = \deg(f) - 1$. Letting $r = g - qf$, then, we have found a pair of polynomials q and r that satisfy the conclusions of the theorem.

Now we show that the q and r we constructed are unique. Suppose that there exist two pairs $q, r \in K[X]$ and $q', r' \in K[X]$ with

$$qf + r = g = q'f + r'$$

and each of r, r' is either zero or of degree less than $\deg f$. Then, subtracting the two representations of g, we have that the zero polynomial is equal to $(q - q')f + (r - r')$, or that

$$(q - q')f = r' - r.$$

If $(q - q')f$ is not the zero polynomial, then its degree is at least $\deg f$; however, if $r' - r$ is not zero, the degree of $r' - r$ is less than $\deg f$. Hence, if equality in $(q - q')f = r' - r$ is to hold, both sides must be the zero polynomial, which implies that $r = r'$ and $q = q'$. □

Replacing the field K in the Division Algorithm with a larger field L (but keeping the same polynomials $f, g \in K[X] \subset L[X]$) *does not change* the outcome of the algorithm. However, the general question of whether or not a polynomial $f \in K[X]$ is reducible *does* *depend* on the field $L \supset K$: if L is sufficiently large, a polynomial irreducible over K may become reducible over L. For example, the polynomial $X^2 + 1$ is irreducible over $K = \mathbb{Q}$, but over a field L containing i (for instance, $L = \mathbb{C}$), $X^2 + 1$ factors into $X + i$ and $X - i$.

Just as with integers, we may define a greatest common divisor of two polynomials in $K[X]$ and find this greatest common divisor by means of a Euclidean Algorithm.

Definition 1.6 (Greatest Common Divisor I). Let K be a field and $f, g \in K[X]$ nonzero polynomials. A nonzero monic polynomial $p \in K[X]$ is the *greatest common divisor* $\gcd(f, g)$, or *GCD*, of f and g if p is a factor of both f and g, and, moreover, whenever a polynomial $h \in K[X]$ is a factor of both f and g, then h is a factor of p.

Theorem 1.7 (Euclidean Algorithm). *Let K be a field and $f, g \in K[X]$ nonzero polynomials. Then the greatest common divisor* $\gcd(f, g) \in K[X]$ *of f and g is the result of the following* Euclidean Algorithm.

Let $r_0 = f$ and $r_1 = g \in K[X]$, and set $i = 0$. Apply the Division Algorithm (Theorem 1.5) repeatedly for successively greater i to find $q_{i+2}, r_{i+2} \in K[X]$ such that $r_i = r_{i+1}q_{i+2} + r_{i+2}$, where $\deg r_{i+2} < \deg r_{i+1}$, until $r_{i+2} = 0$. Let j be the first index such that $r_j = 0$.

Then if a is the leading coefficient of r_{j-1}, then $(1/a)r_{j-1}$ is the greatest common divisor $\gcd(f, g)$ *of f and g.*

Working backwards, one may constructively express $\gcd(f, g)$ *as a* $K[X]$-linear combination *of f and g,* i.e., *there constructively exist $z, w \in K[X]$ such that* $\gcd(f, g) = zf + wg$.

Proof. It is an exercise (5.9) to show that the algorithm must terminate. We show first that r_{j-1} is a common divisor of f and g, and then we show that every common divisor of f and g divides r_{j-1}. Adjusting the coefficient a of the highest-order term, we find that $(1/a)r_{j-1}$ is then a monic polynomial that is the greatest common divisor of f and g.

From the last equation,

$$r_{j-2} = r_{j-1}q_j + r_j = r_{j-1}q_j,$$

we have that r_{j-1} divides r_{j-2}. Since each r_k, $0 \le k \le j-2$, is defined to be a combination of r_{k+1} and r_{k+2}, it follows by induction that r_{j-1} divides every r_k, $0 \le k \le j-2$. But then r_{j-1} divides $r_0 = f$ and $r_1 = g$. Hence r_{j-1} is a common divisor of f and g.

Going the other direction, suppose that a polynomial $h \in K[X]$ is a divisor of f and g. Then h divides $r_0 = f$ and $r_1 = g$. Since each r_k, $2 \le k \le j-1$, is the remainder upon

Cambridge University Press
978-0-521-54499-3 - Exploratory Galois Theory
John Swallow
Excerpt
More information

dividing r_{k-2} by r_{k-1}, it follows by induction that h divides every r_k, $0 \leq k \leq j-1$. But then h divides r_{j-1}.

It is an exercise (5.10) to show that $\gcd(f, g)$ may be expressed as a combination of f and g. □

It is an exercise (5.4) to prove that replacing K by a larger field L in the Euclidean Algorithm does not change its outcome.

Just as integers factor uniquely, up to a reordering of the factors, into a product of ±1 and a set of primes, polynomials similarly factor in a unique way.

Theorem 1.8 ($K[X]$ is a Unique Factorization Domain). *Let K be a field. Then $K[X]$ is a unique factorization domain. In other words, every nonzero element $f \in K[X]$ has a factorization*

$$f = k\prod_{i=1}^{n} f_i, \qquad k \in K^*, \ \ 0 \neq f_i \in K[X],$$

where for each i, $\deg(f_i) \geq 1$ *and f_i is monic and irreducible. Moreover, any such factorization of f is unique up to a reordering of the factors.*

A proof of Theorem 1.8 based on the Euclidean Algorithm is an exercise (5.11).

The definition of a unique factorization domain is usually expressed more generally in terms of associates and irreducibles. Recall that an *integral domain* is a commutative ring with unity having no zero-divisors.

Definition 1.9 (Unique Factorization Domain). Let D be an integral domain. We say that $d \in D$ with $d \neq 0$ is *irreducible* if d is not a unit (i.e., is not invertible) and if $d = ab$ for $a, b \in D$, then either a or b is a unit. Two elements a, b of D are called *associates* if $a = ub$ for u a unit of D. We say that D is a *unique factorization domain* if (a) every nonzero element of D may be expressed as a product of irreducibles in D and (b) for each $d \in D$, all factorizations of d are equivalent by allowing permutation of the elements in the factorization and replacement of irreducibles by associates.

Knowing Theorem 1.8, we may define the greatest common divisor in an alternate fashion.