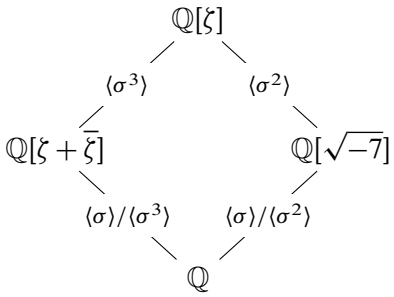
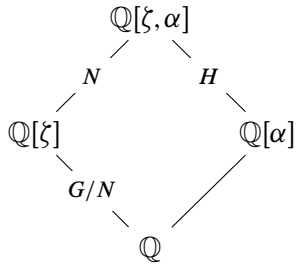
Fields and Galois Theory

J.S. Milne



Splitting field of X^7-1 over $\mathbb{Q}$.



Splitting field of X^5-2 over $\mathbb{Q}$.

Version 4.60
September 2018

These notes give a concise exposition of the theory of fields, including the Galois theory of finite and infinite extensions and the theory of transcendental extensions. The first six chapters form a standard course, and the final three chapters are more advanced.


```
BibTeX information
@misc{milneFT,
  author={Milne, James S.},
  title={Fields and Galois Theory (v4.60)},
  year={2018},
  note={Available at www.jmilne.org/math/},
  pages={138}
}
```


v2.01 (August 21, 1996). First version on the web.

v2.02 (May 27, 1998). Fixed many minor errors; 57 pages.

v3.00 (April 3, 2002). Revised notes; minor additions to text; added 82 exercises with solutions, an examination, and an index; 100 pages.

v3.01 (August 31, 2003). Fixed many minor errors; numbering unchanged; 99 pages.

v4.00 (February 19, 2005). Revised notes; added proofs for Infinite Galois Extensions; expanded Transcendental Extensions; 107 pages.

v4.10 (January 22, 2008). Minor corrections and improvements; added proofs for Kummer theory; 111 pages.

v4.20 (February 11, 2008). Replaced Maple with PARI; 111 pages.

v4.21 (September 28, 2008). Minor corrections; fixed hyperlinks; 111 pages.

v4.22 (March 30, 2011). Minor changes; changed TEX style; 126 pages.

v4.30 (April 15, 2012). Minor fixes; added sections on étale algebras; 124 pages.

v4.40 (March 20, 2013). Minor fixes and additions; 130 pages.

v4.50 (March 18, 2014). Added chapter on the Galois theory of étale algebras (Chapter 8); other improvements; numbering has changed; 138 pages.

v4.53 (May 27, 2017). Minor fixes and additions; numbering unchanged; 138 pages.

v4.60 (September 2018). Minor fixes and additions; numbering unchanged; 138 pages.

Available at www.jmilne.org/math/
Please send comments and corrections to me at the address on my web page.

Contents

Contents **3**
Notations. . . . 6
References. . . . 6

1 Basic Definitions and Results **7**
Rings . . . 7
Fields . . . 8
The characteristic of a field . . . 8
Review of polynomial rings . . . 9
Factoring polynomials . . . 11
Extension fields . . . 13
The subring generated by a subset . . . 14
The subfield generated by a subset . . . 15
Construction of some extension fields . . . 16
Stem fields . . . 17
Algebraic and transcendental elements . . . 17
Transcendental numbers . . . 19
Constructions with straight-edge and compass. . . . 21
Algebraically closed fields . . . 24
Exercises . . . 25

2 Splitting Fields; Multiple Roots **27**
Homomorphisms from simple extensions. . . . 27
Splitting fields . . . 28
Multiple roots . . . 30
Exercises . . . 33

3 The Fundamental Theorem of Galois Theory **35**
Groups of automorphisms of fields . . . 35
Separable, normal, and Galois extensions . . . 37
The fundamental theorem of Galois theory . . . 39
Examples . . . 42
Constructible numbers revisited . . . 43
The Galois group of a polynomial . . . 44
Solvability of equations . . . 45
Exercises . . . 45

4 Computing Galois Groups **47**
When is $G_f \subset A_n$? . . . 47

When does G_f act transitively on the roots? . . . 48
Polynomials of degree at most three . . . 49
Quartic polynomials . . . 49
Examples of polynomials with S_p as Galois group over $\mathbb{Q}$ . . . 51
Finite fields . . . 52
Computing Galois groups over $\mathbb{Q}$ . . . 54
Exercises . . . 57

5 Applications of Galois Theory **59**
Primitive element theorem. . . . 59
Fundamental Theorem of Algebra . . . 61
Cyclotomic extensions . . . 62
Dedekind's theorem on the independence of characters . . . 65
The normal basis theorem . . . 66
Hilbert's Theorem 90 . . . 69
Cyclic extensions . . . 71
Kummer theory . . . 72
Proof of Galois's solvability theorem . . . 74
Symmetric polynomials . . . 75
The general polynomial of degree n . . . 77
Norms and traces . . . 79
Exercises . . . 83

6 Algebraic Closures **85**
Zorn's lemma . . . 85
First proof of the existence of algebraic closures . . . 86
Second proof of the existence of algebraic closures . . . 86
Third proof of the existence of algebraic closures . . . 87
(Non)uniqueness of algebraic closures . . . 88
Separable closures . . . 88

7 Infinite Galois Extensions **91**
Topological groups . . . 91
The Krull topology on the Galois group . . . 92
The fundamental theorem of infinite Galois theory . . . 95
Galois groups as inverse limits . . . 98
Nonopen subgroups of finite index . . . 99
Exercises . . . 100

8 The Galois theory of étale algebras **101**
Review of commutative algebra . . . 101
Étale algebras over a field . . . 102
Classification of étale algebras over a field . . . 104
Comparison with the theory of covering spaces. . . . 107

9 Transcendental Extensions **109**
Algebraic independence . . . 109
Transcendence bases . . . 110
Lüroth's theorem . . . 113
Separating transcendence bases . . . 116

Transcendental Galois theory 117
Exercises 117

A Review Exercises **119**

B Two-hour Examination **125**

C Solutions to the Exercises **127**

Index **137**

Notations.

We use the standard (Bourbaki) notations:

$$\begin{aligned}
\mathbb{N} &= \{0,1,2,\dots\},\\
\mathbb{Z} &= \text{ring of integers},\\
\mathbb{R} &= \text{field of real numbers},\\
\mathbb{C} &= \text{field of complex numbers},\\
\mathbb{F}_p &= \mathbb{Z}/p\mathbb{Z} = \text{field with } p \text{ elements, } p \text{ a prime number.}
\end{aligned}$$

Given an equivalence relation, $[*]$ denotes the equivalence class containing $*$. The cardinality of a set S is denoted by $|S|$ (so $|S|$ is the number of elements in $S$when S is finite). Let I and A be sets. A family of elements of A indexed by I, denoted by $(a_i)_{i\in I}$, is a function $i \mapsto a_i : I \to A$. Throughout the notes, p is a prime number: $p = 2,3,5,7,11,\dots$.

$X \subset Y$	X is a subset of Y (not necessarily proper).
$X \stackrel{\text{def}}{=} Y$	X is defined to be Y, or equals Y by definition.
$X \approx Y$	X is isomorphic to Y.
$X \simeq Y$	X and Y are canonically isomorphic (or there is a given or unique isomorphism).

Prerequisites

Group theory (for example, GT), basic linear algebra, and some elementary theory of rings.

References.

Jacobson, N., 1964, Lectures in Abstract Algebra, Volume III — Theory of Fields and Galois Theory, van Nostrand.

Also, the following of my notes (available at www.jmilne.org/math/).

GT Group Theory, v3.14, 2017.

ANT Algebraic Number Theory, v3.07, 2017.

CA A Primer of Commutative Algebra, v4.02, 2017.

A reference monnnn is to `http://mathoverflow.net/questions/nnnn/`

PARI is an open source computer algebra system freely available here.

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of the notes: Mike Albert, Lior Bary-Soroker, Maren Baumann, Leendert Bleijenga, Jin Ce, Tommaso Centeleghe, Sergio Chouhy, Demetres Christofides, Antoine Chambert-Loir, Dustin Clausen, Keith Conrad, Daniel Duparc, Hardy Falk, Le Minh Ha, Jens Hansen, Albrecht Hess, Tim Holzschuh, Philip Horowitz, Trevor Jarvis, Henry Kim, Martin Klazar, Jasper Loy Jiabao, Weiyi Liu, Dmitry Lyubshin, Geir Arne Magnussen, John McKay, Sarah Manski, Georges E. Melki, Courtney Mewton, C Nebula, Shuichi Otsuka, Dmitri Panov, Artem Pelenitsyn, Alain Pichereau, David G. Radcliffe, Roberto La Scala, Chad Schoen, René Schoof, Prem L Sharma, Dror Speiser, Sam Spiro, Bhupendra Nath Tiwari, Mathieu Vienney, Martin Ward (and class), Xiande Yang, Wei Xu, and others.

CHAPTER 1

Basic Definitions and Results

Rings

A ***ring*** is a set R with two binary operations $+$ and $\cdot$ such that

(a) $(R,+)$ is a commutative group;

(b) $\cdot$ is associative, and there exists[1] an element 1_R such that $a\cdot 1_R = a = 1_R\cdot a$ for all $a\in R$;

(c) the distributive law holds: for all $a,b,c\in R$,

$$(a+b)\cdot c = a\cdot c + b\cdot c$$
$$a\cdot(b+c) = a\cdot b + a\cdot c.$$

We usually omit "$\cdot$" and write 1 for 1_R when this causes no confusion. If $1_R = 0$, then $R = \{0\}$.

A ***subring*** of a ring R is a subset S that contains 1_R and is closed under addition, passage to the negative, and multiplication. It inherits the structure of a ring from that on R.

A ***homomorphism of rings*** $\alpha\colon R\to R'$ is a map such that

$$\alpha(a+b) = \alpha(a)+\alpha(b),\quad \alpha(ab) = \alpha(a)\alpha(b),\quad \alpha(1_R) = 1_{R'}$$

for all $a,b\in R$. A ring R is said to be ***commutative*** if multiplication is commutative:

$$ab = ba \text{ for all } a,b\in R.$$

A commutative ring is said to be an ***integral domain*** if $1_R\neq 0$ and the cancellation law holds for multiplication:

$$ab = ac,\ a\neq 0, \text{ implies } b = c.$$

An ***ideal*** I in a commutative ring R is a subgroup of $(R,+)$ that is closed under multiplication by elements of R:

$$r\in R,\ a\in I, \text{ implies } ra\in I.$$

The ideal generated by elements $a_1,\dots,a_n$ is denoted by $(a_1,\dots,a_n)$. For example, (a) is the principal ideal aR.

[1] We follow Bourbaki in requiring that rings have a 1, which entails that we require homomorphisms to preserve it.

We assume that the reader has some familiarity with the elementary theory of rings. For example, in $\mathbb{Z}$ (more generally, any Euclidean domain) an ideal I is generated by any "smallest" nonzero element of I, and unique factorization into powers of prime elements holds.

Fields

DEFINITION 1.1 A ***field*** is a set F with two composition laws $+$ and $\cdot$ such that

(a) $(F,+)$ is a commutative group;

(b) $(F^\times,\cdot)$, where $F^\times = F \smallsetminus \{0\}$, is a commutative group;

(c) the distributive law holds.

Thus, a field is a nonzero commutative ring such that every nonzero element has an inverse. In particular, it is an integral domain. A field contains at least two distinct elements, 0 and 1. The smallest, and one of the most important, fields is $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0,1\}$.

A ***subfield*** S of a field F is a subring that is closed under passage to the inverse. It inherits the structure of a field from that on F.

LEMMA 1.2 *A nonzero commutative ring R is a field if and only if it has no ideals other than* (0) *and* R.

PROOF. Suppose that R is a field, and let I be a nonzero ideal in R. If a is a nonzero element of I, then $1 = a^{-1}a \in I$, and so $I = R$. Conversely, suppose that R is a commutative ring with no proper nonzero ideals. If $a \neq 0$, then $(a) = R$, and so there exists a b in R such that $ab = 1$. □

EXAMPLE 1.3 The following are fields: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (p prime).

A ***homomorphism of fields*** is simply a homomorphism of rings. Such a homomorphism is always injective, because its kernel is a proper ideal (it doesn't contain 1), which must therefore be zero.

Let F be a field. An ***F-algebra*** (or ***algebra over*** F) is a ring R containing F as a subring (so the inclusion map is a homomorphism). A ***homomorphism of F-algebras*** $\alpha\colon R \to R'$ is a homomorphism of rings such that $\alpha(c) = c$ for every $c \in F$.

The characteristic of a field

One checks easily that the map

$$\mathbb{Z} \to F, \quad n \mapsto n\cdot 1_F \stackrel{\text{def}}{=} 1_F + 1_F + \cdots + 1_F \quad (n \text{ copies of } 1_F),$$

is a homomorphism of rings. For example,

$$(\underbrace{1_F + \cdots + 1_F}_{m}) + (\underbrace{1_F + \cdots + 1_F}_{n}) = \underbrace{1_F + \cdots + 1_F}_{m+n}$$

because of the associativity of addition. Therefore its kernel is an ideal in $\mathbb{Z}$.

CASE 1: The kernel of the map is (0), so that

$$n\cdot 1_F = 0 \quad (\text{in } R) \implies n = 0 \quad (\text{in } \mathbb{Z}).$$

Nonzero integers map to invertible elements of F under $n \mapsto n \cdot 1_F : \mathbb{Z} \to F$, and so this map extends to a homomorphism

$$\frac{m}{n} \mapsto (m \cdot 1_F)(n \cdot 1_F)^{-1} : \mathbb{Q} \hookrightarrow F.$$

Thus, in this case, F contains a copy of $\mathbb{Q}$, and we say that it has ***characteristic zero***.

CASE 2: The kernel of the map is $\neq (0)$, so that $n \cdot 1_F = 0$ for some $n \neq 0$. The smallest positive such n will be a prime p (otherwise there will be two nonzero elements in F whose product is zero), and p generates the kernel. Thus, the map $n \mapsto n \cdot 1_F : \mathbb{Z} \to F$ defines an isomorphism from $\mathbb{Z}/p\mathbb{Z}$ onto the subring

$$\{m \cdot 1_F \mid m \in \mathbb{Z}\}$$

of F. In this case, F contains a copy of $\mathbb{F}_p$, and we say that it has ***characteristic*** p.

The fields $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \dots, \mathbb{Q}$ are called the ***prime fields.*** Every field contains a copy of exactly one of them.

REMARK 1.4 The usual proof by induction shows that the binomial theorem

$$(a+b)^m = a^m + \tbinom{m}{1} a^{m-1}b + \tbinom{m}{2} a^{m-2}b^2 + \cdots + b^m$$

holds in any commutative ring. If p is prime, then p divides $\binom{p^n}{r}$ for all r with $1 \leq r \leq p^n - 1$. Therefore, when F has characteristic p,

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \text{ all } n \geq 1,$$

and so the map $a \mapsto a^p : F \to F$ is a homomorphism. It is called the ***Frobenius endomorphism*** of F. When F is finite, the Frobenius endomorphism is an automorphism.

Review of polynomial rings

Let F be a field.

1.5 The ring $F[X]$ of polynomials in the symbol (or "indeterminate" or "variable") X with coefficients in F is an F-vector space with basis $1, X, \dots, X^n, \dots$, and with the multiplication

$$\left(\sum\nolimits_i a_i X^i\right)\left(\sum\nolimits_j b_j X^j\right) = \sum\nolimits_k \left(\sum\nolimits_{i+j=k} a_i b_j\right) X^k.$$

The F-algebra $F[X]$ has the following universal property: for any F-algebra R and element r of R, there is a unique homomorphism of F-algebras $\alpha : F[X] \to R$ such that $\alpha(X) = r$.

1.6 ***Division algorithm***: given $f(X), g(X) \in F[X]$ with $g \neq 0$, there exist $q(X), r(X) \in F[X]$ with $r = 0$ or $\deg(r) < \deg(g)$ such that

$$f = gq + r;$$

moreover, $q(X)$ and $r(X)$ are uniquely determined. Thus $F[X]$ is a Euclidean domain with deg as norm, and so it is a unique factorization domain.

1.7 Let $f \in F[X]$ be nonconstant, and let $a \in F$. The division algorithm shows that

$$f = (X-a)q + c$$

with $q \in F[X]$ and $c \in F$. Therefore, if a is a root of f (that is, $f(a) = 0$), then $X-a$ divides f. From unique factorization, it now follows that f has at most $\deg(f)$ roots (see also Exercise 1-3).

1.8 ***Euclid's algorithm***: Let $f(X), g(X) \in F[X]$. Euclid's algorithm constructs polynomials $a(X), b(X)$, and $d(X)$ such that

$$a(X)\cdot f(X) + b(X)\cdot g(X) = d(X), \quad \deg(a) < \deg(g), \quad \deg(b) < \deg(f)$$

and $d(X) = \gcd(f,g)$.

Recall how it goes. We may assume that $\deg(f) \geq \deg(g)$ since the argument is the same in the opposite case. Using the division algorithm, we construct a sequence of quotients and remainders

$$\begin{aligned} f &= q_0 g + r_0 \\ g &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + r_n \\ r_{n-1} &= q_{n+1} r_n \end{aligned}$$

with r_n the last nonzero remainder. Then, r_n divides r_{n-1}, hence $r_{n-2}, \ldots$, hence g, and hence f. Moreover,

$$r_n = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = \cdots = af + bg$$

and so every common divisor of f and g divides r_n: we have shown $r_n = \gcd(f,g)$.

Let $af + bg = d$. If $\deg(a) \geq \deg(g)$, write $a = gq + r$ with $\deg(r) < \deg(g)$; then

$$rf + (b + qf)g = d,$$

and $b + qf$ automatically has degree $< \deg(f)$.

PARI knows how to do Euclidean division: typing `divrem(13,5)` in PARI returns $[2,3]$, meaning that $13 = 2\times 5 + 3$, and `gcd(m,n)` returns the greatest common divisor of m and n.

1.9 Let I be a nonzero ideal in $F[X]$, and let f be a nonzero polynomial of least degree in I; then $I = (f)$ (because $F[X]$ is a Euclidean domain). When we choose f to be ***monic***, i.e., to have leading coefficient one, it is uniquely determined by I. Thus, there is a one-to-one correspondence between the nonzero ideals of $F[X]$ and the monic polynomials in $F[X]$. The prime ideals correspond to the irreducible monic polynomials.

1.10 As $F[X]$ is an integral domain, we can form its field of fractions $F(X)$. Its elements are quotients f/g, f and g polynomials, $g \neq 0$.

Factoring polynomials

The following results help in deciding whether a polynomial is reducible, and in finding its factors.

PROPOSITION 1.11 *Let $r \in \mathbb{Q}$ be a root of a polynomial*

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z},$$

and write $r = c/d$, $c, d \in \mathbb{Z}$, $\gcd(c,d) = 1$. Then $c | a_0$ and $d | a_m$.

PROOF. It is clear from the equation

$$a_m c^m + a_{m-1} c^{m-1} d + \cdots + a_0 d^m = 0$$

that $d | a_m c^m$, and therefore, $d | a_m$. Similarly, $c | a_0$. □

EXAMPLE 1.12 The polynomial $f(X) = X^3 - 3X - 1$ is irreducible in $\mathbb{Q}[X]$ because its only possible roots are ± 1, and $f(1) \neq 0 \neq f(-1)$.

PROPOSITION 1.13 (GAUSS'S LEMMA) *Let $f(X) \in \mathbb{Z}[X]$. If $f(X)$ factors nontrivially in $\mathbb{Q}[X]$, then it factors nontrivially in $\mathbb{Z}[X]$.*

PROOF. Let $f = gh$ in $\mathbb{Q}[X]$ with g, h nonconstant. For suitable integers m and n, $g_1 \stackrel{\text{def}}{=} mg$ and $h_1 \stackrel{\text{def}}{=} nh$ have coefficients in $\mathbb{Z}$, and so we have a factorization

$$mnf = g_1 \cdot h_1 \text{ in } \mathbb{Z}[X].$$

If a prime p divides mn, then, looking modulo p, we obtain an equation

$$0 = \overline{g_1} \cdot \overline{h_1} \text{ in } \mathbb{F}_p[X].$$

Since $\mathbb{F}_p[X]$ is an integral domain, this implies that p divides all the coefficients of at least one of the polynomials g_1, h_1, say g_1, so that $g_1 = pg_2$ for some $g_2 \in \mathbb{Z}[X]$. Thus, we have a factorization

$$(mn/p) f = g_2 \cdot h_1 \text{ in } \mathbb{Z}[X].$$

Continuing in this fashion, we eventually remove all the prime factors of mn, and so obtain a nontrivial factorization of f in $\mathbb{Z}[X]$. □

PROPOSITION 1.14 *If $f \in \mathbb{Z}[X]$ is monic, then every monic factor of f in $\mathbb{Q}[X]$ lies in $\mathbb{Z}[X]$.*

PROOF. Let g be a monic factor of f in $\mathbb{Q}[X]$, so that $f = gh$ with $h \in \mathbb{Q}[X]$ also monic. Let m, n be the positive integers with the fewest prime factors such that $mg, nh \in \mathbb{Z}[X]$. As in the proof of Gauss's Lemma, if a prime p divides mn, then it divides all the coefficients of at least one of the polynomials mg, nh, say mg, in which case it divides m because g is monic. Now $\frac{m}{p} g \in \mathbb{Z}[X]$, which contradicts the definition of m. □

ASIDE 1.15 We sketch an alternative proof of Proposition 1.14. A complex number α is said to be an ***algebraic integer*** if it is a root of a monic polynomial in $\mathbb{Z}[X]$. Proposition 1.11 shows that every algebraic integer in $\mathbb{Q}$ lies in $\mathbb{Z}$. The algebraic integers form a subring of $\mathbb{C}$ — see Theorem 6.5 of my notes on Commutative Algebra. Now let $\alpha_1, \ldots, \alpha_m$ be the roots of f in $\mathbb{C}$. By definition, they are algebraic integers, and the coefficients of any monic factor of f are polynomials in (certain of) the α_i, and therefore are algebraic integers. If they lie in $\mathbb{Q}$, then they lie in $\mathbb{Z}$.

PROPOSITION 1.16 (EISENSTEIN'S CRITERION) *Let*

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0, \quad a_i \in \mathbb{Z};$$

suppose that there is a prime p such that:

- ◇ *p does not divide a_m,*
- ◇ *p divides $a_{m-1}, \ldots, a_0$,*
- ◇ *p^2 does not divide a_0.*

Then f is irreducible in $\mathbb{Q}[X]$.

PROOF. If $f(X)$ factors nontrivially in $\mathbb{Q}[X]$, then it factors nontrivially in $\mathbb{Z}[X]$, say,

$$a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0 = (b_r X^r + \cdots + b_0)(c_s X^s + \cdots + c_0)$$

with $b_i, c_i \in \mathbb{Z}$ and $r, s < m$. Since p, but not p^2, divides $a_0 = b_0 c_0$, p must divide exactly one of b_0, c_0, say, b_0. Now from the equation

$$a_1 = b_0 c_1 + b_1 c_0,$$

we see that $p | b_1$, and from the equation

$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0,$$

that $p | b_2$. By continuing in this way, we find that p divides $b_0, b_1, \ldots, b_r$, which contradicts the condition that p does not divide a_m. □

The last three propositions hold *mutatis mutandis* with $\mathbb{Z}$ replaced by a unique factorization domain R (replace $\mathbb{Q}$ with the field of fractions of R and p with a prime element of R).

REMARK 1.17 There is an algorithm for factoring a polynomial in $\mathbb{Q}[X]$. To see this, consider $f \in \mathbb{Q}[X]$. Multiply $f(X)$ by a rational number so that it is monic, and then replace it by $D^{\deg(f)} f(\frac{X}{D})$, with D equal to a common denominator for the coefficients of f, to obtain a monic polynomial with integer coefficients. Thus we need consider only polynomials

$$f(X) = X^m + a_1 X^{m-1} + \cdots + a_m, \quad a_i \in \mathbb{Z}.$$

From the fundamental theorem of algebra (see 5.6 below), we know that f splits completely in $\mathbb{C}[X]$:

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}.$$

From the equation

$$0 = f(\alpha_i) = \alpha_i^m + a_1 \alpha_i^{m-1} + \cdots + a_m,$$

it follows that $|\alpha_i|$ is less than some bound depending only on the degree and coefficients of f; in fact,

$$|\alpha_i| \leq \max\{1, mB\}, \; B = \max |a_i|.$$

Now if $g(X)$ is a monic factor of $f(X)$, then its roots in $\mathbb{C}$ are certain of the α_i, and its coefficients are symmetric polynomials in its roots (see p. 75). Therefore, the absolute values of the coefficients of $g(X)$ are bounded in terms of the degree and coefficients of f. Since they are also integers (by 1.14), we see that there are only finitely many possibilities for

$g(X)$. Thus, to find the factors of $f(X)$ we (better PARI) have to do only a finite amount of checking.[2]

Therefore, we need not concern ourselves with the problem of factoring polynomials in the rings $\mathbb{Q}[X]$ or $\mathbb{F}_p[X]$ since PARI knows how to do it. For example, typing `content(6*X^2+18*X-24)` in PARI returns 6, and `factor(6*X^2+18*X-24)` returns $X-1$ and $X+4$, showing that

$$6X^2+18X-24 = 6(X-1)(X+4)$$

in $\mathbb{Q}[X]$. Typing `factormod(X^2+3*X+3,7)` returns $X+4$ and $X+6$, showing that

$$X^2+3X+3 = (X+4)(X+6)$$

in $\mathbb{F}_7[X]$.

REMARK 1.18 One other observation is useful. Let $f \in \mathbb{Z}[X]$. If the leading coefficient of f is not divisible by a prime p, then a nontrivial factorization $f = gh$ in $\mathbb{Z}[X]$ will give a nontrivial factorization $\overline{f} = \overline{g}\overline{h}$ in $\mathbb{F}_p[X]$. Thus, if $f(X)$ is irreducible in $\mathbb{F}_p[X]$ for some prime p not dividing its leading coefficient, then it is irreducible in $\mathbb{Z}[X]$. This test is very useful, but it is not always effective: for example, X^4-10X^2+1 is irreducible in $\mathbb{Z}[X]$ but it is reducible[3] modulo every prime p.

Extension fields

A field E containing a field F is called an ***extension field*** of F (or simply an ***extension*** of F, and we speak of an extension E/F). Such an E can be regarded as an F-vector space. The dimension of E as an F-vector space is called the ***degree*** of E over F, and is denote by $[E:F]$. We say that E is ***finite*** over F when it has finite degree over F.

When E and E' are extension fields of F, an ***F-homomorphism*** $E \to E'$ is a homomorphism $\varphi: E \to E'$ such that $\varphi(c) = c$ for all $c \in F$.

EXAMPLE 1.19 (a) The field of complex numbers $\mathbb{C}$ has degree 2 over $\mathbb{R}$ (basis $\{1, i\}$).

(b) The field of real numbers $\mathbb{R}$ has infinite degree over $\mathbb{Q}$: the field $\mathbb{Q}$ is countable, and so every finite-dimensional $\mathbb{Q}$-vector space is also countable, but a famous argument of Cantor shows that $\mathbb{R}$ is not countable.

---

[2] Of course, there are much faster methods than this. The Berlekamp–Zassenhaus algorithm factors the polynomial over certain suitable finite fields $\mathbb{F}_p$, lifts the factorizations to rings $\mathbb{Z}/p^m\mathbb{Z}$ for some m, and then searches for factorizations in $\mathbb{Z}[X]$ with the correct form modulo p^m.

[3] Here is a proof using only that the product of two nonsquares in $\mathbb{F}_p^\times$ is a square, which follows from the fact that $\mathbb{F}_p^\times$ is cyclic (see Exercise 1-3). If 2 is a square in $\mathbb{F}_p$, then

$$X^4-10X^2+1 = (X^2-2\sqrt{2}X-1)(X^2+2\sqrt{2}X-1).$$

If 3 is a square in $\mathbb{F}_p$, then

$$X^4-10X^2+1 = (X^2-2\sqrt{3}X+1)(X^2+2\sqrt{3}X+1).$$

If neither 2 nor 3 are squares, 6 will be a square in $\mathbb{F}_p$, and

$$X^4-10X^2+1 = (X^2-(5+2\sqrt{6}))(X^2-(5-2\sqrt{6})).$$

The general study of such polynomials requires nonelementary methods. See, for example, the paper Brandl, AMM, **93** (1986), pp. 286–288, which proves that for every composite integer $n \geq 1$, there exists a polynomial in $\mathbb{Z}[X]$ of degree n that is irreducible over $\mathbb{Z}$ but reducible modulo all primes.

(c) The field of ***Gaussian numbers***

$$\mathbb{Q}(i) \stackrel{\text{def}}{=} \{a+bi \in \mathbb{C} \mid a,b \in \mathbb{Q}\}$$

has degree 2 over $\mathbb{Q}$ (basis $\{1,i\}$).

(d) The field $F(X)$ has infinite degree over F; in fact, even its subspace $F[X]$ has infinite dimension over F (basis $1, X, X^2, \ldots$).

PROPOSITION 1.20 (MULTIPLICATIVITY OF DEGREES) *Consider fields $L \supset E \supset F$. Then L/F is of finite degree if and only if L/E and E/F are both of finite degree, in which case*

$$[L\colon F] = [L\colon E][E\colon F].$$

PROOF. If L is finite over F, then it is certainly finite over E; moreover, E, being a subspace of a finite-dimensional F-vector space, is also finite-dimensional.

Thus, assume that L/E and E/F are of finite degree, and let $(e_i)_{1\le i\le m}$ be a basis for E as an F-vector space and let $(l_j)_{1\le j\le n}$ be a basis for L as an E-vector space. To complete the proof of the proposition, it suffices to show that $(e_i l_j)_{1\le i\le m, 1\le j\le n}$ is a basis for L over F, because then L will be finite over F of the predicted degree.

First, $(e_i l_j)_{i,j}$ spans L. Let $\gamma \in L$. Then, because $(l_j)_j$ spans L as an E-vector space,

$$\gamma = \textstyle\sum_j \alpha_j l_j, \qquad \text{some } \alpha_j \in E,$$

and because $(e_i)_i$ spans E as an F-vector space,

$$\alpha_j = \textstyle\sum_i a_{ij} e_i, \qquad \text{some } a_{ij} \in F.$$

On putting these together, we find that

$$\gamma = \textstyle\sum_{i,j} a_{ij} e_i l_j.$$

Second, $(e_i l_j)_{i,j}$ is linearly independent. A linear relation $\sum a_{ij} e_i l_j = 0$, $a_{ij} \in F$, can be rewritten $\sum_j (\sum_i a_{ij} e_i) l_j = 0$. The linear independence of the l_j's now shows that $\sum_i a_{ij} e_i = 0$ for each j, and the linear independence of the e_i's shows that each $a_{ij} = 0$. □

The subring generated by a subset

An intersection of subrings of a ring is again a ring (this is easy to prove). Let F be a subfield of a field E, and let S be a subset of E. The intersection of all the subrings of E containing F and S is obviously the smallest subring of E containing both F and S. We call it the subring of E ***generated by F and S*** (or ***generated over F by S***), and we denote it by $F[S]$. When $S = \{\alpha_1, \ldots, \alpha_n\}$, we write $F[\alpha_1, \ldots, \alpha_n]$ for $F[S]$. For example, $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$.

LEMMA 1.21 *The ring $F[S]$ consists of the elements of E that can be expressed as finite sums of the form*

$$\sum a_{i_1 \cdots i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n}, \quad a_{i_1 \cdots i_n} \in F, \quad \alpha_i \in S, \quad i_j \in \mathbb{N}. \tag{1}$$

PROOF. Let R be the set of all such elements. Obviously, R is a subring of E containing F and S and contained in every other such subring. Therefore it equals $F[S]$. □

EXAMPLE 1.22 The ring $\mathbb{Q}[\pi]$, $\pi = 3.14159...$, consists of the real numbers that can be expressed as a finite sum

$$a_0 + a_1\pi + a_2\pi^2 + \cdots + a_n\pi^n, \quad a_i \in \mathbb{Q}.$$

The ring $\mathbb{Q}[i]$ consists of the complex numbers of the form $a + bi$, $a, b \in \mathbb{Q}$.

Note that the expression of an element in the form (1) will *not* be unique in general. This is so already in $\mathbb{R}[i]$.

LEMMA 1.23 *Let R be an integral domain containing a subfield F (as a subring). If R is finite-dimensional when regarded as an F-vector space, then it is a field.*

PROOF. Let α be a nonzero element of R — we have to show that α has an inverse in R. The map $x \mapsto \alpha x: R \to R$ is an injective linear map of finite-dimensional F-vector spaces, and is therefore surjective. In particular, there is an element $\beta \in R$ such that $\alpha\beta = 1$. □

Note that the lemma applies to the subrings containing F of an extension field E of F of finite degree.

The subfield generated by a subset

An intersection of subfields of a field is again a field. Let F be a subfield of a field E, and let S be a subset of E. The intersection of all the subfields of E containing F and S is obviously the smallest subfield of E containing both F and S. We call it the subfield of E ***generated by F and S*** (or ***generated over F by S***), and we denote it $F(S)$. It is the field of fractions of $F[S]$ in E because this is a subfield of E containing F and S and contained in every other such field. When $S = \{\alpha_1, ..., \alpha_n\}$, we write $F(\alpha_1, ..., \alpha_n)$ for $F(S)$. Thus, $F[\alpha_1, \ldots, \alpha_n]$ consists of all elements of E that can be expressed as polynomials in the α_i with coefficients in F, and $F(\alpha_1, \ldots, \alpha_n)$ consists of all elements of E that can be expressed as a quotient of two such polynomials.

Lemma 1.23 shows that $F[S]$ is already a field if it is finite-dimensional over F, in which case $F(S) = F[S]$.

EXAMPLE 1.24 (a) The field $\mathbb{Q}(\pi)$, $\pi = 3.14\ldots$, consists of the complex numbers that can be expressed as a quotient

$$g(\pi)/h(\pi), \quad g(X), h(X) \in \mathbb{Q}[X], \quad h(X) \neq 0.$$

(b) The ring $\mathbb{Q}[i]$ is already a field.

An extension E of F is said to be ***simple*** if $E = F(\alpha)$ some $\alpha \in E$. For example, $\mathbb{Q}(\pi)$ and $\mathbb{Q}[i]$ are simple extensions of $\mathbb{Q}$.

Let F and F' be subfields of a field E. The intersection of the subfields of E containing both F and F' is obviously the smallest subfield of E containing both F and F'. We call it the ***composite*** of F and F' in E, and we denote it by $F \cdot F'$. It can also be described as the subfield of E generated over F by F', or the subfield generated over F' by F:

$$F(F') = F \cdot F' = F'(F).$$

Construction of some extension fields

Let $f(X) \in F[X]$ be a monic polynomial of degree m, and let (f) be the ideal generated by f. Consider the quotient ring $F[X]/(f(X))$, and write x for the image of X in $F[X]/(f(X))$, i.e., x is the coset $X + (f(X))$.

(a) The map

$$P(X) \mapsto P(x): F[X] \to F[x]$$

is a homomorphism sending $f(X)$ to 0. Therefore, $f(x) = 0$.

(b) The division algorithm shows that each element g of $F[X]/(f)$ is represented by a unique polynomial r of degree $< m$. Hence each element of $F[x]$ can be expressed uniquely as a sum

$$a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}, \qquad a_i \in F. \tag{2}$$

(c) To add two elements, expressed in the form (2), simply add the corresponding coefficients.

(d) To multiply two elements expressed in the form (2), multiply in the usual way, and use the relation $f(x) = 0$ to express the monomials of degree $\geq m$ in x in terms of lower degree monomials.

(e) Now assume that $f(X)$ is irreducible. Then every nonzero $\alpha \in F[x]$ has an inverse, which can be found as follows. Use (b) to write $\alpha = g(x)$ with $g(X)$ a polynomial of degree $\leq m-1$, and use Euclid's algorithm in $F[X]$ to obtain polynomials $a(X)$ and $b(X)$ such that

$$a(X)f(X) + b(X)g(X) = d(X)$$

with $d(X)$ the gcd of f and g. In our case, $d(X)$ is 1 because $f(X)$ is irreducible and $\deg g(X) < \deg f(X)$. When we replace X with x, the equality becomes

$$b(x)g(x) = 1.$$

Hence $b(x)$ is the inverse of $g(x)$.

From these observations, we conclude:

1.25 *For a monic irreducible polynomial $f(X)$ of degree m in $F[X]$,*

$$F[x] \stackrel{\text{def}}{=} F[X]/(f(X))$$

is a field of degree m over F. Moreover, computations in $F[x]$ reduce to computations in F.

Note that, because $F[x]$ is a field, $F(x) = F[x]$.[4]

EXAMPLE 1.26 Let $f(X) = X^2 + 1 \in \mathbb{R}[X]$. Then $\mathbb{R}[x]$ has:

elements: $a + bx$, $a, b \in \mathbb{R}$;

addition: $(a + bx) + (a' + b'x) = (a + a') + (b + b')x$;

multiplication: $(a + bx)(a' + b'x) = (aa' - bb') + (ab' + a'b)x$.

We usually write i for x and $\mathbb{C}$ for $\mathbb{R}[x]$.

EXAMPLE 1.27 Let $f(X) = X^3 - 3X - 1 \in \mathbb{Q}[X]$. We observed in (1.12) that this is irreducible over $\mathbb{Q}$, and so $\mathbb{Q}[x]$ is a field. It has basis $\{1, x, x^2\}$ as a $\mathbb{Q}$-vector space. Let

$$\beta = x^4 + 2x^3 + 3 \in \mathbb{Q}[x].$$

[4] Most authors use $F(x)$ to denote this field. I use $F[x]$ to emphasize the fact that its elements are polynomials in x.

Then using that $x^3-3x-1=0$, we find that $\beta=3x^2+7x+5$. Because X^3-3X-1 is irreducible,

$$\gcd(X^3-3X-1,3X^2+7X+5)=1.$$

In fact, Euclid's algorithm gives

$$(X^3-3X-1)\left(\tfrac{-7}{37}X+\tfrac{29}{111}\right)+(3X^2+7X+5)\left(\tfrac{7}{111}X^2-\tfrac{26}{111}X+\tfrac{28}{111}\right)=1.$$

Hence

$$(3x^2+7x+5)\left(\tfrac{7}{111}x^2-\tfrac{26}{111}x+\tfrac{28}{111}\right)=1,$$

and we have found the inverse of β.

We can also do this in PARI: `beta=Mod(X^4+2*X^3+3,X^3-3*X-1)` reveals that $\beta=3x^2+7x+5$ in $\mathbb{Q}[x]$, and `beta^(-1)` reveals that $\beta^{-1}=\frac{7}{111}x^2-\frac{26}{111}x+\frac{28}{111}$.

Stem fields

Let f be a monic irreducible polynomial in $F[X]$. A pair (E,α) consisting of an extension E of F and an $\alpha\in E$ is called[5] a ***stem field for*** f if $E=F[\alpha]$ and $f(\alpha)=0$. For example, the pair (E,α) with $E=F[X]/(f)=F[x]$ and $\alpha=x$ is a stem field for f. Let (E,α) be a stem field, and consider the surjective homomorphism of F-algebras

$$g(X)\mapsto g(\alpha)\colon F[X]\to E.$$

Its kernel is generated by a nonzero monic polynomial, which divides f, and so must equal it. Therefore the homomorphism defines an F-isomorphism

$$x\mapsto\alpha\colon F[x]\to E,\quad F[x]\stackrel{\text{def}}{=}F[X]/(f).$$

In other words, the stem field (E,α) of f is F-isomorphic to the standard stem field $(F[X]/(f),x)$. It follows that every element of a stem field (E,α) for f can be written uniquely in the form

$$a_0+a_1\alpha+\cdots+a_{m-1}\alpha^{m-1},\quad a_i\in F,\quad m=\deg(f),$$

and that arithmetic in $F[\alpha]$ can be performed using the same rules as in $F[x]$. If (E',α') is a second stem field for f, then there is a unique F-isomorphism $E\to E'$ sending α to α'. We sometimes abbreviate "stem field $(F[\alpha],\alpha)$" to "stem field $F[\alpha]$".

Algebraic and transcendental elements

For a field F and an element α of an extension field E, we have a homomorphism

$$f(X)\mapsto f(\alpha)\colon F[X]\to E.$$

There are two possibilities.

CASE 1: The kernel of the map is (0), so that, for $f\in F[X]$,

$$f(\alpha)=0\implies f=0\ (\text{in } F[X]).$$

[5] Following A.A. Albert (Modern Higher Algebra, 1937) who calls the splitting field of a polynomial its root field.

In this case, we say that α ***transcendental over*** F. The homomorphism $X \mapsto \alpha: F[X] \to F[\alpha]$ is an isomorphism, and it extends to an isomorphism $F(X) \to F(\alpha)$ on the fields of fractions.

CASE 2: The kernel is $\neq (0)$, so that $g(\alpha) = 0$ for some nonzero $g \in F[X]$. In this case, we say that α is ***algebraic over*** F. The polynomials g such that $g(\alpha) = 0$ form a nonzero ideal in $F[X]$, which is generated by the monic polynomial f of least degree such $f(\alpha) = 0$. We call f the ***minimum (or minimal) polynomial*** of α over F. It is irreducible, because otherwise there would be two nonzero elements of E whose product is zero. The minimum polynomial is characterized as an element of $F[X]$ by each of the following conditions:

- f is monic, $f(\alpha) = 0$, and f divides every other g in $F[X]$ such that $g(\alpha) = 0$;
- f is the monic polynomial of least degree such that $f(\alpha) = 0$;
- f is monic, irreducible, and $f(\alpha) = 0$.

Note that $g(X) \mapsto g(\alpha)$ defines an isomorphism $F[X]/(f) \to F[\alpha]$. Since the first is a field, so also is the second:

$$F(\alpha) = F[\alpha].$$

Thus, $F[\alpha]$ is a stem field for f.

EXAMPLE 1.28 Let $\alpha \in \mathbb{C}$ be such that $\alpha^3 - 3\alpha - 1 = 0$. Then $X^3 - 3X - 1$ is monic, irreducible, and has α as a root, and so it is the minimum polynomial of α over $\mathbb{Q}$. The set $\{1, \alpha, \alpha^2\}$ is a basis for $\mathbb{Q}[\alpha]$ over $\mathbb{Q}$. The calculations in Example 1.27 show that if β is the element $\alpha^4 + 2\alpha^3 + 3$ of $\mathbb{Q}[\alpha]$, then $\beta = 3\alpha^2 + 7\alpha + 5$, and

$$\beta^{-1} = \tfrac{7}{111}\alpha^2 - \tfrac{26}{111}\alpha + \tfrac{28}{111}.$$

REMARK 1.29 PARI knows how to compute in $\mathbb{Q}[\alpha]$. For example, `factor(X^4+4)` returns the factorization

$$X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$$

in $\mathbb{Q}[X]$. Now type `nf=nfinit(a^2+2*a+2)` to define a number field "nf" generated over $\mathbb{Q}$ by a root a of $X^2 + 2X + 2$. Then `nffactor(nf,x^4+4)` returns the factorization

$$X^4 + 4 = (X - a - 2)(X - a)(X + a))(X + a + 2),$$

in $\mathbb{Q}[a]$.

A extension E/F of fields is said to be ***algebraic*** (and E is said to be ***algebraic over*** F), if all elements of E are algebraic over F; otherwise it is said to be ***transcendental*** (and E is said to be ***transcendental over*** F). Thus, E/F is transcendental if at least one element of E is transcendental over F.

PROPOSITION 1.30 *Let $E \supset F$ be fields. If E/F is finite, then E is algebraic and finitely generated (as a field) over F; conversely, if E is generated over F by a finite set of algebraic elements, then it is finite over F.*

PROOF. $\Longrightarrow$: To say that α is transcendental over F amounts to saying that its powers $1, \alpha, \alpha^2, \dots$ are linearly independent over F. Therefore, if E is finite over F, then it is algebraic over F. It remains to show that E is finitely generated over F. If $E = F$, then it is generated by the empty set. Otherwise, there exists an $\alpha_1 \in E \smallsetminus F$. If $E \neq F[\alpha_1]$, there exists an $\alpha_2 \in E \smallsetminus F[\alpha_1]$, and so on. Since

$$[F[\alpha_1]: F] < [F[\alpha_1, \alpha_2]: F] < \cdots < [E: F]$$

this process terminates with $E = F[\alpha_1, \alpha_2, \ldots]$.

$\Longleftarrow$: Let $E = F(\alpha_1, ..., \alpha_n)$ with $\alpha_1, \alpha_2, \ldots \alpha_n$ algebraic over F. The extension $F(\alpha_1)/F$ is finite because α_1 is algebraic over F, and the extension $F(\alpha_1, \alpha_2)/F(\alpha_1)$ is finite because α_2 is algebraic over F and hence over $F(\alpha_1)$. Thus, by (1.20), $F(\alpha_1, \alpha_2)$ is finite over F. Now repeat the argument. □

COROLLARY 1.31 *(a) If E is algebraic over F, then every subring R of E containing F is a field.*

(b) Consider fields $L \supset E \supset F$. If L is algebraic over E and E is algebraic over F, then L is algebraic over F.

PROOF. (a) If $\alpha \in R$, then $F[\alpha] \subset R$. But $F[\alpha]$ is a field because α is algebraic (see p. 18), and so R contains α^{-1}.

(b) By assumption, every $\alpha \in L$ is a root of a monic polynomial

$$X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in E[X].$$

Each of the extensions

$$F[a_0, \ldots, a_{m-1}, \alpha] \supset F[a_0, \ldots, a_{m-1}] \supset F[a_0, \ldots, a_{m-2}] \supset \cdots \supset F$$

is generated by a single algebraic element, and so is finite. Therefore $F[a_0, \ldots, a_{m-1}, \alpha]$ is finite over F (see 1.20), which implies that α is algebraic over F. □

Transcendental numbers

A complex number is said to be ***algebraic*** or ***transcendental*** according as it is algebraic or transcendental over $\mathbb{Q}$. First some history:

1844: Liouville showed that certain numbers, now called Liouville numbers, are transcendental.

1873: Hermite showed that e is transcendental.

1874: Cantor showed that the set of algebraic numbers is countable, but that $\mathbb{R}$ is not countable. Thus most numbers are transcendental (but it is usually very difficult to prove that any particular number is transcendental).[6]

1882: Lindemann showed that π is transcendental.

1934: Gel'fond and Schneider independently showed that α^β is transcendental if α and β are algebraic, $\alpha \neq 0, 1$, and $\beta \notin \mathbb{Q}$. (This was the seventh of Hilbert's famous problems.)

2018: Euler's constant

$$\gamma \stackrel{\text{def}}{=} \lim_{n\to\infty} \left(\sum_{k=1}^{n} 1/k - \log n \right)$$

has not yet been proven to be transcendental or even irrational (see Lagarias, Euler's constant. BAMS 50 (2013), 527–628; arXiv:1303:1856).

2018: The numbers $e + \pi$ and $e - \pi$ are surely transcendental, but again they have not even been proved to be irrational!

PROPOSITION 1.32 *The set of algebraic numbers is countable.*

[6] By contrast, when we suspect that a complex number is algebraic, it is usually possible to prove this, but not always easily.

PROOF. Define the height $h(r)$ of a rational number to be $\max(|m|,|n|)$, where $r = m/n$ is the expression of r in its lowest terms. There are only finitely many rational numbers with height less than a fixed number N. Let $A(N)$ denote the set of algebraic numbers whose minimum equation over $\mathbb{Q}$ has degree $\leq N$ and has coefficients of height $< N$. Then $A(N)$ is finite for each N. Choose a bijection from some segment $[0,n(1)]$ of $\mathbb{N}$ onto $A(10)$; extend it to a bijection from a segment $[0,n(2)]$ onto $A(100)$, and so on. □

A typical Liouville number is $\sum_{n=0}^{\infty} \frac{1}{10^{n!}}$ — in its decimal expansion there are increasingly long strings of zeros. Since its decimal expansion is not periodic, the number is not rational. We prove that the analogue of this number in base 2 is transcendental.

THEOREM 1.33 *The number* $\alpha = \sum \frac{1}{2^{n!}}$ *is transcendental.*

PROOF. [7]Suppose not, and let

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d, \quad a_i \in \mathbb{Q},$$

be the minimum polynomial of α over $\mathbb{Q}$. Thus $[\mathbb{Q}[\alpha]:\mathbb{Q}] = d$. Choose a nonzero integer D such that $D \cdot f(X) \in \mathbb{Z}[X]$.

Let $\Sigma_N = \sum_{n=0}^{N} \frac{1}{2^{n!}}$, so that $\Sigma_N \to \alpha$ as $N \to \infty$, and let $x_N = f(\Sigma_N)$. As α is not rational, $f(X)$, being irreducible of degree > 1, has no rational root. Since $\Sigma_N \neq \alpha$, it can't be a root of $f(X)$, and so $x_N \neq 0$. Obviously, $x_N \in \mathbb{Q}$; in fact $(2^{N!})^d D x_N \in \mathbb{Z}$, and so

$$|(2^{N!})^d D x_N| \geq 1. \tag{3}$$

From the fundamental theorem of algebra (see 5.6 below), we know that f splits in $\mathbb{C}[X]$, say,

$$f(X) = \prod_{i=1}^{d} (X - \alpha_i), \quad \alpha_i \in \mathbb{C}, \quad \alpha_1 = \alpha,$$

and so

$$|x_N| = \prod_{i=1}^{d} |\Sigma_N - \alpha_i| \leq |\Sigma_N - \alpha_1| (\Sigma_N + M)^{d-1}, \quad \text{where } M = \max_{i \neq 1}\{1, |\alpha_i|\}.$$

But

$$|\Sigma_N - \alpha_1| = \sum_{n=N+1}^{\infty} \frac{1}{2^{n!}} \leq \frac{1}{2^{(N+1)!}} \left(\sum_{n=0}^{\infty} \frac{1}{2^n} \right) = \frac{2}{2^{(N+1)!}}.$$

Hence

$$|x_N| \leq \frac{2}{2^{(N+1)!}} \cdot (\Sigma_N + M)^{d-1}$$

and

$$|(2^{N!})^d D x_N| \leq 2 \cdot \frac{2^{d \cdot N!} D}{2^{(N+1)!}} \cdot (\Sigma_N + M)^{d-1}$$

which tends to 0 as $N \to \infty$ because $\frac{2^{d \cdot N!}}{2^{(N+1)!}} = \left(\frac{2^d}{2^{N+1}} \right)^{N!} \to 0$. This contradicts (3). □

[7]This proof, which I learnt from David Masser, also works for $\sum \frac{1}{a^{n!}}$ for every integer $a \geq 2$.

Constructions with straight-edge and compass.

The Greeks understood integers and the rational numbers. They were surprised to find that the length of the diagonal of a square of side 1, namely, $\sqrt{2}$, is not rational. They thus realized that they needed to extend their number system. They then hoped that the "constructible" numbers would suffice. Suppose we are given a length, which we call 1, a straight-edge, and a compass (device for drawing circles). A real number (better a length) is ***constructible*** if it can be constructed by forming successive intersections of

- ◇ lines drawn through two points already constructed, and
- ◇ circles with centre a point already constructed and radius a constructed length.

This led them to three famous questions that they were unable to answer: is it possible to duplicate the cube, trisect an angle, or square the circle by straight-edge and compass constructions? We'll see that the answer to all three is negative.

Let F be a subfield of $\mathbb{R}$. For a positive $a \in F$, $\sqrt{a}$ denotes the positive square root of a in $\mathbb{R}$. The ***F-plane*** is $F \times F \subset \mathbb{R} \times \mathbb{R}$. We make the following definitions:

An ***F-line*** is a line in $\mathbb{R} \times \mathbb{R}$ through two points in the F-plane. These are the lines given by equations

$$ax + by + c = 0, \quad a, b, c \in F.$$

An ***F-circle*** is a circle in $\mathbb{R} \times \mathbb{R}$ with centre an F-point and radius an element of F. These are the circles given by equations

$$(x-a)^2 + (y-b)^2 = c^2, \quad a, b, c \in F.$$

LEMMA 1.34 *Let $L \neq L'$ be F-lines, and let $C \neq C'$ be F-circles.*

(a) *$L \cap L' = \emptyset$ or consists of a single F-point.*

(b) *$L \cap C = \emptyset$ or consists of one or two points in the $F[\sqrt{e}]$-plane, some $e \in F$, $e > 0$.*

(c) *$C \cap C' = \emptyset$ or consists of one or two points in the $F[\sqrt{e}]$-plane, some $e \in F$, $e > 0$.*

PROOF. The points in the intersection are found by solving the simultaneous equations, and hence by solving (at worst) a quadratic equation with coefficients in F. □

LEMMA 1.35 *(a) If c and d are constructible, then so also are $c + d$, $-c$, cd, and $\frac{c}{d}$ $(d \neq 0)$.*

(b) If $c > 0$ is constructible, then so also is $\sqrt{c}$.

SKETCH OF PROOF. First show that it is possible to construct a line perpendicular to a given line through a given point, and then a line parallel to a given line through a given point. Hence it is possible to construct a triangle similar to a given one on a side with given length. By an astute choice of the triangles, one constructs cd and c^{-1}. For (b), draw a circle of radius $\frac{c+1}{2}$ and centre $(\frac{c+1}{2}, 0)$, and draw a vertical line through the point $A = (1, 0)$ to meet the circle at P. The length AP is $\sqrt{c}$. (For more details, see Artin, M., Algebra, 1991, Chapter 13, Section 4.) □

THEOREM 1.36 (a) *The set of constructible numbers is a field.*

(b) *A number α is constructible if and only if it is contained in a subfield of $\mathbb{R}$ of the form*

$$\mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}], \quad a_i \in \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}], \quad a_i > 0.$$

PROOF. (a) This restates (a) of Lemma 1.35.

(b) It follows from Lemma 1.34 that every constructible number is contained in such a field $\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_r}]$. Conversely, if all the elements of $\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_{i-1}}]$ are constructible, then $\sqrt{a_i}$ is constructible (by 1.35b), and so all the elements of $\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_i}]$ are constructible (by (a)). Applying this for $i = 0, 1, \dots$, we find that all the elements of $\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_r}]$ are constructible. □

COROLLARY 1.37 *If α is constructible, then α is algebraic over $\mathbb{Q}$, and $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ is a power of 2.*

PROOF. According to Proposition 1.20, $[\mathbb{Q}[\alpha]:\mathbb{Q}]$ divides

$$[\mathbb{Q}[\sqrt{a_1}]\cdots[\sqrt{a_r}]:\mathbb{Q}]$$

and $[\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_r}]:\mathbb{Q}]$ is a power of 2. □

COROLLARY 1.38 *It is impossible to duplicate the cube by straight-edge and compass constructions.*

PROOF. The problem is to construct a cube with volume 2. This requires constructing the real root of the polynomial X^3-2. But this polynomial is irreducible (by Eisenstein's criterion 1.16 for example), and so $[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}] = 3$. □

COROLLARY 1.39 *In general, it is impossible to trisect an angle by straight-edge and compass constructions.*

PROOF. Knowing an angle is equivalent to knowing the cosine of the angle. Therefore, to trisect 3α, we have to construct a solution to

$$\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha.$$

For example, take $3\alpha = 60$ degrees. As $\cos 60° = \frac{1}{2}$, to construct α, we have to solve $8x^3-6x-1=0$, which is irreducible (apply 1.11), and so $[\mathbb{Q}[\alpha]:\mathbb{Q}] = 3/$ □

COROLLARY 1.40 *It is impossible to square the circle by straight-edge and compass constructions.*

PROOF. A square with the same area as a circle of radius r has side $\sqrt{\pi}r$. Since π is transcendental[8], so also is $\sqrt{\pi}$. □

We next consider another problem that goes back to the ancient Greeks: list the integers n such that the regular n-sided polygon can be constructed using only straight-edge and compass. Here we consider the question for a prime p (see 5.12 for the general case). Note that X^p-1 is not irreducible; in fact

$$X^p-1 = (X-1)(X^{p-1}+X^{p-2}+\cdots+1).$$

LEMMA 1.41 *If p is prime, then $X^{p-1}+\cdots+1$ is irreducible; hence $\mathbb{Q}[e^{2\pi i/p}]$ has degree $p-1$ over $\mathbb{Q}$.*

[8]Proofs of this can be found in many books on number theory, for example, in 11.14 of Hardy, G. H., and Wright, E. M., An Introduction to the Theory of Numbers, Fourth Edition, Oxford, 1960.

PROOF. Let $f(X) = (X^p - 1)/(X - 1) = X^{p-1} + \cdots + 1$; then

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + a_i X^i + \cdots + p,$$

with $a_i = \binom{p}{i+1}$. Now $p | a_i$ for $i = 1, ..., p-2$, and so $f(X+1)$ is irreducible by Eisenstein's criterion 1.16. This implies that $f(X)$ is irreducible. □

In order to construct a regular p-gon, p an odd prime, we need to construct

$$\cos\frac{2\pi}{p} = \frac{e^{\frac{2\pi i}{p}} + e^{-\frac{2\pi i}{p}}}{2}.$$

Note that

$$\mathbb{Q}[e^{\frac{2\pi i}{p}}] \supset \mathbb{Q}[\cos\tfrac{2\pi}{p}] \supset \mathbb{Q}.$$

The degree of $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$ over $\mathbb{Q}[\cos\frac{2\pi}{p}]$ is 2 because the equation

$$\alpha^2 - 2\cos\frac{2\pi}{p}\cdot\alpha + 1 = 0, \quad \alpha = e^{\frac{2\pi i}{p}},$$

shows that it is at most 2, and it is not 1 because $e^{\frac{2\pi i}{p}} \notin \mathbb{R}$. Hence

$$[\mathbb{Q}[\cos\tfrac{2\pi}{p}]:\mathbb{Q}] = \frac{p-1}{2}.$$

We deduce that, if the regular p-gon is constructible, then $(p-1)/2$ is a power of 2; later (5.12) we'll prove the converse statement. Thus, the regular p-gon is constructible if and only if $p = 2^r + 1$ for some positive integer r.

A number $2^r + 1$ can be prime only if r is a power of 2: if t is odd, then

$$Y^t + 1 = (Y+1)(Y^{t-1} - Y^{t-2} + \cdots + 1)$$

and so

$$2^{st} + 1 = (2^s + 1)((2^s)^{t-1} - (2^s)^{t-2} + \cdots + 1).$$

We conclude that the primes p for which the regular p-gon is constructible are exactly those of the form $2^{2^r} + 1$ for some r. Such p are called ***Fermat primes*** (because Fermat conjectured that all numbers of the form $2^{2^r} + 1$ are prime). For $r = 0, 1, 2, 3, 4$, we have $2^{2^r} + 1 = 3, 5, 17, 257, 65537$, which are indeed prime, but Euler showed that $2^{32} + 1 = (641)(6700417)$, and we don't know whether there are any more Fermat primes. Thus, we do not know the list of primes p for which the regular p-gon is constructible.

Gauss showed that[9]

$$\cos\frac{2\pi}{17} = -\frac{1}{16} + \frac{1}{16}\sqrt{17} + \frac{1}{16}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

when he was 18 years old. This success encouraged him to become a mathematician.

[9] Or perhaps that

$$\cos\tfrac{2\pi}{17} = -\tfrac{1}{16} + \tfrac{1}{16}\sqrt{17} + \tfrac{1}{16}\sqrt{34 - 2\sqrt{17}} + \tfrac{1}{8}\sqrt{17 + 3\sqrt{17} - 2\sqrt{34 - 2\sqrt{17}} - \sqrt{170 - 26\sqrt{17}}}$$

— both expressions are correct.

Algebraically closed fields

We say that a polynomial ***splits*** in $F[X]$ (or, more loosely, in F) if it is a product of polynomials of degree 1 in $F[X]$.

PROPOSITION 1.42 *For a field Ω, the following statements are equivalent:*

(a) *Every nonconstant polynomial in $\Omega[X]$ splits in $\Omega[X]$.*

(b) *Every nonconstant polynomial in $\Omega[X]$ has at least one root in Ω.*

(c) *The irreducible polynomials in $\Omega[X]$ are those of degree 1.*

(d) *Every field of finite degree over Ω equals Ω.*

PROOF. The implications (a)⇒(b)⇒(c) are obvious.
(c)⇒(a). This follows from the fact that $\Omega[X]$ is a unique factorization domain.
(c)⇒(d). Let E be a finite extension of Ω, and let $\alpha \in E$. The minimum polynomial of α, being irreducible, has degree 1, and so $\alpha \in \Omega$.
(d)⇒(c). Let f be an irreducible polynomial in $\Omega[X]$. Then $\Omega[X]/(f)$ is an extension field of Ω of degree $\deg(f)$ (see 1.30), and so $\deg(f) = 1$. □

DEFINITION 1.43 (a) A field Ω is ***algebraically closed*** if it satisfies the equivalent statements of Proposition 1.42.

(b) A field Ω is an ***algebraic closure*** of a subfield F if it is algebraically closed and algebraic over F.

For example, the fundamental theorem of algebra (see 5.6 below) says that $\mathbb{C}$ is algebraically closed. It is an algebraic closure of $\mathbb{R}$.

PROPOSITION 1.44 *If Ω is algebraic over F and every polynomial $f \in F[X]$ splits in $\Omega[X]$, then Ω is algebraically closed (hence an algebraic closure of F).*

PROOF. Let f be a nonconstant polynomial in $\Omega[X]$. We have to show that f has a root in Ω. We know (see 1.25) that f has a root α in some finite extension Ω' of Ω. Set

$$f = a_n X^n + \cdots + a_0, \quad a_i \in \Omega,$$

and consider the fields

$$F \subset F[a_0, \ldots, a_n] \subset F[a_0, \ldots, a_n, \alpha].$$

Each extension generated by a finite set of algebraic elements, and hence is finite (1.30). Therefore α lies in a finite extension of F (see 1.20), and so is algebraic over F — it is a root of a polynomial g with coefficients in F. By assumption, g splits in $\Omega[X]$, and so the roots of g in Ω' all lie in Ω. In particular, $\alpha \in \Omega$. □

PROPOSITION 1.45 *Let $\Omega \supset F$; then*

$$\{\alpha \in \Omega \mid \alpha \text{ algebraic over } F\}$$

is a field.

PROOF. If α and β are algebraic over F, then $F[\alpha, \beta]$ is a field (see 1.31) of finite degree over F (see 1.30). Thus, every element of $F[\alpha, \beta]$ is algebraic over F. In particular, $\alpha \pm \beta$, α/β, and $\alpha\beta$ are algebraic over F. □

The field constructed in the proposition is called the ***algebraic closure of F in Ω***.

COROLLARY 1.46 *Let Ω be an algebraically closed field. For any subfield F of Ω, the algebraic closure of F in Ω is an algebraic closure of F.*

PROOF. From its definition, we see that it is algebraic over F and every polynomial in $F[X]$ splits in it. Now Proposition 1.44 shows that it is an algebraic closure of F. □

Thus, when we admit the fundamental theorem of algebra (5.6), every subfield of $\mathbb{C}$ has an algebraic closure (in fact, a canonical algebraic closure). Later (Chapter 6) we'll prove (using the axiom of choice) that every field has an algebraic closure.

ASIDE 1.47 Although various classes of field, for example, number fields and function fields, had been studied earlier, the first systematic account of the theory of abstract fields was given by Steinitz in 1910 (Algebraische Theorie der Körper, J. Reine Angew. Math., 137:167–309). Here he introduced the notion of a prime field, distinguished between separable and inseparable extensions, and showed that every field can be obtained as an algebraic extension of a purely transcendental extension. He also proved that every field has an algebraic closure, unique up to isomorphism. His work influenced later algebraists (Noether, van der Waerden, Artin, ...) and his article has been described by Bourbaki as "... a fundamental work which may be considered as the origin of today's concept of algebra". See: Roquette, Peter, In memoriam Ernst Steinitz (1871–1928). J. Reine Angew. Math. 648 (2010), 1–11.

Exercises

1-1 Let $E = \mathbb{Q}[\alpha]$, where $\alpha^3 - \alpha^2 + \alpha + 2 = 0$. Express $(\alpha^2 + \alpha + 1)(\alpha^2 - \alpha)$ and $(\alpha - 1)^{-1}$ in the form $a\alpha^2 + b\alpha + c$ with $a, b, c \in \mathbb{Q}$.

1-2 Determine $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$.

1-3 Let F be a field, and let $f(X) \in F[X]$.

(a) For every $a \in F$, show that there is a polynomial $q(X) \in F[X]$ such that

$$f(X) = q(X)(X - a) + f(a).$$

(b) Deduce that $f(a) = 0$ if and only if $(X - a) \mid f(X)$.

(c) Deduce that $f(X)$ can have at most $\deg f$ roots.

(d) Let G be a finite abelian group. If G has at most m elements of order dividing m for each divisor m of $(G : 1)$, show that G is cyclic.

(e) Deduce that a finite subgroup of $F^\times$, F a field, is cyclic.

1-4 Show that with straight-edge, compass, and angle-trisector, it is possible to construct a regular 7-gon.

1-5 Let $f(X)$ be an irreducible polynomial over F of degree n, and let E be a field extension of F with $[E : F] = m$. If $\gcd(m, n) = 1$, show that f is irreducible over E.

1-6 Show that there does not exist a polynomial $f(X) \in \mathbb{Z}[X]$ of degree > 1 that is irreducible modulo p for all primes p.

CHAPTER 2

Splitting Fields; Multiple Roots

Homomorphisms from simple extensions.

Let E and E' be fields containing F. Recall that an F-homomorphism is a homomorphism

$$\varphi: E \to E'$$

such that $\varphi(a) = a$ for all $a \in F$. Thus an F-homomorphism φ maps a polynomial

$$\sum a_{i_1 \cdots i_m} \alpha_1^{i_1} \cdots \alpha_m^{i_m}, \quad a_{i_1 \cdots i_m} \in F, \quad \alpha_i \in E,$$

to

$$\sum a_{i_1 \cdots i_m} \varphi(\alpha_1)^{i_1} \cdots \varphi(\alpha_m)^{i_m}.$$

An ***F-isomorphism*** is a bijective F-homomorphism.

An F-homomorphism $E \to E'$ of fields is, in particular, an injective F-linear map of F-vector spaces, and so it will be an F-isomorphism if E and E' have the same finite degree over F.

PROPOSITION 2.1 *Let $F(\alpha)$ be a simple field extension of a field F, and let Ω be a second field containing F.*

(a) *Let α be transcendental over F. For every F-homomorphism $\varphi: F(\alpha) \to \Omega$, $\varphi(\alpha)$ is transcendental over F, and the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{F\text{-homomorphisms } F(\alpha) \to \Omega\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } F\}.$$

(b) *Let α be algebraic over F with minimum polynomial $f(X)$. For every F-homomorphism $\varphi: F[\alpha] \to \Omega$, $\varphi(\alpha)$ is a root of $f(X)$ in Ω, and the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{F\text{-homomorphisms } \varphi: F[\alpha] \to \Omega\} \leftrightarrow \{\text{roots of } f \text{ in } \Omega\}.$$

In particular, the number of such maps is the number of distinct roots of f in Ω.

PROOF. (a) To say that α is transcendental over F means that $F[\alpha]$ is isomorphic to the polynomial ring in the symbol α. Therefore, for every $\gamma \in \Omega$, there is a unique F-homomorphism $\varphi: F[\alpha] \to \Omega$ such that $\varphi(\alpha) = \gamma$ (see 1.5). This φ extends to the field of fractions $F(\alpha)$ of $F[\alpha]$ if and only if the nonzero elements of $F[\alpha]$ are sent to nonzero elements of Ω, which is the case if and only if γ is transcendental over F. Thus we see that

there are one-to-one correspondences between (a) the F-homomorphisms $F(\alpha) \to \Omega$, (b) the F-homomorphisms $\varphi: F[\alpha] \to \Omega$ such that $\varphi(\alpha)$ is transcendental, (c) the transcendental elements of Ω.

(b) Let $f(X) = \sum a_i X^i$, and consider an F-homomorphism $\varphi: F[\alpha] \to \Omega$. On applying φ to the equality $\sum a_i \alpha^i = 0$, we obtain the equality $\sum a_i \varphi(\alpha)^i = 0$, which shows that $\varphi(\alpha)$ is a root of $f(X)$ in Ω. Conversely, if $\gamma \in \Omega$ is a root of $f(X)$, then the map $F[X] \to \Omega$, $g(X) \mapsto g(\gamma)$, factors through $F[X]/(f(X))$. When composed with the inverse of the isomorphism $X + f(X) \mapsto \alpha: F[X]/(f(X)) \to F[\alpha]$, this becomes a homomorphism $F[\alpha] \to \Omega$ sending α to γ. □

We'll need a slight generalization of this result.

PROPOSITION 2.2 *Let $F(\alpha)$ be a simple field extension of a field F, and let $\varphi_0: F \to \Omega$ be a homomorphism from F into a second field Ω.*

(a) *If α is transcendental over F, then the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{\text{extensions } \varphi: F(\alpha) \to \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{elements of } \Omega \text{ transcendental over } \varphi_0(F)\}.$$

(b) *If α is algebraic over F, with minimum polynomial $f(X)$, then the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

$$\{\text{extensions } \varphi: F[\alpha] \to \Omega \text{ of } \varphi_0\} \leftrightarrow \{\text{roots of } \varphi_0 f \text{ in } \Omega\}.$$

In particular, the number of such maps is the number of distinct roots of $\varphi_0 f$ in Ω.

By $\varphi_0 f$ we mean the polynomial obtained by applying φ_0 to the coefficients of f. By an extension of φ_0 to $F(\alpha)$ we mean a homomorphism $\varphi: F(\alpha) \to \Omega$ whose restriction to F is φ_0.

The proof of the proposition is essentially the same as that of the preceding proposition.

Splitting fields

Let f be a polynomial with coefficients in F. A field E containing F is said to ***split*** f if f splits in $E[X]$:

$$f(X) = a \prod_{i=1}^{m} (X - \alpha_i) \text{ with all } \alpha_i \in E.$$

If E splits f and is generated by the roots of f,

$$E = F[\alpha_1, \dots, \alpha_m],$$

then it is called a ***splitting*** or ***root field*** for f.

Note that $\prod f_i(X)^{m_i}$ $(m_i \geq 1)$ and $\prod f_i(X)$ have the same splitting fields. Note also that f splits in E if it has $\deg(f) - 1$ roots in E because the sum of the roots of f lies in F (if $f = aX^m + a_1 X^{m-1} + \cdots$, then $\sum \alpha_i = -a_1/a$).

EXAMPLE 2.3 (a) Let $f(X) = aX^2 + bX + c \in \mathbb{Q}[X]$, and let $\alpha = \sqrt{b^2 - 4ac}$. The subfield $\mathbb{Q}[\alpha]$ of $\mathbb{C}$ is a splitting field for f.

(b) Let $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ be irreducible, and let $\alpha_1, \alpha_2, \alpha_3$ be its roots in $\mathbb{C}$. Then $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] = \mathbb{Q}[\alpha_1, \alpha_2]$ is a splitting field for $f(X)$. Note that $[\mathbb{Q}[\alpha_1]: \mathbb{Q}] = 3$ and that $[\mathbb{Q}[\alpha_1, \alpha_2]: \mathbb{Q}[\alpha_1]] = 1$ or 2, and so $[\mathbb{Q}[\alpha_1, \alpha_2]: \mathbb{Q}] = 3$ or 6. We'll see later (4.2) that the degree is 3 if and only if the discriminant of $f(X)$ is a square in $\mathbb{Q}$. For example, the discriminant of $X^3 + bX + c$ is $-4b^3 - 27c^2$, and so the splitting field of $X^3 + 10X + 1$ has degree 6 over $\mathbb{Q}$.

PROPOSITION 2.4 *Every polynomial $f \in F[X]$ has a splitting field E_f, and*

$$[E_f : F] \leq (\deg f)! \quad (\textit{factorial } \deg f).$$

PROOF. Let $F_1 = F[\alpha_1]$ be a stem field for some monic irreducible factor of f in $F[X]$. Then $f(\alpha_1) = 0$, and we let $F_2 = F_1[\alpha_2]$ be a stem field for some monic irreducible factor of $f(X)/(X-\alpha_1)$ in $F_1[X]$. Continuing in this fashion, we arrive at a splitting field E_f. Let $n = \deg f$. Then $[F_1 : F] = \deg g_1 \leq n$, $[F_2 : F_1] \leq n-1, \ldots$, and so $[E_f : F] \leq n!$. □

ASIDE 2.5 Let F be a field. For a given integer n, there may or may not exist polynomials of degree n in $F[X]$ whose splitting field has degree $n!$ — this depends on F. For example, there do not exist such polynomials for $n > 1$ if $F = \mathbb{C}$ (see 5.6), nor for $n > 2$ if $F = \mathbb{F}_p$ (see 4.22) or $F = \mathbb{R}$. However, later (4.33) we'll see how to write down infinitely many polynomials of degree n in $\mathbb{Q}[X]$ with splitting fields of degree $n!$.

EXAMPLE 2.6 (a) Let $f(X) = (X^p - 1)/(X-1) \in \mathbb{Q}[X]$, p prime. If ζ is one root of f, then the remaining roots are $\zeta^2, \zeta^3, \ldots, \zeta^{p-1}$, and so the splitting field of f is $\mathbb{Q}[\zeta]$.

(b) Let F have characteristic $p \neq 0$, and let $f = X^p - X - a \in F[X]$. If α is one root of f in some extension of F, then the remaining roots are $\alpha + 1, \ldots, \alpha + p - 1$, and so the splitting field of f is $F[\alpha]$.

(c) If α is one root of $X^n - a$, then the remaining roots are all of the form $\zeta\alpha$, where $\zeta^n = 1$. Therefore, if F contains all the nth roots of 1 (by which we mean that $X^n - 1$ splits in $F[X]$), then $F[\alpha]$ is a splitting field for $X^n - a$. Note that if p is the characteristic of F, then $X^p - 1 = (X-1)^p$, and so F automatically contains all the pth roots of 1.

PROPOSITION 2.7 *Let $f \in F[X]$ be monic*[1]*. Let E be a field containing F and generated over F by roots of f, and let Ω be a field containing F in which f splits.*

(a) *There exists an F-homomorphism $\varphi : E \to \Omega$; the number of such homomorphisms is at most $[E : F]$, and equals $[E : F]$ if f has distinct roots in Ω.*

(b) *If E and Ω are both splitting fields for f, then every F-homomorphism $E \to \Omega$ is an isomorphism. In particular, any two splitting fields for f are F-isomorphic.*

To say that f splits in Ω means that $f(X) = \prod_{i=1}^{\deg(f)}(X - \alpha_i)$ with $\alpha_1, \alpha_2, \ldots \in \Omega$; to say that f has distinct roots in Ω means that $\alpha_i \neq \alpha_j$ if $i \neq j$.

PROOF. We begin with an observation: let F, f, and Ω be as in the statement of the proposition, let L be a subfield of Ω containing F, and let g be a monic factor of f in $L[X]$; then g divides f in $\Omega[X]$ and so (by unique factorization in $\Omega[X]$), g is product of certain number of the factors $X - \alpha_i$ of f in $\Omega[X]$; in particular, we see that g splits in Ω, and that its roots are distinct if the roots of f are distinct.

(a) By hypothesis, $E = F[\alpha_1, \ldots, \alpha_m]$ with each α_i a root of $f(X)$. The minimum polynomial of α_1 is an irreducible polynomial f_1 dividing f. From the initial observation with $L = F$, we see that f_1 splits in Ω, and that its roots are distinct if the roots of f are distinct. According to Proposition 2.1, there exists an F-homomorphism $\varphi_1 : F[\alpha_1] \to \Omega$, and the number of such homomorphisms is at most $[F[\alpha_1] : F]$, with equality holding when f has distinct roots in Ω.

The minimum polynomial of α_2 over $F[\alpha_1]$ is an irreducible factor f_2 of f in $F[\alpha_1][X]$. On applying the initial observation with $L = \varphi_1 F[\alpha_1]$ and $g = \varphi_1 f_2$, we see that $\varphi_1 f_2$ splits in Ω, and that its roots are distinct if the roots of f are distinct. According to Proposition

[1] This hypothesis is not necessary but simplifies the exposition.

2.2, each φ_1 extends to a homomorphism $\varphi_2: F[\alpha_1,\alpha_2] \to \Omega$, and the number of extensions is at most $[F[\alpha_1,\alpha_2]: F[\alpha_1]]$, with equality holding when f has distinct roots in Ω.

On combining these statements we conclude that there exists an F-homomorphism

$$\varphi: F[\alpha_1,\alpha_2] \to \Omega,$$

and that the number of such homomorphisms is at most $[F[\alpha_1,\alpha_2]: F]$, with equality holding if f has distinct roots in Ω.

After repeating the argument m times, we obtain (a).

(b) Every F-homomorphism $E \to \Omega$ is injective, and so, if there exists such a homomorphism, then $[E:F] \le [\Omega:F]$. If E and Ω are both splitting fields for f, then (a) shows that there exist homomorphisms $E \leftrightarrows \Omega$, and so $[E:F] = [\Omega:F]$. It follows that every F-homomorphism $E \to \Omega$ is an F-isomorphism. □

COROLLARY 2.8 *Let E and L be extension fields of F, with E finite over F.*

(a) *The number of F-homomorphisms $E \to L$ is at most $[E:F]$.*

(b) *There exists a finite extension Ω/L and an F-homomorphism $E \to \Omega$.*

PROOF. Write $E = F[\alpha_1,\dots,\alpha_m]$, and let $f \in F[X]$ be the product of the minimum polynomials of the α_i; thus E is generated over F by roots of f. Let Ω be a splitting field for f regarded as an element of $L[X]$. The proposition shows that there exists an F-homomorphism $E \to \Omega$, and the number of such homomorphisms is $\le [E:F]$. This proves (b), and since an F-homomorphism $E \to L$ can be regarded as an F-homomorphism $E \to \Omega$, it also proves (a). □

REMARK 2.9 (a) Let $E_1, E_2, \dots, E_m$ be finite extensions of F, and let L be an extension of F. From the corollary we see that there exists a finite extension L_1/L such that L_1 contains an isomorphic image of E_1; then that there exists a finite extension L_2/L_1 such that L_2 contains an isomorphic image of E_2. On continuing in this fashion, we find that there exists a finite extension Ω/L such that Ω contains an isomorphic copy of every E_i.

(b) Let $f \in F[X]$. If E and E' are both splitting fields of f, then we know there exists an F-isomorphism $E \to E'$, but there will in general be no *preferred* such isomorphism. Error and confusion can result if the fields are simply identified. Also, it makes no sense to speak of "the field $F[\alpha]$ generated by a root of f" unless f is irreducible (the fields generated by the roots of two different factors are unrelated). Even when f is irreducible, it makes no sense to speak of "the field $F[\alpha,\beta]$ generated by two roots α,β of f" (the extensions of $F[\alpha]$ generated by the roots of two different factors of f in $F[\alpha][X]$ may be very different).

Multiple roots

Even when polynomials in $F[X]$ have no common factor in $F[X]$, one might expect that they could acquire a common factor in $\Omega[X]$ for some $\Omega \supset F$. In fact, this doesn't happen — greatest common divisors don't change when the field is extended.

PROPOSITION 2.10 *Let f and g be polynomials in $F[X]$, and let Ω be an extension of F. If $r(X)$ is the gcd of f and g computed in $F[X]$, then it is also the gcd of f and g in $\Omega[X]$. In particular, distinct monic irreducible polynomials in $F[X]$ do not acquire a common root in any extension field of F.*

PROOF. Let $r_F(X)$ and $r_\Omega(X)$ be the greatest common divisors of f and g in $F[X]$ and $\Omega[X]$ respectively. Certainly $r_F(X)|r_\Omega(X)$ in $\Omega[X]$, but Euclid's algorithm (1.8) shows that there are polynomials a and b in $F[X]$ such that

$$a(X)f(X)+b(X)g(X)=r_F(X),$$

and so $r_\Omega(X)$ divides $r_F(X)$ in $\Omega[X]$.

For the second statement, note that the hypotheses imply that $\gcd(f,g)=1$ (in $F[X]$), and so f and g can't acquire a common factor in any extension field. □

The proposition allows us to speak of the greatest common divisor of f and g without reference to a field.

Let $f\in F[X]$. Then f splits into linear factors

$$f(X)=a\prod_{i=1}^{r}(X-\alpha_i)^{m_i},\ \alpha_i \text{ distinct}, m_i\geq 1,\ \sum_{i=1}^{r}m_i=\deg(f), \tag{4}$$

in $\Omega[X]$ for some extension field Ω of F (see 2.4). We say that α_i is a root of f of ***multiplicity*** m_i in Ω. If $m_i>1$, then α_i is said to be a ***multiple root*** of f, and otherwise it is a ***simple root***.

The unordered sequence of integers $m_1,\dots,m_r$ in (4) is independent of the extension field Ω chosen to split f. Certainly, it is unchanged when Ω is replaced with its subfield $F[\alpha_1,\dots,\alpha_m]$, but $F[\alpha_1,\dots,\alpha_m]$ is a splitting field for f, and any two splitting fields are F-isomorphic (2.7b). We say that f ***has a multiple root*** when at least one of the $m_i>1$, and we say that f has ***only simple roots*** when all $m_i=1$.

We wish to determine when a polynomial has a multiple root. If f has a multiple factor in $F[X]$, say $f=\prod f_i(X)^{m_i}$ with some $m_i>1$, then obviously it will have a multiple root. If $f=\prod f_i$ with the f_i distinct monic irreducible polynomials, then Proposition 2.10 shows that f has a multiple root if and only if at least one of the f_i has a multiple root. Thus, it suffices to determine when an *irreducible* polynomial has a multiple root.

EXAMPLE 2.11 Let F be of characteristic $p\neq 0$, and assume that F contains an element a that is not a pth-power, for example, $a=T$ in the field $\mathbb{F}_p(T)$. Then X^p-a is irreducible in $F[X]$, but by 1.4 we have $X^p-a=(X-\alpha)^p$ in its splitting field. Thus an irreducible polynomial can have multiple roots.

The derivative of a polynomial $f(X)=\sum a_iX^i$ is defined to be $f'(X)=\sum ia_iX^{i-1}$. When f has coefficients in $\mathbb{R}$, this agrees with the definition in calculus. The usual rules for differentiating sums and products still hold, but note that in characteristic p the derivative of X^p is zero.

PROPOSITION 2.12 *For a nonconstant irreducible polynomial f in $F[X]$, the following statements are equivalent:*

(a) *f has a multiple root;*

(b) $\gcd(f,f')\neq 1$;

(c) *F has nonzero characteristic p and f is a polynomial in X^p;*

(d) *all the roots of f are multiple.*

PROOF. (a) $\Rightarrow$ (b). Let α be a multiple root of f, and write $f = (X-\alpha)^m g(X)$, $m > 1$, in some field splitting f. Then

$$f'(X) = m(X-\alpha)^{m-1}g(X) + (X-\alpha)^m g'(X). \tag{5}$$

Hence f and f' have $X-\alpha$ as a common factor.

(b) $\Rightarrow$ (c). As f is irreducible and $\deg(f') < \deg(f)$,

$$\gcd(f, f') \neq 1 \implies f' = 0.$$

But, because f is nonconstant, f' can be zero only if F has characteristic $p \neq 0$ and f is a polynomial in X^p.

(c) $\Rightarrow$ (d). Suppose $f(X) = g(X^p)$, and let $g(X) = \prod_i (X-a_i)^{m_i}$ in some field splitting f. Then

$$f(X) = g(X^p) = \prod\nolimits_i (X^p - a_i)^{m_i} = \prod\nolimits_i (X-\alpha_i)^{pm_i}$$

where $\alpha_i^p = a_i$. Hence every root of $f(X)$ has multiplicity at least p.

(d) $\Rightarrow$ (a). Obvious. □

PROPOSITION 2.13 *For a nonconstant polynomial f in $F[X]$, the following statements are equivalent:*

(a) $\gcd(f, f') = 1$;

(b) *f has only simple roots (in any field splitting f).*

PROOF. Let Ω be an extension of F splitting f. From (5), p. 32, we see that a root α of f in Ω is multiple if and only if it is also a root of f'.

If $\gcd(f, f') = 1$, then f and f' have no common factor in $\Omega[X]$ (see 2.10). In particular, they have no common root, and so f has only simple roots.

If f has only simple roots, then $\gcd(f, f')$ must be the constant polynomial, because otherwise it would have a root in Ω which would then be a common root of f and f'. □

DEFINITION 2.14 A polynomial is ***separable*** if it has only simple roots (in any field splitting the polynomial).[2]

Thus a nonconstant irreducible polynomial f is not separable if and only if F has characteristic $p \neq 0$ and f is a polynomial in X^p (see 2.12). A nonconstant polynomial f is separable if and only if $\gcd(f, f') = 1$ (see 2.13). Let $f = \prod f_i$ with f and the f_i monic and the f_i irreducible; then f is separable if and only if the f_i are distinct and separable. If f is separable as a polynomial in $F[X]$, then it is separable as a polynomial in $\Omega[X]$ for every field Ω containing F.

DEFINITION 2.15 A field F is ***perfect*** if every irreducible polynomial in $F[X]$ is separable.

PROPOSITION 2.16 *A field F is perfect if and only if*

(a) *F has characteristic zero, or*

(b) *F has nonzero characteristic p and every element of F is a pth power.*

[2]This is Bourbaki's definition. Often (e.g., in the books of Jacobson and in earlier versions of these notes) a polynomial f is said to be separable if none of its irreducible factors has a multiple root.

PROOF. A field of characteristic zero is obviously perfect, and so we may suppose F has characteristic $p \neq 0$. If F contains an element a that is not a pth power, then $X^p - a$ is irreducible in $F[X]$ but not separable (see 2.11). Conversely, if every element of F is a pth power, then every polynomial in X^p with coefficients in F is a pth power in $F[X]$,

$$\sum a_i X^{ip} = \left(\sum b_i X^i\right)^p \quad \text{if} \quad a_i = b_i^p,$$

and so it is not irreducible. □

EXAMPLE 2.17 (a) A finite field F is perfect, because the Frobenius endomorphism $a \mapsto a^p : F \to F$ is injective and therefore surjective (by counting).

(b) A field that can be written as a union of perfect fields is perfect. Therefore, every field algebraic over $\mathbb{F}_p$ is perfect.

(c) Every algebraically closed field is perfect.

(d) If F_0 has characteristic $p \neq 0$, then $F = F_0(X)$ is not perfect, because X is not a pth power.

ASIDE 2.18 We'll see later (5.1) that every finite separable extension E/F is simple: $E = F[\alpha]$ with α a root of a monic separable polynomial $f \in F[X]$ of degree $[E:F]$. This makes it obvious that, for any field Ω containing F, the number of F-homomorphisms $E \to \Omega$ is $\leq [E:F]$, with equality if and only if f splits in Ω. We can't use this argument here because it would make the exposition circular.

Exercises

2-1 Let F be a field of characteristic $\neq 2$.

(a) Let E be quadratic extension of F (i.e., $[E:F] = 2$); show that

$$S(E) = \{a \in F^\times \mid a \text{ is a square in } E\}$$

is a subgroup of $F^\times$ containing $F^{\times 2}$.

(b) Let E and E' be quadratic extensions of F; show that there is an F-isomorphism $\varphi : E \to E'$ if and only if $S(E) = S(E')$.

(c) Show that there is an infinite sequence of fields $E_1, E_2, \ldots$ with E_i a quadratic extension of $\mathbb{Q}$ such that E_i is not isomorphic to E_j for $i \neq j$.

(d) Let p be an odd prime. Show that, up to isomorphism, there is exactly one field with p^2 elements.

2-2 (a) Let F be a field of characteristic p. Show that if $X^p - X - a$ is reducible in $F[X]$, then it splits into distinct factors in $F[X]$.

(b) For every prime p, show that $X^p - X - 1$ is irreducible in $\mathbb{Q}[X]$.

2-3 Construct a splitting field for $X^5 - 2$ over $\mathbb{Q}$. What is its degree over $\mathbb{Q}$?

2-4 Find a splitting field of $X^{p^m} - 1 \in \mathbb{F}_p[X]$. What is its degree over $\mathbb{F}_p$?

2-5 Let $f \in F[X]$, where F is a field of characteristic 0. Let $d(X) = \gcd(f, f')$. Show that $g(X) = f(X)d(X)^{-1}$ has the same roots as $f(X)$, and these are all simple roots of $g(X)$.

2-6 Let $f(X)$ be an irreducible polynomial in $F[X]$, where F has characteristic p. Show that $f(X)$ can be written $f(X) = g(X^{p^e})$ where $g(X)$ is irreducible and separable. Deduce that every root of $f(X)$ has the same multiplicity p^e in any splitting field.

CHAPTER 3

The Fundamental Theorem of Galois Theory

In this chapter, we prove the fundamental theorem of Galois theory, which classifies the subfields of the splitting field of a separable polynomial f in terms of the Galois group of f.

Groups of automorphisms of fields

Consider fields $E \supset F$. An F-isomorphism $E \to E$ is called an ***F-automorphism*** of E. The F-automorphisms of E form a group, which we denote $\mathrm{Aut}(E/F)$.

EXAMPLE 3.1 (a) There are two obvious automorphisms of $\mathbb{C}$, namely, the identity map and complex conjugation. We'll see later (9.18) that by using the Axiom of Choice we can construct uncountably many more.

(b) Let $E = \mathbb{C}(X)$. A $\mathbb{C}$-automorphism of E sends X to another generator of E over $\mathbb{C}$. It follows from (9.24) below that these are exactly the elements $\frac{aX+b}{cX+d}$, $ad-bc \neq 0$. Therefore $\mathrm{Aut}(E/\mathbb{C})$ consists of the maps $f(X) \mapsto f\left(\frac{aX+b}{cX+d}\right)$, $ad-bc \neq 0$, and so

$$\mathrm{Aut}(E/\mathbb{C}) \simeq \mathrm{PGL}_2(\mathbb{C}),$$

the group of invertible 2×2 matrices with complex coefficients modulo its centre. Analysts will note that this is the same as the automorphism group of the Riemann sphere. Here is the explanation. The field E of meromorphic functions on the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$ consists of the rational functions in z, i.e., $E = \mathbb{C}(z) \simeq \mathbb{C}(X)$, and the natural map $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}}) \to \mathrm{Aut}(E/\mathbb{C})$ is an isomorphism.

(c) The group $\mathrm{Aut}(\mathbb{C}(X_1, X_2)/\mathbb{C})$ is quite complicated — there is a map

$$\mathrm{PGL}_3(\mathbb{C}) = \mathrm{Aut}(\mathbb{P}^2_{\mathbb{C}}) \hookrightarrow \mathrm{Aut}(\mathbb{C}(X_1, X_2)/\mathbb{C}),$$

but this is very far from being surjective. When there are even more variables X, the group is not known. The group $\mathrm{Aut}(\mathbb{C}(X_1, \dots, X_n)/\mathbb{C})$ is the group of birational automorphisms of projective n-space $\mathbb{P}^n_{\mathbb{C}}$, and is called the ***Cremona group.*** Its study is part of algebraic geometry (Wikipedia: Cremona group).

In this section, we'll be concerned with the groups $\mathrm{Aut}(E/F)$ when E is a finite extension of F.

PROPOSITION 3.2 *Let E be a splitting field of a separable polynomial f in $F[X]$; then* $\mathrm{Aut}(E/F)$ *has order* $[E:F]$.

PROOF. As f is separable, it has $\deg f$ distinct roots in E. Therefore Proposition 2.7 shows that the number of F-homomorphisms $E \to E$ is $[E:F]$. Because E is finite over F, all such homomorphisms are isomorphisms. □

EXAMPLE 3.3 Consider a simple extension $E = F[\alpha]$, and let f be a polynomial in $F[X]$ having α as a root. If α is the only root of f in E, then $\mathrm{Aut}(E/F) = 1$ (see 2.1b).

For example, let $\sqrt[3]{2}$ denote the real cube root of 2; then $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = 1$.

As another example, let F be a field of characteristic $p \neq 0$, and let a be an element of F that is not a pth power. Let E be a splitting field of $f = X^p - a$. Then f has only one root in E (see 2.11), and so $\mathrm{Aut}(E/F) = 1$.

These examples show that, in the statement of the proposition, is necessary that E be a *splitting* field of a *separable* polynomial.

When G is a group of automorphisms of a field E, we set

$$E^G = \mathrm{Inv}(G) = \{\alpha \in E \mid \sigma\alpha = \alpha, \text{ all } \sigma \in G\}.$$

It is a subfield of E, called the subfield of G-***invariants*** of E or the ***fixed field*** of G.

In this section, we'll show that, when E is the splitting field of a separable polynomial in $F[X]$ and $G = \mathrm{Aut}(E/F)$, then the maps

$$M \mapsto \mathrm{Aut}(E/M), \quad H \mapsto \mathrm{Inv}(H)$$

give a one-to-one correspondence between the set of intermediate fields M, $F \subset M \subset E$, and the set of subgroups H of G.

THEOREM 3.4 (E. ARTIN) *Let G be a finite group of automorphisms of a field E, and let $F = E^G$; then* $[E:F] \leq (G:1)$.

PROOF. Let $G = \{\sigma_1, \dots, \sigma_m\}$ with σ_1 the identity map. It suffices to show that every set $\{\alpha_1, \dots, \alpha_n\}$ of elements of E with $n > m$ is linearly dependent over F. For such a set, consider the system of linear equations

$$\begin{aligned} \sigma_1(\alpha_1)X_1 + \cdots + \sigma_1(\alpha_n)X_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)X_1 + \cdots + \sigma_m(\alpha_n)X_n &= 0 \end{aligned} \tag{6}$$

with coefficients in E. There are m equations and $n > m$ unknowns, and hence there are nontrivial solutions in E. We choose one $(c_1, \dots, c_n)$ having the fewest possible nonzero elements. After renumbering the α_i, we may suppose that $c_1 \neq 0$, and then, after multiplying by a scalar, that $c_1 \in F$. With these normalizations, we'll show that all $c_i \in F$. Then the first equation

$$\alpha_1 c_1 + \cdots + \alpha_n c_n = 0$$

(recall that $\sigma_1 = \mathrm{id}$) will be a linear relation on the α_i.

If not all c_i are in F, then $\sigma_k(c_i) \neq c_i$ for some $k \neq 1$ and $i \neq 1$. On applying σ_k to the equations

$$\begin{aligned} \sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n &= 0 \\ &\vdots \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n &= 0 \end{aligned}$$

and using that $\{\sigma_k\sigma_1,\dots,\sigma_k\sigma_m\}$ is a permutation of $\{\sigma_1,\dots,\sigma_m\}$, we find that

$$(c_1,\sigma_k(c_2),\dots,\sigma_k(c_i),\dots)$$

is also a solution to the system of equations (6). On subtracting it from the first, we obtain a solution $(0,\dots,c_i-\sigma_k(c_i),\dots)$, which is nonzero (look at the ith entry), but has more zeros than the first solution (look at the first entry) — contradiction. □

COROLLARY 3.5 *Let G be a finite group of automorphisms of a field E; then $G = \mathrm{Aut}(E/E^G)$.*

PROOF. As $G \subset \mathrm{Aut}(E/E^G)$, we have inequalities

$$[E:E^G] \overset{3.4}{\leq} (G:1) \leq (\mathrm{Aut}(E/E^G):1) \overset{2.8a}{\leq} [E:E^G].$$

All the inequalities must be equalities, and so $G = \mathrm{Aut}(E/E^G)$. □

Separable, normal, and Galois extensions

DEFINITION 3.6 An algebraic extension E/F is ***separable*** if the minimum polynomial of every element of E is separable; otherwise, it is ***inseparable***.

Thus, an algebraic extension E/F is separable if every irreducible polynomial in $F[X]$ having a root in E is separable, and it is inseparable if

- ◇ F is nonperfect, and in particular has characteristic $p \neq 0$, *and*
- ◇ there is an element α of E whose minimum polynomial is of the form $g(X^p)$, $g \in F[X]$.

See 2.14 *et seq.* For example, $E = \mathbb{F}_p(T)$ is an inseparable extension of $\mathbb{F}_p(T^p)$ because T has minimum polynomial $X^p - T^p$.

DEFINITION 3.7 An algebraic extension E/F is ***normal*** if the minimum polynomial of every element of E splits in $E[X]$.

In other words, an algebraic extension E/F is normal if and only if every irreducible polynomial $f \in F[X]$ having a root in E splits in $E[X]$.

Let f be an irreducible polynomial of degree m in $F[X]$, and let E be an algebraic extension of F. If f has a root in E, then

$$\left.\begin{array}{lll} E/F \text{ separable} & \Longrightarrow & \text{roots of } f \text{ distinct} \\ E/F \text{ normal} & \Longrightarrow & f \text{ splits in } E \end{array}\right\} \Longrightarrow f \text{ has } m \text{ distinct roots in } E.$$

It follows that E/F is separable and normal if and only if the minimum polynomial of every element α of E has $[F[\alpha]:F]$ distinct roots in E.

EXAMPLE 3.8 (a) The polynomial X^3-2 has one real root $\sqrt[3]{2}$ and two nonreal roots in $\mathbb{C}$. Therefore the extension $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ (which is separable) is not normal.

(b) The extension $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$ (which is normal) is not separable because the minimum polynomial of T is not separable.

DEFINITION 3.9 An extension E/F of fields is ***Galois*** if it is of finite degree and F is the fixed field of the group of F-automorphisms of E.

THEOREM 3.10 *For an extension E/F, the following statements are equivalent:*

(a) *E is the splitting field of a separable polynomial $f \in F[X]$;*

(b) *E is Galois over F;*

(c) *$F = E^G$ for some finite group G of automorphisms of E;*

(d) *E is normal, separable, and finite over F.*

PROOF. (a) $\Rightarrow$ (b). Let $G = \mathrm{Aut}(E/F)$, and let $F' = E^G \supset F$. We have to show that $F' = F$. Note that E is also the splitting field of f regarded as a polynomial with coefficients in F', and that f is still separable when it is regarded in this way. Hence

$$\left|\mathrm{Aut}(E/F')\right| \overset{3.2}{=} [E:F'] \leq [E:F] \overset{3.2}{=} |\mathrm{Aut}(E/F)|.$$

According to Corollary 3.5, $\mathrm{Aut}(E/F') = G$. As $G = \mathrm{Aut}(E/F)$, we deduce that $[E:F'] = [E:F]$, and so $F = F'$.

(b) $\Rightarrow$ (c). By definition, $F = E^{\mathrm{Aut}(E/F)}$. As E is finite over F, Corollary 2.8a shows $\mathrm{Aut}(E/F)$ to be finite.

(c) $\Rightarrow$ (d). By Theorem 3.4, we know that $[E:F] \leq (G:1)$; in particular, it is finite. Let $\alpha \in E$, and let f be the minimum polynomial of α; we have to show that f splits into distinct factors in $E[X]$. Let $\{\alpha_1 = \alpha, \alpha_2, ..., \alpha_m\}$ be the orbit of α under the action of G on E, and let

$$g(X) = \prod\nolimits_{i=1}^{m}(X - \alpha_i) = X^m + a_1X^{m-1} + \cdots + a_m.$$

The coefficients a_j are symmetric polynomials in the α_i, and each $\sigma \in G$ permutes the α_i, and so $\sigma a_j = a_j$ for all j. Thus $g(X) \in F[X]$. As it is monic and $g(\alpha) = 0$, it is divisible by the minimum polynomial f (see the definition p. 18). Let $\alpha_i = \sigma\alpha$; on applying σ to the equation $f(\alpha) = 0$ we find that $f(\alpha_i) = 0$. Therefore every α_i is a root of f, and we conclude that g divides f. Hence $f = g$, and so $f(X)$ splits into distinct factors in E.

(d) $\Rightarrow$ (a). Because E has finite degree over F, it is generated over F by a finite number of elements, say, $E = F[\alpha_1, ..., \alpha_m]$, $\alpha_i \in E$, α_i algebraic over F. Let f_i be the minimum polynomial of α_i over F, and let f be the product of the distinct f_i. Because E is normal over F, each f_i splits in E, and so E is the splitting field of f. Because E is separable over F, each f_i is separable, and so f is separable. □

Any one of the four conditions in the theorem can be used as the definition of a Galois extension. When E/F is Galois, the group $\mathrm{Aut}(E/F)$ is called the ***Galois group*** of E over F, and it is denoted by $\mathrm{Gal}(E/F)$.

REMARK 3.11 (a) Let E be Galois over F with Galois group G, and let $\alpha \in E$. The elements $\alpha_1, \alpha_2, ..., \alpha_m$ of the orbit of α under G are called the ***conjugates*** of α. In the course of proving the theorem we showed that the minimum polynomial of α is $\prod(X - \alpha_i)$.

(b) Let G be a finite group of automorphisms of a field E, and let $F = E^G$. Then E/F satisfies the equivalent conditions of Theorem 3.10. Hence E is Galois over F. Moreover, $\mathrm{Gal}(E/F) = G$ (apply 3.5) and $[E:F] = |\mathrm{Gal}(E/F)|$ (apply 3.2).

COROLLARY 3.12 *Every finite separable extension E of F is contained in a Galois extension.*

PROOF. Let $E = F[\alpha_1, ..., \alpha_m]$, and let f_i be the minimum polynomial of α_i over F. The product of the distinct f_i is a separable polynomial iin $F[X]$ whose splitting field is a Galois extension of F containing E. □

COROLLARY 3.13 *Let $E \supset M \supset F$; if E is Galois over F, then it is Galois over M.*

PROOF. We know E is the splitting field of some separable $f \in F[X]$; it is also the splitting field of f regarded as an element of $M[X]$. □

REMARK 3.14 When we relax the separability conditions, we can still say something. An element α of an algebraic extension of F is said to be ***separable*** over F if its minimum polynomial over F is separable. The proof of Corollary 3.12 shows that a finite extension generated by separable elements is separable. Therefore, the elements of an algebraic extension E of F that are separable over F form a subfield E_{sep} of E that is separable over F. When E is finite over F, we let $[E:F]_{\text{sep}} = [E_{\text{sep}}:F]$ and call it the ***separable degree*** of E over F. If Ω is an algebraically closed field containing F, then every F-homomorphism $E_{\text{sep}} \to \Omega$ extends uniquely to E, and so the number of F-homomorphisms $E \to \Omega$ is $[E:F]_{\text{sep}}$. When $E \supset M \supset F$ (finite extensions),

$$[E:F]_{\text{sep}} = [E:M]_{\text{sep}}[M:F]_{\text{sep}}.$$

In particular,

$$E \text{ is separable over } F \iff E \text{ is separable over } M \text{ and } M \text{ is separable over } F.$$

See Jacobson 1964, I 10, for more details.

DEFINITION 3.15 A finite extension $E \supset F$ is a ***cyclic***, ***abelian,*** ..., ***solvable*** extension if it is Galois and its Galois group is cyclic, abelian, ..., solvable Galois group.

The fundamental theorem of Galois theory

THEOREM 3.16 (FUNDAMENTAL THEOREM OF GALOIS THEORY) *Let E be a Galois extension of F, and let $G = \text{Gal}(E/F)$. The maps $H \mapsto E^H$ and $M \mapsto \text{Gal}(E/M)$ are inverse bijections between the set of subgroups of G and the set of intermediate fields between E and F:*

$$\{\text{subgroups of } G\} \leftrightarrow \{\text{intermediate fields } F \subset M \subset E\}.$$

Moreover,

(a) *the correspondence is inclusion-reversing: $H_1 \supset H_2 \iff E^{H_1} \subset E^{H_2}$;*

(b) *indexes equal degrees: $(H_1:H_2) = [E^{H_2}:E^{H_1}]$;*

(c) *$\sigma H \sigma^{-1} \leftrightarrow \sigma M$, i.e., $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$; $\text{Gal}(E/\sigma M) = \sigma\,\text{Gal}(E/M)\sigma^{-1}$.*

(d) *H is normal in $G \iff E^H$ is normal (hence Galois) over F, in which case*

$$\text{Gal}(E^H/F) \simeq G/H.$$

PROOF. For the first statement, we have to show that $H \mapsto E^H$ and $M \mapsto \text{Gal}(E/M)$ are inverse maps. Let H be a subgroup of G. Then, Corollary 3.5 shows that $\text{Gal}(E/E^H) = H$. Let M be an intermediate field. Then E is Galois over M by (3.13), which means that $E^{\text{Gal}(E/M)} = M$.

(a) We have the obvious implications,

$$H_1 \supset H_2 \implies E^{H_1} \subset E^{H_2} \implies \text{Gal}(E/E^{H_1}) \supset \text{Gal}(E/E^{H_2}).$$

As $\text{Gal}(E/E^{H_i}) = H_i$, this proves (a).

(b) Let H be a subgroup of G. According to 3.11b,

$$(\mathrm{Gal}(E/E^H):1) = [E:E^H].$$

This proves (b) in the case $H_2 = 1$, and the general case follows, using that

$$\begin{aligned}(H_1:1) &= (H_1:H_2)(H_2:1)\\ [E:E^{H_1}] &\overset{1.20}{=} [E:E^{H_2}][E^{H_2}:E^{H_1}].\end{aligned}$$

(c) For $\tau \in G$ and $\alpha \in E$,

$$\tau\alpha = \alpha \iff \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha.$$

Therefore, τ fixes M if and only if $\sigma\tau\sigma^{-1}$ fixes σM, and so $\sigma\,\mathrm{Gal}(E/M)\sigma^{-1} = \mathrm{Gal}(E/\sigma M)$. This shows that $\sigma\,\mathrm{Gal}(E/M)\sigma^{-1}$ corresponds to σM.

(d) Let H be a normal subgroup of G. Because $\sigma H\sigma^{-1} = H$ for all $\sigma \in G$, we must have $\sigma E^H = E^H$ for all $\sigma \in G$, i.e., the action of G on E stabilizes E^H. We therefore have a homomorphism

$$\sigma \mapsto \sigma|E^H : G \to \mathrm{Aut}(E^H/F)$$

whose kernel is H. As $(E^H)^{G/H} = F$, we see that E^H is Galois over F (by Theorem 3.10) and that $G/H \simeq \mathrm{Gal}(E^H/F)$ (by 3.11b).

Conversely, suppose that M is normal over F, and let $\alpha_1, \dots, \alpha_m$ generate M over F. For $\sigma \in G$, $\sigma\alpha_i$ is a root of the minimum polynomial of α_i over F, and so lies in M. Hence $\sigma M = M$, and this implies that $\sigma H\sigma^{-1} = H$ (by (c)). □

REMARK 3.17 The theorem shows that there is an order reversing bijection between the intermediate fields of E/F and the subgroups of G. Using this we can read off more results.

(a) Let $M_1, M_2, \dots, M_r$ be intermediate fields, and let H_i be the subgroup corresponding to M_i (i.e., $H_i = \mathrm{Gal}(E/M_i)$). Then (by definition) $M_1M_2\cdots M_r$ is the smallest field containing all M_i; hence it must correspond to the largest subgroup contained in all H_i, which is $\bigcap H_i$. Therefore

$$\mathrm{Gal}(E/M_1\cdots M_r) = H_1 \cap \dots \cap H_r.$$

(b) Let H be a subgroup of G and let $M = E^H$. The largest normal subgroup contained in H is $N = \bigcap_{\sigma\in G} \sigma H\sigma^{-1}$ (see GT 4.10), and so E^N is the smallest normal extension of F containing M. Note that, by (a), E^N is the composite of the fields σM. It is called the ***normal***, or ***Galois***, closure of M in E.

PROPOSITION 3.18 *Let E and L be field extensions of F contained in some common field. If E/F is Galois, then EL/L and $E/E\cap L$ are Galois, and the map*

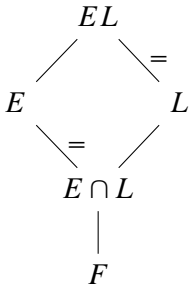
$$\sigma \mapsto \sigma|E : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E\cap L)$$

is an isomorphism.

PROOF. Because E is Galois over F, it is the splitting field of a separable polynomial

$f \in F[X]$. Then EL is the splitting field of f over L, and E is the splitting field of f over $E \cap L$. Hence EL/L and $E/E \cap L$ are Galois. Every automorphism σ of EL fixing the elements of L maps roots of f to roots of f, and so $\sigma E = E$. There is therefore a homomorphism

$$\sigma \mapsto \sigma|E : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E \cap L).$$



If $\sigma \in \mathrm{Gal}(EL/L)$ fixes the elements of E, then it fixes the elements of EL, and hence is the identity map. Thus, $\sigma \mapsto \sigma|E$ is injective. If $\alpha \in E$ is fixed by all $\sigma \in \mathrm{Gal}(EL/L)$, then $\alpha \in E \cap L$. By Corollary 3.5, this implies that the image of $\sigma \mapsto \sigma|E$ is $\mathrm{Gal}(E/E \cap L)$. □

COROLLARY 3.19 *Suppose, in the proposition, that L is finite over F. Then*

$$[EL : F] = \frac{[E : F][L : F]}{[E \cap L : F]}.$$

PROOF. According to Proposition 1.20,

$$[EL : F] = [EL : L][L : F],$$

but

$$[EL : L] \overset{3.18}{=} [E : E \cap L] \overset{1.20}{=} \frac{[E : F]}{[E \cap L : F]}.$$

□

PROPOSITION 3.20 *Let E_1 and E_2 be field extensions of F contained in some common field. If E_1 and E_2 are Galois over F, then E_1E_2 and $E_1 \cap E_2$ are Galois over F, and the map*

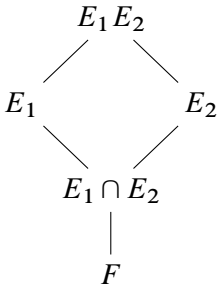
$$\sigma \mapsto (\sigma|E_1, \sigma|E_2) : \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

is an isomorphism of $\mathrm{Gal}(E_1E_2/F)$ *onto the subgroup*

$$H = \{(\sigma_1, \sigma_2) \mid \sigma_1|E_1 \cap E_2 = \sigma_2|E_1 \cap E_2\}$$

of $\mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$.

PROOF: Let $a \in E_1 \cap E_2$, and let f be its minimum polynomial over F. Then f has $\deg f$ distinct roots in E_1 and $\deg f$ distinct roots in E_2. Since f can have at most $\deg f$ roots in E_1E_2, it follows that it has $\deg f$ distinct roots in $E_1 \cap E_2$. This shows that $E_1 \cap E_2$ is normal and separable over F, and hence Galois (3.10). As E_1 and E_2 are Galois over F, they are splitting fields for separable polynomials $f_1, f_2 \in F[X]$. Now E_1E_2 is a splitting field for $\mathrm{lcm}(f_1, f_2)$, and hence it also is Galois over F. The map $\sigma \mapsto (\sigma|E_1, \sigma|E_2)$ is clearly an injective homomorphism, and its image is contained in H. We'll prove that the image is the whole of H by counting.



From the fundamental theorem,

$$\frac{\mathrm{Gal}(E_2/F)}{\mathrm{Gal}(E_2/E_1 \cap E_2)} \simeq \mathrm{Gal}(E_1 \cap E_2/F),$$

and so, for each $\sigma_1 \in \mathrm{Gal}(E_1/F)$, $\sigma_1|E_1 \cap E_2$ has exactly $[E_2 : E_1 \cap E_2]$ extensions to an element of $\mathrm{Gal}(E_2/F)$. Therefore,

$$(H : 1) = [E_1 : F][E_2 : E_1 \cap E_2] = \frac{[E_1 : F] \cdot [E_2 : F]}{[E_1 \cap E_2 : F]},$$

which equals $[E_1E_2 : F]$ by (3.19). □

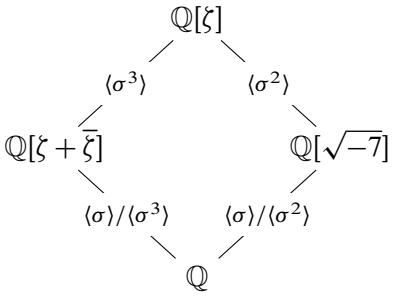
Examples

EXAMPLE 3.21 We analyse the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$, where ζ is a primitive 7th root of 1, say $\zeta = e^{2\pi i/7}$.

Note that $\mathbb{Q}[\zeta]$ is the splitting field of the polynomial X^7-1, and that ζ has minimum polynomial

$$X^6+X^5+X^4+X^3+X^2+X+1$$

(see 1.41). Therefore, $\mathbb{Q}[\zeta]$ is Galois of degree 6 over $\mathbb{Q}$. For any $\sigma \in \mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$, $\sigma\zeta = \zeta^i$, some i, $1 \le i \le 6$, and the map $\sigma \mapsto i$ defines an isomorphism $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q}) \to (\mathbb{Z}/7\mathbb{Z})^\times$. Let σ be the element of $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ such that $\sigma\zeta = \zeta^3$. Then σ generates $\mathrm{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ because the class of 3 in $(\mathbb{Z}/7\mathbb{Z})^\times$ generates it (the powers of 3 mod 7 are $3,2,6,4,5,1$). We investigate the subfields of $\mathbb{Q}[\zeta]$ corresponding to the subgroups $\langle\sigma^3\rangle$ and $\langle\sigma^2\rangle$.



Note that $\sigma^3\zeta = \zeta^6 = \bar{\zeta}$ (complex conjugate of ζ), and so $\zeta+\bar{\zeta} = 2\cos\frac{2\pi}{7}$ is fixed by σ^3. Now $\mathbb{Q}[\zeta] \supset \mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} \supset \mathbb{Q}[\zeta+\bar{\zeta}] \neq \mathbb{Q}$, and so $\mathbb{Q}[\zeta]^{\langle\sigma^3\rangle} = \mathbb{Q}[\zeta+\bar{\zeta}]$ (look at degrees). As $\langle\sigma^3\rangle$ is a normal subgroup of $\langle\sigma\rangle$, $\mathbb{Q}[\zeta+\bar{\zeta}]$ is Galois over $\mathbb{Q}$, with Galois group $\langle\sigma\rangle/\langle\sigma^3\rangle$. The conjugates of $\alpha_1 \overset{\text{def}}{=} \zeta+\bar{\zeta}$ are $\alpha_3 = \zeta^3+\zeta^{-3}$, $\alpha_2 = \zeta^2+\zeta^{-2}$. Direct calculation shows that

$$\begin{aligned}
\alpha_1+\alpha_2+\alpha_3 &= \textstyle\sum_{i=1}^{6}\zeta^i = -1,\\
\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= -2,\\
\alpha_1\alpha_2\alpha_3 &= (\zeta+\zeta^6)(\zeta^2+\zeta^5)(\zeta^3+\zeta^4)\\
&= (\zeta+\zeta^3+\zeta^4+\zeta^6)(\zeta^3+\zeta^4)\\
&= (\zeta^4+\zeta^6+1+\zeta^2+\zeta^5+1+\zeta+\zeta^3)\\
&= 1.
\end{aligned}$$

Hence the minimum polynomial[1] of $\zeta+\bar{\zeta}$ is

$$g(X) = X^3+X^2-2X-1.$$

The minimum polynomial of $\cos\frac{2\pi}{7} = \frac{\alpha_1}{2}$ is therefore

$$\frac{g(2X)}{8} = X^3+X^2/2-X/2-1/8.$$

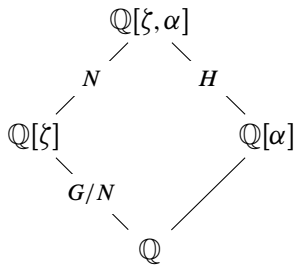
The subfield of $\mathbb{Q}[\zeta]$ corresponding to $\langle\sigma^2\rangle$ is generated by $\beta = \zeta+\zeta^2+\zeta^4$. Let $\beta' = \sigma\beta$. Then $(\beta-\beta')^2 = -7$. Hence the field fixed by $\langle\sigma^2\rangle$ is $\mathbb{Q}[\sqrt{-7}]$.

[1] More directly, on setting $X = \zeta+\bar{\zeta}$ in

$$(X^3-3X)+(X^2-2)+X+1$$

one obtains $1+\zeta+\zeta^2+\cdots+\zeta^6 = 0$.

EXAMPLE 3.22 We compute the Galois group of a splitting field E of $X^5-2\in\mathbb{Q}[X]$. Recall from Exercise 2-3 that $E=\mathbb{Q}[\zeta,\alpha]$ where ζ is a primitive 5th root of 1, and α is a root of X^5-2. For example, we could take E to be the splitting field of X^5-2 in $\mathbb{C}$, with $\zeta=e^{2\pi i/5}$ and α equal to the real 5th root of 2. We have the picture at right, and



$$[\mathbb{Q}[\zeta]:\mathbb{Q}]=4,\quad [\mathbb{Q}[\alpha]:\mathbb{Q}]=5.$$

Because 4 and 5 are relatively prime,

$$[\mathbb{Q}[\zeta,\alpha]:\mathbb{Q}]=20.$$

Hence $G=\mathrm{Gal}(\mathbb{Q}[\zeta,\alpha]/\mathbb{Q})$ has order 20, and the subgroups N and H fixing $\mathbb{Q}[\zeta]$ and $\mathbb{Q}[\alpha]$ have orders 5 and 4 respectively. Because $\mathbb{Q}[\zeta]$ is normal over $\mathbb{Q}$ (it is the splitting field of X^5-1), N is normal in G. Because $\mathbb{Q}[\zeta]\cdot\mathbb{Q}[\alpha]=\mathbb{Q}[\zeta,\alpha]$, we have $H\cap N=1$, and so $G=N\rtimes_\theta H$. Moreover, $H\simeq G/N\simeq(\mathbb{Z}/5\mathbb{Z})^\times$, which is cyclic, being generated by the class of 2. Let τ be the generator of H corresponding to 2 under this isomorphism, and let σ be a generator of N. Thus $\sigma(\alpha)$ is another root of X^5-2, which we can take to be $\zeta\alpha$ (after possibly replacing σ by a power). Hence:

$$\begin{cases}\tau\zeta &= \zeta^2\\ \tau\alpha &= \alpha\end{cases}\quad\begin{cases}\sigma\zeta &= \zeta\\ \sigma\alpha &= \zeta\alpha.\end{cases}$$

Note that $\tau\sigma\tau^{-1}(\alpha)=\tau\sigma\alpha=\tau(\zeta\alpha)=\zeta^2\alpha$ and it fixes ζ; therefore $\tau\sigma\tau^{-1}=\sigma^2$. Thus G has generators σ and τ and defining relations

$$\sigma^5=1,\quad \tau^4=1,\quad \tau\sigma\tau^{-1}=\sigma^2.$$

The subgroup H has five conjugates, which correspond to the five fields $\mathbb{Q}[\zeta^i\alpha]$,

$$\sigma^iH\sigma^{-i}\leftrightarrow\sigma^i\mathbb{Q}[\alpha]=\mathbb{Q}[\zeta^i\alpha],\qquad 1\le i\le 5.$$

Constructible numbers revisited

Earlier (1.36) we showed that a real number α is constructible if and only if it is contained in a subfield of $\mathbb{R}$ of the form $\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_r}]$ with each a_i a positive element of $\mathbb{Q}[\sqrt{a_1},\dots,\sqrt{a_{i-1}}]$. In particular

$$\alpha\text{ constructible}\implies[\mathbb{Q}[\alpha]:\mathbb{Q}]=2^s\text{ some }s.\tag{7}$$

Now we can prove a partial converse to this last statement.

THEOREM 3.23 *If α is contained in a subfield of $\mathbb{R}$ that is Galois of degree 2^r over $\mathbb{Q}$, then it is constructible.*

PROOF. Suppose $\alpha\in E\subset\mathbb{R}$ where E is Galois of degree 2^r over $\mathbb{Q}$, and let $G=\mathrm{Gal}(E/\mathbb{Q})$. Because finite p-groups are solvable (GT 6.7), there exists a sequence of groups

$$\{1\}=G_0\subset G_1\subset G_2\subset\cdots\subset G_r=G$$

with G_i/G_{i-1} of order 2. Correspondingly, there will be a sequence of fields,

$$E=E_0\supset E_1\supset E_2\supset\cdots\supset E_r=\mathbb{Q}$$

with E_{i-1} of degree 2 over E_i. The next lemma shows that $E_i = E_{i-1}[\sqrt{a_i}]$ for some $a_i \in E_{i-1}$, and $a_i > 0$ because otherwise E_i would not be real. This proves the theorem. □

LEMMA 3.24 *Let E/F be a quadratic extension of fields of characteristic $\neq 2$. Then $E = F[\sqrt{d}]$ for some $d \in F$.*

PROOF. Let $\alpha \in E$, $\alpha \notin F$, and let $X^2 + bX + c$ be the minimum polynomial of α. Then $\alpha = \frac{-b \pm \sqrt{b^2-4c}}{2}$, and so $E = F[\sqrt{b^2-4c}]$. □

COROLLARY 3.25 *If p is a prime of the form $2^k + 1$, then $\cos\frac{2\pi}{p}$ is constructible.*

PROOF. The field $\mathbb{Q}[e^{2\pi i/p}]$ is Galois over $\mathbb{Q}$ with Galois group $G \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, which has order $p-1 = 2^k$. The field $\mathbb{Q}[\cos\frac{2\pi}{p}]$ is contained in $\mathbb{Q}[e^{2\pi i/p}]$, and therefore is Galois of degree dividing 2^k (fundamental theorem 3.16 and 1.20). As $\mathbb{Q}[\cos\frac{2\pi}{p}]$ is a subfield of $\mathbb{R}$, we can apply the theorem. □

Thus a regular p-gon, p prime, is constructible if and only if p is a Fermat prime, i.e., of the form $2^{2^r} + 1$. For example, we have proved that the regular 65537-polygon is constructible, without (happily) having to exhibit an explicit formula for $\cos\frac{2\pi}{65537}$.

REMARK 3.26 The converse to (7) is false; in particular, there are nonconstructible algebraic numbers of degree 4 over $\mathbb{Q}$. The polynomial $f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$ is irreducible, and we'll show below (4.9) that the Galois group of a splitting field E for f is S_4. Each root of $f(X)$ lies in an extension of degree 2^2 of $\mathbb{Q}$. If the four roots of $f(X)$ were constructible, then all the elements of E would be constructible (1.36a), but if H denotes a Sylow 2-subgroup of S_4, then E^H has odd degree over $\mathbb{Q}$, and so no element of $E^H \smallsetminus \mathbb{Q}$ is constructible.[2]

The Galois group of a polynomial

If a polynomial $f \in F[X]$ is separable, then its splitting field F_f is Galois over F, and we call $\mathrm{Gal}(F_f/F)$ the ***Galois group*** G_f of f.

Let $f(X) = \prod_{i=1}^n (X - \alpha_i)$ in a splitting field F_f. We know that the elements of $\mathrm{Gal}(F_f/F)$ map roots of f to roots of f, i.e., they map the set $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ into itself. Being automorphisms, they act as permutations on $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$. As as the α_i generate F_f over F, an element of $\mathrm{Gal}(F_f/F)$ is uniquely determined by the permutation it defines. Thus G_f can be identified with a subset of $\mathrm{Sym}(\{\alpha_1, \alpha_2, \dots, \alpha_n\}) \approx S_n$ (symmetric group on n symbols). In fact, G_f consists exactly of the permutations σ of $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ such that, for $P \in F[X_1, \dots, X_n]$,

$$P(\alpha_1, \dots, \alpha_n) = 0 \implies P(\sigma\alpha_1, \dots, \sigma\alpha_n) = 0. \tag{8}$$

To see this, note that the kernel of the map

$$F[X_1, \dots, X_n] \to F_f, \quad X_i \mapsto \alpha_i, \tag{9}$$

[2]It is possible to prove this without appealing to the Sylow theorems. If a root α of $f(X)$ were constructible, then there would exist a tower of quadratic extensions $\mathbb{Q}[\alpha] \supset M \supset \mathbb{Q}$. By Galois theory, the groups $\mathrm{Gal}(E/M) \supset \mathrm{Gal}(E/\mathbb{Q}[\alpha])$ have orders 12 and 6 respectively. As $\mathrm{Gal}(E/\mathbb{Q}) = S_4$, $\mathrm{Gal}(E/M)$ would be A_4. But A_4 has no subgroup of order 6, a contradiction. Thus no root of $f(X)$ is constructible. (Actually $\mathrm{Gal}(E/\mathbb{Q}[\alpha]) = S_3$, but that does not matter here.)

consists of the polynomials $P(X_1,\dots,X_n)$ such that $P(\alpha_1,\dots,\alpha_n)=0$. Let σ be a permutation of the α_i satisfying the condition (8). Then the map

$$F[X_1,\dots,X_n]\to F_f,\quad X_i\mapsto\sigma\alpha_i,$$

factors through the map (9), and defines an F-isomorphism $F_f\to F_f$, i.e., an element of the Galois group. This shows that every permutation satisfying the condition (8) extends uniquely to an element of G_f, and it is obvious that every element of G_f arises in this way.

This gives a description of G_f not mentioning fields or abstract groups, neither of which were available to Galois. Note that it shows again that $(G_f:1)$, hence $[F_f:F]$, divides $\deg(f)$!.

Solvability of equations

For a polynomial $f\in F[X]$, we say that $f(X)=0$ is ***solvable in radicals*** if its solutions can be obtained by the algebraic operations of addition, subtraction, multiplication, division, and the extraction of mth roots, or, more precisely, if there exists a tower of fields

$$F=F_0\subset F_1\subset F_2\subset\cdots\subset F_m$$

such that

(a) $F_i=F_{i-1}[\alpha_i]$, $\alpha_i^{m_i}\in F_{i-1}$;

(b) F_m contains a splitting field for f.

THEOREM 3.27 (GALOIS, 1832) *Let F be a field of characteristic zero, and let $f\in F[X]$. The equation $f(X)=0$ is solvable in radicals if and only if the Galois group of f is solvable.*

We'll prove this later (5.33). Also we'll exhibit polynomials $f(X)\in\mathbb{Q}[X]$ with Galois group S_n, which are therefore not solvable when $n\ge 5$ by GT 4.37.

REMARK 3.28 When F has characteristic p, the theorem fails for two reasons:

(a) f need not be separable, and so not have a Galois group;

(b) $X^p-X-a=0$ need not be solvable in radicals even though it is separable with abelian Galois group (cf. Exercise 2-2).

If the definition of solvable is changed to allow extensions defined by polynomials of the type in (b) in the chain, then the theorem holds for fields F of characteristic $p\neq 0$ and separable $f\in F[X]$.

NOTES Much of what has been written about Galois is unreliable — see Tony Rothman, "Genius and Biographers: The Fictionalization of Evariste Galois," Amer. Math. Mon. 89, 84 (1982). For a careful explanation of Galois's "Premier Mémoire", see Edwards, Harold M., Galois for 21st-century readers. Notices A.M.S. 59 (2012), no. 7, 912–923.

Exercises

3-1 Let F be a field of characteristic 0. Show that $F(X^2)\cap F(X^2-X)=F$ (intersection inside $F(X)$). [Hint: Find automorphisms σ and τ of $F(X)$, each of order 2, fixing $F(X^2)$ and $F(X^2-X)$ respectively, and show that $\sigma\tau$ has infinite order.]

3-2 [3] Let p be an odd prime, and let ζ be a primitive pth root of 1 in $\mathbb{C}$. Let $E = \mathbb{Q}[\zeta]$, and let $G = \mathrm{Gal}(E/\mathbb{Q})$; thus $G = (\mathbb{Z}/(p))^\times$. Let H be the subgroup of index 2 in G. Put $\alpha = \sum_{i\in H} \zeta^i$ and $\beta = \sum_{i\in G\setminus H} \zeta^i$. Show:

(a) α and β are fixed by H;

(b) if $\sigma \in G \setminus H$, then $\sigma\alpha = \beta, \sigma\beta = \alpha$.

Thus α and β are roots of the polynomial $X^2 + X + \alpha\beta \in \mathbb{Q}[X]$. Compute[4] $\alpha\beta$ and show that the fixed field of H is $\mathbb{Q}[\sqrt{p}]$ when $p \equiv 1 \mod 4$ and $\mathbb{Q}[\sqrt{-p}]$ when $p \equiv 3 \mod 4$.

3-3 Let $M = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ and $E = M[\sqrt{(\sqrt{2}+2)(\sqrt{3}+3)}]$ (subfields of $\mathbb{R}$).

(a) Show that M is Galois over $\mathbb{Q}$ with Galois group the 4-group $C_2 \times C_2$.

(b) Show that E is Galois over $\mathbb{Q}$ with Galois group the quaternion group.

3-4 Let E be a Galois extension of F with Galois group G, and let L be the fixed field of a subgroup H of G. Show that the automomorphism group of L/F is N/H where N is the normalizer of H in G.

3-5 Let E be a finite extension of F. Show that the order of $\mathrm{Aut}(E/F)$ divides the degree $[E:F]$.

[3] This problem shows that every quadratic extension of $\mathbb{Q}$ is contained in a cyclotomic extension of $\mathbb{Q}$. The Kronecker-Weber theorem says that *every* abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

[4] Schoof suggests computing $\alpha - \beta$ instead.

CHAPTER 4

Computing Galois Groups

In this chapter, we investigate general methods for computing Galois groups.

When is $G_f \subset A_n$?

Let σ be a permutation of the set $\{1,2,\dots,n\}$. The pairs (i,j) with $i<j$ but $\sigma(i)>\sigma(j)$ are called the ***inversions*** of σ, and σ is said to be ***even*** or ***odd*** according as the number of inversions is even or odd. The ***signature*** of σ, $\operatorname{sign}(\sigma)$, is $+1$ or -1 according as σ is even or odd. We can define the signature of a permutation σ of any set S of n elements by choosing a numbering of the set and identifying σ with a permutation of $\{1,\dots,n\}$. Then sign is the unique homomorphism $\operatorname{Sym}(S)\to\{\pm1\}$ such that $\operatorname{sign}(\sigma)=-1$ for every transposition. In particular, it is independent of the choice of the numbering. See GT, 4.25.

Now consider a monic polynomial

$$f(X)=X^n+a_1X^{n-1}+\cdots+a_n$$

and let $f(X)=\prod_{i=1}^n(X-\alpha_i)$ in some splitting field. Set

$$\Delta(f)=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j),\qquad D(f)=\Delta(f)^2=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)^2.$$

The ***discriminant*** of f is defined to be $D(f)$. Note that $D(f)$ is nonzero if and only if f has only simple roots, i.e., is separable. Let G_f be the Galois group of f, and identify it with a subgroup of $\operatorname{Sym}(\{\alpha_1,\dots,\alpha_n\})$ (as on p. 44).

PROPOSITION 4.1 *Let $f\in F[X]$ be a separable polynomial, and let $\sigma\in G_f$.*

(a) $\sigma\Delta(f)=\operatorname{sign}(\sigma)\Delta(f)$, *where* $\operatorname{sign}(\sigma)$ *is the signature of* σ.

(b) $\sigma D(f)=D(f)$.

PROOF. Each inversion of σ introduces a negative sign into $\sigma\Delta(f)$, and so (a) follows from the definition of $\operatorname{sign}(\sigma)$. The equation in (b) is obtained by squaring that in (a). □

While $\Delta(f)$ depends on the choice of the numbering of the roots of f, $D(f)$ does not.

COROLLARY 4.2 *Let $f(X)\in F[X]$ be separable of degree n. Let F_f be a splitting field for f and let $G_f=\operatorname{Gal}(F_f/F)$.*

(a) *The discriminant $D(f)\in F$.*

(b) *The subfield of F_f corresponding to $A_n \cap G_f$ is $F[\Delta(f)]$. Hence*

$$G_f \subset A_n \iff \Delta(f) \in F \iff D(f) \text{ is a square in } F.$$

PROOF. (a) The discriminant of f is an element of F_f fixed by $G_f \stackrel{\text{def}}{=} \mathrm{Gal}(F_f/F)$, and hence lies in F (by the fundamental theorem).

(b) Because f has simple roots, $\Delta(f) \neq 0$, and so the formula $\sigma\Delta(f) = \mathrm{sign}(\sigma)\Delta(f)$ shows that an element of G_f fixes $\Delta(f)$ if and only if it lies in A_n. Thus, under the Galois correspondence,

$$G_f \cap A_n \leftrightarrow F[\Delta(f)].$$

Hence,

$$G_f \cap A_n = G_f \iff F[\Delta(f)] = F. \qquad \square$$

The roots of $X^2 + bX + c$ are $\frac{-b \pm \sqrt{b^2-4c}}{2}$ and so

$$\Delta(X^2 + bX + c) = \sqrt{b^2-4c} \text{ (or } -\sqrt{b^2-4c}),$$
$$D(X^2 + bX + c) = b^2 - 4c.$$

Similarly,

$$D(X^3 + bX + c) = -4b^3 - 27c^2.$$

By completing the cube, one can put any cubic polynomial in this form (in characteristic $\neq 3$).

Although there is a not a universal formula for the roots of f in terms of its coefficients when the $\deg(f) > 4$, there is for its discriminant. However, the formulas for the discriminant rapidly become very complicated, for example, that for $X^5 + aX^4 + bX^3 + cX^2 + dX + e$ has 59 terms. Fortunately, PARI knows them. For example, typing `poldisc(X^3+a*X^2+b*X+c,X)` returns the discriminant of $X^3 + aX^2 + bX + c$, namely,

$$-4ca^3 + b^2a^2 + 18cba + (-4b^3 - 27c^2).$$

REMARK 4.3 Suppose $F \subset \mathbb{R}$. Then $D(f)$ will not be a square if it is negative. It is known that the sign of $D(f)$ is $(-1)^s$ where $2s$ is the number of nonreal roots of f in $\mathbb{C}$ (see ANT 2.40). Thus if s is odd, then G_f is not contained in A_n. This can be proved more directly by noting that complex conjugation acts on the roots as the product of s disjoint transpositions.

The converse is not true: when s is even, G_f is not necessarily contained in A_n.

When does G_f act transitively on the roots?

PROPOSITION 4.4 *Let $f(X) \in F[X]$ be separable. Then $f(X)$ is irreducible if and only if G_f permutes the roots of f transitively.*

PROOF. $\Longrightarrow$: If α and β are two roots of $f(X)$ in a splitting field F_f for f, then they both have $f(X)$ as their minimum polynomial, and so $F[\alpha]$ and $F[\beta]$ are both stem fields for f. Hence, there is an F-isomorphism

$$F[\alpha] \simeq F[\beta], \qquad \alpha \leftrightarrow \beta.$$

Write $F_f = F[\alpha_1, \alpha_2, \ldots]$ with $\alpha_1 = \alpha$ and $\alpha_2, \alpha_3, \ldots$ the other roots of $f(X)$. Then the F-homomorphism $\alpha \mapsto \beta : F[\alpha] \to F_f$ extends (step by step) to an F-homomorphism $F_f \to F_f$ (use 2.2b), which is an F-isomorphism sending α to β.

$\Longleftarrow$: Let $g(X) \in F[X]$ be an irreducible factor of f, and let α be one of its roots. If β is a second root of f, then (by assumption) $\beta = \sigma\alpha$ for some $\sigma \in G_f$. Now, because g has coefficients in F,

$$g(\sigma\alpha) = \sigma g(\alpha) = 0,$$

and so β is also a root of g. Therefore, every root of f is also a root of g, and so $f(X) = g(X)$. □

Note that when $f(X)$ is irreducible of degree n, $n|(G_f : 1)$ because $[F[\alpha]: F] = n$ and $[F[\alpha]: F]$ divides $[F_f : F] = (G_f : 1)$. Thus G_f is a transitive subgroup of S_n whose order is divisible by n.

Polynomials of degree at most three

EXAMPLE 4.5 Let $f(X) \in F[X]$ be a polynomial of degree 2. Then f is inseparable $\Longleftrightarrow$ F has characteristic 2 and $f(X) = X^2 - a$ for some $a \in F \smallsetminus F^2$. If f is separable, then $G_f = 1 (= A_2)$ or S_2 according as $D(f)$ is a square in F or not.

EXAMPLE 4.6 Let $f(X) \in F[X]$ be a polynomial of degree 3. We can assume f to be irreducible, for otherwise we are essentially back in the previous case. Then f is inseparable if and only if F has characteristic 3 and $f(X) = X^3 - a$ for some $a \in F \smallsetminus F^3$. If f is separable, then G_f is a transitive subgroup of S_3 whose order is divisible by 3. There are only two possibilities: $G_f = A_3$ or S_3 according as $D(f)$ is a square in F or not. Note that A_3 is generated by the cycle (123).

For example, $X^3 - 3X + 1$ is irreducible in $\mathbb{Q}[X]$ (see 1.12). Its discriminant is $-4(-3)^3 - 27 = 81 = 9^2$, and so its Galois group is A_3.

On the other hand, $X^3 + 3X + 1 \in \mathbb{Q}[X]$ is also irreducible (apply 1.11), but its discriminant is -135 which is not a square in $\mathbb{Q}$, and so its Galois group is S_3.

Quartic polynomials

Let $f(X)$ be a separable quartic polynomial. In order to determine G_f we'll exploit the fact that S_4 has

$$V = \{1, (12)(34), (13)(24), (14)(23)\}$$

as a normal subgroup — it is normal because it contains all elements of type $2+2$ (GT 4.29). Let E be a splitting field of f, and let $f(X) = \prod(X - \alpha_i)$ in E. We identify the Galois group G_f of f with a subgroup of the symmetric group $\mathrm{Sym}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$. Consider the partially symmetric elements

$$\begin{aligned} \alpha &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \gamma &= \alpha_1\alpha_4 + \alpha_2\alpha_3. \end{aligned}$$

They are distinct because the α_i are distinct; for example,

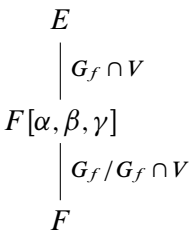
$$\alpha - \beta = \alpha_1(\alpha_2 - \alpha_3) + \alpha_4(\alpha_3 - \alpha_2) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3).$$

The group $\mathrm{Sym}(\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\})$ permutes $\{\alpha, \beta, \gamma\}$ transitively. The stabilizer of each of α, β, γ must therefore be a subgroup of index 3 in S_4, and hence has order 8. For example,

the stabilizer of β is $\langle(1234),(13)\rangle$. Groups of order 8 in S_4 are Sylow 2-subgroups. There are three of them, all isomorphic to D_4. By the Sylow theorems, V is contained in a Sylow 2-subgroup; in fact, because the Sylow 2-subgroups are conjugate and V is normal, it is contained in all three. It follows that V is the intersection of the three Sylow 2-subgroups. Each Sylow 2-subgroup fixes exactly one of α,β, or γ, and therefore their intersection V is the subgroup of $\mathrm{Sym}(\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\})$ fixing α, β, and γ.

LEMMA 4.7 *The fixed field of $G_f \cap V$ is $F[\alpha,\beta,\gamma]$. Hence $F[\alpha,\beta,\gamma]$ is Galois over F with Galois group $G_f/G_f\cap V$.*

PROOF. The above discussion shows that the subgroup of G_f of elements fixing $F[\alpha,\beta,\gamma]$ is $G_f\cap V$, and so $E^{G_f\cap V} = F[\alpha,\beta,\gamma]$ by the fundamental theorem of Galois theory. The remaining statements follow from the fundamental theorem using that V is normal. □



Let $M = F[\alpha,\beta,\gamma]$, and let $g(X) = (X-\alpha)(X-\beta)(X-\gamma) \in M[X]$ — it is called the ***resolvent cubic*** of f. Every permutation of the α_i (*a fortiori*, every element of G_f) merely permutes α,β,γ, and so fixes $g(X)$. Therefore (by the fundamental theorem) $g(X)$ has coefficients in F. More explicitly, we have:

LEMMA 4.8 *The resolvent cubic of $f = X^4+bX^3+cX^2+dX+e$ is*

$$g = X^3 - cX^2 + (bd-4e)X - b^2e + 4ce - d^2.$$

The discriminants of f and g are equal.

SKETCH OF PROOF. Expand $f = (X-\alpha_1)(X-\alpha_2)(X-\alpha_3)(X-\alpha_4)$ to express b,c,d,e in terms of $\alpha_1,\alpha_2,\alpha_3,\alpha_4$. Expand $g = (X-\alpha)(X-\beta)(X-\gamma)$ to express the coefficients of g in terms of $\alpha_1,\alpha_2,\alpha_3,\alpha_4$, and substitute to express them in terms of b,c,d,e. □

Now let f be an irreducible separable quartic. Then $G = G_f$ is a transitive subgroup of S_4 whose order is divisible by 4. There are the following possibilities for G:

G	$(G\cap V:1)$	$(G:V\cap G)$
S_4	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

$(G\cap V:1) = [E:M]$
$(G:V\cap G) = [M:F]$

The groups of type D_4 are the Sylow 2-subgroups discussed above, and the groups of type C_4 are those generated by cycles of length 4.

We can compute $(G:V\cap G)$ from the resolvent cubic g, because $G/V\cap G = \mathrm{Gal}(M/F)$ and M is the splitting field of g. Once we know $(G:V\cap G)$, we can deduce G except in the case that it is 2. If $[M:F]=2$, then $G\cap V = V$ or C_2. Only the first group acts transitively on the roots of f, and so (from 4.4) we see that in this case $G = D_4$ or C_4 according as f is irreducible or not in $M[X]$.

EXAMPLE 4.9 Consider $f(X) = X^4 - 4X + 2 \in \mathbb{Q}[X]$. It is irreducible by Eisenstein's criterion (1.16), and its resolvent cubic is $g(X) = X^3 - 8X - 16$, which is irreducible because it has no roots in $\mathbb{F}_5$. The discriminant of $g(X)$ is -4864, which is not a square, and so the Galois group of $g(X)$ is S_3. From the table, we see that the Galois group of $f(X)$ is S_4.

EXAMPLE 4.10 Consider $f(X) = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$. It is irreducible by Eisenstein's criterion (1.16), and its resolvent cubic is $(X-4)(X^2-8)$; thus $M = \mathbb{Q}[\sqrt{2}]$. From the table we see that G_f is of type D_4 or C_4, but f factors over M (even as a polynomial in X^2), and hence G_f is of type C_4.

EXAMPLE 4.11 Consider $f(X) = X^4 - 10X^2 + 4 \in \mathbb{Q}[X]$. It is irreducible in $\mathbb{Q}[X]$ because (by inspection) it is irreducible in $\mathbb{Z}[X]$. Its resolvent cubic is $(X+10)(X+4)(X-4)$, and so G_f is of type V.

EXAMPLE 4.12 Consider $f(X) = X^4 - 2 \in \mathbb{Q}[X]$. It is irreducible by Eisenstein's criterion (1.16), and its resolvent cubic is $g(X) = X^3 + 8X$. Hence $M = \mathbb{Q}[i\sqrt{2}]$. One can check that f is irreducible over M, and G_f is of type D_4.

Alternatively, analyse the equation as in (3.22).

As we explained in (1.29), PARI knows how to factor polynomials with coefficients in $\mathbb{Q}[\alpha]$.

EXAMPLE 4.13 (From the web, sci.math.research, search for "final analysis".) Consider $f(X) = X^4 - 2cX^3 - dX^2 + 2cdX - dc^2 \in \mathbb{Z}[X]$ with $a > 0$, $b > 0$, $c > 0$, $a > b$ and $d = a^2 - b^2$. Let $r = d/c^2$ and let w be the unique positive real number such that $r = w^3/(w^2+4)$. Let m be the number of roots of $f(X)$ in $\mathbb{Z}$ (counted with multiplicities). The Galois group of f is as follows:

- ◇ If $m = 0$ and w not rational, then G is S_4.
- ◇ If $m = 1$ and w not rational then G is S_3.
- ◇ If w is rational and $w^2 + 4$ is not a square then $G = D4$.
- ◇ If w is rational and $w^2 + 4$ is a square then $G = V = C_2 \times C_2$.

This covers all possible cases. The hard part was to establish that $m = 2$ could never happen.

ASIDE 4.14 For a discussion of whether the method of solving a quartic by reducing to a cubic generalizes to other even degrees, see mo149099.

Examples of polynomials with S_p as Galois group over $\mathbb{Q}$

The next lemma gives a criterion for a subgroup of S_p to be the whole of S_p.

LEMMA 4.15 *For p prime, the symmetric group S_p is generated by any transposition and any p-cycle.*

PROOF. After renumbering, we may assume that the transposition is $\tau = (12)$, and we may write the p-cycle σ so that 1 occurs in the first position, $\sigma = (1\, i_2 \cdots i_p)$. Now some power of σ will map 1 to 2 and will still be a p-cycle (here is where we use that p is prime). After replacing σ with the power, we have $\sigma = (1\, 2\, j_3 \ldots j_p)$, and after renumbering again, we have $\sigma = (1\, 2\, 3 \ldots p)$. Now

$$(i\ i+1) = \sigma^i (12) \sigma^{-i}$$

(see GT 4.29) and so lies in the subgroup generated by σ and τ. These transpositions generate S_p. □

PROPOSITION 4.16 *Let f be an irreducible polynomial of prime degree p in $\mathbb{Q}[X]$. If f splits in $\mathbb{C}$ and has exactly two nonreal roots, then $G_f = S_p$.*

PROOF. Let E be the splitting field of f in $\mathbb{C}$, and let $\alpha \in E$ be a root of f. Because f is irreducible, $[\mathbb{Q}[\alpha]:\mathbb{Q}] = \deg f = p$, and so $p|[E:\mathbb{Q}] = (G_f:1)$. Therefore G_f contains an element of order p (Cauchy's theorem, GT 4.13), but the only elements of order p in S_p are p-cycles (here we use that p is prime again).

Let σ be complex conjugation on $\mathbb{C}$. Then σ transposes the two nonreal roots of $f(X)$ and fixes the rest. Therefore $G_f \subset S_p$ and contains a transposition and a p-cycle, and so is the whole of S_p. □

It remains to construct polynomials satisfying the conditions of the Proposition.

EXAMPLE 4.17 Let $p \geq 5$ be a prime number. Choose a positive even integer m and even integers

$$n_1 < n_2 < \cdots < n_{p-2},$$

and let

$$g(X) = (X^2 + m)(X - n_1)...(X - n_{p-2}).$$

The graph of g crosses the x-axis exactly at the points $n_1, \ldots, n_{p-2}$, and it doesn't have a local maximum or minimum at any of those points (because the n_i are simple roots). Thus $e = \min_{g'(x)=0} |g(x)| > 0$, and we can choose an odd positive integer n such that $\frac{2}{n} < e$.

Consider

$$f(X) = g(X) - \frac{2}{n}.$$

As $\frac{2}{n} < e$, the graph of f also crosses the x-axis at exactly $p-2$ points, and so f has exactly two nonreal roots. On the other hand, when we write

$$nf(X) = nX^p + a_1X^{p-1} + \cdots + a_p,$$

the a_i are all even and a_p is not divisible by 2^2, and so Eisenstein's criterion implies that f is irreducible. Over $\mathbb{R}$, f has $p-2$ linear factors and one irreducible quadratic factor, and so it certainly splits over $\mathbb{C}$ (high school algebra). Therefore, the proposition applies to f.[1]

EXAMPLE 4.18 The reader shouldn't think that, in order to have Galois group S_p, a polynomial must have exactly two nonreal roots. For example, the polynomial $X^5 - 5X^3 + 4X - 1$ has Galois group S_5 but all of its roots are real.

Finite fields

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements. As we noted in §1, every field E of characteristic p contains a copy of $\mathbb{F}_p$, namely, $\{m1_E \mid m \in \mathbb{Z}\}$. No harm results if we identify $\mathbb{F}_p$ with this subfield of E.

Let E be a field of degree n over $\mathbb{F}_p$. Then E has $q = p^n$ elements, and so $E^\times$ is a group of order $q-1$. Therefore the nonzero elements of E are roots of $X^{q-1} - 1$, and *all* elements of E are roots of $X^q - X$. Hence E is a splitting field for $X^q - X$, and so any two fields with q elements are isomorphic.

[1] If m is taken sufficiently large, then $g(X) - 2$ will have exactly two nonreal roots, i.e., we can take $n = 1$, but the proof is longer (see Jacobson 1964, p. 107, who credits the example to Brauer). The shorter argument in the text was suggested to me by Martin Ward.

PROPOSITION 4.19 *Every extension of finite fields is simple.*

PROOF. Consider $E \supset F$. Then $E^\times$ is a finite subgroup of the multiplicative group of a field, and hence is cyclic (see Exercise 1-3). If ζ generates $E^\times$ as a multiplicative group, then certainly $E = F[\zeta]$. □

Now let E be a splitting field of $f(X) = X^q - X$, $q = p^n$. The derivative $f'(X) = -1$, which is relatively prime to $f(X)$ (in fact, to every polynomial), and so $f(X)$ has q distinct roots in E. Let S be the set of its roots. Then S is obviously closed under multiplication and the formation of inverses, but it is also closed under subtraction: if $a^q = a$ and $b^q = b$, then

$$(a-b)^q = a^q - b^q = a - b.$$

Hence S is a field, and so $S = E$. In particular, E has p^n elements.

PROPOSITION 4.20 *For each power $q = p^n$ of p there exists a field $\mathbb{F}_q$ with q elements. Every such field is a splitting field for $X^q - X$, and so any two are isomorphic. Moreover, $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ with cyclic Galois group generated by the Frobenius automorphism $\sigma(a) = a^p$.*

PROOF. Only the final statement remains to be proved. The field $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ because it is the splitting field of a separable polynomial. We noted in 1.4 that $x \overset{\sigma}{\mapsto} x^p$ is an automorphism of $\mathbb{F}_q$. An element a of $\mathbb{F}_q$ is fixed by σ if and only if $a^p = a$, but $\mathbb{F}_p$ consists exactly of such elements, and so the fixed field of $\langle\sigma\rangle$ is $\mathbb{F}_p$. This proves that $\mathbb{F}_q$ is Galois over $\mathbb{F}_p$ and that $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ (see 3.11b). □

COROLLARY 4.21 *Let E be a field with p^n elements. For each divisor m of n, $m \geq 0$, E contains exactly one field with p^m elements.*

PROOF. We know that E is Galois over $\mathbb{F}_p$ and that $\mathrm{Gal}(E/\mathbb{F}_p)$ is the cyclic group of order n generated by σ. The group $\langle\sigma\rangle$ has one subgroup of order n/m for each m dividing n, namely, $\langle\sigma^m\rangle$, and so E has exactly one subfield of degree m over $\mathbb{F}_p$ for each m dividing n, namely, $E^{\langle\sigma^m\rangle}$. Because it has degree m over $\mathbb{F}_p$, $E^{\langle\sigma^m\rangle}$ has p^m elements. □

COROLLARY 4.22 *Each monic irreducible polynomial f of degree $d|n$ in $\mathbb{F}_p[X]$ occurs exactly once as a factor of $X^{p^n} - X$; hence, the degree of the splitting field of f is $\leq d$.*

PROOF. First, the factors of $X^{p^n} - X$ are distinct because it has no common factor with its derivative. If $f(X)$ is irreducible of degree d, then $f(X)$ has a root in a field of degree d over $\mathbb{F}_p$. But the splitting field of $X^{p^n} - X$ contains a copy of every field of degree d over $\mathbb{F}_p$ with $d|n$. Hence some root of $X^{p^n} - X$ is also a root of $f(X)$, and therefore $f(X)|X^{p^n} - X$. In particular, f divides $X^{p^d} - X$, and therefore it splits in its splitting field, which has degree d over $\mathbb{F}_p$. □

PROPOSITION 4.23 *Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_p$. Then $\mathbb{F}$ contains exactly one field $\mathbb{F}_{p^n}$ for each integer $n \geq 1$, and $\mathbb{F}_{p^n}$ consists of the roots of $X^{p^n} - X$. Moreover,*

$$\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n} \iff m|n.$$

The partially ordered set of finite subfields of $\mathbb{F}$ is isomorphic to the set of integers $n \geq 1$ partially ordered by divisibility.

PROOF. Obvious from what we have proved. □

PROPOSITION 4.24 *The field $\mathbb{F}_p$ has an algebraic closure $\mathbb{F}$.*

PROOF. Choose a sequence of integers $1 = n_1 < n_2 < n_3 < \cdots$ such that $n_i | n_{i+1}$ for all i, and every integer n divides some n_i. For example, let $n_i = i!$. Define the fields $\mathbb{F}_{p^{n_i}}$ inductively as follows: $\mathbb{F}_{p^{n_1}} = \mathbb{F}_p$; $\mathbb{F}_{p^{n_i}}$ is the splitting field of $X^{p^{n_i}} - X$ over $\mathbb{F}_{p^{n_{i-1}}}$. Then, $\mathbb{F}_{p^{n_1}} \subset \mathbb{F}_{p^{n_2}} \subset \mathbb{F}_{p^{n_3}} \subset \cdots$, and we define $\mathbb{F} = \bigcup \mathbb{F}_{p^{n_i}}$. As a union of a chain of fields algebraic over $\mathbb{F}_p$, it is again a field algebraic over $\mathbb{F}_p$. Moreover, every polynomial in $\mathbb{F}_p[X]$ splits in $\mathbb{F}$, and so it is an algebraic closure of $\mathbb{F}$ (by 1.44). □

REMARK 4.25 Since the $\mathbb{F}_{p^n}$ are not subsets of a fixed set, forming the union requires explanation. Define S to be the disjoint union of the $\mathbb{F}_{p^n}$. For $a, b \in S$, set $a \sim b$ if $a = b$ in one of the $\mathbb{F}_{p^n}$. Then $\sim$ is an equivalence relation, and we let $\mathbb{F} = S/\sim$.

Any two fields with q elements are isomorphic, but not necessarily *canonically* isomorphic. However, once we have chosen an algebraic closure $\mathbb{F}$ of $\mathbb{F}_p$, there is a *unique* subfield of $\mathbb{F}$ with q elements.

PARI factors polynomials modulo p very quickly. Recall that the syntax is `factormod(f(X),p)`. For example, to obtain a list of all monic polynomials of degree $1, 2$, or 4 over $\mathbb{F}_5$, ask PARI to factor $X^{625} - X$ modulo 5 (note that $625 = 5^4$).

ASIDE 4.26 In one of the few papers published during his lifetime, Galois defined finite fields of arbitrary prime power order and established their basic properties, for example, the existence of a primitive element (Notices A.M.S., Feb. 2003, p. 198). For this reason finite fields are often called ***Galois fields*** and the field with q elements is often denoted by GF(q).

Computing Galois groups over $\mathbb{Q}$

In the remainder of this chapter, I describe a practical method for computing Galois groups over $\mathbb{Q}$ and similar fields. Recall that for a separable polynomial $f \in F[X]$, F_f denotes a splitting field for F, and $G_f = \mathrm{Gal}(F_f/F)$ denotes the Galois group of f. Moreover, G_f permutes the roots $\alpha_1, \dots, \alpha_m$, $m = \deg f$, of f in F_f:

$$G \subset \mathrm{Sym}\{\alpha_1, \dots, \alpha_m\}.$$

The first result generalizes Proposition 4.4.

PROPOSITION 4.27 *Let $f(X)$ be a separable polynomial in $F[X]$, and suppose that the orbits of G_f acting on the roots of f have $m_1, \dots, m_r$ elements respectively. Then f factors as $f = f_1 \cdots f_r$ with f_i irreducible of degree m_i.*

PROOF. We may suppose that f is monic. Let $\alpha_1, \dots, \alpha_m$, be the roots of $f(X)$ in F_f. The monic factors of $f(X)$ in $F_f[X]$ correspond to subsets S of $\{\alpha_1, \dots, \alpha_m\}$,

$$S \leftrightarrow f_S = \prod_{\alpha \in S} (X - \alpha),$$

and f_S is fixed under the action of G_f (and hence has coefficients in F) if and only if S is stable under G_f. Therefore the irreducible factors of f in $F[X]$ are the polynomials f_S corresponding to minimal subsets S of $\{\alpha_1, \dots, \alpha_m\}$ stable under G_f, but these subsets S are precisely the orbits of G_f in $\{\alpha_1, \dots, \alpha_m\}$. □

REMARK 4.28 Note that the proof shows the following: let $\{\alpha_1,\dots,\alpha_m\} = \bigcup O_i$ be the decomposition of $\{\alpha_1,\dots,\alpha_m\}$ into a disjoint union of orbits for the group G_f; then

$$f = \prod f_i, \quad f_i = \prod_{\alpha_j \in O_i} (X - \alpha_j)$$

is the decomposition of f into a product of irreducible polynomials in $F[X]$.

Now suppose that F is finite, with p^n elements say. Then G_f is a cyclic group generated by the Frobenius automorphism $\sigma: x \mapsto x^{p^n}$. When we regard σ as a permutation of the roots of f, then the orbits of σ correspond to the factors in its cycle decomposition (GT 4.26). Hence, if the degrees of the distinct irreducible factors of f are $m_1, m_2, \dots, m_r$, then σ has a cycle decomposition of type

$$m_1 + \cdots + m_r = \deg f.$$

PROPOSITION 4.29 *Let R be a unique factorization domain with field of fractions F, and let f be a monic polynomial in $R[X]$. Let P be a prime ideal in R, let $\overline{F} = R/P$, and let $\overline{f}$ be the image of f in $\overline{F}[X]$. Assume that $\overline{f}$ is separable. Then f is separable, and its roots $\alpha_1,\dots,\alpha_m$ lie in some finite extension R' of R. Their reductions $\overline{\alpha}_i$ modulo PR' are the roots of $\overline{f}$, and $G_{\overline{f}} \subset G_f$ when both are identified with subgroups of* $\mathrm{Sym}\{\alpha_1,\dots,\alpha_m\} = \mathrm{Sym}\{\overline{\alpha}_1,\dots,\overline{\alpha}_m\}$.

We defer the proof to the end of this section.

On combining these results, we obtain the following theorem.

THEOREM 4.30 (DEDEKIND) *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree m, and let p be a prime such that $f \mod p$ has simple roots (equivalently, $D(f)$ is not divisible by p). Suppose that $\overline{f} = \prod f_i$ with f_i irreducible of degree m_i in $\mathbb{F}_p[X]$. Then G_f contains an element whose cycle decomposition is of type*

$$m = m_1 + \cdots + m_r.$$

EXAMPLE 4.31 Consider $X^5 - X - 1$. Modulo 2, this factors as

$$(X^2 + X + 1)(X^3 + X^2 + 1),$$

and modulo 3 it is irreducible. The theorem shows that G_f contains permutations $(ik)(lmn)$ and (12345), and so also $((ik)(lmn))^3 = (ik)$. Therefore $G_f = S_5$ by (4.15).

LEMMA 4.32 *A transitive subgroup of $H \subset S_n$ containing a transposition and an $(n-1)$-cycle is equal to S_n.*

PROOF. After renumbering, we may suppose that the $(n-1)$-cycle is $(123\dots n-1)$. Because of the transitivity, the transposition can be transformed into (in), some $1 \le i \le n-1$. Conjugating (in) by $(123\dots n-1)$ and its powers will transform it into $(1n)$, $(2n)$, …, $(n-1\,n)$, and these elements obviously generate S_n. □

EXAMPLE 4.33 Select separable monic polynomials of degree n, f_1, f_2, f_3 with coefficients in $\mathbb{Z}$ with the following factorizations:

(a) f_1 is irreducible modulo 2;

(b) $f_2 =$ (degree 1)(irreducible of degree $n-1$) mod 3;

(c) $f_3 =$ (irreducible of degree 2)(product of 1 or 2 irreducible polynomials of odd degree) mod 5.

Take

$$f = -15f_1 + 10f_2 + 6f_3.$$

Then

(i) G_f is transitive (it contains an n-cycle because $f \equiv f_1 \bmod 2$);

(ii) G_f contains a cycle of length $n-1$ (because $f \equiv f_2 \bmod 3$);

(iii) G_f contains a transposition (because $f \equiv f_3 \bmod 5$, and so it contains the product of a transposition with a commuting element of odd order; on raising this to an appropriate odd power, we are left with the transposition). Hence G_f is S_n.

The above results give the following strategy for computing the Galois group of an irreducible polynomial $f \in \mathbb{Q}[X]$. Factor f modulo a sequence of primes p not dividing $D(f)$ to determine the cycle types of the elements in G_f — a difficult theorem in number theory, the effective Chebotarev density theorem, says that if a cycle type occurs in G_f, then this will be seen by looking modulo a set of prime numbers of positive density, and will occur for a prime less than some bound. Now look up a table of transitive subgroups of S_n with order divisible by n and their cycle types. If this doesn't suffice to determine the group, then look at its action on the set of subsets of r roots for some r.

See, Butler and McKay, *The transitive groups of degree up to eleven*, Comm. Algebra 11 (1983), 863–911. This lists all transitive subgroups of S_n, $n \leq 11$, and gives the cycle types of their elements and the orbit lengths of the subgroup acting on the r-sets of roots. With few exceptions, these invariants are sufficient to determine the subgroup up to isomorphism.

PARI can compute Galois groups for polynomials of degree ≤ 11 over $\mathbb{Q}$. The syntax is `polgalois(f)` where f is an irreducible polynomial of degree ≤ 11 (or ≤ 7 depending on your setup), and the output is (n,s,k,name) where n is the order of the group, s is $+1$ or -1 according as the group is a subgroup of the alternating group or not, and "name" is the name of the group. For example, `polgalois(X^5-5*X^3+4*X-1)` (see 4.18) returns the symmetric group S_5, which has order 120, `polgalois(X^11-5*X^3+4*X-1)` returns the symmetric group S_{11}, which has order 39916800, and `polgalois(X^12-5*X^3+4*X-1)` returns an apology. The reader should use PARI to check the examples 4.9–4.12.

See also, Soicher and McKay, *Computing Galois groups over the rationals*, J. Number Theory, 20 (1985) 273–281.

PROOF OF PROPOSITION 4.29

We follow the elegant argument in van der Waerden, Modern Algebra, I, §61.

Let $f(X)$ be a separable polynomial in $F[X]$ and $\alpha_1,\dots,\alpha_m$ its roots. Let $T_1,\dots,T_m$ be symbols. For a permutation σ of $\{1,\dots,m\}$, we let σ_α and σ_T respectively denote the corresponding permutations of $\{\alpha_1,\dots,\alpha_m\}$ and $\{T_1,\dots,T_m\}$.

Let

$$\theta = T_1\alpha_1 + \cdots + T_m\alpha_m$$

and

$$f(X,T) = \prod_{\sigma\in S_m} (X - \sigma_T\theta).$$

Clearly $f(X,T)$ is symmetric in the α_i, and so its coefficients lie in F. Let

$$f(X,T) = f_1(X,T)\cdots f_r(X,T) \tag{10}$$

be the factorization of $f(X,T)$ into a product of irreducible monic polynomials. Here we use that $F[X,T_1,\dots,T_m]$ is a unique factorization domain (CA 4.10). The permutations σ such that σ_T carries any one of the factors, say $f_1(X,T)$, into itself form a subgroup G of S_m.

LEMMA 4.34 *The map $\sigma \mapsto \sigma_\alpha$ is an isomorphism from G onto G_f.*

PROOF. In any F-algebra containing the roots of f, the polynomial $f_1(X,T)$ is a product of factors of the form $X-\sigma\theta$. After possibly renumbering the roots of f, we may suppose that $f_1(X,T)$ contains the factor $X-\theta$. Note that $s_T s_\alpha$ leaves θ invariant, i.e., $s_T s_\alpha \theta = \theta$, and so

$$s_\alpha\theta = s_T^{-1}\theta. \tag{11}$$

Let σ be a permutation of $\{1,\dots,m\}$. If σ_T leaves $f_1(X,T)$ invariant, then it permutes its roots. Therefore, it maps $X-\theta$ into a linear factor of $f_1(X,T)$. Conversely, if σ_T maps $X-\theta$ into a linear factor of $f_1(X,T)$, then this linear factor will be a common factor of $f_1(X,T)$ and the image of $f_1(X,T)$ under σ_T, which implies that the two are equal, and so σ_T leaves $f_1(X,T)$ invariant. We conclude that σ_T leaves $f_1(X,T)$ invariant if and only if σ_T maps $X-\theta$ into a linear factor of $f_1(X,T)$.

Again, let σ be a permutation of $\{1,\dots,m\}$. Then $\sigma_\alpha \in G_f$ if and only if it maps $F(T)[\theta]$ isomorphically onto $F(T)[\sigma_\alpha\theta]$, i.e., if and only if θ and $\sigma_\alpha\theta$ have the same minimum polynomial. The minimum polynomial of θ is $f_1(X,T)$, and so this shows that s_α lies in G_f if and only if σ_α leaves $f_1(X,T)$ invariant, i.e., if and only if σ_α maps $X-\theta$ into a linear factor of $f_1(X,T)$.

From the last two paragraphs and (11), we see that the condition for σ to lie in G is the same as the condition for σ_α to lie in G_f, which concludes the proof. □

After these preliminaries, we prove Lemma 4.29. With the notation of the lemma, let $R' = R[\alpha_1,\dots,\alpha_m]$. Then R' is generated by a finite number of elements, each integral over R, and so it is finite as an R-algebra (CA 6.2). Clearly, the map $a \mapsto \bar{a}\colon R' \to R'/PR'$ sends the roots of f onto the roots of $\bar{f}$. As the latter are distinct, so are the former, and the map is bijective.

A general form of Proposition 1.14 shows that, in the factorization (10), the f_i lie in $R[X,T]$. Hence (10) gives a factorization

$$\bar{f}(X,T) = \bar{f}_1(X,T)\cdots\bar{f}_r(X,T)$$

in $\bar{F}[X,T]$. Let $\bar{f}_1(X,T)_1$ be an irreducible factor of $\bar{f}_1(X,T)$. According to Lemma 4.34, G_f is the set of permutations σ_α such that σ_T leaves $f_1(X,T)$ invariant, and $G_{\bar{f}}$ is the set of permutations σ_α such that σ_T leaves $\bar{f}_1(X,T)_1$ invariant. Clearly $G_{\bar{f}} \subset G_f$.

Exercises

4-1 Find the splitting field of $X^m - 1 \in \mathbb{F}_p[X]$.

4-2 Find the Galois group of $X^4 - 2X^3 - 8X - 3$ over $\mathbb{Q}$.

4-3 Find the degree of the splitting field of $X^8 - 2$ over $\mathbb{Q}$.

4-4 Give an example of a field extension E/F of degree 4 such that there does not exist a field M with $F \subset M \subset E$, $[M:F] = 2$.

4-5 List all irreducible polynomials of degree 3 over $\mathbb{F}_7$ in 10 seconds or less (there are 112).

4-6 "It is a thought-provoking question that few graduate students would know how to approach the question of determining the Galois group of, say,

$$X^6 + 2X^5 + 3X^4 + 4X^3 + 5X^2 + 6X + 7.$$"

[over $\mathbb{Q}$].

(a) Can you find it?

(b) Can you find it without using the "`polgalois`" command in PARI?

4-7 Let $f(X) = X^5 + aX + b$, $a, b \in \mathbb{Q}$. Show that $G_f \approx D_5$ (dihedral group) if and only if

(a) $f(X)$ is irreducible in $\mathbb{Q}[X]$, and

(b) the discriminant $D(f) = 4^4a^5 + 5^5b^4$ of $f(X)$ is a square, and

(c) the equation $f(X) = 0$ is solvable by radicals.

4-8 Show that a polynomial f of degree $n = \prod_{i=1}^{k} p_i^{r_i}$ (the p_i are distinct primes) is irreducible over $\mathbb{F}_p$ if and only if (a) $\gcd(f(X), X^{p^{n/p_i}} - X) = 1$ for all $1 \le i \le k$ and (b) f divides $X^{p^n} - X$ (Rabin irreducibility test[2]).

4-9 Let $f(X)$ be an irreducible polynomial in $\mathbb{Q}[X]$ with both real and nonreal roots. Show that its Galois group is nonabelian. Can the condition that f is irreducible be dropped?

4-10 Let F be a Galois extension of $\mathbb{Q}$, and let α be an element of F such that $\alpha F^{\times 2}$ is not fixed by the action of $\mathrm{Gal}(F/\mathbb{Q})$ on $F^\times/F^{\times 2}$. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the orbit of α under $\mathrm{Gal}(F/\mathbb{Q})$. Show:

(a) $F[\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n}]/F$ is Galois with commutative Galois group contained in $(\mathbb{Z}/2\mathbb{Z})^n$.

(b) $F[\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_n}]/\mathbb{Q}$ is Galois with noncommutative Galois group contained in $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \mathrm{Gal}(F/\mathbb{Q})$. (Cf. mo113794.)

[2]Rabin, Michael O. Probabilistic algorithms in finite fields. SIAM J. Comput. 9 (1980), no. 2, 273–280.

CHAPTER 5

Applications of Galois Theory

In this chapter, we apply the fundamental theorem of Galois theory to obtain other results about polynomials and extensions of fields.

Primitive element theorem.

Recall that a finite extension of fields E/F is simple if $E = F[\alpha]$ for some element α of E. Such an α is called a ***primitive element*** of E. We'll show that (at least) all separable extensions have primitive elements.

Consider for example $\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q}$. We know (see Exercise 3-3) that its Galois group over $\mathbb{Q}$ is a 4-group $\langle\sigma,\tau\rangle$, where

$$\begin{cases} \sigma\sqrt{2} &= -\sqrt{2} \\ \sigma\sqrt{3} &= \sqrt{3} \end{cases}, \quad \begin{cases} \tau\sqrt{2} &= \sqrt{2} \\ \tau\sqrt{3} &= -\sqrt{3} \end{cases}.$$

Note that

$$\begin{aligned} \sigma(\sqrt{2}+\sqrt{3}) &= -\sqrt{2}+\sqrt{3}, \\ \tau(\sqrt{2}+\sqrt{3}) &= \sqrt{2}-\sqrt{3}, \\ (\sigma\tau)(\sqrt{2}+\sqrt{3}) &= -\sqrt{2}-\sqrt{3}. \end{aligned}$$

These all differ from $\sqrt{2}+\sqrt{3}$, and so only the identity element of $\mathrm{Gal}(\mathbb{Q}[\sqrt{2},\sqrt{3}]/\mathbb{Q})$ fixes the elements of $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$. According to the fundamental theorem, this implies that $\sqrt{2}+\sqrt{3}$ is a primitive element:

$$\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}].$$

It is clear that this argument should work much more generally.

Recall that an element α algebraic over a field F is separable over F if its minimum polynomial over F has no multiple roots.

THEOREM 5.1 *Let $E = F[\alpha_1,\ldots,\alpha_r]$ be a finite extension of F, and assume that $\alpha_2,\ldots,\alpha_r$ are separable over F (but not necessarily α_1). Then there is an element $\gamma \in E$ such that $E = F[\gamma]$.*

PROOF. For finite fields, we proved this in 4.19. Hence we may assume F to be infinite. It suffices to prove the statement for $r = 2$, for then

$$F[\alpha_1,\alpha_2,\ldots,\alpha_r] = F[\alpha_1',\alpha_3,\ldots,\alpha_r] = F[\alpha_1'',\alpha_4,\ldots,\alpha_r] = \cdots.$$

Thus let $E = F[\alpha, \beta]$ with β separable over F. Let f and g be the minimum polynomials of α and β over F, and let L be a splitting field for fg containing E. Let $\alpha_1 = \alpha, \dots, \alpha_s$ be the roots of f in L, and let $\beta_1 = \beta, \beta_2, \dots, \beta_t$ be the roots of g. For $j \neq 1$, $\beta_j \neq \beta$, and so the the equation

$$\alpha_i + X\beta_j = \alpha + X\beta,$$

has exactly one solution, namely, $X = \frac{\alpha_i - \alpha}{\beta - \beta_j}$. If we choose a $c \in F$ different from any of these solutions (using that F is infinite), then

$$\alpha_i + c\beta_j \neq \alpha + c\beta \text{ unless } i = 1 = j.$$

Let $\gamma = \alpha + c\beta$. I claim that

$$F[\alpha, \beta] = F[\gamma].$$

The polynomials $g(X)$ and $f(\gamma - cX)$ have coefficients in $F[\gamma]$, and have β as a root:

$$g(\beta) = 0, \quad f(\gamma - c\beta) = f(\alpha) = 0.$$

In fact, β is their only common root, because we chose c so that $\gamma - c\beta_j \neq \alpha_i$ unless $i = 1 = j$. Therefore

$$\gcd(g(X), f(\gamma - cX)) = X - \beta.$$

Here we computed the gcd in $L[X]$, but this is equal to the gcd computed in $F[\gamma][X]$ (Proposition 2.10). Hence $\beta \in F[\gamma]$, and this implies that $\alpha = \gamma - c\beta$ also lies in $F[\gamma]$. This proves the claim. □

REMARK 5.2 When F is infinite, the proof shows that γ can be chosen to be of the form

$$\gamma = \alpha_1 + c_2\alpha_2 + \cdots + c_r\alpha_r, \quad c_i \in F.$$

If $F[\alpha_1, \dots, \alpha_r]$ is Galois over F, then an element of this form will be a primitive element provided it is moved by every nontrivial element of the Galois group. This remark makes it very easy to write down primitive elements.

Our hypotheses are minimal: if *two* of the α are not separable, then the extension need not be simple. Before giving an example to illustrate this, we need another result.

PROPOSITION 5.3 *Let $E = F[\gamma]$ be a simple algebraic extension of F. Then there are only finitely many intermediate fields M,*

$$F \subset M \subset E.$$

PROOF. Let M be such a field, and let $g(X)$ be the minimum polynomial of γ over M. Let M' be the subfield of E generated over F by the coefficients of $g(X)$. Clearly $M' \subset M$, but (equally clearly) $g(X)$ is the minimum polynomial of γ over M'. Hence

$$[E : M'] = \deg(g) = [E : M],$$

and so $M = M'$; we have shown that M is generated by the coefficients of $g(X)$.

Let $f(X)$ be the minimum polynomial of γ over F. Then $g(X)$ divides $f(X)$ in $M[X]$, and hence also in $E[X]$. Therefore, there are only finitely many possible g, and consequently only finitely many possible M. □

REMARK 5.4 (a) Note that the proof in fact gives a description of all the intermediate fields: each is generated over F by the coefficients of a factor $g(X)$ of $f(X)$ in $E[X]$. The coefficients of such a $g(X)$ are partially symmetric polynomials in the roots of $f(X)$ (that is, fixed by some, but not necessarily all, of the permutations of the roots).

(b) The proposition has a converse: if E is a finite extension of F and there are only finitely many intermediate fields M, $F \subset M \subset E$, then E is a simple extension of F. This gives another proof of Theorem 5.1 in the case that E is separable over F, because Galois theory shows that there are only finitely many intermediate fields in this case (even the Galois closure of E over F has only finitely many intermediate fields).

EXAMPLE 5.5 The simplest nonsimple algebraic extension is $k(X,Y) \supset k(X^p, Y^p)$, where k is an algebraically closed field of characteristic p. Let $F = k(X^p, Y^p)$. For all $c \in k$, we have

$$k(X,Y) = F[X,Y] \supset F[X+cY] \supset F$$

with the degree of each extension equal to p. If

$$F[X+cY] = F[X+c'Y], \quad c \neq c',$$

then $F[X+cY]$ would contain both X and Y, which is impossible because $[k(X,Y)\colon F] = p^2$. Hence there are infinitely many distinct intermediate fields.[1]

Alternatively, note that the degree of $k(X,Y)$ over $k(X^p, Y^p)$ is p^2, but if $\alpha \in k(X,Y)$, then $\alpha^p \in k(X^p, Y^p)$, and so α generates a field of degree at most p over $k(X^p, Y^p)$.

Fundamental Theorem of Algebra

We finally prove the misnamed[2] fundamental theorem of algebra.

THEOREM 5.6 *The field $\mathbb{C}$ of complex numbers is algebraically closed.*

PROOF. We define $\mathbb{C}$ to be the splitting field of X^2+1 over $\mathbb{R}$, and we let i denote a root of X^2+1 in $\mathbb{C}$. Thus $\mathbb{C} = \mathbb{R}[i]$. We have to show (see 1.44) that every $f(X) \in \mathbb{R}[X]$ has a root in $\mathbb{C}$. We may suppose that f is monic, irreducible, and $\neq X^2+1$.

We'll need to use the following two facts about $\mathbb{R}$:

- ◇ positive real numbers have square roots;
- ◇ every polynomial of odd degree with real coefficients has a real root.

Both are immediate consequences of the Intermediate Value Theorem, which says that a continuous function on a closed interval takes every value between its maximum and minimum values (inclusive). (Intuitively, this says that, unlike the rationals, the real line has no "holes".)

[1] Zariski showed that there is even an intermediate field M that is not isomorphic to $F(X,Y)$, and Piotr Blass showed, using the methods of algebraic geometry, that there is an infinite sequence of intermediate fields, no two of which are isomorphic.

[2] Because it is not strictly a theorem in algebra: it is a statement about $\mathbb{R}$ whose construction is part of analysis (or maybe topology). In fact, I prefer the proof based on Liouville's theorem in complex analysis to the more algebraic proof given in the text: if $f(z)$ is a polynomial without a root in $\mathbb{C}$, then $f(z)^{-1}$ will be bounded and holomorphic on the whole complex plane, and hence (by Liouville) constant. The Fundamental Theorem was quite difficult to prove. Gauss gave a proof in his doctoral dissertation in 1798 in which he used some geometric arguments which he didn't justify. He gave the first rigorous proof in 1816. The elegant argument given here is a simplification by Emil Artin of earlier proofs (see Artin, E., Algebraische Konstruction reeller Körper, Hamb. Abh., Bd. 5 (1926), 85-90; translation available in Artin, Emil. Exposition by Emil Artin: a selection. AMS; LMS 2007).

We first show that every element of $\mathbb{C}$ has a square root. Write $\alpha = a + bi$, with $a, b \in \mathbb{R}$, and choose c, d to be real numbers such that

$$c^2 = \frac{(a + \sqrt{a^2 + b^2})}{2}, \quad d^2 = \frac{(-a + \sqrt{a^2 + b^2})}{2}.$$

Then $c^2 - d^2 = a$ and $(2cd)^2 = b^2$. If we choose the signs of c and d so that cd has the same sign as b, then $(c + di)^2 = \alpha$ and so $c + di$ is a square root of α.

Let $f(X) \in \mathbb{R}[X]$, and let E be a splitting field for $f(X)(X^2 + 1)$. Then E contains $\mathbb{C}$, and we have to show that it equals $\mathbb{C}$. Since $\mathbb{R}$ has characteristic zero, the polynomial is separable, and so E is Galois over $\mathbb{R}$ (see 3.10). Let G be its Galois group, and let H be a Sylow 2-subgroup of G.

Let $M = E^H$ and let $\alpha \in M$. Then M has of degree $(G\colon H)$ over $\mathbb{R}$, which is odd, and so the minimum polynomial of α over $\mathbb{R}$ has odd degree (by the multiplicativity of degrees, 1.20). This implies that it has a real root, and so is of degree 1. Hence $\alpha \in \mathbb{R}$, and so $M = \mathbb{R}$ and $G = H$.

We deduce that $\mathrm{Gal}(E/\mathbb{C})$ is a 2-group. If it is $\neq 1$, then it has a subgroup N of index 2 (GT 4.17). The field E^N has degree 2 over $\mathbb{C}$, and so it is generated by the square root of an element of $\mathbb{C}$ (see 3.24), but all square roots of elements of $\mathbb{C}$ lie in $\mathbb{C}$. Hence $E^N = \mathbb{C}$, which is a contradiction. Thus $\mathrm{Gal}(E/\mathbb{C}) = 1$ and $E = \mathbb{C}$. □

COROLLARY 5.7 *(a) The field $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.*

(b) The set of all algebraic numbers is an algebraic closure of $\mathbb{Q}$.

PROOF. Part (a) is obvious from the definition of "algebraic closure" (1.43), and (b) follows from Corollary 1.46. □

Cyclotomic extensions

A ***primitive*** nth root of 1 in F is an element of order n in $F^\times$. Such an element can exist only if F has characteristic 0 or if its characteristic p does not divide n.

PROPOSITION 5.8 *Let F be a field of characteristic 0 or characteristic p not dividing n, and let E be the splitting field of $X^n - 1$.*

(a) *There exists a primitive nth root of 1 in E.*

(b) *If ζ is a primitive nth root of 1 in E, then $E = F[\zeta]$.*

(c) *The field E is Galois over F; for each $\sigma \in \mathrm{Gal}(E/F)$, there is an $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma\zeta = \zeta^i$ for all ζ with $\zeta^n = 1$; the map $\sigma \mapsto [i]$ is an injective homomorphism*

$$\mathrm{Gal}(E/F) \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

PROOF. (a) The roots of $X^n - 1$ are distinct, because its derivative nX^{n-1} has only zero as a root (here we use the condition on the characteristic), and so E contains n distinct nth roots of 1. The nth roots of 1 form a finite subgroup of $E^\times$, and so (see Exercise 3) they form a cyclic group. Every generator has order n, and hence is a primitive nth root of 1.

(b) The roots of $X^n - 1$ are the powers of ζ, and $F[\zeta]$ contains them all.

(c) The extension E/F is Galois because E is the splitting field of a separable polynomial. If ζ_0 is one primitive nth root of 1, then the remaining primitive nth roots of 1 are the elements ζ_0^i with i relatively prime to n. Since, for any automorphism σ of E, $\sigma\zeta_0$ is again a primitive nth root of 1, it equals ζ_0^i for some i relatively prime to n, and the map $\sigma \mapsto i \mod n$ is

injective because ζ_0 generates E over F. It obviously is a homomorphism. Moreover, for any other nth root of 1, say, $\zeta = \zeta_0^m$, we have

$$\sigma\zeta = (\sigma\zeta_0)^m = \zeta_0^{im} = \zeta^i,$$

and so the homomorphism does not depend on the choice of ζ_0. □

The map $\sigma \mapsto [i]: \mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ need not be surjective. For example, if $F = \mathbb{C}$, then its image is $\{1\}$, and if $F = \mathbb{R}$, it is either $\{[1]\}$ or $\{[-1],[1]\}$. On the other hand, when $n = p$ is prime, we showed in (1.41) that $[\mathbb{Q}[\zeta]:\mathbb{Q}] = p-1$, and so the map is surjective. We now prove that the map is surjective for all n when $F = \mathbb{Q}$.

The polynomial $X^n - 1$ has some obvious factors in $\mathbb{Q}[X]$, namely, the polynomials $X^d - 1$ for any $d \mid n$. When we remove all factors of $X^n - 1$ of this form with $d < n$, the polynomial we are left with is called the nth ***cyclotomic polynomial*** Φ_n. Thus

$$\Phi_n = \prod (X - \zeta) \qquad \text{(product over the primitive } n\text{th roots of 1)}.$$

It has degree $\varphi(n)$, the order of $(\mathbb{Z}/n\mathbb{Z})^\times$. Since every nth root of 1 is a primitive dth root of 1 for exactly one d dividing n, we see that

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

For example, $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, and

$$\Phi_6(X) = \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1.$$

This gives an easy inductive method of computing the cyclotomic polynomials. Alternatively type `polcyclo(n,X)` in PARI.

Because $X^n - 1$ has coefficients in $\mathbb{Z}$ and is monic, every monic factor of it in $\mathbb{Q}[X]$ has coefficients in $\mathbb{Z}$ (see 1.14). In particular, the cyclotomic polynomials lie in $\mathbb{Z}[X]$.

LEMMA 5.9 *Let F be a field of characteristic 0 or p not dividing n, and let ζ be a primitive nth root of 1 in some extension field. The following are equivalent:*

(a) *the nth cyclotomic polynomial Φ_n is irreducible;*

(b) *the degree $[F[\zeta]: F] = \varphi(n)$;*

(c) *the homomorphism*

$$\mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

is an isomorphism.

PROOF. Because ζ is a root of Φ_n, the minimum polynomial of ζ divides Φ_n. It equals it if and only if $[F[\zeta]: F] = \varphi(n)$, which is true if and only if the injection $\mathrm{Gal}(F[\zeta]/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is onto. □

THEOREM 5.10 *The nth cyclotomic polynomial Φ_n is irreducible in $\mathbb{Q}[X]$.*

PROOF. Let $f(X)$ be a monic irreducible factor of Φ_n in $\mathbb{Q}[X]$. Its roots will be primitive nth roots of 1, and we have to show they include *all* primitive nth roots of 1. For this it suffices to show that

$$\zeta \text{ a root of } f(X) \implies \zeta^i \text{ a root of } f(X) \text{ for all } i \text{ such that } \gcd(i,n) = 1.$$

Such an i is a product of primes not dividing n, and so it suffices to show that

$$\zeta \text{ a root of } f(X) \implies \zeta^p \text{ a root of } f(X) \text{ for all primes } p \text{ not dividing } n.$$

Write

$$\Phi_n(X) = f(X)g(X).$$

Proposition 1.14 shows that $f(X)$ and $g(X)$ lie in $\mathbb{Z}[X]$. Suppose that ζ is a root of f but that, for some prime p not dividing n, ζ^p is not a root of f. Then ζ^p is a root of $g(X)$, $g(\zeta^p) = 0$, and so ζ is a root of $g(X^p)$. As $f(X)$ and $g(X^p)$ have a common root, they have a nontrivial common factor in $\mathbb{Q}[X]$ (2.10), which automatically lies in $\mathbb{Z}[X]$ (1.14).

Write $h(X) \mapsto \overline{h}(X)$ for the quotient map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$, and note that, because $f(X)$ and $g(X^p)$ have a common factor of degree ≥ 1 in $\mathbb{Z}[X]$, so also do $\overline{f}(X)$ and $\overline{g}(X^p)$ in $\mathbb{F}_p[X]$. The mod p binomial theorem shows that

$$\overline{g}(X)^p = \overline{g}(X^p)$$

(recall that $a^p = a$ for all $a \in \mathbb{F}_p$), and so $\overline{f}(X)$ and $\overline{g}(X)$ have a common factor of degree ≥ 1 in $\mathbb{F}_p[X]$. Hence $X^n - 1$, when regarded as an element of $\mathbb{F}_p[X]$, has multiple roots, but we saw in the proof of Proposition 5.8 that it doesn't. Contradiction. □

REMARK 5.11 This proof is very old — in essence it goes back to Dedekind in 1857 — but its general scheme has recently become popular: take a statement in characteristic zero, reduce modulo p (where the statement may no longer be true), and exploit the existence of the Frobenius automorphism $a \mapsto a^p$ to obtain a proof of the original statement. For example, commutative algebraists use this method to prove results about commutative rings, and there are theorems about complex manifolds that were first proved by reducing things to characteristic p.

There are some beautiful relations between what happens in characteristic 0 and in characteristic p. For example, let $f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$. We can

(a) look at the solutions of $f = 0$ in $\mathbb{C}$, and so get a topological space;

(b) reduce mod p, and look at the solutions of $\overline{f} = 0$ in $\mathbb{F}_{p^n}$.

The Weil conjectures (Weil 1949; proved in part by Grothendieck in the 1960s and completely by Deligne in 1973) assert that the Betti numbers of the space in (a) control the cardinalities of the sets in (b).

THEOREM 5.12 *The regular n-gon is constructible if and only if $n = 2^k p_1 \cdots p_s$ where the p_i are distinct Fermat primes.*

PROOF. The regular n-gon is constructible if and only if $\cos \frac{2\pi}{n}$ (equivalently, $\zeta = e^{2\pi i/n}$) is constructible. We know that $\mathbb{Q}[\zeta]$ is Galois over $\mathbb{Q}$, and so (according to 1.37 and 3.23) ζ is constructible if and only if $[\mathbb{Q}[\zeta]:\mathbb{Q}]$ is a power of 2. When we write $n = \prod p^{n(p)}$,

$$\varphi(n) = \prod_{p|n} (p-1)p^{n(p)-1},$$

(GT 3.5), and this is a power of 2 if and only if n has the required form. □

REMARK 5.13 (a) As mentioned earlier, the Fermat primes are those of the form $2^{2^r} + 1$. It is known that these numbers are prime when $r = 0, 1, 2, 3, 4$, but it is not known whether or not there are more Fermat primes. Thus the problem of listing the n for which the regular n-gon is constructible is not yet solved (Wikipedia: Fermat numbers).

(b) The final section of Gauss's, *Disquisitiones Arithmeticae* (1801) is titled "Equations defining sections of a Circle". In it Gauss proves that the nth roots of 1 form a cyclic group, that $X^n - 1$ is solvable (this was before the theory of abelian groups had been developed, and before Galois), and that the regular n-gon is constructible when n is as in the Theorem. He also claimed to have proved the converse statement. This leads some people to credit him with the above proof of the irreducibility of Φ_n, but in the absence of further evidence, I'm sticking with Dedekind.

Dedekind's theorem on the independence of characters

THEOREM 5.14 (DEDEKIND) *Let F be a field and G a group. Then every finite set $\{\chi_1, \dots, \chi_m\}$ of group homomorphisms $G \to F^\times$ is linearly independent over F, i.e.,*

$$\sum a_i \chi_i = 0 \text{ (as a function } G \to F) \implies a_1 = 0, \dots, a_m = 0.$$

PROOF. We use induction on m. For $m = 1$, the statement is obvious. Assume it for $m-1$, and suppose that, for some set $\{\chi_1, \dots, \chi_m\}$ of homomorphisms $G \to F^\times$ and $a_i \in F$,

$$a_1\chi_1(x) + a_2\chi_2(x) + \cdots + a_m\chi_m(x) = 0 \quad \text{for all } x \in G.$$

We have to show that the a_i are zero. As χ_1 and χ_2 are distinct, they will take distinct values on some $g \in G$. On replacing x with gx in the equation, we find that

$$a_1\chi_1(g)\chi_1(x) + a_2\chi_2(g)\chi_2(x) + \cdots + a_m\chi_m(g)\chi_m(x) = 0 \quad \text{for all } x \in G.$$

On multiplying the first equation by $\chi_1(g)$ and subtracting it from the second, we obtain the equation

$$a_2'\chi_2 + \cdots + a_m'\chi_m = 0, \qquad a_i' = a_i(\chi_i(g) - \chi_1(g)).$$

The induction hypothesis shows that $a_i' = 0$ for $i = 2, 3, \dots$. As $\chi_2(g) - \chi_1(g) \neq 0$, this implies that $a_2 = 0$, and so

$$a_1\chi_1 + a_3\chi_3 + \cdots + a_m\chi_m = 0.$$

The induction hypothesis now shows that the remaining a_i are also zero. □

COROLLARY 5.15 *Let F and E be fields, and let $\sigma_1, \dots, \sigma_m$ be distinct homomorphisms $F \to E$. Then $\sigma_1, \dots, \sigma_m$ are linearly independent over E.*

PROOF. Apply the theorem to $\chi_i = \sigma_i | F^\times$. □

COROLLARY 5.16 *Let E be a finite separable extension of F of degree m. Let $\alpha_1, \dots, \alpha_m$ be a basis for E as an F-vector space, and let $\sigma_1, \dots, \sigma_m$ be distinct F-homomorphisms from E into a field Ω. Then the matrix whose (i, j)th-entry is $\sigma_i\alpha_j$ is invertible.*

PROOF. If not, there exist $c_i \in \Omega$ such that $\sum_{i=1}^m c_i\sigma_i(\alpha_j) = 0$ for all j. But the map $\sum_{i=1}^m c_i\sigma_i : E \to \Omega$ is F-linear, and so this implies that $\sum_{i=1}^m c_i\sigma_i(\alpha) = 0$ for all $\alpha \in E$, which contradicts Corollary 5.15. □

The normal basis theorem

DEFINITION 5.17 Let E be a finite Galois extension of F. A basis for E as an F-vector space is called a ***normal basis*** if it consists of the conjugates of a single element of E.

In other words, a normal basis is one of the form

$$\{\sigma\alpha \mid \sigma \in \mathrm{Gal}(E/F)\}$$

for some $\alpha \in E$.

THEOREM 5.18 (NORMAL BASIS THEOREM) *Every Galois extension has a normal basis.*

The ***group algebra*** FG of a group G is the F-vector space with basis the elements of G endowed with the multiplication extending that of G. Thus an element of FG is a sum $\sum_{\sigma\in G} a_\sigma\sigma$, $a_\sigma \in F$, and

$$\left(\textstyle\sum_\sigma a_\sigma\sigma\right)\left(\sum_\sigma b_\sigma\sigma\right) = \sum_\sigma \left(\sum_{\sigma_1\sigma_2=\sigma} a_{\sigma_1}b_{\sigma_2}\right)\sigma.$$

Every F-linear action of G on an F-vector space V extends uniquely to an action of FG on V.

Let E/F be a Galois extension with Galois group G. Then E is an FG-module, and Theorem 5.18 says that there exists an element $\alpha \in E$ such that the map

$$\textstyle\sum_\sigma a_\sigma\sigma \mapsto \sum_\sigma a_\sigma\sigma\alpha\colon FG \to E$$

is an isomorphism of FG-modules, i.e., that E is a free FG-module of rank 1.

We give three proofs of Theorem 5.18. The first assumes that F is infinite and the second that G is cyclic. Since every Galois extension of a finite field is cyclic (4.20), this covers all cases. The third proof applies to both finite and infinite fields, but uses the Krull-Schmidt theorem.

PROOF FOR INFINITE FIELDS

LEMMA 5.19 *Let $f \in F[X_1,\dots,X_m]$, and let S be an infinite subset of F. If $f(a_1,\dots,a_m) = 0$ for all $a_1,\dots,a_m \in S$, then f is the zero polynomial (i.e., $f = 0$ in $F[X_1,\dots,X_m]$).*

PROOF. We prove this by induction on m. For $m = 1$, the lemma becomes the statement that a nonzero polynomial in one symbol has only finitely many roots (see 1.7). For $m > 1$, write f as a polynomial in X_m with coefficients in $F[X_1,\dots,X_{m-1}]$, say,

$$f = \sum c_i(X_1,\dots,X_{m-1})X_m^i.$$

For any $(m-1)$-tuple $a_1,\dots,a_{m-1}$ of elements of S,

$$f(a_1,\dots,a_{m-1},X_m)$$

is a polynomial in X_m having every element of S as a root. Therefore, each of its coefficients is zero: $c_i(a_1,\dots,a_{m-1}) = 0$ for all i. Since this holds for all $(a_1,\dots,a_{m-1})$, the induction hypothesis shows that $c_i(X_1,\dots,X_{m-1})$ is the zero polynomial. □

We now prove 5.18 in the case that F is infinite. Number the elements of G as $\sigma_1, \dots, \sigma_m$ with σ_1 the identity map.

Let $f \in F[X_1, \dots, X_m]$ have the property that

$$f(\sigma_1\alpha, \dots, \sigma_m\alpha) = 0$$

for all $\alpha \in E$. For a basis $\alpha_1, \dots, \alpha_m$ of E over F, let

$$g(Y_1, \dots, Y_m) = f(\textstyle\sum_{i=1}^m Y_i\sigma_1\alpha_i, \sum_{i=1}^m Y_i\sigma_2\alpha_i, \dots) \in E[Y_1, \dots, Y_m].$$

The hypothesis on f implies that $g(a_1, \dots, a_m) = 0$ for all $a_i \in F$, and so $g = 0$ (because F is infinite). But the matrix $(\sigma_i\alpha_j)$ is invertible (5.16). Since g is obtained from f by an invertible linear change of variables, f can be obtained from g by the inverse linear change of variables. Therefore it also is zero.

Write $X_i = X(\sigma_i)$, and let $A = (X(\sigma_i\sigma_j))$, i.e., A is the $m \times m$ matrix having X_k in the (i, j)th place if $\sigma_i\sigma_j = \sigma_k$. Then $\det(A)$ is a polynomial in $X_1, \dots, X_m$, say, $\det(A) = h(X_1, \dots, X_m)$. Clearly, $h(1, 0, \dots, 0)$ is the determinant of a matrix having exactly one 1 in each row and each column and its remaining entries 0. Hence the rows of the matrix are a permutation of the rows of the identity matrix, and so its determinant is ± 1. In particular, h is not identically zero, and so there exists an $\alpha \in E^\times$ such that $h(\sigma_1\alpha, \dots, \sigma_m\alpha)$ $(= \det(\sigma_i\sigma_j\alpha))$ is nonzero. We'll show that $\{\sigma_i\alpha\}$ is a normal basis. For this, it suffices to show that the $\sigma_i\alpha$ are linearly independent over F. Suppose that

$$\textstyle\sum_{j=1}^m a_j\sigma_j\alpha = 0$$

for some $a_j \in F$. On applying $\sigma_1, \dots, \sigma_m$ successively, we obtain a system of m-equations

$$\textstyle\sum a_j\sigma_i\sigma_j\alpha = 0$$

in the m "unknowns" a_j. Because this system of equations is nonsingular, the a_j are zero. This completes the proof of the theorem in the case that F is infinite.

Proof when G is cyclic.

Assume that G is generated by an element σ_0 of order n. Then $[E\colon F] = n$. The minimum polynomial of σ_0 regarded as an endomorphism of the F-vector space E is the monic polynomial in $F[X]$ of least degree such that $P(\sigma_0) = 0$ (as an endomorphism of E). It has the property that it divides every polynomial $Q(X) \in F[X]$ such that $Q(\sigma_0) = 0$. Since $\sigma_0^n = 1$, $P(X)$ divides $X^n - 1$. On the other hand, Dedekind's theorem on the independence of characters (5.14) implies that $1, \sigma_0, \dots, \sigma_0^{n-1}$ are linearly independent over F, and so $\deg P(X) > n - 1$. We conclude that $P(X) = X^n - 1$. Therefore, as an $F[X]$-module with X acting as σ_0, E is isomorphic to $F[X]/(X^n - 1)$. For any generator α of E as an $F[X]$-module, $\alpha, \sigma_0\alpha, \dots, \sigma_0\alpha^{n-1}$ is an F-basis for E.

Uniform proof

The Krull-Schmidt theorem says that every module M of finite length over a ring can be written as a direct sum of indecomposable modules and that the indecomposable modules occurring in a decomposition are unique up to order and isomorphism. Thus $M = \bigoplus_i m_i M_i$ where M_i is indecomposable and $m_i M_i$ denotes the direct sum of m_i copies of M_i; the set of isomorphism classes of the M_i is uniquely determined and, when we choose the M_i to

be pairwise nonisomorphic, each m_i is uniquely determined. From this it follows that two modules M and M' of finite length over a ring are isomorphic if $mM \approx mM'$ for some $m \geq 1$.

Consider the F-vector space $E \otimes_F E$. We let E act on the first factor, and G act on the second factor (so $a(x \otimes y) = ax \otimes y$, $a \in E$, and $\sigma(x \otimes y) = x \otimes \sigma y$, $\sigma \in G$). We'll prove Theorem 5.18 by showing that

$$\underbrace{FG \oplus \cdots \oplus FG}_{n} \approx E \otimes_F E \approx \underbrace{E \oplus \cdots \oplus E}_{n}$$

as FG-modules ($n = [E:F]$).

For $\sigma \in G$, let $\lambda_\sigma : E \otimes_F E \to E$ denote the map $x \otimes y \mapsto x \cdot \sigma y$. Then λ_σ is obviously E-linear, and $\lambda_\sigma(\tau z) = \lambda_{\sigma\tau}(z)$ for all $\tau \in G$ and $z \in E \otimes_F E$. I claim that $\{\lambda_\sigma \mid \sigma \in G\}$ is an E-basis for $\mathrm{Hom}_{E\text{-linear}}(E \otimes_F E, E)$. As this space has dimension n, it suffices to show that the set is linearly independent. But if $\sum_\sigma c_\sigma \lambda_\sigma = 0$, $c_\sigma \in E$, then

$$0 = \sum\nolimits_\sigma c_\sigma(\lambda_\sigma(1 \otimes y)) = \sum\nolimits_\sigma c_\sigma \cdot \sigma y$$

for all $y \in E$, which implies that all $c_\sigma = 0$ by Dedekind's theorem 5.14.

Consider the map

$$\phi : E \otimes_F E \to EG, \quad z \mapsto \sum\nolimits_\sigma \lambda_\sigma(z) \cdot \sigma^{-1}.$$

Then ϕ is E-linear. If $\phi(z) = 0$, then $\lambda_\sigma(z) = 0$ for all $\sigma \in G$, and so $z = 0$ in $E \otimes_F E$ (because the λ_σ span the dual space). Therefore ϕ is injective, and as $E \otimes_F E$ and EG both have dimension n over E, it is an isomorphism. For $\tau \in G$,

$$\begin{aligned} \phi(\tau z) &= \sum\nolimits_\sigma \lambda_\sigma(\tau z) \cdot \sigma^{-1} \\ &= \sum\nolimits_\sigma \lambda_{\sigma\tau}(z) \cdot \tau(\sigma\tau)^{-1} \\ &= \tau\phi(z), \end{aligned}$$

and so ϕ is an isomorphism of EG-modules. Thus

$$E \otimes_K E \simeq EG \approx FG \oplus \cdots \oplus FG$$

as an FG-module.

On the other hand, for any basis $\{e_1, \ldots, e_n\}$ for E as an F-vector space,

$$E \otimes_F E = (e_1 \otimes E) \oplus \cdots \oplus (e_n \otimes E) \simeq E \oplus \cdots \oplus E$$

as FG-modules. This completes the proof.

NOTES The normal basis theorem was stated for finite fields by Eisenstein in 1850, and proved for finite fields by Hensel in 1888. Dedekind used normal bases in number fields in his work on the discriminant in 1880, but he had no general proof. Noether gave a proof for some infinite fields (1932) and Deuring gave a uniform proof (also 1932). The above uniform proof simplifies that of Deuring — see Blessenohl, Dieter. On the normal basis theorem. Note Mat. 27 (2007), 5–10. According to the Wikipedia, normal bases are frequently used in cryptographic applications that are based on the discrete logarithm problem such as elliptic curve cryptography.

Hilbert's Theorem 90

Let G be a group. A ***G-module*** is an abelian group M together with an action of G, i.e., a map $G \times M \to M$ such that

(a) $\sigma(m+m') = \sigma m + \sigma m'$ for all $\sigma \in G$, $m, m' \in M$;

(b) $(\sigma\tau)(m) = \sigma(\tau m)$ for all $\sigma, \tau \in G$, $m \in M$;

(c) $1m = m$ for all $m \in M$.

Thus, to give an action of G on M is the same as giving a homomorphism $G \to \mathrm{Aut}(M)$ (automorphisms of M as an abelian group).

EXAMPLE 5.20 Let E be a Galois extension of F with Galois group G. Then $(E,+)$ and $(E^\times,\cdot)$ are G-modules.

Let M be a G-module. A ***crossed homomorphism*** is a map $f: G \to M$ such that

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \text{ for all } \sigma, \tau \in G.$$

Note that the condition implies that $f(1) = f(1\cdot 1) = f(1) + f(1)$, and so $f(1) = 0$.

EXAMPLE 5.21 (a) Let $f: G \to M$ be a crossed homomorphism. For any $\sigma \in G$,

$$\begin{aligned} f(\sigma^2) &= f(\sigma) + \sigma f(\sigma), \\ f(\sigma^3) &= f(\sigma\cdot\sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma) \\ &\cdots \\ f(\sigma^n) &= f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma). \end{aligned}$$

Thus, if G is a cyclic group of order n generated by σ, then a crossed homomorphism $f: G \to M$ is determined by its value, x say, on σ, and x satisfies the equation

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0, \tag{12}$$

Moreover, if $x \in M$ satisfies (12), then the formulas $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1} x$ define a crossed homomorphism $f: G \to M$. Thus, for a finite group $G = \langle\sigma\rangle$, there is a one-to-one correspondence

$$\{\text{crossed homs } f: G \to M\} \overset{f \leftrightarrow f(\sigma)}{\longleftrightarrow} \{x \in M \text{ satisfying (12)}\}.$$

(b) For every $x \in M$, we obtain a crossed homomorphism by putting

$$f(\sigma) = \sigma x - x, \qquad \text{all } \sigma \in G.$$

A crossed homomorphism of this form is called a ***principal crossed homomorphism***.

(c) If G acts trivially on M, i.e., $\sigma m = m$ for all $\sigma \in G$ and $m \in M$, then a crossed homomorphism is simply a homomorphism, and there are no nonzero principal crossed homomorphisms.

The sum and difference of two crossed homomorphisms is again a crossed homomorphism, and the sum and difference of two principal crossed homomorphisms is again principal. Thus we can define

$$H^1(G,M) = \frac{\{\text{crossed homomorphisms}\}}{\{\text{principal crossed homomorphisms}\}}$$

(quotient abelian group). The cohomology groups $H^n(G,M)$ have been defined for all $n \in \mathbb{N}$, but since this was not done until the twentieth century, it will not be discussed in this course. An exact sequence of G-modules

$$0 \to M' \to M \to M'' \to 0$$

gives rise to an exact sequence

$$0 \longrightarrow M'^G \longrightarrow M^G \longrightarrow M''^G \xrightarrow{d} H^1(G,M') \longrightarrow H^1(G,M) \longrightarrow H^1(G,M'').$$

Let $m'' \in M''^G$, and let $m \in M$ map to m''. For all $\sigma \in G$, $\sigma m - m$ lies in the submodule M' of M, and the crossed homomorphism $\sigma \mapsto \sigma m - m : G \to M'$ represents $d(m'')$. It is left as an exercise for the reader to check the exactness.

EXAMPLE 5.22 Let $\pi : \widetilde{X} \to X$ be the universal covering space of a topological space X, and let Γ be the group of covering transformations. Under some fairly general hypotheses, a Γ-module M will define a sheaf $\mathcal{M}$ on X, and $H^1(X,\mathcal{M}) \simeq H^1(\Gamma,M)$. For example, when $M = \mathbb{Z}$ with the trivial action of Γ, this becomes the isomorphism $H^1(X,\mathbb{Z}) \simeq H^1(\Gamma,\mathbb{Z}) = \operatorname{Hom}(\Gamma,\mathbb{Z})$.

THEOREM 5.23 *Let E be a Galois extension of F with group G; then $H^1(G,E^\times) = 0$, i.e., every crossed homomorphism $G \to E^\times$ is principal.*

PROOF. Let f be a crossed homomorphism $G \to E^\times$. In multiplicative notation, this means that

$$f(\sigma\tau) = f(\sigma)\cdot\sigma(f(\tau)), \quad \sigma,\tau \in G,$$

and we have to find a $\gamma \in E^\times$ such that $f(\sigma) = \frac{\sigma\gamma}{\gamma}$ for all $\sigma \in G$. Because the $f(\tau)$ are nonzero, Corollary 5.15 implies that

$$\sum\nolimits_{\tau\in G} f(\tau)\tau : E \to E$$

is not the zero map, i.e., there exists an $\alpha \in E$ such that

$$\beta \stackrel{\text{def}}{=} \sum\nolimits_{\tau\in G} f(\tau)\tau\alpha \neq 0.$$

But then, for $\sigma \in G$,

$$\begin{aligned}\sigma\beta &= \textstyle\sum_{\tau\in G} \sigma(f(\tau))\cdot\sigma\tau(\alpha)\\ &= \textstyle\sum_{\tau\in G} f(\sigma)^{-1}\ f(\sigma\tau)\cdot\sigma\tau(\alpha)\\ &= f(\sigma)^{-1}\ \textstyle\sum_{\tau\in G} f(\sigma\tau)\sigma\tau(\alpha),\end{aligned}$$

which equals $f(\sigma)^{-1}\beta$ because, as τ runs over G, so also does $\sigma\tau$. Therefore, $f(\sigma) = \frac{\beta}{\sigma(\beta)}$ and we can take $\beta = \gamma^{-1}$. □

Let E be a Galois extension of F with Galois group G. We define the ***norm*** of an element $\alpha \in E$ to be

$$\operatorname{Nm}\alpha = \prod\nolimits_{\sigma\in G} \sigma\alpha.$$

For $\tau \in G$,

$$\tau(\operatorname{Nm}\alpha) = \prod\nolimits_{\sigma\in G} \tau\sigma\alpha = \operatorname{Nm}\alpha,$$

and so $\operatorname{Nm}\alpha \in F$. The map

$$\alpha \mapsto \operatorname{Nm}\alpha : E^\times \to F^\times$$

is a obviously a homomorphism.

EXAMPLE 5.24 The norm map $\mathbb{C}^\times \to \mathbb{R}^\times$ is $\alpha \mapsto |\alpha|^2$ and the norm map $\mathbb{Q}[\sqrt{d}]^\times \to \mathbb{Q}^\times$ is $a + b\sqrt{d} \mapsto a^2 - db^2$.

We are interested in determining the kernel of the norm map. Clearly an element of the form $\frac{\beta}{\tau\beta}$ has norm 1, and our next result shows that, for cyclic extensions, all elements with norm 1 are of this form.

COROLLARY 5.25 (HILBERT'S THEOREM 90) *Let E be a finite cyclic extension of F and let σ generate $\mathrm{Gal}(E/F)$. Let $\alpha \in E^\times$; if $\mathrm{Nm}_{E/F}\,\alpha = 1$, then $\alpha = \beta/\sigma\beta$ for some $\beta \in E$.*

PROOF. Let $m = [E\colon F]$. The condition on α is that $\alpha \cdot \sigma\alpha \cdots \sigma^{m-1}\alpha = 1$, and so (see 5.21a) there is a crossed homomorphism $f\colon \langle\sigma\rangle \to E^\times$ with $f(\sigma) = \alpha$. Theorem 5.23 now shows that f is principal, which means that there is a β with $f(\sigma) = \beta/\sigma\beta$. □

NOTES The corollary is Satz 90 in Hilbert's book, Theorie der Algebraischen Zahlkörper, 1897. The theorem was discovered by Kummer in the special case of $\mathbb{Q}[\zeta_p]/\mathbb{Q}$, and generalized to Theorem 5.23 by E. Noether. Theorem 5.23, as well as various vast generalizations of it, are also referred to as Hilbert's Theorem 90. For an illuminating discussion of Hilbert's book, see the introduction to its English translation, written by F. Lemmermeyer and N. Schappacher.

Cyclic extensions

Let F be a field containing a primitive nth root of 1, some $n \geq 2$, and write μ_n for the group of nth roots of 1 in F. Then μ_n is a cyclic subgroup of $F^\times$ of order n with generator ζ say. In this section, we classify the cyclic extensions of degree n of F.

Consider a field $E = F[\alpha]$ generated by an element α whose nth power (but no smaller power) is in F. Then α is a root of $X^n - a$, and the remaining roots are the elements $\zeta^i\alpha$, $1 \leq i \leq n-1$. Since these all lie in E, E is a Galois extension of F, with Galois group G say. For every $\sigma \in G$, $\sigma\alpha$ is also a root of $X^n - a$, and so $\sigma\alpha = \zeta^i\alpha$ for some i. Hence $\sigma\alpha/\alpha \in \mu_n$. The map

$$\sigma \mapsto \sigma\alpha/\alpha\colon G \to \mu_n$$

doesn't change when α is replaced by a conjugate, and it follows that the map is a homomorphism:

$$\frac{\sigma\tau\alpha}{\alpha} = \frac{\sigma(\tau\alpha)}{\tau\alpha}\frac{\tau\alpha}{\alpha}.$$

Because α generates E over F, the map is injective. If it is not surjective, then G maps into a subgroup μ_d of μ_n, some $d\,|\,n$, $d < n$. In this case, $(\sigma\alpha/\alpha)^d = 1$, i.e., $\sigma\alpha^d = \alpha^d$, for all $\sigma \in G$, and so $\alpha^d \in F$, contradicting the hypothesis on α. Thus the map is surjective. We have proved the first part of the following statement.

PROPOSITION 5.26 *Let F be a field containing a primitive nth root of 1. Let $E = F[\alpha]$ where $\alpha^n \in F$ and no smaller power of α is in F. Then E is a Galois extension of F with cyclic Galois group of order n. Conversely, if E is a cyclic extension of F of degree n, then $E = F[\alpha]$ for some α with $\alpha^n \in F$.*

PROOF. It remains to prove the last statement. Let σ generate G and let ζ generate μ_n. It suffices to find an element $\alpha \in E^\times$ such that $\sigma\alpha = \zeta^{-1}\alpha$, for then α^n is the smallest power of α lying in F. As $1, \sigma, \dots, \sigma^{n-1}$ are distinct homomorphisms $F^\times \to F^\times$, Dedekind's Theorem 5.14 shows that $\sum_{i=0}^{n-1} \zeta^i\sigma^i$ is not the zero function, and so there exists a γ such that $\alpha \stackrel{\text{def}}{=} \sum \zeta^i\sigma^i\gamma \neq 0$. Now $\sigma\alpha = \zeta^{-1}\alpha$. □

ASIDE 5.27 (a) It is not difficult to show that the polynomial $X^n - a$ is irreducible in $F[X]$ if a is not a pth power for any prime p dividing n. When we drop the condition that F contains a primitive nth root of 1, this is still true except that, if $4|n$, we need to add the condition that $a \notin -4F^4$. See Lang, Algebra, Springer, 2002, VI, §9, Theorem 9.1, p. 297.

(b) If F has characteristic p (hence has no pth roots of 1 other than 1), then $X^p - X - a$ is irreducible in $F[X]$ unless $a = b^p - b$ for some $b \in F$, and when it is irreducible, its Galois group is cyclic of order p (generated by $\alpha \mapsto \alpha + 1$ where α is a root). Moreover, every cyclic extension of F of degree p is the splitting field of such a polynomial.

PROPOSITION 5.28 *Let F be a field containing a primitive nth root of 1. Two cyclic extensions $F[a^{\frac{1}{n}}]$ and $F[b^{\frac{1}{n}}]$ of F of degree n are equal if and only if $a = b^r c^n$ for some $r \in \mathbb{Z}$ relatively prime to n and some $c \in F^\times$, i.e., if and only if a and b generate the same subgroup of $F^\times/F^{\times n}$.*

PROOF. Only the "only if" part requires proof. We are given that $F[\alpha] = F[\beta]$ with $\alpha^n = a$ and $\beta^n = b$. Let σ be the generator of the Galois group with $\sigma\alpha = \zeta\alpha$, and let $\sigma\beta = \zeta^i\beta$, $(i,n) = 1$. We can write

$$\beta = \sum_{j=0}^{n-1} c_j \alpha^j, \quad c_j \in F,$$

and then

$$\sigma\beta = \sum_{j=0}^{n-1} c_j \zeta^j \alpha^j.$$

On comparing this with $\sigma\beta = \zeta^i\beta$, we find that $\zeta^i c_j = \zeta^j c_j$ for all j. Hence $c_j = 0$ for $j \neq i$, and therefore $\beta = c_i\alpha^i$. □

Kummer theory

Throughout this section, F is a field and ζ is a primitive nth root of 1 in F. In particular, F either has characteristic 0 or characteristic p not dividing n.

The last two proposition give us a complete classification of the cyclic extensions of F of degree n. We now extend this to a classification of all abelian extensions of F whose Galois group has exponent n. (Recall that a group G has ***exponent*** n if $\sigma^n = 1$ for all $\sigma \in G$ and n is the smallest positive integer for which this is true. A finite abelian group of exponent n is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^r$ for some r.)

Let E/F be a finite Galois extension with Galois group G. From the exact sequence

$$1 \to \mu_n \longrightarrow E^\times \xrightarrow{x \mapsto x^n} E^{\times n} \to 1$$

we obtain a cohomology sequence

$$1 \to \mu_n \to F^\times \xrightarrow{x \mapsto x^n} F^\times \cap E^{\times n} \to H^1(G, \mu_n) \to 1.$$

The 1 at the right is because of Hilbert's Theorem 90. Thus we obtain an isomorphism

$$F^\times \cap E^{\times n}/F^{\times n} \to \mathrm{Hom}(G, \mu_n).$$

This map can be described as follows: let a be an element of $F^\times$ that becomes an nth power in E, say $a = \alpha^n$; then a maps to the homomorphism $\sigma \mapsto \frac{\sigma\alpha}{\alpha}$. If G is abelian of exponent n, then

$$|\mathrm{Hom}(G, \mu_n)| = (G:1).$$

THEOREM 5.29 *The map*

$$E \mapsto F^\times \cap E^{\times n}$$

defines a one-to-one correspondence between the sets

(a) *of finite abelian extensions of F of exponent n contained in some fixed algebraic closure Ω of F, and*

(b) *of subgroups B of $F^\times$ containing $F^{\times n}$ as a subgroup of finite index.*

The extension corresponding to B is $F[B^{\frac{1}{n}}]$, the smallest subfield of Ω containing F and an nth root of each element of B. If $E \leftrightarrow B$, then $[E\colon F] = (B\colon F^{\times n})$.

PROOF. For any finite Galois extension E of F, define $B(E) = F^\times \cap E^{\times n}$. Then $E \supset F[B(E)^{\frac{1}{n}}]$, and for any group B containing $F^{\times n}$ as a subgroup of finite index, $B(F[B^{\frac{1}{n}}]) \supset B$. Therefore,

$$[E\colon F] \geq [F[B(E)^{\frac{1}{n}}]\colon F] = (B(F[B(E)^{\frac{1}{n}}])\colon F^{\times n}) \geq (B(E)\colon F^{\times n}).$$

If E/F is abelian of exponent n, then $[E\colon F] = (B(E)\colon F^{\times n})$, and so equalities hold throughout: $E = F[B(E)^{\frac{1}{n}}]$.

Next consider a group B containing $F^{\times n}$ as a subgroup of finite index, and let $E = F[B^{\frac{1}{n}}]$. Then E is a composite of the extensions $F[a^{\frac{1}{n}}]$ for a running through a set of generators for $B/F^{\times n}$, and so it is a finite abelian extension of exponent n. Therefore

$$a \mapsto \left(\sigma \mapsto \frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}}\right)\colon B(E)/F^{\times n} \to \mathrm{Hom}(G, \mu_n), \quad G = \mathrm{Gal}(E/F),$$

is an isomorphism. This map sends $B/F^{\times n}$ isomorphically onto the subgroup $\mathrm{Hom}(G/H, \mu_n)$ of $\mathrm{Hom}(G, \mu_n)$ where H consists of the $\sigma \in G$ such that $\sigma a^{\frac{1}{n}}/a^{\frac{1}{n}} = 1$ for all $a \in B$. But such a σ fixes all $a^{\frac{1}{n}}$ for $a \in B$, and therefore is the identity automorphism on $E = F[B^{\frac{1}{n}}]$. This shows that $B(E) = B$, and hence $E \mapsto B(E)$ and $B \mapsto F[B^{\frac{1}{n}}]$ are inverse bijections. □

EXAMPLE 5.30 (a) The theorem says that the abelian extensions of $\mathbb{R}$ of exponent 2 are indexed by the subgroups of $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$. This is certainly true.

(b) The theorem says that the finite abelian extensions of $\mathbb{Q}$ of exponent 2 are indexed by the finite subgroups of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Modulo squares, every nonzero rational number has a unique representative of the form $\pm p_1 \cdots p_r$ with the p_i prime numbers. Therefore $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ is a direct sum of cyclic groups of order 2 indexed by the prime numbers plus ∞. The extension corresponding to the subgroup generated by the primes $p_1, \dots, p_r$ (and -1) is obtained by adjoining the square roots of $p_1, \dots, p_r$ (and -1) to $\mathbb{Q}$.

REMARK 5.31 Let E be an abelian extension of F of exponent n, and let

$$B(E) = \{a \in F^\times \mid a \text{ becomes an } n\text{th power in } E\}.$$

There is a perfect pairing

$$(a, \sigma) \mapsto \frac{\sigma a^{\frac{1}{n}}}{a^{\frac{1}{n}}}\colon \frac{B(E)}{F^{\times n}} \times \mathrm{Gal}(E/F) \to \mu_n.$$

Cf. Exercise 2-1 for the case $n = 2$.

Proof of Galois's solvability theorem

LEMMA 5.32 *Let $f \in F[X]$ be separable, and let F' be a field containing F. Then the Galois group of f as an element of $F'[X]$ is a subgroup of the Galois group of f as an element of $F[X]$.*

PROOF. Let E' be a splitting field for f over F', and let $\alpha_1, \dots, \alpha_m$ be the roots of $f(X)$ in E'. Then $E = F[\alpha_1, ..., \alpha_m]$ is a splitting field of f over F. Every element of $\mathrm{Gal}(E'/F')$ permutes the α_i and so maps E into itself. The map $\sigma \mapsto \sigma|E$ is an injection $\mathrm{Gal}(E'/F') \to \mathrm{Gal}(E/F)$. □

THEOREM 5.33 *Let F be a field of characteristic 0. A polynomial in $F[X]$ is solvable if and only if its Galois group is solvable.*

PROOF. $\Longleftarrow$: Let $f \in F[X]$ have solvable Galois group G_f. Let $F' = F[\zeta]$ where ζ is a primitive nth root of 1 for some large n — for example, $n = (\deg f)!$ will do. The lemma shows that the Galois group G of f as an element of $F'[X]$ is a subgroup of G_f, and hence is also solvable (GT 6.6a). This means that there is a sequence of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = \{1\}$$

such that each G_i is normal in G_{i-1} and G_{i-1}/G_i is cyclic. Let E be a splitting field of $f(X)$ over F', and let $F_i = E^{G_i}$. We have a sequence of fields

$$F \subset F[\zeta] = F' = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = E$$

with F_i cyclic over F_{i-1}. Theorem 5.26 shows that $F_i = F_{i-1}[\alpha_i]$ with $\alpha_i^{[F_i:F_{i-1}]} \in F_{i-1}$, each i, and this shows that f is solvable.

$\Longrightarrow$: It suffices to show that G_f is a quotient of a solvable group (GT 6.6a). Hence it suffices to find a solvable extension $\widetilde{E}$ of F such that $f(X)$ splits in $\widetilde{E}[X]$.

We are given that there exists a tower of fields

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m$$

such that

(a) $F_i = F_{i-1}[\alpha_i]$, $\alpha_i^{r_i} \in F_{i-1}$;

(b) F_m contains a splitting field for f.

Let $n = r_1 \cdots r_m$, and let Ω be a field Galois over F and containing (a copy of) F_m and a primitive nth root ζ of 1. For example, choose a primitive element γ for F_m over F (see 5.1), and take Ω to be a splitting field of $g(X)(X^n - 1)$ where $g(X)$ is the minimum polynomial of γ over F. Alternatively, apply 2.9a.

Let G be the Galois group of Ω/F, and let $\widetilde{E}$ be the Galois closure of $F_m[\zeta]$ in Ω. According to (3.17a), $\widetilde{E}$ is the composite of the fields $\sigma F_m[\zeta]$, $\sigma \in G$, and so it is generated over F by the elements

$$\zeta, \alpha_1, \alpha_2, \dots, \alpha_m, \sigma\alpha_1, \dots, \sigma\alpha_m, \sigma'\alpha_1, \dots.$$

We adjoin these elements to F one by one to get a sequence of fields

$$F \subset F[\zeta] \subset F[\zeta, \alpha_1] \subset \cdots \subset F' \subset F'' \subset \cdots \subset \widetilde{E}$$

in which each field F'' is obtained from its predecessor F' by adjoining an rth root of an element of F' ($r = r_1, \dots, r_m$, or n). According to (5.8) and (5.26), each of these extensions is abelian (and even cyclic after the first), and so $\widetilde{E}/F$ is a solvable extension. □

ASIDE 5.34 One of Galois's major achievements was to show that an irreducible polynomial of prime degree in $\mathbb{Q}[X]$ is solvable by radicals if and only if its splitting field is generated by any two roots of the polynomial.[3] This theorem of Galois answered a question on mathoverflow in 2010 (mo24081). For a partial generalization of Galois's theorem, see mo110727.

Symmetric polynomials

Let R be a commutative ring (with 1). A polynomial $P(X_1,...,X_n) \in R[X_1,\dots,X_n]$ is said to be ***symmetric*** if it is unchanged when its variables are permuted, i.e., if

$$P(X_{\sigma(1)},\dots,X_{\sigma(n)}) = P(X_1,\dots,X_n), \quad \text{all } \sigma \in S_n.$$

For example

$$\begin{aligned}
p_1 &= \textstyle\sum_i X_i && = X_1 + X_2 + \cdots + X_n,\\
p_2 &= \textstyle\sum_{i<j} X_i X_j && = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n,\\
p_3 &= \textstyle\sum_{i<j<k} X_i X_j X_k, && = X_1X_2X_3 + \cdots\\
&\cdots\\
p_r &= \textstyle\sum_{i_1<\cdots<i_r} X_{i_1}\dots X_{i_r}\\
&\cdots\\
p_n &= X_1X_2\cdots X_n
\end{aligned}$$

are each symmetric because p_r is the sum of *all* monomials of degree r made up out of distinct X_i. These particular polynomials are called the ***elementary symmetric polynomials***.

THEOREM 5.35 (SYMMETRIC POLYNOMIALS THEOREM) *Every symmetric polynomial $P(X_1,...,X_n)$ in $R[X_1,...,X_n]$ is equal to a polynomial in the elementary symmetric polynomials with coefficients in R, i.e., $P \in R[p_1,...,p_n]$.*

PROOF. We define an ordering on the monomials in the X_i by requiring that

$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} > X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n}$$

if either

$$i_1 + i_2 + \cdots + i_n > j_1 + j_2 + \cdots + j_n$$

or equality holds and, for some s,

$$i_1 = j_1,\ \dots,\ i_s = j_s, \text{ but } i_{s+1} > j_{s+1}.$$

For example,

$$X_1X_2X_3^3 > X_1X_2^2X_3 > X_1X_2X_3^2.$$

Let $P(X_1,\dots,X_n)$ be a symmetric polynomial, and let $X_1^{i_1}\cdots X_n^{i_n}$ be the highest monomial occurring in P with a nonzero coefficient, so

$$P = cX_1^{i_1}\cdots X_n^{i_n} + \text{lower terms}, \quad c \neq 0.$$

[3] Pour qu'une équation de degré premier soit résoluble par radicaux, il faut et il suffit que deux quelconques de ces racines étant connues, les autres s'en déduisent rationnellement (Évariste Galois, Bulletin de M. Férussac, XIII (avril 1830), p. 271).

Because P is symmetric, it contains all monomials obtained from $X_1^{i_1}\cdots X_n^{i_n}$ by permuting the X. Hence $i_1 \geq i_2 \geq \cdots \geq i_n$.

The highest monomial in p_i is $X_1\cdots X_i$, and it follows that the highest monomial in $p_1^{d_1}\cdots p_n^{d_n}$ is

$$X_1^{d_1+d_2+\cdots+d_n} X_2^{d_2+\cdots+d_n} \cdots X_n^{d_n}. \tag{13}$$

Therefore the highest monomial of

$$P(X_1,\ldots,X_n) - c p_1^{i_1-i_2} p_2^{i_2-i_3}\cdots p_n^{i_n} \tag{14}$$

is strictly less than the highest monomial in $P(X_1,\ldots,X_n)$. We can repeat this argument with the polynomial (14), and after a finite number of steps, we will arrive at a representation of P as a polynomial in $p_1,\ldots,p_n$. □

REMARK 5.36 (a) The proof is algorithmic. Consider, for example,[4]

$$\begin{aligned} P(X_1,X_2) &= (X_1 + 7X_1X_2 + X_2)^2 \\ &= X_1^2 + 2X_1X_2 + 14X_1^2X_2 + X_2^2 + 14X_1X_2^2 + 49X_1^2X_2^2. \end{aligned}$$

The highest monomial is $49X_1^2X_2^2$, and so we subtract $49p_2^2$, getting

$$P - 49p_2^2 = X_1^2 + 2X_1X_2 + 14X_1^2X_2 + X_2^2 + 14X_1X_2^2.$$

Continuing, we get

$$P - 49p_2^2 - 14p_1p_2 = X_1^2 + 2X_1X_2 + X_2^2$$

and finally,

$$P - 49p_2^2 - 14p_1p_2 - p_1^2 = 0.$$

(b) The expression of P as a polynomial in the p_i in (5.35) is unique. Otherwise, by subtracting, we would get a nontrivial polynomial $Q(p_1,\ldots,p_n)$ in the p_i which is zero when expressed as a polynomial in the X_i. But the highest monomials (13) in the polynomials $p_1^{d_1}\cdots p_n^{d_n}$ are distinct (the map $(d_1,\ldots,d_n) \mapsto (d_1+\cdots+d_n,\ldots,d_n)$ is injective), and so they can't cancel.

Let

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in R[X],$$

and suppose that f splits over some ring S containing R:

$$f(X) = \textstyle\prod_{i=1}^n (X-\alpha_i), \quad \alpha_i \in S.$$

Then

$$a_1 = -p_1(\alpha_1,\ldots,\alpha_n), \quad a_2 = p_2(\alpha_1,\ldots,\alpha_n), \quad \ldots, \quad a_n = (-1)^n p_n(\alpha_1,\ldots,\alpha_n).$$

Thus the *elementary* symmetric polynomials in the roots of $f(X)$ lie in R, and so the theorem implies that *every* symmetric polynomial in the roots of $f(X)$ lies in R. For example, the discriminant

$$D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

of f lies in R.

[4] From the Wikipedia: Elementary symmetric polynomials.

THEOREM 5.37 (SYMMETRIC FUNCTIONS THEOREM) *Let F be a field. When S_n acts on $F(X_1,...,X_n)$ by permuting the X_i, the field of invariants is $F(p_1,...,p_n)$.*

PROOF. Let $f \in F(X_1,\dots,X_n)$ be symmetric (i.e., fixed by S_n). Set $f = g/h$, $g,h \in F[X_1,\dots,X_n]$. The polynomials $H = \prod_{\sigma\in S_n} \sigma h$ and Hf are symmetric, and therefore lie in $F[p_1,\dots,p_n]$ by 5.35. Hence their quotient $f = Hf/H$ lies in $F(p_1,\dots,p_n)$. □

COROLLARY 5.38 *The field $F(X_1,...,X_n)$ is Galois over $F(p_1,...,p_n)$ with Galois group S_n (acting by permuting the X_i).*

PROOF. We have shown that $F(p_1,\dots,p_n) = F(X_1,\dots,X_n)^{S_n}$, and so this follows from (3.10). □

The field $F(X_1,\dots,X_n)$ is the splitting field over $F(p_1,\dots,p_n)$ of

$$g(T) = (T-X_1)\cdots(T-X_n) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n.$$

Therefore, the Galois group of $g(T) \in F(p_1,\dots,p_n)[T]$ is S_n.

ASIDE 5.39 Symmetric polynomials played an important role in the work of Galois. In his *Mémoire sur les conditions de résolubilité des équations par radicaux*, he prove the following proposition:

> Let f be a polynomial with coefficients $\sigma_1,\dots,\sigma_n$. Let $x_1,\dots,x_n$ be its roots, and let $U,V,\dots$ be certain numbers that are rational functions in the x_i. Then there exists a group G of permutations of the x_i such that the rational functions in the x_i that are fixed under all permutations in G are exactly those that are rationally expressible in terms of $\sigma_1,\dots,\sigma_n$ and $U,V,\dots$

When we take $U,V,\dots$ to be the elements of a field E intermediate between the field of coefficients of f and the splitting field of f, this says that the exists a group G of permutations of the x_i whose fixed field (when G acts on the splitting field) is exactly E.

The general polynomial of degree n

When we say that the roots of

$$aX^2 + bX + c$$

are

$$\frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

we are thinking of a,b,c as symbols: for any particular values of a,b,c, the formula gives the roots of the particular equation. We'll prove in this section that there is no similar formula for the roots of the "general polynomial" of degree ≥ 5.

We define the ***general polynomial of degree*** n to be

$$f(X) = X^n - t_1X^{n-1} + \cdots + (-1)^n t_n \in F[t_1,...,t_n][X]$$

where the t_i are symbols. We'll show that, when we regard f as a polynomial in X with coefficients in the field $F(t_1,\dots,t_n)$, its Galois group is S_n. Then Theorem 5.33 proves the above remark (at least in characteristic zero).

THEOREM 5.40 *The Galois group of the general polynomial of degree n is S_n.*

PROOF. Let $f(X)$ be the general polynomial of degree n,

$$f(X) = X^n - t_1X^{n-1} + \cdots + (-1)^n t_n \in F[t_1, ..., t_n][X].$$

If we can show that the homomorphism

$$t_i \mapsto p_i : F[t_1, \ldots, t_n] \to F[p_1, \ldots, p_n]$$

is injective, then it will extend to an isomorphism

$$F(t_1, \ldots, t_n) \to F(p_1, \ldots, p_n)$$

sending $f(X)$ to

$$g(X) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n \in F(p_1, \ldots, p_n)[X].$$

Then the statement will follow from Corollary 5.38.

We now prove that the homomorphism is injective.[5] Suppose on the contrary that there exists a $P(t_1, \ldots, t_n)$ such that $P(p_1, \ldots, p_n) = 0$. Equation (13), p. 76, shows that if $m_1(t_1, \ldots, t_n)$ and $m_2(t_1, \ldots, t_n)$ are distinct monomials, then $m_1(p_1, \ldots, p_n)$ and $m_2(p_1, \ldots, p_n)$ have distinct highest monomials. Therefore, cancellation can't occur, and so $P(t_1, \ldots, t_n)$ must be the zero polynomial. □

REMARK 5.41 Since S_n occurs as a Galois group over $\mathbb{Q}$, and every finite group occurs as a subgroup of some S_n, it follows that every finite group occurs as a Galois group over some finite extension of $\mathbb{Q}$, but does every finite Galois group occur as a Galois group over $\mathbb{Q}$ itself? This is known as the inverse Galois problem.

The Hilbert-Noether program for proving this was the following. Hilbert proved that if G occurs as the Galois group of an extension $E \supset \mathbb{Q}(t_1, ..., t_n)$ (the t_i are symbols), then it occurs infinitely often as a Galois group over $\mathbb{Q}$. For the proof, realize E as the splitting field of a polynomial $f(X) \in k[t_1, \ldots, t_n][X]$ and prove that for infinitely many values of the t_i, the polynomial you obtain in $\mathbb{Q}[X]$ has Galois group G. (This is quite a difficult theorem — see Serre, J.-P., *Lectures on the Mordell-Weil Theorem,* 1989, Chapter 9.) Noether conjectured the following: Let $G \subset S_n$ act on $F(X_1, ..., X_n)$ by permuting the X_i; then $F(X_1, \ldots, X_n)^G \approx F(t_1, ..., t_n)$ (for symbols t_i). However, Swan proved in 1969 that the conjecture is false for G the cyclic group of order 47. Hence this approach can not lead to a proof that all finite groups occur as Galois groups over $\mathbb{Q}$, but it doesn't exclude other approaches. For more information on the problem, see Serre, ibid., Chapter 10; Serre, J.-P., *Topics in Galois Theory*, 1992; and the Wikipedia: Inverse Galois problem.

REMARK 5.42 Take $F = \mathbb{C}$, and consider the subset of $\mathbb{C}^{n+1}$ defined by the equation

$$X^n - T_1X^{n-1} + \cdots + (-1)^n T_n = 0.$$

It is a beautiful complex manifold S of dimension n. Consider the projection

$$\pi : S \to \mathbb{C}^n, \quad (x, t_1, \ldots, t_n) \mapsto (t_1, \ldots, t_n).$$

Its fibre over a point $(a_1, \ldots, a_n)$ is the set of roots of the polynomial

$$X^n - a_1X^{n-1} + \cdots + (-1)^n a_n.$$

The discriminant $D(f)$ of $f(X) = X^n - T_1X^{n-1} + \cdots + (-1)^n T_n$ is a polynomial in $\mathbb{C}[T_1, \ldots, T_n]$. Let Δ be the zero set of $D(f)$ in $\mathbb{C}^n$. Then over each point of $\mathbb{C}^n \smallsetminus \Delta$, there are exactly n points of S, and $S \smallsetminus \pi^{-1}(\Delta)$ is a covering space over $\mathbb{C}^n \smallsetminus \Delta$.

[5] To say that the homomorphism is injective means that the p_i are algebraically independent over F (see p. 109). This can be proved by noting that, because $F(X_1, \ldots, X_n)$ is algebraic over $F(p_1, \ldots, p_n)$, the latter must have transcendence degree n (see §8).

A BRIEF HISTORY

As far back as 1500 BC, the Babylonians (at least) knew a general formula for the roots of a quadratic polynomial. Cardan (about 1515 AD) found a general formula for the roots of a cubic polynomial. Ferrari (about 1545 AD) found a general formula for the roots of a quartic polynomial (he introduced the resolvent cubic, and used Cardan's result). Over the next 275 years there were many fruitless attempts to obtain similar formulas for higher degree polynomials, until, in about 1820, Ruffini and Abel proved that there are none.

Norms and traces

Recall that, for an $n \times n$ matrix $A = (a_{ij})$

$$\begin{array}{rcll} \mathrm{Tr}(A) & = & \sum_i a_{ii} & \text{(trace of } A\text{)} \\ \det(A) & = & \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}, & \text{(determinant of } A\text{)} \\ c_A(X) & = & \det(XI_n - A) & \text{(characteristic polynomial of } A\text{).} \end{array}$$

Moreover,

$$c_A(X) = X^n - \mathrm{Tr}(A)X^{n-1} + \cdots + (-1)^n \det(A).$$

None of these is changed when A is replaced by its conjugate UAU^{-1} by an invertible matrix U. Therefore, for any endomorphism α of a finite-dimensional vector space V, we can define[6]

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(A), \quad \det(\alpha) = \det(A), \quad c_\alpha(X) = c_A(X)$$

where A is the matrix of α with respect to a basis of V. If β is a second endomorphism of V,

$$\begin{aligned} \mathrm{Tr}(\alpha + \beta) &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta); \\ \det(\alpha\beta) &= \det(\alpha)\det(\beta). \end{aligned}$$

Now let E be a finite field extension of F of degree n. An element α of E defines an F-linear map

$$\alpha_L : E \to E, \quad x \mapsto \alpha x,$$

and we define

$$\begin{array}{rcll} \mathrm{Tr}_{E/F}(\alpha) & = & \mathrm{Tr}(\alpha_L) & \text{(trace of } \alpha\text{)} \\ \mathrm{Nm}_{E/F}(\alpha) & = & \det(\alpha_L) & \text{(norm of } \alpha\text{)} \\ c_{\alpha,E/F}(X) & = & c_{\alpha_L}(X) & \text{(characteristic polynomial of } \alpha\text{).} \end{array}$$

Thus, $\mathrm{Tr}_{E/F}$ is a homomorphism $(E,+) \to (F,+)$, and $\mathrm{Nm}_{E/F}$ is a homomorphism $(E^\times,\cdot) \to (F^\times,\cdot)$.

[6]The coefficients of the characteristic polynomial

$$c_\alpha(X) = X^n + c_1 X^{n-1} + \cdots + c_n,$$

of α have the following description

$$c_i = (-1)^i \,\mathrm{Tr}(\alpha | \textstyle\bigwedge^i V)$$

— see Bourbaki, N., Algebra, Chapter 3, 8.11.

EXAMPLE 5.43 (a) Consider the field extension $\mathbb{C} \supset \mathbb{R}$. For $\alpha = a + bi$, the matrix of α_L with respect to the basis $\{1, i\}$ is $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$, and so

$$\mathrm{Tr}_{\mathbb{C}/\mathbb{R}}(\alpha) = 2\Re(\alpha),\ \mathrm{Nm}_{\mathbb{C}/\mathbb{R}}(\alpha) = |\alpha|^2.$$

(b) For $a \in F$, a_L is multiplication by the scalar a. Therefore

$$\mathrm{Tr}_{E/F}(a) = na \quad \mathrm{Nm}_{E/F}(a) = a^n \quad c_{a,E/F}(X) = (X-a)^n$$

where $n = [E\colon F]$.

Let $E = \mathbb{Q}[\alpha, i]$ be the splitting field of $X^8 - 2$ (see Exercise 4-3). Then E has degree 16 over $\mathbb{Q}$, and so to compute the trace and norm an element of E, the definition requires us to compute the trace and norm of a 16×16 matrix. The next proposition gives us a quicker method.

PROPOSITION 5.44 *Let E/F be a finite extension of fields, and let $f(X)$ be the minimum polynomial of $\alpha \in E$. Then*

$$c_{\alpha,E/F}(X) = f(X)^{[E:F[\alpha]]}.$$

PROOF. Suppose first that $E = F[\alpha]$. In this case, we have to show that $c_\alpha(X) = f(X)$. Note that $\alpha \mapsto \alpha_L$ is an ***injective*** homomorphism from E into the ring of endomorphisms of E as a vector space over F. The Cayley-Hamilton theorem shows that $c_\alpha(\alpha_L) = 0$, and therefore $c_\alpha(\alpha) = 0$. Hence $f \,|\, c_\alpha$, but they are monic of the same degree, and so they are equal.

For the general case, let $\beta_1, \ldots, \beta_n$ be a basis for $F[\alpha]$ over F, and let $\gamma_1, \ldots, \gamma_m$ be a basis for E over $F[\alpha]$. As we saw in the proof of (1.20), $\{\beta_i\gamma_k\}$ is a basis for E over F. Write $\alpha\beta_i = \sum a_{ji}\beta_j$. Then, according to the first case proved, $A \overset{\text{def}}{=} (a_{ij})$ has characteristic polynomial $f(X)$. But $\alpha\beta_i\gamma_k = \sum a_{ji}\beta_j\gamma_k$, and so the matrix of α_L with respect to $\{\beta_i\gamma_k\}$ breaks up into $n \times n$ blocks with A's down the diagonal and zero matrices elsewhere, from which it follows that $c_{\alpha_L}(X) = c_A(X)^m = f(X)^m$. □

COROLLARY 5.45 *Suppose that the roots of the minimum polynomial of α are $\alpha_1, \ldots, \alpha_n$ (in some splitting field containing E), and that $[E\colon F[\alpha]] = m$. Then*

$$\mathrm{Tr}(\alpha) = m\textstyle\sum_{i=1}^n \alpha_i, \qquad \mathrm{Nm}_{E/F}\,\alpha = \left(\prod_{i=1}^n \alpha_i\right)^m.$$

PROOF. Write the minimum polynomial of α as

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n = \textstyle\prod(X - \alpha_i),$$

so that

$$a_1 = -\textstyle\sum\alpha_i, \text{ and}$$
$$a_n = (-1)^n\textstyle\prod\alpha_i.$$

Then

$$c_\alpha(X) = (f(X))^m = X^{mn} + ma_1X^{mn-1} + \cdots + a_n^m,$$

so that

$$\mathrm{Tr}_{E/F}(\alpha) = -ma_1 = m\textstyle\sum\alpha_i, \text{ and}$$
$$\mathrm{Nm}_{E/F}(\alpha) = (-1)^{mn}a_n^m = (\textstyle\prod\alpha_i)^m.$$

□

EXAMPLE 5.46 (a) Consider the extension $\mathbb{C} \supset \mathbb{R}$. If $\alpha \in \mathbb{C} \smallsetminus \mathbb{R}$, then

$$c_\alpha(X) = f(X) = X^2 - 2\Re(\alpha)X + |\alpha|^2.$$

If $\alpha \in \mathbb{R}$, then $c_\alpha(X) = (X-a)^2$.

(b) Let E be the splitting field of $X^8 - 2$. Then E has degree 16 over $\mathbb{Q}$ and is generated by $\alpha = \sqrt[8]{2}$ and $i = \sqrt{-1}$ (see Exercise 4-3). The minimum polynomial of α is $X^8 - 2$, and so

$$\begin{aligned} c_{\alpha,\mathbb{Q}[\alpha]/\mathbb{Q}}(X) &= X^8 - 2, & c_{\alpha,E/\mathbb{Q}}(X) &= (X^8-2)^2 \\ \mathrm{Tr}_{\mathbb{Q}[\alpha]/\mathbb{Q}}\alpha &= 0, & \mathrm{Tr}_{E/\mathbb{Q}}\alpha &= 0 \\ \mathrm{Nm}_{\mathbb{Q}[\alpha]/\mathbb{Q}}\alpha &= -2, & \mathrm{Nm}_{E/\mathbb{Q}}\alpha &= 4 \end{aligned}$$

REMARK 5.47 Let E be a separable extension of F, and let Σ be the set of F-homomorphisms of E into an algebraic closure Ω of F. Then

$$\begin{aligned} \mathrm{Tr}_{E/F}\alpha &= \textstyle\sum_{\sigma\in\Sigma}\sigma\alpha \\ \mathrm{Nm}_{E/F}\alpha &= \textstyle\prod_{\sigma\in\Sigma}\sigma\alpha. \end{aligned}$$

When $E = F[\alpha]$, this follows from 5.45 and the observation (cf. 2.1b) that the $\sigma\alpha$ are the roots of the minimum polynomial $f(X)$ of α over F. In the general case, the $\sigma\alpha$ are still roots of $f(X)$ in Ω, but now each root of $f(X)$ occurs $[E\colon F[\alpha]]$ times (because each F-homomorphism $F[\alpha] \to \Omega$ has $[E\colon F[\alpha]]$ extensions to E). For example, if E is Galois over F with Galois group G, then

$$\begin{aligned} \mathrm{Tr}_{E/F}\alpha &= \textstyle\sum_{\sigma\in G}\sigma\alpha \\ \mathrm{Nm}_{E/F}\alpha &= \textstyle\prod_{\sigma\in G}\sigma\alpha. \end{aligned}$$

PROPOSITION 5.48 *For finite extensions $E \supset M \supset F$, we have*

$$\begin{aligned} \mathrm{Tr}_{M/F} \circ \mathrm{Tr}_{E/M} &= \mathrm{Tr}_{E/F}, \\ \mathrm{Nm}_{M/F} \circ \mathrm{Nm}_{E/M} &= \mathrm{Nm}_{E/F}. \end{aligned}$$

PROOF. If E is separable over F, then this can be proved fairly easily using the descriptions in the above remark. We omit the proof in the general case. □

PROPOSITION 5.49 *Let $f(X)$ be a monic irreducible polynomial with coefficients in F, and let α be a root of f in some splitting field of f. Then*

$$\mathrm{disc}\, f(X) = (-1)^{m(m-1)/2}\,\mathrm{Nm}_{F[\alpha]/F}\, f'(\alpha)$$

where f' is the formal derivative $\frac{df}{dX}$ of f.

PROOF. Let $f(X) = \prod_{i=1}^{m}(X-\alpha_i)$ be the factorization of f in the given splitting field, and number the roots so that $\alpha = \alpha_1$. Compute that

$$\begin{aligned} \mathrm{disc}\, f(X) &\overset{\text{def}}{=} \prod_{i<j}(\alpha_i - \alpha_j)^2 \\ &= (-1)^{m(m-1)/2} \cdot \prod_i \Big(\prod_{j\neq i}(\alpha_i - \alpha_j)\Big) \\ &= (-1)^{m(m-1)/2} \cdot \prod_i f'(\alpha_i) \\ &= (-1)^{m(m-1)/2}\,\mathrm{Nm}_{F[\alpha]/F}(f'(\alpha)) \qquad \text{(by 5.47).} \end{aligned}$$

□

EXAMPLE 5.50 We compute the discriminant of

$$f(X) = X^n + aX + b, \quad a, b \in F,$$

assumed to be irreducible and separable, by computing the norm of

$$\gamma \stackrel{\text{def}}{=} f'(\alpha) = n\alpha^{n-1} + a, \quad f(\alpha) = 0.$$

On multiplying the equation

$$\alpha^n + a\alpha + b = 0$$

by $n\alpha^{-1}$ and rearranging, we obtain the equation

$$n\alpha^{n-1} = -na - nb\alpha^{-1}.$$

Hence

$$\gamma = n\alpha^{n-1} + a = -(n-1)a - nb\alpha^{-1}.$$

Solving for α gives

$$\alpha = \frac{-nb}{\gamma + (n-1)a}.$$

From the last two equations, it is clear that $F[\alpha] = F[\gamma]$, and so the minimum polynomial of γ over F has degree n also. If we write

$$f\left(\frac{-nb}{X + (n-1)a}\right) = \frac{P(X)}{Q(X)}$$
$$P(X) = (X + (n-1)a)^n - na(X + (n-1)a)^{n-1} + (-1)^n n^n b^{n-1}$$
$$Q(X) = (X + (n-1)a)^n / b,$$

then

$$P(\gamma) = f(\alpha) \cdot Q(\gamma) = 0.$$

As

$$Q(\gamma) = \frac{(\gamma + (n-1)a)^n}{b} = \frac{(-nb)^n}{\alpha^n b} \neq 0$$

and $P(X)$ is monic of degree n, it must be the minimum polynomial of γ. Therefore $\operatorname{Nm}\gamma$ is $(-1)^n$ times the constant term of $P(X)$, namely,

$$\operatorname{Nm}\gamma = n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n.$$

Therefore,

$$\operatorname{disc}(X^n + aX + b) = (-1)^{n(n-1)/2}(n^n b^{n-1} + (-1)^{n-1}(n-1)^{n-1}a^n),$$

which is something PARI doesn't know (because it doesn't understand symbols as exponents). For example,

$$\operatorname{disc}(X^5 + aX + b) = 5^5 b^4 + 4^4 a^5.$$

Exercises

5-1 For $a \in \mathbb{Q}$, let G_a be the Galois group of $X^4 + X^3 + X^2 + X + a$. Find integers a_1, a_2, a_3, a_4 such that $i \neq j \implies G_{a_i}$ is not isomorphic to G_{a_j}.

5-2 Prove that the rational solutions $a, b \in \mathbb{Q}$ of Pythagoras's equation $a^2 + b^2 = 1$ are of the form

$$a = \frac{s^2 - t^2}{s^2 + t^2}, \quad b = \frac{2st}{s^2 + t^2}, \qquad s, t \in \mathbb{Q},$$

and deduce that every right triangle with integer sides has sides of length

$$d(m^2 - n^2, 2mn, m^2 + n^2)$$

for some integers d, m, and n (Hint: Apply Hilbert's Theorem 90 to the extension $\mathbb{Q}[i]/\mathbb{Q}$.)

5-3 Prove that a finite extension of $\mathbb{Q}$ can contain only finitely many roots of 1.

CHAPTER 6

Algebraic Closures

In this chapter, we use Zorn's lemma to show that every field F has an algebraic closure Ω. Recall that if F is a subfield $\mathbb{C}$, then the algebraic closure of F in $\mathbb{C}$ is an algebraic closure of F (1.46). If F is countable, then the existence of Ω can be proved as in the finite field case (4.24), namely, the set of monic irreducible polynomials in $F[X]$ is countable, and so we can list them $f_1, f_2, \ldots$; define E_i inductively by, $E_0 = F$, $E_i =$ a splitting field of f_i over E_{i-1}; then $\Omega = \bigcup E_i$ is an algebraic closure of F.

The difficulty in showing the existence of an algebraic closure of an arbitrary field F is in the set theory. Roughly speaking, we would like to take a union of a family of splitting fields indexed by the monic irreducible polynomials in $F[X]$, but we need to find a way of doing this that is allowed by the axioms of set theory. After reviewing the statement of Zorn's lemma, we sketch three solutions[1] to the problem.

Zorn's lemma

DEFINITION 6.1 (a) A relation $\leq$ on a set S is a ***partial ordering*** if it reflexive, transitive, and anti-symmetric ($a \leq b$ and $b \leq a \implies a = b$).

(b) A partial ordering is a ***total ordering*** if, for all $s, t \in T$, either $s \leq t$ or $t \leq s$.

(c) An ***upper bound*** for a subset T of a partially ordered set $(S, \leq)$ is an element $s \in S$ such that $t \leq s$ for all $t \in T$.

(d) A ***maximal element*** of a partially ordered set S is an element s such that $s \leq s' \implies s = s'$.

A partially ordered set need not have any maximal elements, for example, the set of finite subsets of an infinite set is partially ordered by inclusion, but it has no maximal elements.

LEMMA 6.2 (ZORN) *Let $(S, \leq)$ be a nonempty partially ordered set for which every totally ordered subset has an upper bound in S. Then S has a maximal element.*

Zorn's lemma[2] is equivalent to the Axiom of Choice, and hence independent of the axioms of set theory.

[1] There do exist naturally occurring uncountable fields not contained in $\mathbb{C}$. For example, the field of formal Laurent series $F((T))$ over a field F is uncountable even when F is finite.

[2] The following is quoted from A.J. Berrick and M.E. Keating, An Introduction to Rings and Modules, 2000: The name of the statement, although widely used (allegedly first by Lefschetz), has attracted the attention of historians (Campbell 1978). As a 'maximum principle', it was first brought to prominence, and used for algebraic purposes in Zorn 1935, apparently in ignorance of its previous usage in topology, most notably in Kuratowski 1922. Zorn attributed to Artin the realization that the 'lemma' is in fact equivalent to the Axiom of

REMARK 6.3 The set S of finite subsets of an infinite set doesn't contradict Zorn's lemma, because it contains totally ordered subsets with no upper bound in S.

The following proposition is a typical application of Zorn's lemma — we shall use a * to signal results that depend on Zorn's lemma (equivalently, the Axiom of Choice).

PROPOSITION 6.4 (*) *Every nonzero commutative ring A has a maximal ideal (meaning, maximal among* proper *ideals).*

PROOF. Let S be the set of all proper ideals in A, partially ordered by inclusion. If T is a totally ordered set of ideals, then $J = \bigcup_{I\in T} I$ is again an ideal, and it is proper because if $1 \in J$ then $1 \in I$ for some I in T, and I would not be proper. Thus J is an upper bound for T. Now Zorn's lemma implies that S has a maximal element, which is a maximal ideal in A. □

First proof of the existence of algebraic closures

(Bourbaki, Algèbre, Chap. V, §4.) Recall that an ***F-algebra*** is a ring containing F as a subring. Let $(A_i)_{i\in I}$ be a family of commutative F-algebras, and define $\bigotimes_F A_i$ to be the quotient of the F-vector space with basis $\prod_{i\in I} A_i$ by the subspace generated by elements of the form:

$(x_i)+(y_i)-(z_i)$ with $x_j + y_j = z_j$ for one $j \in I$ and $x_i = y_i = z_i$ for all $i \neq j$;

$(x_i) - a(y_i)$ with $x_j = ay_j$ for one $j \in I$ and $x_i = y_i$ for all $i \neq j$,

(ibid., Chap. II, 3.9). It can be made into a commutative F-algebra in an obvious fashion, and there are canonical homomorphisms $A_i \to \bigotimes_F A_i$ of F-algebras.

For each polynomial $f \in F[X]$, choose a splitting field E_f, and let $\Omega = (\bigotimes_F E_f)/M$ where M is a maximal ideal in $\bigotimes_F E_f$ (whose existence is ensured by Zorn's lemma). Note that $F \subset \bigotimes_F E_f$ and $M \cap F = 0$. As Ω has no ideals other than (0) and Ω, it is a field (see 1.2). The composite of the F-homomorphisms $E_f \to \bigotimes_F E_f \to \Omega$, being a homomorphism of fields, is injective. Since f splits in E_f, it must also split in the larger field Ω. The algebraic closure of F in Ω is therefore an algebraic closure of F (by 1.44).

ASIDE 6.5 In fact, it suffices to take $\Omega = (\bigotimes_F E_f)/M$ where f runs over the monic irreducible polynomials in $F[X]$ and E_f is the stem field $F[X]/(f)$ of f (apply the statement in 6.7 below).

Second proof of the existence of algebraic closures

(Jacobson 1964, p144.) After 4.24 we may assume F to be infinite. This implies that the cardinality of every field algebraic over F is the same as that of F (ibid. p. 143). Choose an uncountable set Ξ of cardinality greater than that of F, and identify F with a subset of Ξ. Let S be the set of triples $(E,+,\cdot)$ with $E \subset \Xi$ and $(+,\cdot)$ a field structure on E such that $(E,+,\cdot)$ contains F as a subfield and is algebraic over it. Write $(E,+,\cdot) \leq (E',+',\cdot')$ if the first is a subfield of the second. Apply Zorn's lemma to show that S has maximal elements, and then show that a maximal element is algebraically closed. (See ibid. p. 144 for the details.)

Choice (see Jech 1973). Zorn's contribution was to observe that it is more suited to algebraic applications like ours.

Third proof of the existence of algebraic closures

(Emil Artin.) Consider the polynomial ring $F[\dots,x_f,\dots]$ in a family of symbols x_f indexed by the nonconstant monic polynomials $f \in F[X]$. If 1 lies in the ideal I of $F[\dots,x_f,\dots]$ generated by the polynomials $f(x_f)$, then

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) = 1 \qquad (\text{in } F[\dots,x_f,\dots])$$

for some $g_i \in F[\dots,x_f,\dots]$ and some nonconstant monic $f_i \in F[X]$. Let E be an extension of F such that each f_i, $i = 1,\dots,n$, has a root α_i in E. Under the F-homomorphism $F[\dots,x_f,\dots] \to E$ sending

$$\begin{cases} x_{f_i} \mapsto \alpha_i \\ x_f \mapsto 0, \quad f \notin \{f_1,\dots,f_n\} \end{cases}$$

the above relation becomes $0 = 1$. From this contradiction, we deduce that 1 does not lie in I, and so Proposition 6.4 applied to $F[\dots,x_f,\dots]/I$ shows that I is contained in a maximal ideal M of $F[\dots,x_f,\dots]$. Let $\Omega = F[\dots,x_f,\dots]/M$. Then Ω is a field containing (a copy of) F in which every nonconstant polynomial in $F[X]$ has at least one root. Repeat the process starting with E_1 instead of F to obtain a field E_2. Continue in this fashion to obtain a sequence of fields

$$F = E_0 \subset E_1 \subset E_2 \subset \cdots,$$

and let $E = \bigcup_i E_i$. Then E is algebraically closed because the coefficients of any nonconstant polynomial g in $E[X]$ lie in E_i for some i, and so g has a root in E_{i+1}. Therefore, the algebraic closure of F in E is an algebraic closure of F (1.46).

ASIDE 6.6 In fact, E is algebraic over F. To see this, note that E_1 is generated by algebraic elements over F, and so is algebraic over F (apply 1.45). Similarly, E_2 is algebraic over E_1, and hence over F (apply 1.31b). Continuing in this fashion, we find that every element of every E_i is algebraic over F.

ASIDE 6.7 In fact, E_1 is already algebraically closed (hence the algebraic closure of F). This follows from the statement:

> Let Ω be a field. If Ω is algebraic over a subfield F and every nonconstant polynomial in $F[X]$ has a root in Ω, then Ω is algebraically closed.

In order to prove this, it suffices to show that every irreducible polynomial f in $F[X]$ splits in $\Omega[X]$ (see 1.44). Suppose first that f is separable, and let E be a splitting field for f. According to Theorem 5.1, $E = F[\gamma]$ for some $\gamma \in E$. Let $g(X)$ be the minimum polynomial of γ over F. Then $g(X)$ has coefficients in F, and so it has a root β in Ω. Both of $F[\gamma]$ and $F[\beta]$ are stem fields for g, and so there is an F-isomorphism $F[\gamma] \to F[\beta] \subset \Omega$. As f splits over $F[\gamma]$, it must split over Ω.

This completes the proof when F is perfect. Otherwise, F has characteristic $p \neq 0$, and we let F' be the set of elements x of Ω such that $x^{p^m} \in F$ for some m. It is easy to see that F' is a field, and we'll complete the proof of the lemma by showing that (a) F' is perfect, and (b) every polynomial in $F'[X]$ has a root in Ω.

PROOF OF (a). Let $a \in F'$, so that $b \overset{\text{def}}{=} a^{p^m} \in F$ for some m. The polynomial $X^{p^{m+1}} - b$ has coefficients in F, and so it has a root $\alpha \in \Omega$, which automatically lies in F'. Now $\alpha^{p^{m+1}} = a^{p^m}$, which implies that $\alpha^p = a$, because the pth power map is injective on fields of characteristic p.

Before continuing, we note that, because Ω is algebraic over a perfect field F', it is itself perfect: let $a \in \Omega$, and let g be the minimum polynomial of a over F'; if $X^p - a$ is irreducible in $\Omega[X]$, then $g(X^p)$ is irreducible in $F'[X]$, but it is not separable, which is a contradiction.

PROOF OF (b). Let $f(X) \in F'[X]$, say, $f(X) = \sum_i a_i X^i$, $a_i \in F'$. For some m, the polynomial $\sum_i a_i^{p^m} X^i$ has coefficients in F, and therefore has a root $\alpha \in \Omega$. As Ω is perfect, we can write $\alpha = \beta^{p^m}$ with $\beta \in \Omega$. Now

$$(f(\beta))^{p^m} = \left(\textstyle\sum_i a_i \beta^i\right)^{p^m} = \textstyle\sum_i a_i^{p^m} \alpha^i = 0,$$

and so β is a root of f.

(Non)uniqueness of algebraic closures

THEOREM 6.8 (*) *Let Ω be an algebraic closure of F, and let E be an algebraic extension of F. There exists an F-homomorphism $E \to \Omega$, and, if E is also an algebraic closure of F, then every such homomorphism is an isomorphism.*

PROOF. Suppose first that E is countably generated over F, i.e., $E = F[\alpha_1, ..., \alpha_n, \ldots]$. Then we can extend the inclusion map $F \to \Omega$ to $F[\alpha_1]$ (map α_1 to any root of its minimum polynomial in Ω), then to $F[\alpha_1, \alpha_2]$, and so on (see 2.2).

In the uncountable case, we use Zorn's lemma. Let S be the set of pairs (M, φ_M) with M a field $F \subset M \subset E$ and φ_M an F-homomorphism $M \to \Omega$. Write $(M, \varphi_M) \leq (N, \varphi_N)$ if $M \subset N$ and $\varphi_N | M = \varphi_M$. This makes S into a partially ordered set. Let T be a totally ordered subset of S. Then $M' = \bigcup_{M \in T} M$ is a subfield of E, and we can define a homomorphism $\varphi' : M' \to \Omega$ by requiring that $\varphi'(x) = \varphi_M(x)$ if $x \in M$. The pair (M', φ') is an upper bound for T in S. Hence Zorn's lemma gives us a maximal element (M, φ) in S. Suppose that $M \neq E$. Then there exists an element $\alpha \in E$, $\alpha \notin M$. Since α is algebraic over M, we can apply (2.2) to extend φ to $M[\alpha]$, contradicting the maximality of M. Hence $M = E$, and the proof of the first statement is complete.

If E is algebraically closed, then every polynomial $f \in F[X]$ splits in $E[X]$ and hence in $\varphi(E)[X]$. Let $\alpha \in \Omega$, and let $f(X)$ be the minimum polynomial of α. Then $X - \alpha$ is a factor of $f(X)$ in $\Omega[X]$, but, as we just observed, $f(X)$ splits in $\varphi(E)[X]$. Because of unique factorization, this implies that $\alpha \in \varphi(E)$. □

The above proof is a typical application of Zorn's lemma: once we know how to do something in a finite (or countable) situation, Zorn's lemma allows us to do it in general.

REMARK 6.9 Even for a finite field F, there will exist uncountably many isomorphisms from one algebraic closure to a second, none of which is to be preferred over any other. Thus it is (uncountably) sloppy to say that the algebraic closure of F is unique. All one can say is that, given two algebraic closures Ω, Ω' of F, then, thanks to Zorn's lemma, there exists an F-isomorphism $\Omega \to \Omega'$.

Separable closures

Let Ω be a field containing F, and let $\mathcal{E}$ be a set of intermediate fields $F \subset E \subset \Omega$ with the following property:

(*) for all $E_1, E_2 \in \mathcal{E}$, there exists an $E \in \mathcal{E}$ such that $E_1, E_2 \subset E$.

Then $E(\mathcal{E}) = \bigcup_{E \in \mathcal{E}} E$ is a subfield of Ω (and we call $\bigcup_{E \in \mathcal{E}} E$ a ***directed*** union), because (*) implies that every finite set of elements of $E(\mathcal{E})$ is contained in a common $E \in \mathcal{E}$, and therefore their product, sum, etc., also lie in $E(\mathcal{E})$.

We apply this remark to the set of subfields E of Ω that are finite and separable over F. As the composite of any two such subfields is again finite and separable over F (cf. 3.14), we see that the union L of all such E is a subfield of Ω. We call L the ***separable closure*** of F in Ω — clearly, it is separable over F and every element of Ω separable over F lies in L. Moreover, because a separable extension of a separable extension is separable, Ω is purely inseparable over L.

DEFINITION 6.10 (a) A field Ω is ***separably closed*** if every nonconstant separable polynomial in $\Omega[X]$ splits in Ω.

(b) A field Ω is a ***separable closure*** of a subfield F if it is separable and algebraic over F and it is separably closed.

THEOREM 6.11 (*) *(a) Every field has a separable closure.*

(b) Let E be a separable algebraic extension of F, and let Ω be a separable algebraic closure of F. There exists an F-homomorphism $E \to \Omega$, and, if E is also a separable closure of F, then every such homomorphism is an isomorphism.

PROOF. Replace "polynomial" with "separable polynomial" in the proofs of the corresponding theorems for algebraic closures. Alternatively, define Ω to be the separable closure of F in an algebraic closure, and apply the preceding theorems. □

ASIDE 6.12 It is not necessary to assume the full axiom of choice to prove the existence of algebraic closures and their uniqueness up to isomorphism, but only a weaker axiom. See Banaschewski, Bernhard. Algebraic closure without choice. Z. Math. Logik Grundlag. Math. 38 (1992), no. 4, 383–385.

CHAPTER 7

Infinite Galois Extensions

In this chapter, we make free use of the axiom of choice.[1] We also assume the reader is familiar with infinite topological products, including Tychonoff's theorem.

As in the finite case, an algebraic extension Ω of a field F is said to be Galois if it is normal and separable. For each finite Galois subextension M/F of Ω, we have a restriction map $\mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(M/F)$, and hence a homomorphism $\mathrm{Gal}(\Omega/F) \to \prod_M \mathrm{Gal}(M/F)$, where the product is over all such subextensions. Clearly every element of Ω lies in some M, and so this homomorphism is injective. When we endow each group $\mathrm{Gal}(M/F)$ with the discrete topology, the product acquires a topology for which it is compact. The image of the homomorphism is closed, and so $\mathrm{Gal}(\Omega/F)$ also acquires a compact topology. Now, all of the Galois theory of finite extensions holds for infinite extensions[2] provided "subgroup" is replaced everywhere with "closed subgroup". The reader prepared to accept this, can skip to the examples and exercises.

Topological groups

DEFINITION 7.1 A set G together with a group structure and a topology is a ***topological group*** if the maps

$$(g,h) \mapsto gh\colon G \times G \to G,$$
$$g \mapsto g^{-1}\colon G \to G$$

are both continuous.

Let a be an element of a topological group G. Then $a_L\colon G \xrightarrow{g \mapsto ag} G$ is continuous because it is the composite of

$$G \xrightarrow{g \mapsto (a,g)} G \times G \xrightarrow{(g,h) \mapsto gh} G.$$

In fact, it is a homeomorphism with inverse $(a^{-1})_L$. Similarly $a_R\colon g \mapsto ga$ and $g \mapsto g^{-1}$ are both homeomorphisms. In particular, for any subgroup H of G, the coset aH of H is open

[1] It is necessary to assume some choice axiom in order to have a sensible Galois theory of infinite extensions. For example, it is consistent with Zermelo-Fraenkel set theory that there exist an algebraic closure L of the $\mathbb{Q}$ with no nontrivial automorphisms. See: Hodges, Wilfrid, Läuchli's algebraic closure of $\mathbb{Q}$. Math. Proc. Cambridge Philos. Soc. 79 (1976), no. 2, 289–297.

[2] One difference: it need no longer be true that the order of $\mathrm{Gal}(\Omega/F)$ equals the degree $[\Omega\colon F]$. Certainly, $\mathrm{Gal}(\Omega/F)$ is infinite if and only if $[\Omega\colon F]$ is infinite, but $\mathrm{Gal}(\Omega/F)$ is always uncountable when infinite whereas $[\Omega\colon F]$ need not be.

or closed if H is open or closed. As the complement of H in G is a union of such cosets, this shows that H is closed if it is open, and it is open if it is closed and of finite index.

Recall that a ***neighbourhood base*** for a point x of a topological space X is a set of neighbourhoods $\mathcal{N}$ such that every open subset U of X containing x contains an N from $\mathcal{N}$.

PROPOSITION 7.2 *Let G be a topological group, and let $\mathcal{N}$ be a neighbourhood base for the identity element e of G. Then*[3]

(a) *for all $N_1, N_2 \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $e \in N' \subset N_1 \cap N_2$;*

(b) *for all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N'N' \subset N$;*

(c) *for all $N \in \mathcal{N}$, there exists an $N' \in \mathcal{N}$ such that $N' \subset N^{-1}$;*

(d) *for all $N \in \mathcal{N}$ and all $g \in G$, there exists an $N' \in \mathcal{N}$ such that $N' \subset gNg^{-1}$;*

(e) *for all $g \in G$, $\{gN \mid N \in \mathcal{N}\}$ is a neighbourhood base for g.*

Conversely, if G is a group and $\mathcal{N}$ is a nonempty set of subsets of G satisfying (a,b,c,d), then there is a (unique) topology on G for which (e) holds.

PROOF. If $\mathcal{N}$ is a neighbourhood base at e in a topological group G, then (b), (c), and (d) are consequences of the continuity of $(g,h) \mapsto gh$, $g \mapsto g^{-1}$, and $h \mapsto ghg^{-1}$ respectively. Moreover, (a) is a consequence of the definitions and (e) of the fact that g_L is a homeomorphism.

Conversely, let $\mathcal{N}$ be a nonempty collection of subsets of a group G satisfying the conditions (a)–(d). Note that (a) implies that e lies in all the N in $\mathcal{N}$. Define $\mathcal{U}$ to be the collection of subsets U of G such that, for every $g \in U$, there exists an $N \in \mathcal{N}$ with $gN \subset U$. Clearly, the empty set and G are in $\mathcal{U}$, and unions of sets in $\mathcal{U}$ are in $\mathcal{U}$. Let $U_1, U_2 \in \mathcal{U}$, and let $g \in U_1 \cap U_2$; by definition there exist $N_1, N_2 \in \mathcal{N}$ with $gN_1, gN_2 \subset U$; on applying (a) we obtain an $N' \in \mathcal{N}$ such that $gN' \subset U_1 \cap U_2$, which shows that $U_1 \cap U_2 \in \mathcal{U}$. It follows that the elements of $\mathcal{U}$ are the open sets of a topology on G. In fact, one sees easily that it is the unique topology for which (e) holds.

We next use (b) and (d) to show that $(g,g') \mapsto gg'$ is continuous. Note that the sets $g_1N_1 \times g_2N_2$ form a neighbourhood base for (g_1,g_2) in $G \times G$. Therefore, given an open $U \subset G$ and a pair (g_1,g_2) such that $g_1g_2 \in U$, we have to find $N_1, N_2 \in \mathcal{N}$ such that $g_1N_1g_2N_2 \subset U$. As U is open, there exists an $N \in \mathcal{N}$ such that $g_1g_2N \subset U$. Apply (b) to obtain an N' such that $N'N' \subset N$; then $g_1g_2N'N' \subset U$. But $g_1g_2N'N' = g_1(g_2N'g_2^{-1})g_2N'$, and it remains to apply (d) to obtain an $N_1 \in \mathcal{N}$ such that $N_1 \subset g_2N'g_2^{-1}$.

Finally, we use (c) and (d) to show that $g \mapsto g^{-1}$ is continuous. Given an open $U \subset G$ and a $g \in G$ such that $g^{-1} \in U$, we have to find an $N \in \mathcal{N}$ such that $gN \subset U^{-1}$. By definition, there exists an $N \in \mathcal{N}$ such that $g^{-1}N \subset U$. Now $N^{-1}g \subset U^{-1}$, and we use (c) to obtain an $N' \in \mathcal{N}$ such that $N'g \subset U^{-1}$, and (d) to obtain an $N'' \in \mathcal{N}$ such that $gN'' \subset g(g^{-1}N'g) \subset U^{-1}$. □

The Krull topology on the Galois group

Recall (3.9) that a finite extension Ω of F is Galois over F if it is normal and separable, i.e., if every irreducible polynomial $f \in F[X]$ having a root in Ω has $\deg f$ distinct roots in Ω. Similarly, we define an algebraic extension Ω of F to be ***Galois*** over F if it is normal and separable. For example, F^{sep} is a Galois extension of F. Clearly, Ω is Galois over F if and only if it is a union of finite Galois extensions.

[3]For subsets S and S' of G, we let $SS' = \{ss' \mid s \in S, s' \in S'\}$ and $S^{-1} = \{s^{-1} \mid s \in S\}$.

PROPOSITION 7.3 *If Ω is Galois over F, then it is Galois over every intermediate field M.*

PROOF. Let $f(X)$ be an irreducible polynomial in $M[X]$ having a root a in Ω. The minimum polynomial $g(X)$ of a over F splits into distinct degree-one factors in $\Omega[X]$. As f divides g (in $M[X]$), it also must split into distinct degree-one factors in $\Omega[X]$. □

PROPOSITION 7.4 *Let Ω be a Galois extension of F and let E be a subfield of Ω containing F. Then every F-homomorphism $E \to \Omega$ extends to an F-isomorphism $\Omega \to \Omega$.*

PROOF. The same Zorn's lemma argument as in the proof of Theorem 6.8 shows that every F-homomorphism $E \to \Omega$ extends to an F-homomorphism $\alpha\colon \Omega \to \Omega$. Let $a \in \Omega$, and let f be its minimum polynomial over F. Then Ω contains exactly $\deg(f)$ roots of f, and so therefore does $\alpha(\Omega)$. Hence $a \in \alpha(\Omega)$, which shows that α is surjective. □

COROLLARY 7.5 *Let $\Omega \supset E \supset F$ be as in the proposition. If E is stable under* $\mathrm{Aut}(\Omega/F)$, *then E is Galois over F.*

PROOF. Let $f(X)$ be an irreducible polynomial in $F[X]$ having a root a in E. Because Ω is Galois over F, $f(X)$ has $n = \deg(f)$ distinct roots $a_1, \dots, a_n$ in Ω. There is an F-isomorphism $F[a] \to F[a_i] \subset \Omega$ sending a to a_i (they are both stem fields for f), which extends to an F-isomorphism $\Omega \to \Omega$. As E is stable under $\mathrm{Aut}(\Omega/F)$, this shows that $a_i \in E$. □

Let Ω be a Galois extension of F, and let $G = \mathrm{Aut}(\Omega/F)$. For any finite subset S of Ω, let

$$G(S) = \{\sigma \in G \mid \sigma s = s \text{ for all } s \in S\}.$$

PROPOSITION 7.6 *There is a unique structure of a topological group on G for which the sets $G(S)$ form an open neighbourhood base of* 1. *For this topology, the sets $G(S)$ with S G-stable form a neighbourhood base of* 1 *consisting of open normal subgroups.*

PROOF. We show that the collection of sets $G(S)$ satisfies (a,b,c,d) of (7.2). It satisfies (a) because $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$. It satisfies (b) and (c) because each set $G(S)$ is a group. Let S be a finite subset of Ω. Then $F(S)$ is a finite extension of F, and so there are only finitely many F-homomorphisms $F(S) \to \Omega$. Since $\sigma S = \tau S$ if $\sigma|F(S) = \tau|F(S)$, this shows that $\overline{S} = \bigcup_{\sigma \in G} \sigma S$ is finite. Now $\sigma \overline{S} = \overline{S}$ for all $\sigma \in G$, and it follows that $G(\overline{S})$ is normal in G. Therefore, $\sigma G(\overline{S})\sigma^{-1} = G(\overline{S}) \subset G(S)$, which proves (d). It also proves the second statement. □

The topology on $\mathrm{Aut}(\Omega/F)$ defined in the proposition is called the ***Krull topology***. We write $\mathrm{Gal}(\Omega/F)$ for $\mathrm{Aut}(\Omega/F)$ endowed with the Krull topology, and call it the ***Galois group*** of Ω/F. The Galois group of F^{sep} over F is called the ***absolute Galois group***[4] of F.

If S is a finite set stable under G, then $F(S)$ is a finite extension of F stable under G, and hence Galois over F (7.5). Therefore,

$$\{\mathrm{Gal}(\Omega/E) \mid E \text{ finite and Galois over } F\}$$

is a neighbourhood base of 1 consisting of open normal subgroups.

[4]But note that the absolute Galois group of F is only defined up to an inner automorphism: let F' be a second separable algebraic closure of F; the choice of an isomorphism $F' \to F^{\mathrm{sep}}$ determines an isomorphism $\mathrm{Gal}(F'/F) \to \mathrm{Gal}(F^{\mathrm{sep}}/F)$; a second isomorphism $F' \to F^{\mathrm{sep}}$ will differ from the first by an element σ of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$, and the isomorphism $\mathrm{Gal}(F'/F) \to \mathrm{Gal}(F^{\mathrm{sep}}/F)$ it defines differs from the first by $\mathrm{inn}(\sigma)$.

PROPOSITION 7.7 *Let Ω be Galois over F. For every intermediate field E finite and Galois over F, the map*

$$\sigma \mapsto \sigma|E : \mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$$

is a continuous surjection (discrete topology on $\mathrm{Gal}(E/F)$*).*

PROOF. Let $\sigma \in \mathrm{Gal}(E/F)$, and regard it as an F-homomorphism $E \to \Omega$. Then σ extends to an F-isomorphism $\Omega \to \Omega$ (see 7.4), which shows that the map is surjective. For every finite set S of generators of E over F, $\mathrm{Gal}(\Omega/E) = G(S)$, which shows that the inverse image of $1_{\mathrm{Gal}(E/F)}$ is open in G. By homogeneity, the same is true for every element of $\mathrm{Gal}(E/F)$. □

PROPOSITION 7.8 *The Galois group G of a Galois extension Ω/F is compact and totally disconnected.*[5]

PROOF. We first show that G is Hausdorff. If $\sigma \neq \tau$, then $\sigma^{-1}\tau \neq 1_G$, and so it moves some element of Ω, i.e., there exists an $a \in \Omega$ such that $\sigma(a) \neq \tau(a)$. For any S containing a, $\sigma G(S)$ and $\tau G(S)$ are disjoint because their elements act differently on a. Hence they are disjoint open subsets of G containing σ and τ respectively.

We next show that G is compact. As we noted above, if S is a finite set stable under G, then $G(S)$ is a normal subgroup of G, and it has finite index because it is the kernel of

$$G \to \mathrm{Sym}(S).$$

Since every finite set is contained in a stable finite set,[6] the argument in the last paragraph shows that the map

$$G \to \prod_{S \text{ finite stable under } G} G/G(S)$$

is injective. When we endow $\prod G/G(S)$ with the product topology, the induced topology on G is that for which the $G(S)$ form an open neighbourhood base of e, i.e., it is the Krull topology. According to the Tychonoff theorem, $\prod G/G(S)$ is compact, and so it remains to show that G is closed in the product. For each $S_1 \subset S_2$, there are two continuous maps $\prod G/G(S) \to G/G(S_1)$, namely, the projection onto $G/G(S_1)$ and the projection onto $G/G(S_2)$ followed by the quotient map $G/G(S_2) \to G/G(S_1)$. Let $E(S_1, S_2)$ be the closed subset of $\prod G/G(S)$ on which the two maps agree. Then $\bigcap_{S_1 \subset S_2} E(S_1, S_2)$ is closed, and equals the image of G.

Finally, for each finite set S stable under G, $G(S)$ is a subgroup that is open and hence closed. Since $\bigcap G(S) = \{1_G\}$, this shows that the connected component of G containing 1_G is just $\{1_G\}$. By homogeneity, a similar statement is true for every element of G. □

PROPOSITION 7.9 *For every Galois extension Ω/F, $\Omega^{\mathrm{Gal}(\Omega/F)} = F$.*

PROOF. Every element of $\Omega \smallsetminus F$ lies in a finite Galois extension of F, and so this follows from the surjectivity in Proposition 7.7. □

[5] Following Bourbaki, we require compact spaces to be Hausdorff. A topological space is ***totally disconnected*** if its connected components are the one-point sets.

[6] Each element of Ω is algebraic over F, and its orbit is the set of its conjugates (roots of its minimum polynomial over F).

ASIDE 7.10 There is a converse to Proposition 7.8: every compact totally disconnected group arises as the Galois group of some Galois extension of fields of characteristic zero (Douady, A., Cohomologie des groupes compact totalement discontinus (d'après J. Tate), Séminaire Bourbaki 1959/60, no. 189). However, not all such groups arise as the absolute Galois group of a field of characteristic zero. For example, the absolute Galois group of a field of characteristic zero, if finite, must have order 1 or 2.[7]

The fundamental theorem of infinite Galois theory

PROPOSITION 7.11 *Let Ω be Galois over F, with Galois group G.*

(a) *Let M be a subfield of Ω containing F. Then Ω is Galois over M, the Galois group $\mathrm{Gal}(\Omega/M)$ is closed in G, and $\Omega^{\mathrm{Gal}(\Omega/M)} = M$.*

(b) *For every subgroup H of G, $\mathrm{Gal}(\Omega/\Omega^H)$ is the closure of H.*

PROOF. (a) The first assertion was proved in (7.3). For each finite subset $S \subset M$, $G(S)$ is an open subgroup of G, and hence it is closed. But $\mathrm{Gal}(\Omega/M) = \bigcap_{S\subset M} G(S)$, and so it also is closed. The final statement now follows from (7.9).

(b) Since $\mathrm{Gal}(\Omega/\Omega^H)$ contains H and is closed, it certainly contains the closure $\bar{H}$ of H. On the other hand, let $\sigma \in G \smallsetminus \bar{H}$; we have to show that σ moves some element of Ω^H. Because σ is not in the closure of H,

$$\sigma\,\mathrm{Gal}(\Omega/E) \cap H = \emptyset$$

for some finite Galois extension E of F in Ω (because the sets $\mathrm{Gal}(\Omega/E)$ form a neighbourhood base of 1; see above). Let ϕ denote the surjective map $\mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$. Then $\sigma|E \notin \phi H$, and so σ moves some element of $E^{\phi H} \subset \Omega^H$ (apply 3.11b). □

THEOREM 7.12 *Let Ω be Galois over F with Galois group G. The maps*

$$H \mapsto \Omega^H, \quad M \mapsto \mathrm{Gal}(\Omega/M)$$

are inverse bijections between the set of closed subgroups of G and the set of intermediate fields between Ω and F:

$$\{\textit{closed subgroups of } G\} \leftrightarrow \{\textit{intermediate fields } F \subset M \subset \Omega\}.$$

Moreover,

(a) *the correspondence is inclusion-reversing: $H_1 \supset H_2 \iff \Omega^{H_1} \subset \Omega^{H_2}$;*

(b) *a closed subgroup H of G is open if and only if Ω^H has finite degree over F, in which case $(G:H) = [\Omega^H:F]$;*

(c) *$\sigma H \sigma^{-1} \leftrightarrow \sigma M$, i.e., $\Omega^{\sigma H\sigma^{-1}} = \sigma(\Omega^H)$; $\mathrm{Gal}(\Omega/\sigma M) = \sigma\,\mathrm{Gal}(\Omega/M)\sigma^{-1}$;*

(d) *a closed subgroup H of G is normal if and only if Ω^H is Galois over F, in which case $\mathrm{Gal}(\Omega^H/F) \simeq G/H$.*

PROOF. For the first statement, we have to show that $H \mapsto \Omega^H$ and $M \mapsto \mathrm{Gal}(\Omega/M)$ are inverse maps.

Let H be a closed subgroup of G. Then Ω is Galois over Ω^H and $\mathrm{Gal}(\Omega/\Omega^H) = H$ (see 7.11).

[7] Theorem (Artin-Schreier, 1927): Let E be an algebraically closed field and let F be a proper subfield of E with $[E:F] < \infty$. Then F is real-closed and $E = F[\sqrt{-1}]$. See, for example, Jacobson 1964, Chapter VI.

Let M be an intermediate field. Then $\mathrm{Gal}(\Omega/M)$ is a closed subgroup of G and $\Omega^{\mathrm{Gal}(\Omega/M)} = M$ (see 7.11).

(a) We have the obvious implications:

$$H_1 \supset H_2 \implies \Omega^{H_1} \subset \Omega^{H_2} \implies \mathrm{Gal}(\Omega/\Omega^{H_1}) \supset \mathrm{Gal}(\Omega/\Omega^{H_2}).$$

But $\mathrm{Gal}(\Omega/\Omega^{H_i}) = H_i$ (see 7.11).

(b) As we noted earlier, a closed subgroup of finite index in a topological group is always open. Because G is compact, conversely an open subgroup of G is always of finite index. Let H be such a subgroup. The map $\sigma \mapsto \sigma|\Omega^H$ defines a bijection

$$G/H \to \mathrm{Hom}_F(\Omega^H, \Omega)$$

(apply 7.4) from which the statement follows.

(c) For $\tau \in G$ and $\alpha \in \Omega$, $\tau\alpha = \alpha \iff \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha$. Therefore, $\mathrm{Gal}(\Omega/\sigma M) = \sigma\,\mathrm{Gal}(\Omega/M)\sigma^{-1}$, and so $\sigma\,\mathrm{Gal}(\Omega/M)\sigma^{-1} \leftrightarrow \sigma M$.

(d) Let $H \leftrightarrow M$. It follows from (c) that H is normal if and only if M is stable under the action of G. But M is stable under the action of G if and only it is a union of finite extensions of F stable under G, i.e., of finite Galois extensions of G. We have already observed that an extension is Galois if and only if it is a union of finite Galois extensions. □

REMARK 7.13 As in the finite case (3.17), we can deduce the following statements.

(a) Let $(M_i)_{i\in I}$ be a (possibly infinite) family of intermediate fields, and let $H_i \leftrightarrow M_i$. Let $\prod M_i$ be the smallest field containing all the M_i; then because $\bigcap_{i\in I} H_i$ is the largest (closed) subgroup contained in all the H_i,

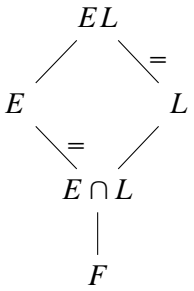
$$\mathrm{Gal}(\Omega/\textstyle\prod M_i) = \bigcap_{i\in I} H_i.$$

(b) Let $M \leftrightarrow H$. The largest (closed) normal subgroup contained in H is $N = \bigcap_\sigma \sigma H\sigma^{-1}$ (cf. GT 4.10), and so Ω^N, which is the composite of the fields σM, is the smallest normal extension of F containing M.

PROPOSITION 7.14 *Let E and L be field extensions of F contained in some common field. If E/F is Galois, then EL/L and $E/E\cap L$ are Galois, and the map*

$$\sigma \mapsto \sigma|E : \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E\cap L)$$

is an isomorphism of topological groups.



PROOF. We first prove that the map is continuous. Let $G_1 = \mathrm{Gal}(EL/L)$ and let $G_2 = \mathrm{Gal}(E/E\cap L)$. For any finite set S of elements of E, the inverse image of $G_2(S)$ in G_1 is $G_1(S)$.

We next show that the map is an isomorphism of groups (neglecting the topology). As in the finite case, it is an injective homomorphism (3.18). Let H be the image of the map. Then the fixed field of H is $E\cap L$, which implies that H is dense in $\mathrm{Gal}(E/E\cap L)$. But H is closed because it is the continuous image of a compact space in a Hausdorff space, and so $H = \mathrm{Gal}(E/E\cap L)$.

Finally, we prove that it is open. An open subgroup of $\mathrm{Gal}(EL/L)$ is closed (hence compact) of finite index; therefore its image in $\mathrm{Gal}(E/E\cap L)$ is compact (hence closed) of finite index, and hence open. □

COROLLARY 7.15 *Let Ω be an algebraically closed field containing F, and let E and L be as in the proposition. If $\rho: E \to \Omega$ and $\sigma: L \to \Omega$ are F-homomorphisms such that $\rho|E \cap L = \sigma|E \cap L$, then there exists an F-homomorphism $\tau: EL \to \Omega$ such that $\tau|E = \rho$ and $\tau|L = \sigma$.*

PROOF. According to (7.4), σ extends to an F-homomorphism $s: EL \to \Omega$. As $s|E \cap L = \rho|E \cap L$, we can write $s|E = \rho \circ \varepsilon$ for some $\varepsilon \in \mathrm{Gal}(E/E \cap L)$. According to the proposition, there exists a unique $e \in \mathrm{Gal}(EL/L)$ such that $e|E = \varepsilon$. Define $\tau = s \circ e^{-1}$. □

EXAMPLE 7.16 Let Ω be an algebraic closure of the finite field $\mathbb{F}_p$. Then $G = \mathrm{Gal}(\Omega/\mathbb{F}_p)$ contains a canonical Frobenius element, $\sigma = (a \mapsto a^p)$, and it is generated by it as a topological group, i.e., G is the closure of $\langle\sigma\rangle$. We now determine the structure of G.

Endow $\mathbb{Z}$ with the topology for which the groups $n\mathbb{Z}$, $n \geq 1$, form a fundamental system of neighbourhoods of 0. Thus two integers are close if their difference is divisible by a large integer.

As for any topological group, we can complete $\mathbb{Z}$ for this topology. A Cauchy sequence in $\mathbb{Z}$ is a sequence $(a_i)_{i\geq 1}$, $a_i \in \mathbb{Z}$, satisfying the following condition: for all $n \geq 1$, there exists an N such that $a_i \equiv a_j \mod n$ for $i, j > N$. Call a Cauchy sequence in $\mathbb{Z}$ trivial if $a_i \to 0$ as $i \to \infty$, i.e., if for all $n \geq 1$, there exists an N such that $a_i \equiv 0 \mod n$ for all $i > N$. The Cauchy sequences form a commutative group, and the trivial Cauchy sequences form a subgroup. We define $\hat{\mathbb{Z}}$ to be the quotient of the first group by the second. It has a ring structure, and the map sending $m \in \mathbb{Z}$ to the constant sequence $m, m, m, \ldots$ identifies $\mathbb{Z}$ with a subgroup of $\hat{\mathbb{Z}}$.

Let $\alpha \in \hat{\mathbb{Z}}$ be represented by the Cauchy sequence (a_i). The restriction of the Frobenius element σ to $\mathbb{F}_{p^n}$ has order n. Therefore $(\sigma|\mathbb{F}_{p^n})^{a_i}$ is independent of i provided it is sufficiently large, and we can define $\sigma^\alpha \in \mathrm{Gal}(\Omega/\mathbb{F}_p)$ to be such that, for each n, $\sigma^\alpha|\mathbb{F}_{p^n} = (\sigma|\mathbb{F}_{p^n})^{a_i}$ for all i sufficiently large (depending on n). The map $\alpha \mapsto \sigma^\alpha: \hat{\mathbb{Z}} \to \mathrm{Gal}(\Omega/\mathbb{F}_p)$ is an isomorphism.

The group $\hat{\mathbb{Z}}$ is uncountable. To most analysts, it is a little weird—its connected components are one-point sets. To number theorists it will seem quite natural — the Chinese remainder theorem implies that it is isomorphic to $\prod_{p \text{ prime}} \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of p-adic integers.

EXAMPLE 7.17 Let $\mathbb{Q}^{\mathrm{al}}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Then $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ is one of the most basic, and intractable, objects in mathematics. It is expected that *every* finite group occurs as a quotient of it. This is known, for example, for S_n and for every sporadic simple group except possibly M_{23}. See (5.41) and mo80359.

On the other hand, we do understand $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ where $F \subset \mathbb{Q}^{\mathrm{al}}$ is a finite extension of $\mathbb{Q}$ and F^{ab} is the union of all finite abelian extensions of F contained in $\mathbb{Q}^{\mathrm{al}}$. For example, $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^\times$. This is abelian class field theory — see my notes Class Field Theory.

ASIDE 7.18 A ***simple Galois correspondence*** is a system consisting of two partially ordered sets P and Q and order reversing maps $f: P \to Q$ and $g: Q \to P$ such that $gf(p) \geq p$ for all $p \in P$ and $fg(q) \geq q$ for all $q \in Q$. Then $fgf = f$, because $fg(fp) \geq fp$ and $gf(p) \geq p$ implies $f(gfp) \leq f(p)$ for all $p \in P$. Similarly, $gfg = g$, and it follows that f and g define a one-to-one correspondence between the sets $g(Q)$ and $f(P)$.

From a Galois extension Ω of F we get a simple Galois correspondence by taking P to be the set of subgroups of $\mathrm{Gal}(\Omega/F)$ and Q to be the set of subsets of Ω, and by setting $f(H) = \Omega^H$ and $g(S) = G(S)$. Thus, to prove the one-to-one correspondence in the fundamental theorem, it suffices to identify the closed subgroups as exactly those in the image of g and the intermediate fields as exactly those in the image of f. This is accomplished by (7.11).

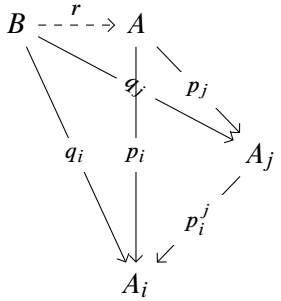
Galois groups as inverse limits

DEFINITION 7.19 A partial ordering $\leq$ on a set I is ***directed***, and the pair $(I, \leq)$ is a ***directed set***, if for all $i, j \in I$ there exists a $k \in I$ such that $i, j \leq k$.

DEFINITION 7.20 Let $(I, \leq)$ be a directed set, and let C be a category (for example, the category of groups and homomorphisms, or the category of topological groups and continuous homomorphisms).

(a) An ***inverse system*** in C indexed by $(I, \leq)$ is a family $(A_i)_{i\in I}$ of objects of C together with a family $(p_i^j : A_j \to A_i)_{i\leq j}$ of morphisms such that $p_i^i = \mathrm{id}_{A_i}$ and $p_i^j \circ p_j^k = p_i^k$ all $i \leq j \leq k$.

(b) An object A of C together with a family $(p_j : A \to A_j)_{j\in I}$ of morphisms satisfying $p_i^j \circ p_j = p_i$ all $i \leq j$ is an ***inverse limit*** of the system in (a) if it has the following universal property: for any other object B and family $(q_j : B \to A_j)$ of morphisms such $p_i^j \circ q_j = q_i$ all $i \leq j$, there exists a unique morphism $r : B \to A$ such that $p_j \circ r = q_j$ for j,



Clearly, the inverse limit (if it exists), is uniquely determined by this condition up to a unique isomorphism. We denote it by $\varprojlim(A_i, p_i^j)$, or just $\varprojlim A_i$.

EXAMPLE 7.21 Let $(G_i, p_i^j : G_j \to G_i)$ be an inverse system of groups. Let

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ all } i \leq j\},$$

and let $p_i : G \to G_i$ be the projection map. Then $p_i^j \circ p_j = p_i$ is just the equation $p_i^j(g_j) = g_i$. Let (H, q_i) be a second family such that $p_i^j \circ q_j = q_i$. The image of the homomorphism

$$h \mapsto (q_i(h)) : H \to \prod G_i$$

is contained in G, and this is the unique homomorphism $H \to G$ carrying q_i to p_i. Hence $(G, p_i) = \varprojlim(G_i, p_i^j)$.

EXAMPLE 7.22 Let $(G_i, p_i^j : G_j \to G_i)$ be an inverse system of topological groups and continuous homomorphisms. When endowed with the product topology, $\prod G_i$ becomes a topological group

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ all } i \leq j\},$$

and G becomes a topological subgroup with the subspace topology. The projection maps p_i are continuous. Let H be (H, q_i) be a second family such that $p_i^j \circ q_j = q_i$. The homomorphism

$$h \mapsto (q_i(h)) : H \to \prod G_i$$

is continuous because its composites with projection maps are continuous (universal property of the product). Therefore $H \to G$ is continuous, and this shows that $(G, p_i) = \varprojlim(G_i, p_i^j)$.

EXAMPLE 7.23 Let $(G_i, p_i^j : G_j \to G_i)$ be an inverse system of finite groups, and regard it as an inverse system of topological groups by giving each G_i the discrete topology. A topological group G arising as an inverse limit of such a system is said to be ***profinite***[8].

If $(x_i) \notin G$, say $p_{i_0}^{j_0}(x_{j_0}) \neq x_{i_0}$, then

$$G \cap \{(g_j) \mid g_{j_0} = x_{j_0}, \quad g_{i_0} = x_{i_0}\} = \emptyset.$$

As the second set is an open neighbourhood of (x_i), this shows that G is closed in $\prod G_i$. By Tychonoff's theorem, $\prod G_i$ is compact, and so G is also compact. The map $p_i : G \to G_i$ is continuous, and its kernel U_i is an open subgroup of finite index in G (hence also closed). As $\bigcap U_i = \{e\}$, the connected component of G containing e is just $\{e\}$. By homogeneity, the same is true for every point of G: the connected components of G are the one-point sets — G is totally disconnected.

We have shown that a profinite group is compact and totally disconnected, and it is an exercise to prove the converse.[9]

EXAMPLE 7.24 Let Ω be a Galois extension of F. The composite of two finite Galois extensions of in Ω is again a finite Galois extension, and so the finite Galois subextensions of Ω form a directed set I. For each E in I we have a finite group $\mathrm{Gal}(E/F)$, and for each $E \subset E'$ we have a restriction homomorphism $p_E^{E'} : \mathrm{Gal}(E'/F) \to \mathrm{Gal}(E/F)$. In this way, we get an inverse system of finite groups $(\mathrm{Gal}(E/F), p_E^{E'})$ indexed by I.

For each E, there is a restriction homomorphism $p_E : \mathrm{Gal}(\Omega/F) \to \mathrm{Gal}(E/F)$ and, because of the universal property of inverse limits, these maps define a homomorphism

$$\mathrm{Gal}(\Omega/F) \to \varprojlim \mathrm{Gal}(E/F).$$

This map is an isomorphism of topological groups. This is a restatement of what we showed in the proof of (7.8).

Nonopen subgroups of finite index

We apply Zorn's lemma[10] to construct a nonopen subgroup of finite index in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$.[11]

LEMMA 7.25 *Let V be an infinite-dimensional vector space. For all $n \geq 1$, there exists a subspace V_n of V such that V/V_n has dimension n.*

PROOF. Zorn's lemma shows that V contains maximal linearly independent subsets, and then the usual argument shows that such a subset spans V, i.e., is a basis. Choose a basis, and take V_n to be the subspace spanned by the set obtained by omitting n elements from the basis. □

PROPOSITION 7.26 *The group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ has nonopen normal subgroups of index 2^n for all $n > 1$.*

[8] An inverse limit is also called a projective limit. Thus a profinite group is a projective limit of finite groups.

[9] More precisely, it is Exercise 3 of §7 of Chapter 3 of Bourbaki's General Topology.

[10] This is really needed — see mo106216.

[11] Contrast: "... it is not known, even when $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, whether every subgroup of finite index in G is open; this is one of a number of related unsolved problems, all of which appear to be very difficult." Swinnerton-Dyer, H. P. F., A brief guide to algebraic number theory. Cambridge, 2001, p133.

PROOF. Let E be the subfield $\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \dots, \sqrt{p}, \dots]$, p prime, of $\mathbb{C}$. For each p,

$$\mathrm{Gal}(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \dots, \sqrt{p}]/\mathbb{Q})$$

is a product of copies of $\mathbb{Z}/2\mathbb{Z}$ indexed by the set $\{\text{primes} \le p\} \cup \{\infty\}$ (apply 5.31; see also 5.30b). As

$$\mathrm{Gal}(E/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \dots, \sqrt{p}]/\mathbb{Q}),$$

it is a direct product of copies of $\mathbb{Z}/2\mathbb{Z}$ indexed by the primes l of $\mathbb{Q}$ (including $l = \infty$) endowed with the product topology. Let $G = \mathrm{Gal}(E/\mathbb{Q})$, and let

$$H = \{(a_l) \in G \mid a_l = 0 \text{ for all but finitely many } l\}.$$

This is a subgroup of G (in fact, it is a direct *sum* of copies of $\mathbb{Z}/2\mathbb{Z}$ indexed by the primes of $\mathbb{Q}$), and it is dense in G because[12] clearly every open subset of G contains an element of H. We can regard G/H as vector space over $\mathbb{F}_2$ and apply the lemma to obtain subgroups G_n of index 2^n in G containing H. If G_n is open in G, then it is closed, which contradicts the fact that H is dense. Therefore, G_n is not open, and its inverse image in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ is the desired subgroup.[13] □

ASIDE 7.27 Let $G = \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$. We showed in the above proof that there is a closed normal subgroup $N = \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/E)$ of G such that G/N is an uncountable vector space over $\mathbb{F}_2$. Let $(G/N)^\vee$ be the dual of this vector space (also uncountable). Every nonzero $f \in (G/N)^\vee$ defines a surjective map $G \to \mathbb{F}_2$ whose kernel is a subgroup of index 2 in G. These subgroups are distinct, and so G has uncountably many subgroups of index 2. Only countably many of them are open because $\mathbb{Q}$ has only countably many quadratic extensions in a fixed algebraic closure.

ASIDE 7.28 Let G be a profinite group that is finitely generated as a topological group. It is a difficult theorem, only recently proved, that every subgroup of finite index in G is open (Nikolov, Nikolay; Segal, Dan. On finitely generated profinite groups. I. Strong completeness and uniform bounds. Ann. of Math. (2) 165 (2007), no. 1, 171–238.)

Exercises

7-1 Let p be a prime number, and let Ω be the subfield of $\mathbb{C}$ generated over $\mathbb{Q}$ by all p^mth roots of 1 for $m \in \mathbb{N}$. Show that Ω is Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}_p \overset{\text{def}}{=} \varprojlim \mathbb{Z}/p^m\mathbb{Z}$. (Hint: Use that Ω is the union of a tower of subfields

$$\mathbb{Q} \subset \mathbb{Q}[\zeta_p] \subset \cdots \subset \mathbb{Q}[\zeta_{p^m}] \subset \mathbb{Q}[\zeta_{p^{m+1}}] \subset \cdots .)$$

7-2 Let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_p$, and let $\mathbb{F}_{p^m}$ be the subfield of $\mathbb{F}$ with p^m elements. Show that

$$\varprojlim_{m \ge 1} \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \simeq \varprojlim_{m \ge 1} \mathbb{Z}/m\mathbb{Z}$$

and deduce that $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}}$.

[12] Alternatively, let $(a_l) \in G$; then the sequence

$$(a_\infty, 0, 0, 0, \dots), (a_\infty, a_2, 0, 0, \dots), (a_\infty, a_2, a_3, 0, \dots), \dots$$

in H converges to (a_l).

[13] The inverse image is not open because every continuous homomorphism from a compact group to a separated group is open. Alternatively, if the inverse image were open, its fixed field would be a nontrivial extension E of $\mathbb{Q}$ contained in $\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \dots, \sqrt{p}, \dots]$; but then E would be fixed by G_n, which is dense.

CHAPTER 8

The Galois theory of étale algebras

For Grothendieck, the classification of field extensions by Galois groups, and the classification of covering spaces by fundamental groups, are two aspects of the same theory. In this chapter, we re-interprete classical Galois theory from Grothendieck's point of view. We assume the reader is familiar with the language of category theory (Wikipedia: Category theory; Equivalence of categories).

Throughout, F is a field, all rings and F-algebras are commutative, and unadorned tensor products are over F. An F-algebra A is finite if it is finitely generated as an F-module.

Review of commutative algebra

We'll need the following standard results from commutative algebra.

Two ideals I and J in a ring A are said to be ***relatively prime*** if $I+J=A$. For example, any two distinct maximal ideals in A are relatively prime.

THEOREM 8.1 (CHINESE REMAINDER THEOREM) *Let $I_1,\dots,I_n$ be ideals in a ring A. If I_i is relatively prime to I_j whenever $i\neq j$, then the map*

$$a\mapsto(\dots,a+I_i,\dots)\colon A\to A/I_1\times\cdots\times A/I_n \tag{15}$$

is surjective with kernel $\prod I_i$ (so $\prod I_i=\bigcap I_i$).

PROOF. CA 2.12. □

THEOREM 8.2 (STRONG NULLSTELLENSATZ) *Let I be an ideal in the polynomial ring $F[X_1,\dots,X_n]$ and let $Z(I)$ denote the set of zeros of I in $(F^{\mathrm{al}})^n$. If a polynomial $h\in F[X_1,\dots,X_n]$ vanishes on $Z(I)$, then some power of it lies in I.*

PROOF. CA 12.8. □

The ***radical*** of an ideal I in a ring A is the set of $f\in A$ such that $f^n\in I$ for some $n\in\mathbb{N}$. It is again an ideal, and it is equal to its own radical.

The ***nilradical*** N of A is the radical of the ideal (0). It consists of the nilpotents in A. If $N=0$, then A is said to be ***reduced***.

PROPOSITION 8.3 *Let A be a finitely generated F-algebra, and let I be an ideal in A. The radical of I is equal to the intersection of the maximal ideals containing it:*

$$\operatorname{rad}(I)=\bigcap\{M\mid M\supset I,\ M\ \text{maximal}\}.$$

In particular, A is reduced if and only if $\bigcap\{M\mid M\ \text{maximal}\}=0$.

PROOF. Because of the correspondence between ideals in a ring and in a quotient of the ring, it suffices to prove this for $A = F[X_1, \dots, X_n]$.

The inclusion $\text{rad}(I) \subset \bigcap\{M \mid M \supset I, M \text{ maximal}\}$ holds in any ring (because maximal ideals are radical and $\text{rad}(I)$ is the smallest radical ideal containing I).

For the reverse inclusion, let h lie in all maximal ideals containing I, and let $(a_1, \dots, a_n) \in Z(I)$. The image of the evaluation map

$$f \mapsto f(a_1, \dots, a_n): F[X_1, \dots, X_n] \to F^{\text{al}}$$

is a subring of F^{al} which is algebraic over F, and hence is a field (see 1.31a). Therefore, the kernel of the map is a maximal ideal, which contains I, and therefore also contains h. This shows that $h(a_1, \dots, a_n) = 0$, and we conclude from the strong Nullstellensatz that $h \in \text{rad}(I)$. □

Étale algebras over a field

DEFINITION 8.4 An F-algebra A is ***diagonalizable*** if it is isomorphic to the product algebra F^n for some n, and it is ***étale*** if $L \otimes A$ is diagonalizable for some field L containing F.[1] The ***degree*** $[A: F]$ of a finite F-algebra A is its dimension as an F-vector space.

Let A be a finite F-algebra. For any finite set S of maximal ideals in A, the Chinese remainder theorem (8.1) shows that the map $A \to \prod_{M \in S} A/M$ is surjective with kernel $\bigcap_{M \in S} M$. In particular, $|S| \leq [A: F]$, and so A has only finitely many maximal ideals. If S is the set of all maximal ideals in A, then $\bigcap_{M \in S} M$ is the nilradical N of A (8.3), and so A/N is a finite product of fields.

PROPOSITION 8.5 *The following conditions on a finite F-algebra A are equivalent:*

(a) *A is étale;*

(b) *$L \otimes A$ is reduced for all fields L containing F;*

(c) *A is a product of separable field extensions of F.*

PROOF. (a)⇒(b). Let L be a field containing F. By hypothesis, there exists a field L' containing F such that $L' \otimes A$ is diagonalizable. Let L'' be a field containing (copies of) both L and L' (e.g., take L'' to be a quotient of $L \otimes L'$ by a maximal ideal). Then $L'' \otimes A = L'' \otimes_{L'} L' \otimes A$ is diagonalizable, and the map $L \otimes A \to L'' \otimes A$ defined by the inclusion $L \to L''$ is injective, and so $L \otimes A$ is reduced.

(b)⇒(c). The map $a \mapsto 1 \otimes a: A \to L \otimes A$ is injective, and so if $L \otimes A$ is reduced, then so also is A. The discussion above shows that it is a finite product of fields. Let F' be one of the factors of A. If F' is not separable over F, then F has characteristic $p \neq 0$ and there exists an element u of F' whose minimum polynomial is of the form $f(X^p)$ with $f \in F[X]$ (see 3.6 *et seq.*). Let L be a field containing F such that all the coefficients of f are pth powers in L. Then

$$L \otimes F[u] \simeq L \otimes (F[X]/(f(X^p)) \simeq L[X]/(f(X^p)),$$

which is not reduced because $f(X^p)$ is a pth power in $L[X]$. Hence $L \otimes A$ is not reduced.

[1] This is Bourbaki's terminology

(c)⇒(a). We may suppose that A itself is a separable field extension of F. From the primitive element theorem (5.1), we know that $A = F[u]$ for some u. Because $F[u]$ is separable over F, the minimum polynomial $f(X)$ of u is separable, which means that

$$f(X) = \prod(X - u_i), \quad u_i \neq u_j \text{ for } i \neq j,$$

in a splitting field L for f. Now

$$L \otimes A \simeq L \otimes F[X]/(f) \simeq L[X]/(f),$$

and, according to the Chinese remainder theorem (8.1),

$$L[X]/(f) \simeq \prod\nolimits_i L[X]/(X - u_i) \simeq L \times \cdots \times L.$$

□

COROLLARY 8.6 *An F-algebra A is étale if and only if $F^{\text{sep}} \otimes A$ is diagonalizable.*

PROOF. The proof that (c) implies (a) in (8.5) shows that $L \otimes A$ is diagonalizable if certain separable polynomials split in L. By definition, all separable polynomials split in F^{sep}. □

EXAMPLE 8.7 Let $f \in F[X]$, and let $A = F[X]/(f)$. Let $f = \prod f_i^{m_i}$ with the f_i irreducible and distinct. According to the Chinese remainder theorem (CA 2.12)

$$A \simeq \prod\nolimits_i F[X]/(f_i^{m_i}).$$

The F-algebra $F[X]/(f_i^{m_i})$ is a field if and only if $m_i = 1$, in which case it is a separable extension of F if and only if f_i is separable. Therefore A is an étale F-algebra if and only if f is a separable polynomial.

PROPOSITION 8.8 *Finite products, tensor products, and quotients of diagonalizable (resp. étale) F-algebras are diagonalizable (resp. étale).*

PROOF. This is obvious for diagonalizable algebras, and it follows for étale algebras. □

COROLLARY 8.9 *The composite of any finite set of étale subalgebras of a F-algebra is étale.*

PROOF. Let A_i be étale subalgebras of B. Then $A_1 \cdots A_n$ is the image of the map

$$a_1 \otimes \cdots \otimes a_n \mapsto a_1 \cdots a_n : A_1 \otimes \cdots \otimes A_n \to B,$$

and so is a quotient of $A_1 \otimes \cdots \otimes A_n$. □

PROPOSITION 8.10 *Let A be étale over F, and let F' be a field containing F. Then $F' \otimes A$ is étale over F'.*

PROOF. Let L be such that $L \otimes A \approx L^m$, and let L' be a field containing (copies of) both L and F'. Then

$$L' \otimes_{F'} \big(F' \otimes A\big) \simeq L' \otimes A \simeq L' \otimes_L (L \otimes A) \approx L' \otimes_L L^m \simeq \big(L'\big)^m.$$

□

REMARK 8.11 Let A be an étale algebra over F, and write A as a product of fields, $A = \prod_i A_i$. A generator α for A as an F-algebra is a tuple (α_i) with each α_i a generator for A_i as an F-algebra. Because each A_i is separable over F, such an α exists (primitive element theorem 5.1). Choose an α, and let $f = \prod_i f_i$ be the product of the minimum polynomials of the α_i. Then f is a monic polynomial whose irreducible factors are separable.

Conversely, let f be a monic polynomial whose irreducible factors $(f_i)_i$ are separable. Then $A \stackrel{\text{def}}{=} \prod_i F[X]/(f_i)$ is an étale algebra over F with a canonical generator.

In this way, we get a one-to-one correspondence between the set of isomorphism classes of pairs (A,α) consisting of an étale F-algebra and a generator and the set of monic polynomials whose irreducible factors are separable.

Classification of étale algebras over a field

Fix a separable closure Ω of F, and let G be the Galois group of Ω over F. Recall (Chapter 7) that this is the group of F-automorphisms of Ω equipped with the Krull topology. Let E be a subfield of Ω, finite and Galois over F. An argument using Zorn's lemma shows that

$$\sigma \mapsto \sigma|E : G \to \mathrm{Gal}(E/F)$$

is surjective. The open normal subgroups of G are exactly the kernels of such homomorphisms, and $G = \varprojlim \mathrm{Gal}(E/F)$.

Let X be a finite set with an action of G,

$$G \times X \to X.$$

We say that the action is continuous if the map is continuous for the discrete topology on X and the Krull topology on G. Because X is finite, this is equivalent to saying that the action factors through $G \to \mathrm{Gal}(E/F)$ for some subfield E of Ω finite and Galois over F.

For an étale F-algebra A, let $\mathcal{F}(A)$ denote the set of F-algebra homomorphisms $A \to \Omega$. Then G acts on $\mathcal{F}(A)$ through its action on Ω:

$$(\sigma f)(a) = \sigma(f(a)), \quad \sigma \in G,\ f \in \mathcal{F}(A),\ a \in A,$$

i.e., $\sigma f = \sigma \circ f$. There exists a finite Galois extension E of F containing the image of every homomorphism $A \to \Omega$, and the action of G on $\mathcal{F}(A)$ factors through $\mathrm{Gal}(E/F)$; therefore it is continuous.

Now $A \rightsquigarrow \mathcal{F}(A)$ is a contravariant functor from the category of étale F-algebras to the category of finite continuous G-sets.

EXAMPLE 8.12 Let $A = F[X]/(f)$ where f is a separable polynomial in $F[X]$. Then

$$\mathcal{F}(A) \simeq \{\text{roots of } f(X) \text{ in } \Omega\}.$$

Suppose that A is a product of étale F-algebras, $A = A_1 \times \cdots \times A_n$. Because Ω has no nonzero zero divisors, every homomorphism $f : A \to \Omega$ is zero on all but one A_i, and so, to give a homomorphism $A \to \Omega$ amounts to giving a homomorphism $A_i \to \Omega$ for some i. In other words,

$$\mathcal{F}(\textstyle\prod_i A_i) \simeq \coprod_i \mathcal{F}(A_i).$$

In particular, for an étale F-algebra $A \simeq \prod_i F_i$,

$$\mathcal{F}(A) \simeq \coprod_i \mathrm{Hom}_{F\text{-algebra}}(F_i, \Omega).$$

From Proposition 2.7, we deduce that $\mathcal{F}(A)$ is finite of order $[A:F]$.

THEOREM 8.13 *The functor $A \rightsquigarrow \mathcal{F}(A)$ is a contravariant equivalence from the category of étale F-algebras to the category of finite continuous G-sets.*

PROOF. We have to prove the following two statements.

(a) The functor $\mathcal{F}$ is fully faithful, i.e., for all étale F-algebras A and B, the map

$$\mathrm{Hom}_{F\text{-algebras}}(A,B) \to \mathrm{Hom}_{G\text{-sets}}(\mathcal{F}(B),\mathcal{F}(A))$$

is bijective.

(b) The functor $\mathcal{F}$ is essentially surjective, i.e., every finite continuous G-set is isomorphic to $\mathcal{F}(A)$ for some étale F-algebra A.

Let V be a vector space over F, and let $V_\Omega = \Omega \otimes_F V$. Then G acts on V_Ω through its action on Ω, and

$$V \simeq (V_\Omega)^G \stackrel{\text{def}}{=} \{v \in V_\Omega \mid \sigma v = v \text{ for all } \sigma \in G\}.$$

To see this, choose an F-basis $e = \{e_1,\dots,e_n\}$ for V. Then e is an Ω-basis for V_Ω, and

$$\sigma(a_1e_1 + \cdots + a_ne_n) = (\sigma a_1)e_1 + \cdots + (\sigma a_n)e_n, \quad a_i \in \Omega.$$

Therefore $a_1e_1 + \cdots + a_ne_n$ is fixed by all $\sigma \in G$ if and only if $a_1,\dots,a_n \in F$.

Similarly, if W is a second vector space over F, then G acts on $\mathrm{Hom}_{\Omega\text{-linear}}(V_\Omega, W_\Omega)$ by $\sigma\alpha = \sigma \circ \alpha \circ \sigma^{-1}$, and

$$\mathrm{Hom}_{F\text{-linear}}(V,W) \simeq \mathrm{Hom}_{\Omega\text{-linear}}(V_\Omega, W_\Omega)^G. \tag{16}$$

Indeed, a choice of bases for V and W determines isomorphisms $\mathrm{Hom}_{F\text{-linear}}(V,W) \simeq M_{m,n}(F)$ ($m \times n$ matrices with entries from F) and $\mathrm{Hom}_{\Omega\text{-linear}}(V_\Omega, W_\Omega) \simeq M_{m,n}(\Omega)$, and G acts on $M_{m,n}(\Omega)$ in the obvious way. Now (16) follows from the obvious statement: $M_{m,n}(F) = M_{m,n}(\Omega)^G$.

Let A and B be étale F-algebras. Under the isomorphism

$$\mathrm{Hom}_{F\text{-linear}}(A,B) \simeq \mathrm{Hom}_{\Omega\text{-linear}}(A_\Omega, B_\Omega)^G,$$

F-algebra homomorphisms correspond to Ω-algebra homomorphisms, and so

$$\mathrm{Hom}_{F\text{-algebra}}(A,B) \simeq \mathrm{Hom}_{\Omega\text{-algebra}}(A_\Omega, B_\Omega)^G.$$

From (8.6), we know that A_Ω (resp. B_Ω) is a product of copies of Ω indexed by the elements of $\mathcal{F}(A)$ (resp. $\mathcal{F}(B)$). Let t be a map of sets $\mathcal{F}(B) \to \mathcal{F}(A)$. Then

$$(a_i)_{i\in\mathcal{F}(A)} \mapsto (b_j)_{j\in\mathcal{F}(B)}, \quad b_j = a_{t(j)},$$

is a homomorphism of Ω-algebras $A_\Omega \to B_\Omega$, and every homomorphism of Ω-algebras $A_\Omega \to B_\Omega$ is of this form for a unique t. Thus

$$\mathrm{Hom}_{\Omega\text{-algebra}}(A_\Omega, B_\Omega) \simeq \mathrm{Hom}_{\mathrm{Sets}}(\mathcal{F}(B),\mathcal{F}(A)).$$

This isomorphism is compatible with the actions of G, and so

$$\mathrm{Hom}_{\Omega\text{-algebra}}(A_\Omega, B_\Omega)^G \simeq \mathrm{Hom}_{\mathrm{Sets}}(\mathcal{F}(B),\mathcal{F}(A))^G.$$

In other words,

$$\mathrm{Hom}_{F\text{-algebra}}(A,B) \simeq \mathrm{Hom}_{G\text{-sets}}(\mathcal{F}(B),\mathcal{F}(A)).$$

This proves (a). For (b), let S be a finite G-set, and let $S = \bigsqcup_{i\in I} S_i$ be the decomposition of S into a union of G-orbits. For each i, choose an $s_i \in S_i$, and let F_i be the subfield of Ω fixed by the stabilizer of s_i. Then

$$\mathcal{F}\left(\textstyle\prod_{i\in I} F_i\right) \simeq S.$$

□

SECOND PROOF OF THEOREM 8.13

We sketch a second proof of the theorem. For a finite set S with a continuous action of G, we let

$$\Omega^S = \mathrm{Hom}(S, \Omega).$$

In other words, Ω^S is a product of copies of Ω indexed by the elements of S. We let G act on Ω^S through its actions on both Ω and S:

$$(\gamma f)(\sigma) = \gamma(f(\gamma^{-1}\sigma)), \quad \gamma \in G, \quad f: S \to \Omega, \quad \sigma \in S,$$

For every étale F-algebra A, there is a canonical isomorphism

$$a \otimes c \mapsto (\sigma a \cdot c)_{\sigma \in \mathcal{F}(A)}: \Omega \otimes A \to \Omega^{\mathcal{F}(A)}. \tag{17}$$

When we let G act on $\Omega \otimes A$ through its action on Ω, the map (17) becomes equivariant. Now:

(a) for every étale F-algebra A,
$$A \simeq (\Omega \otimes A)^G;$$

(b) for every finite set S with a continuous action of G, $(\Omega^S)^G$ is an étale F-subalgebra of Ω^S, and
$$\mathcal{F}((\Omega^S)^G) \simeq S.$$

Therefore, $A \rightsquigarrow \mathcal{F}(A)$ is an equivalence of categories with quasi-inverse $S \rightsquigarrow (\Omega^S)^G$.

IMPROVEMENT OF THEOREM 8.13

Fix a Galois extension Ω of F (finite or infinite), and let $G = \mathrm{Gal}(\Omega/F)$. An étale F-algebra A is ***split*** by Ω if $\Omega \otimes A$ is isomorphic to a product of copies of Ω. For such an F-algebra, let $\mathcal{F}(A) = \mathrm{Hom}_{k\text{-algebra}}(A, \Omega)$.

THEOREM 8.14 *The functor $A \rightsquigarrow \mathcal{F}(A)$ is a contravariant equivalence from the category of étale F-algebras split by Ω to the category of finite continuous G-sets.*

The proof is the same as that of Theorem 8.13. When Ω is a finite extension of F, "continuous" may be omitted.

GEOMETRIC RE-STATEMENT OF THEOREM 8.13

In this subsection, we assume that the reader is familiar with the notion of an algebraic variety over a field F (geometrically-reduced separated scheme of finite type over F). The functor $A \rightsquigarrow \mathrm{Spec}(A)$ is a contravariant equivalence from the category of étale algebras over F to the category of zero-dimensional algebraic varieties over F. In particular, all zero-dimensional algebraic varieties are affine. If $V = \mathrm{Spec}(A)$, then

$$\mathrm{Hom}_{F\text{-algebra}}(A, \Omega) \simeq \mathrm{Hom}_{\mathrm{Spec}(F)}(\mathrm{Spec}(\Omega), V) \stackrel{\mathrm{def}}{=} V(\Omega)$$

(set of points of V with coordinates in Ω).

THEOREM 8.15 *The functor $V \rightsquigarrow V(\Omega)$ is an equivalence from the category of zero-dimensional algebraic varieties over F to the category of finite continuous G-sets. Under this equivalence, connected varieties correspond to sets with a transitive action.*

PROOF. Combine Theorem 8.13 with the equivalence $A \rightsquigarrow \mathrm{Spec}(A)$. □

Comparison with the theory of covering spaces.

The reader should note the similarity of (8.13) and (8.15) with the following statement:

> Let F be a connected and locally simply connected topological space, and let $\pi:\Omega \to F$ be a universal covering space of F. Let G denote the group of covering transformations of Ω/F (the choice of a point $e \in \Omega$ determines an isomorphism of G with the fundamental group $\pi_1(F,\pi e)$). For a covering space E of F, let $\mathcal{F}(E)$ denote the set of covering maps $\Omega \to E$. Then $E \rightsquigarrow \mathcal{F}(E)$ is an equivalence from the category of covering spaces of F to the category of (right) G-sets.

For more on this, see the section on the étale fundamental group in my "Lectures on Étale Cohomology" and Szamuely, Tamás, Galois groups and fundamental groups. CUP, 2009.

ASIDE 8.16 (FOR THE EXPERTS) It is possible to define the "absolute Galois group" of a field F canonically and without assuming the axiom of choice. Consider the category of Artin motives over F (Milne and Deligne 1982, §6). This is a Tannakian category equivalent to the category of sheaves S of $\mathbb{Q}$-vector spaces on $\mathrm{Spec}(F)_{\mathrm{et}}$ such that $S(A)$ is a finite-dimensional vector space for all A and the dimension of $S(K)$, K a field, is bounded. Define the absolute Galois group π of F to be the fundamental group of this category — this is an affine group scheme in the category (Deligne 1989, Le groupe fondamental ..., §6). For any choice of a separable closure F^{sep} of F, we get a fibre functor ω on the category and $\omega(\pi) = \mathrm{Gal}(F^{\mathrm{sep}}/F)$. See Julian Rosen, A choice-free absolute Galois group and Artin motives, arXiv:1706.06573.

CHAPTER 9

Transcendental Extensions

In this chapter we consider fields $\Omega \supset F$ with Ω much bigger than F. For example, we could have $\mathbb{C} \supset \mathbb{Q}$.

Algebraic independence

Elements $\alpha_1, ..., \alpha_n$ of Ω give rise to an F-homomorphism

$$f \mapsto f(\alpha_1, ..., \alpha_n) : F[X_1, \dots, X_n] \to \Omega.$$

If the kernel of this homomorphism is zero, then the α_i are said to be ***algebraically independent*** over F, and otherwise, they are ***algebraically dependent*** over F. Thus, the α_i are algebraically dependent over F if there exists a nonzero polynomial $f(X_1, ..., X_n) \in F[X_1, ..., X_n]$ such that $f(\alpha_1, ..., \alpha_n) = 0$, and they are algebraically independent if

$$a_{i_1,...,i_n} \in F, \quad \sum a_{i_1,...,i_n} \alpha_1^{i_1} ... \alpha_n^{i_n} = 0 \implies a_{i_1,...,i_n} = 0 \text{ all } i_1, ..., i_n.$$

Note the similarity with linear independence. In fact, if f is required to be homogeneous of degree 1, then the definition becomes that of linear independence.

EXAMPLE 9.1 (a) A single element α is algebraically independent over F if and only if it is transcendental over F.

(b) The complex numbers π and e are almost certainly algebraically independent over $\mathbb{Q}$, but this has not been proved.

An infinite set A is ***algebraically independent*** over F if every finite subset of A is algebraically independent; otherwise, it is ***algebraically dependent*** over F.

REMARK 9.2 If $\alpha_1, ..., \alpha_n$ are algebraically independent over F, then the map

$$f(X_1, ..., X_n) \mapsto f(\alpha_1, ..., \alpha_n) : F[X_1, ..., X_n] \to F[\alpha_1, ..., \alpha_n]$$

is an injection, and hence an isomorphism. This isomorphism then extends to the fields of fractions,

$$X_i \mapsto \alpha_i : F(X_1, ..., X_n) \to F(\alpha_1, ..., \alpha_n)$$

In this case, $F(\alpha_1, ..., \alpha_n)$ is called a ***pure transcendental extension*** of F. The polynomial

$$f(X) = X^n - \alpha_1 X^{n-1} + \cdots + (-1)^n \alpha_n$$

has Galois group S_n over $F(\alpha_1, ..., \alpha_n)$ (see 5.40).

LEMMA 9.3 *Let $\gamma \in \Omega$ and let $A \subset \Omega$. The following conditions are equivalent:*

(a) *γ is algebraic over $F(A)$;*

(b) *there exist $\beta_1, \dots, \beta_n \in F(A)$ such that $\gamma^n + \beta_1\gamma^{n-1} + \cdots + \beta_n = 0$;*

(c) *there exist $\beta_0, \beta_1, \dots, \beta_n \in F[A]$, not all 0, such that $\beta_0\gamma^n + \beta_1\gamma^{n-1} + \cdots + \beta_n = 0$;*

(d) *there exists an $f(X_1, \dots, X_m, Y) \in F[X_1 \dots, X_m, Y]$ and $\alpha_1, \dots, \alpha_m \in A$ such that $f(\alpha_1, \dots, \alpha_m, Y) \neq 0$ but $f(\alpha_1, \dots, \alpha_m, \gamma) = 0$.*

PROOF. (a) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (a) are obvious.

(d) $\Longrightarrow$ (c). Write $f(X_1, \dots, X_m, Y)$ as a polynomial in Y with coefficients in the ring $F[X_1, \dots, X_m]$,

$$f(X_1, \dots, X_m, Y) = \sum f_i(X_1, \dots, X_m)Y^{n-i}.$$

Then (c) holds with $\beta_i = f_i(\alpha_1, \dots, \alpha_m)$.

(c) $\Longrightarrow$ (d). The β_i in (c) can be expressed as polynomials in a finite number of elements $\alpha_1, \dots, \alpha_m$ of A, say, $\beta_i = f_i(\alpha_1, \dots, \alpha_m)$ with $f_i \in F[X_1, \dots, X_m]$. Then (d) holds with $f = \sum f_i(X_1, \dots, X_m)Y^{n-i}$. □

DEFINITION 9.4 When γ satisfies the equivalent conditions of Lemma 9.3, it is said to be ***algebraically dependent*** on A (over F). A set B is ***algebraically dependent*** on A if each element of B is algebraically dependent on A.

The theory in the remainder of this chapter is logically very similar to a part of linear algebra. It is useful to keep the following correspondences in mind:

Linear algebra	Transcendence
linearly independent	algebraically independent
$A \subset \text{span}(B)$	A algebraically dependent on B
basis	transcendence basis
dimension	transcendence degree

Transcendence bases

THEOREM 9.5 (FUNDAMENTAL RESULT) *Let $A = \{\alpha_1, ..., \alpha_m\}$ and $B = \{\beta_1, ..., \beta_n\}$ be two subsets of Ω. Assume*

(a) *A is algebraically independent (over F);*

(b) *A is algebraically dependent on B (over F).*

Then $m \leq n$.

We first prove two lemmas.

LEMMA 9.6 (THE EXCHANGE PROPERTY) *Let $\{\alpha_1, ..., \alpha_m\}$ be a subset of Ω; if β is algebraically dependent on $\{\alpha_1, ..., \alpha_m\}$ but not on $\{\alpha_1, ..., \alpha_{m-1}\}$, then α_m is algebraically dependent on $\{\alpha_1, ..., \alpha_{m-1}, \beta\}$.*

PROOF. Because β is algebraically dependent on $\{\alpha_1, \dots, \alpha_m\}$, there exists a polynomial $f(X_1, ..., X_m, Y)$ with coefficients in F such that

$$f(\alpha_1, ..., \alpha_m, Y) \neq 0, \quad f(\alpha_1, ..., \alpha_m, \beta) = 0.$$

Write f as a polynomial in X_m,

$$f(X_1,...,X_m,Y) = \sum_i a_i(X_1,...,X_{m-1},Y)X_m^{n-i},$$

and observe that, because $f(\alpha_1,\dots,\alpha_m,Y) \neq 0$, at least one of the polynomials

$$a_i(\alpha_1,...,\alpha_{m-1},Y),$$

say a_{i_0}, is not the zero polynomial. Because β is not algebraically dependent on

$$\{\alpha_1,...,\alpha_{m-1}\},$$

$a_{i_0}(\alpha_1,...,\alpha_{m-1},\beta) \neq 0$. Therefore, $f(\alpha_1,...,\alpha_{m-1},X_m,\beta) \neq 0$. Since $f(\alpha_1,...,\alpha_m,\beta) = 0$, this shows that α_m is algebraically dependent on $\{\alpha_1,...,\alpha_{m-1},\beta\}$. □

LEMMA 9.7 (TRANSITIVITY OF ALGEBRAIC DEPENDENCE) *If C is algebraically dependent on B, and B is algebraically dependent on A, then C is algebraically dependent on A.*

PROOF. The argument in the proof of Proposition 1.44 shows that if γ is algebraic over a field E which is algebraic over a field F, then γ is algebraic over F (if $a_1,\dots,a_n$ are the coefficients of the minimum polynomial of γ over E, then the field $F[a_1,\dots,a_n,\gamma]$ has finite degree over F). Apply this with $E = F(A \cup B)$ and $F = F(A)$. □

PROOF (OF THEOREM 9.5) Let k be the number of elements that A and B have in common. If $k = m$, then $A \subset B$, and certainly $m \leq n$. Suppose that $k < m$, and write $B = \{\alpha_1,...,\alpha_k,\beta_{k+1},...,\beta_n\}$. Since α_{k+1} is algebraically dependent on $\{\alpha_1,...,\alpha_k,\beta_{k+1},...,\beta_n\}$ but not on $\{\alpha_1,...,\alpha_k\}$, there will be a β_j, $k+1 \leq j \leq n$, such that α_{k+1} is algebraically dependent on $\{\alpha_1,...,\alpha_k,\beta_{k+1},...,\beta_j\}$ but not

$$\{\alpha_1,...,\alpha_k,\beta_{k+1},...,\beta_{j-1}\}.$$

The exchange lemma then shows that β_j is algebraically dependent on

$$B_1 \stackrel{\text{def}}{=} B \cup \{\alpha_{k+1}\} \smallsetminus \{\beta_j\}.$$

Therefore B is algebraically dependent on B_1, and so A is algebraically dependent on B_1 (by 9.7). If $k+1 < m$, repeat the argument with A and B_1. Eventually we'll achieve $k = m$, and $m \leq n$. □

DEFINITION 9.8 A ***transcendence basis*** for Ω over F is an algebraically independent set A such that Ω is algebraic over $F(A)$.

LEMMA 9.9 *If Ω is algebraic over $F(A)$, and A is minimal among subsets of Ω with this property, then it is a transcendence basis for Ω over F.*

PROOF. If A is not algebraically independent, then there is an $\alpha \in A$ that is algebraically dependent on $A \smallsetminus \{\alpha\}$. It follows from Lemma 9.7 that Ω is algebraic over $F(A \smallsetminus \{\alpha\})$. □

THEOREM 9.10 *If there is a finite subset $A \subset \Omega$ such that Ω is algebraic over $F(A)$, then Ω has a finite transcendence basis over F. Moreover, every transcendence basis is finite, and they all have the same number of elements.*

PROOF. In fact, every minimal subset A' of A such that Ω is algebraic over $F(A')$ will be a transcendence basis. The second statement follows from Theorem 9.5. □

LEMMA 9.11 *Suppose that A is algebraically independent, but that $A \cup \{\beta\}$ is algebraically dependent. Then β is algebraic over $F(A)$.*

PROOF. The hypothesis is that there exists a nonzero polynomial

$$f(X_1, ..., X_n, Y) \in F[X_1, ..., X_n, Y]$$

such that $f(\alpha_1, ..., \alpha_n, \beta) = 0$, some distinct $\alpha_1, ..., \alpha_n \in A$. Because A is algebraically independent, Y does occur in f. Therefore

$$f = g_0 Y^m + g_1 Y^{m-1} + \cdots + g_m, \quad g_i \in F[X_1, ..., X_n], \quad g_0 \neq 0, \quad m \geq 1.$$

As $g_0 \neq 0$ and the α_i are algebraically independent, $g_0(\alpha_1, ..., \alpha_n) \neq 0$. Because β is a root of

$$f = g_0(\alpha_1, ..., \alpha_n) X^m + g_1(\alpha_1, ..., \alpha_n) X^{m-1} + \cdots + g_m(\alpha_1, ..., \alpha_n),$$

it is algebraic over $F(\alpha_1, ..., \alpha_n) \subset F(A)$. □

PROPOSITION 9.12 *Every maximal algebraically independent subset of Ω is a transcendence basis for Ω over F.*

PROOF. We have to prove that Ω is algebraic over $F(A)$ if A is maximal among algebraically independent subsets. But the maximality implies that, for every $\beta \in \Omega \smallsetminus A$, $A \cup \{\beta\}$ is algebraically dependent, and so the lemma shows that β is algebraic over $F(A)$. □

Recall that (except in §7), we use an asterisk to signal a result depending on Zorn's lemma.

THEOREM 9.13 (*) *Every algebraically independent subset of Ω is contained in a transcendence basis for Ω over F; in particular, transcendence bases exist.*

PROOF. Let S be the set of algebraically independent subsets of Ω containing the given set. We can partially order it by inclusion. Let T be a totally ordered subset of S, and let $B = \bigcup\{A \mid A \in T\}$. I claim that $B \in S$, i.e., that B is algebraically independent. If not, there exists a finite subset B' of B that is not algebraically independent. But such a subset will be contained in one of the sets in T, which is a contradiction. Now Zorn's lemma shows that there exists a maximal algebraically independent containing S, which Proposition 9.12 shows to be a transcendence basis for Ω over F. □

It is possible to show that any two (possibly infinite) transcendence bases for Ω over F have the same cardinality. The cardinality of a transcendence basis for Ω over F is called the ***transcendence degree*** of Ω over F. For example, the pure transcendental extension $F(X_1, \ldots, X_n)$ has transcendence degree n over F.

EXAMPLE 9.14 Let $p_1, \ldots, p_n$ be the elementary symmetric polynomials in $X_1, \ldots, X_n$. The field $F(X_1, \ldots, X_n)$ is algebraic over $F(p_1, \ldots, p_n)$, and so $\{p_1, p_2, \ldots, p_n\}$ contains a transcendence basis for $F(X_1, \ldots, X_n)$. Because $F(X_1, \ldots, X_n)$ has transcendence degree n, the p_i's must themselves be a transcendence basis.

EXAMPLE 9.15 Let Ω be the field of meromorphic functions on a compact complex manifold M.

(a) The only meromorphic functions on the Riemann sphere are the rational functions in z. Hence, in this case, Ω is a pure transcendental extension of $\mathbb{C}$ of transcendence degree 1.

(b) If M is a Riemann surface, then the transcendence degree of Ω over $\mathbb{C}$ is 1, and Ω is a pure transcendental extension of $\mathbb{C} \iff M$ is isomorphic to the Riemann sphere

(c) If M has complex dimension n, then the transcendence degree is $\leq n$, with equality holding if M is embeddable in some projective space.

PROPOSITION 9.16 *Any two algebraically closed fields with the same transcendence degree over F are F-isomorphic.*

PROOF. Choose transcendence bases A and A' for the two fields. By assumption, there exists a bijection $A \to A'$, which extends uniquely to an F-isomorphism $F[A] \to F[A']$, and hence to an F-isomorphism of the fields of fractions $F(A) \to F(A')$. Use this isomorphism to identify $F(A)$ with $F(A')$. Then the two fields in question are algebraic closures of the same field, and hence are isomorphic (Theorem 6.8). □

REMARK 9.17 Any two algebraically closed fields with the same uncountable cardinality and the same characteristic are isomorphic. The idea of the proof is as follows. Let F and F' be the prime subfields of Ω and Ω'; we can identify F with F'. Then show that when Ω is uncountable, the cardinality of Ω is the same as the cardinality of a transcendence basis over F. Finally, apply the proposition.

REMARK 9.18 What are the automorphisms of $\mathbb{C}$? There are only two continuous automorphisms (cf. Exercise A-8 and solution). If we assume Zorn's lemma, then it is easy to construct many: choose any transcendence basis A for $\mathbb{C}$ over $\mathbb{Q}$, and choose any permutation α of A; then α defines an isomorphism $\mathbb{Q}(A) \to \mathbb{Q}(A)$ that can be extended to an automorphism of $\mathbb{C}$. Without Zorn's lemma, there are only two, because the noncontinuous automorphisms are nonmeasurable,[1] and it is known that the Zorn's lemma is required to construct nonmeasurable functions.[2]

Lüroth's theorem

THEOREM 9.19 (LÜROTH) *Let $L = F(X)$ with X transcendental over F. Every subfield E of L properly containing F is of the form $E = F(u)$ for some $u \in L$ transcendental over F.*

We first sketch a geometric proof of Lüroth's theorem. The inclusion of E into L corresponds to a map from the projective line $\mathbb{P}^1$ onto a complete regular curve C. Now the Riemann-Hurwitz formula shows that C has genus 0. Since it has an F-rational point (the image of any F-rational point of $\mathbb{P}^1$), it is isomorphic to $\mathbb{P}^1$. Therefore $E = F(u)$ for some $u \in L$ transcendental over F.

Before giving the elementary proof, we review Gauss's lemma and its consequences.

[1] A fairly elementary theorem of G. Mackey says that measurable homomorphisms of Lie groups are continuous (see Theorem B.3, p. 198 of Zimmer, Robert J., Ergodic theory and semisimple groups. Birkhäuser, 1984.)

[2] "We show that the existence of a non-Lebesgue measurable set cannot be proved in Zermelo-Frankel set theory (ZF) if use of the axiom of choice is disallowed..." R. Solovay, Ann. of Math., 92 (1970), 1–56.

GAUSS'S LEMMA

Let R be a unique factorization domain, and let Q be its field of fractions, for example, $R = F[X]$ and $Q = F(X)$. A polynomial $f(T) = \sum a_i T^i$ in $R[T]$ is said to be ***primitive*** if its coefficients a_i have no common factor other than units. Every polynomial f in $Q[X]$ can be written $f = c(f) \cdot f_1$ with $c(f) \in Q$ and f_1 primitive (write $f = af/a$ with a a common denominator for the coefficients of f, and then write $f = (b/a) f_1$ with b the greatest common divisor of the coefficients of af). The element $c(f)$ is uniquely determined up to a unit, and $f \in R[X]$ if and only if $c(f) \in R$.

9.20 *If $f, g \in R[T]$ are primitive, so also is fg.*

Let $f = \sum a_i T^i$ and $g = \sum b_i T^i$, and let p be a prime element of R. Because f is primitive, there exists a coefficient a_i not divisible by p — let a_{i_1} be the first such coefficient. Similarly, let b_{i_2} be the first coefficient of g not divisible by p. Then the coefficient of $T^{i_1+i_2}$ in fg is not divisible by p. This shows that fg is primitive.

9.21 *For any $f, g \in R[T]$, $c(fg) = c(f)c(g)$ and $(fg)_1 = f_1 g_1$.*

Let $f = c(f) f_1$ and $g = c(g) g_1$ with f_1 and g_1 primitive. Then $fg = c(f)c(g) f_1 g_1$ with $f_1 g_1$ primitive, and so $c(fg) = c(f)c(g)$ and $(fg)_1 = f_1 g_1$.

9.22 *Let f be a polynomial in $R[T]$. If f factors into the product of two nonconstant polynomials in $Q[T]$, then it factors into the product of two nonconstant polynomials in $R[T]$.*

Suppose that $f = gh$ in $Q[T]$. Then $f_1 = g_1 h_1$ in $R[T]$, and so $f = c(f) \cdot f_1 = (c(f) \cdot g_1) h_1$ with $c(f) \cdot g_1$ and h_1 in $R[T]$.

9.23 *Let $f, g \in R[T]$. If f divides g in $Q[T]$ and f is primitive, then it divides g in $R[T]$.*

Let $fq = g$ with $q \in Q[T]$. Then $c(q) = c(g) \in R$, and so $q \in R[T]$.

PROOF OF LÜROTH'S THEOREM

We define the degree $\deg(u)$ of an element u of $F(X)$ to be the larger of the degrees of the numerator and denominator of u when it is expressed in its simplest form.

LEMMA 9.24 *Let $u \in F(X) \smallsetminus F$. Then u is transcendental over F, X is algebraic over $F(u)$, and $[F(X) : F(u)] = \deg(u)$.*

PROOF. Let $u(X) = a(X)/b(X)$ with $a(X)$ and $b(X)$ relatively prime polynomials. Now $a(T) - b(T)u \in F(u)[T]$, and it has X as a root, and so X is algebraic over $F(u)$. It follows that u is transcendental over F (otherwise X would be algebraic over F; 1.31b).

The polynomial $a(T) - b(T)Z \in F[Z, T]$ is clearly irreducible. As u is transcendental over F,

$$F[Z, T] \simeq F[u, T], \quad Z \leftrightarrow u, \quad T \leftrightarrow T,$$

and so $a(T) - b(T)u$ is irreducible in $F[u, T]$, and hence also in $F(u)[T]$ by Gauss's lemma (9.22). It has X as a root, and so, up to a constant, it is the minimum polynomial of X over $F(u)$, and its degree is $\deg(u)$, which proves the lemma. □

EXAMPLE 9.25 We have $F(X) = F(u)$ if and if

$$u = \frac{aX+b}{cX+d}$$

with $ac \neq 0$ and neither $aX+b$ nor $cX+d$ a constant multiple of the other. These conditions are equivalent to $ad-bc \neq 0$.

We now prove Theorem 9.19. Let u be an element of E not in F. Then

$$[F(X)\colon E] \leq [F(X)\colon F(u)] = \deg(u),$$

and so X is algebraic over E. Let

$$f(T) = T^n + a_1 T^{n-1} + \cdots + a_n, \quad a_i \in E,$$

be its minimum polynomial. As X is transcendental over F, some $a_j \notin F$, and we'll show that $E = F(a_j)$.

Let $d(X) \in F[X]$ be a polynomial of least degree such that $d(X)a_i(X) \in F[X]$ for all i, and let

$$f_1(X,T) = df(T) = dT^n + da_1 T^{n-1} + \cdots + da_n \in F[X,T].$$

Then f_1 is primitive as a polynomial in T, i.e., $\gcd(d, da_1, \ldots, da_n) = 1$ in $F[X]$. The degree m of f_1 in X is the largest degree of one of the polynomials $da_1, da_2, \ldots$, say $m = \deg(da_i)$. Write $a_i = b/c$ with b, c relatively prime polynomials in $F[X]$. Now $b(T) - c(T)a_i(X)$ is a polynomial in $E[T]$ having X as a root, and so it is divisible by f, say

$$f(T)\cdot q(T) = b(T) - c(T)\cdot a_i(X), \quad q(T) \in E[T].$$

On multiplying through by $c(X)$, we find that

$$c(X)\cdot f(T)\cdot q(T) = c(X)\cdot b(T) - c(T)\cdot b(X).$$

As f_1 differs from f by a nonzero element of $F(X)$, the equation shows that f_1 divides $c(X)\cdot b(T) - c(T)\cdot b(X)$ in $F(X)[T]$. But f_1 is primitive in $F[X][T]$, and so it divides $c(X)\cdot b(T) - c(T)\cdot b(X)$ in $F[X][T] = F[X,T]$ (by 9.23), i.e., there exists a polynomial $h \in F[X,T]$ such that

$$f_1(X,T)\cdot h(X,T) = c(X)\cdot b(T) - c(T)\cdot b(X). \tag{18}$$

In (18), the polynomial $c(X)\cdot b(T) - c(T)\cdot b(X)$ has degree at most m in X, and m is the degree of $f_1(X,T)$ in X. Therefore, $c(X)\cdot b(T) - c(T)\cdot b(X)$ has degree exactly m in X, and $h(X,T)$ has degree 0 in X, i.e., $h \in F[T]$. It now follows from (18) that $c(X)\cdot b(T) - c(T)\cdot b(X)$ is not divisible by a nonconstant polynomial in $F[X]$.

The polynomial $c(X)\cdot b(T) - c(T)\cdot b(X)$ is symmetric in X and T, i.e., it is unchanged when they are swapped. Therefore, it has degree m in T and it is not divisible by a nonconstant polynomial in $F[T]$. It now follows from (18) that h is not divisible by a nonconstant polynomial in $F[T]$, and so it lies in $F^\times$. We conclude that $f_1(X,T)$ is a constant multiple of $c(X)\cdot b(T) - c(T)\cdot b(X)$.

On comparing degrees in T in (18), we see that $n = m$. Thus

$$[F(X)\colon F(a_i)] \overset{9.24}{=} \deg(a_i) \leq \deg(da_i) = m = n = [F(X)\colon E] \leq [F(X)\colon F(a_i)].$$

Hence, equality holds throughout, and so $E = F[a_i]$.

Finally, if $a_j \notin F$, then

$$[F(X):E] \leq [F(X):F(a_j)] \overset{9.24}{=} \deg(a_j) \leq \deg(da_j) \leq \deg(da_i) = m = [F(X):E],$$

and so $E = F(a_j)$ as claimed.

REMARK 9.26 Lüroth's theorem fails when there is more than one variable — see Zariski's example (footnote to Remark 5.5) and Swan's example (Remark 5.41). However, the following is true: if $[F(X,Y):E] < \infty$ and F is algebraically closed of characteristic zero, then E is a pure transcendental extension of F (Theorem of Zariski, 1958).

NOTES Lüroth proved his theorem over $\mathbb{C}$ in 1876. For general fields, it was proved by Steinitz in 1910, by the above argument.

Separating transcendence bases

Let $E \supset F$ be fields with E finitely generated over F. A subset $\{x_1,\dots,x_d\}$ of E is a ***separating transcendence basis*** for E/F if it is algebraically independent over F and E is a finite *separable* extension of $F(x_1,\dots,x_d)$.

THEOREM 9.27 *If F is perfect, then every finitely generated extension E of F admits a separating transcendence basis over F.*

PROOF. If F has characteristic zero, then every transcendence basis is separating, and so the statement becomes that of (9.10). Thus, we may assume F has characteristic $p \neq 0$. Because F is perfect, every polynomial in $X_1^p,\dots,X_n^p$ with coefficients in F is a pth power in $F[X_1,\dots,X_n]$:

$$\sum a_{i_1\cdots i_n} X_1^{i_1 p}\dots X_n^{i_n p} = \left(\sum a_{i_1\cdots i_n}^{\frac{1}{p}} X_1^{i_1}\dots X_n^{i_n}\right)^p.$$

Let $E = F(x_1,\dots,x_n)$, and assume $n > d+1$ where d is the transcendence degree of E over F. After renumbering, we may suppose that $x_1,\dots,x_d$ are algebraically independent (9.9). Then $f(x_1,\dots,x_{d+1}) = 0$ for some nonzero irreducible polynomial $f(X_1,\dots,X_{d+1})$ with coefficients in F. Not all $\partial f/\partial X_i$ are zero, for otherwise f would be a polynomial in $X_1^p,\dots,X_{d+1}^p$, which implies that it is a pth power. After renumbering $x_1,\dots,x_{d+1}$, we may suppose that $\partial f/\partial X_{d+1} \neq 0$. Then x_{d+1} is separably algebraic over $F(x_1,\dots,x_d)$ and $F(x_1,\dots,x_{d+1},x_{d+2})$ is algebraic over $F(x_1,\dots,x_{d+1})$, hence over $F(x_1,\dots,x_d)$ (1.31), and so, by the primitive element theorem (5.1), there is an element y such that $F(x_1,\dots,x_{d+2}) = F(x_1,\dots,x_d,y)$. Thus E is generated by $n-1$ elements (as a field containing F). After repeating the process, possibly several times, we will have $E = F(z_1,\dots,z_{d+1})$ with z_{d+1} separable over $F(z_1,\dots,z_d)$. □

ASIDE 9.28 In fact, we showed that E admits a separating transcendence basis with $d+1$ elements where d is the transcendence degree. This has the following geometric interpretation: every irreducible algebraic variety of dimension d over a perfect field F is birationally equivalent with a hypersurface H in $\mathbb{A}^{d+1}$ for which the projection $(a_1,\dots,a_{d+1}) \mapsto (a_1,\dots,a_d)$ realizes $F(H)$ as a finite separable extension of $F(\mathbb{A}^d)$ (see my notes on Algebraic Geometry).

Transcendental Galois theory

THEOREM 9.29 *Let Ω be an algebraically closed field and let F be a perfect subfield of Ω. If $\alpha \in \Omega$ is fixed by all F-automorphisms of Ω, then $\alpha \in F$, i.e., $\Omega^{\mathrm{Aut}(\Omega/F)} = F$.*

PROOF. Let $\alpha \in \Omega \smallsetminus F$. If α is algebraic over F, then there is an F-homomorphism $F[\alpha] \to \Omega$ sending α to a conjugate of α in Ω different from α. This homomorphism extends to a homomorphism from the algebraic closure F^{al} of F in Ω to Ω (by 6.8). Now choose a transcendence basis A for Ω over F^{al}. We can extend our homomorphism to a homomorphism $F(A) \to \Omega$ by mapping each element of A to itself. Finally, we can extend this homomorphism to a homomorphism from the algebraic closure Ω of $F(A)$ to Ω. The F-homomorphism $\Omega \to \Omega$ we obtain is automatically an isomorphism (cf. 6.8).

If α is transcendental over F, then it is part of a transcendence basis A for Ω over F (see 9.13). If A has at least two elements, then there exists an automorphism σ of A such that $\sigma(\alpha) \neq \alpha$. Now σ defines an F-homomorphism $F(A) \to \Omega$, which extends to an isomorphism $\Omega \to \Omega$ as before. If $A = \{\alpha\}$, then we let $F(\alpha) \to \Omega$ be the F-homomorphism sending α to $\alpha + 1$. Again, this extends to an isomorphism $\Omega \to \Omega$. □

Let $\Omega \supset F$ be fields and let $G = \mathrm{Aut}(\Omega/F)$. For any finite subset S of Ω, let

$$G(S) = \{\sigma \in G \mid \sigma s = s \text{ for all } s \in S\}.$$

Then, as in §7, the subgroups $G(S)$ of G form a neighbourhood base for a unique topology on G, which we again call the ***Krull topology***. The same argument as in §7 shows that this topology is Hausdorff (but it is not necessarily compact).

THEOREM 9.31 *Let $\Omega \supset F$ be fields such that $\Omega^G = F$, $G = \mathrm{Aut}(\Omega/F)$.*

(a) For every finite extension E of F in Ω, $\Omega^{\mathrm{Aut}(\Omega/E)} = E$.

(b) The maps

$$H \mapsto \Omega^H, \quad M \mapsto \mathrm{Aut}(\Omega/M) \tag{19}$$

are inverse bijections between the set of compact subgroups of G and the set of intermediate fields over which Ω is Galois (possibly infinite):

$$\{\text{compact subgroups of } G\} \leftrightarrow \{\text{fields } M \text{ such that } F \subset M \overset{\text{Galois}}{\subset} \Omega\}.$$

(c) If there exists an M finitely generated over F such that Ω is Galois over M, then G is locally compact, and under (19):

$$\{\text{open compact subgroups of } G\} \overset{1:1}{\leftrightarrow} \{\text{fields } M \text{ such that } F \overset{\text{finitely generated}}{\subset} M \overset{\text{Galois}}{\subset} \Omega\}.$$

(d) Let H be a subgroup of G, and let $M = \Omega^H$. Then the algebraic closure M_1 of M is Galois over M. If moreover $H = \mathrm{Aut}(\Omega/M)$, then $\mathrm{Aut}(\Omega/M_1)$ is a normal subgroup of H, and $\sigma \mapsto \sigma|M_1$ maps $H/\mathrm{Aut}(\Omega/M_1)$ isomorphically onto a dense subgroup of $\mathrm{Aut}(M_1/M)$.

PROOF. See 6.3 of Shimura, Goro., Introduction to the arithmetic theory of automorphic functions. Princeton, 1971. □

Exercises

9-1 Find the centralizer of complex conjugation in $\mathrm{Aut}(\mathbb{C}/\mathbb{Q})$.

APPENDIX **A**

Review Exercises

A-1 Let p be a prime number, and let m and n be positive integers.

(a) Give necessary and sufficient conditions on m and n for $\mathbb{F}_{p^n}$ to have a subfield isomorphic with $\mathbb{F}_{p^m}$. Prove your answer.

(b) If there is such a subfield, how many subfields isomorphic with $\mathbb{F}_{p^m}$ are there, and why?

A-2 Show that the Galois group of the splitting field F of $X^3 - 7$ over $\mathbb{Q}$ is isomorphic to S_3, and exhibit the fields between $\mathbb{Q}$ and F. Which of the fields between $\mathbb{Q}$ and F are normal over $\mathbb{Q}$?

A-3 Prove that the two fields $\mathbb{Q}[\sqrt{7}]$ and $\mathbb{Q}[\sqrt{11}]$ are not isomorphic.

A-4 (a) Prove that the multiplicative group of all nonzero elements in a finite field is cyclic.

(b) Construct explicitly a field of order 9, and exhibit a generator for its multiplicative group.

A-5 Let X be transcendental over a field F, and let E be a subfield of $F(X)$ properly containing F. Prove that X is algebraic over E.

A-6 Prove as directly as you can that if ζ is a primitive pth root of 1, p prime, then the Galois group of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$ is cyclic of order $p - 1$.

A-7 Let G be the Galois group of the polynomial $X^5 - 2$ over $\mathbb{Q}$.

(a) Determine the order of G.

(b) Determine whether G is abelian.

(c) Determine whether G is solvable.

A-8 (a) Show that every field homomorphism from $\mathbb{R}$ to $\mathbb{R}$ is bijective.

(b) Prove that $\mathbb{C}$ is isomorphic to infinitely many different subfields of itself.

A-9 Let F be a field with 16 elements. How many roots in F does each of the following polynomials have? $X^3 - 1$; $X^4 - 1$; $X^{15} - 1$; $X^{17} - 1$.

A-10 Find the degree of a splitting field of the polynomial $(X^3 - 5)(X^3 - 7)$ over $\mathbb{Q}$.

A-11 Find the Galois group of the polynomial $X^6 - 5$ over each of the fields $\mathbb{Q}$ and $\mathbb{R}$.

A-12 The coefficients of a polynomial $f(X)$ are algebraic over a field F. Show that $f(X)$ divides some nonzero polynomial $g(X)$ with coefficients in F.

A-13 Let $f(X)$ be a polynomial in $F[X]$ of degree n, and let E be a splitting field of f. Show that $[E:F]$ divides $n!$.

A-14 Find a primitive element for the field $\mathbb{Q}[\sqrt{3},\sqrt{7}]$ over $\mathbb{Q}$, i.e., an element such that $\mathbb{Q}[\sqrt{3},\sqrt{7}] = \mathbb{Q}[\alpha]$.

A-15 Let G be the Galois group of $(X^4-2)(X^3-5)$ over $\mathbb{Q}$.

(a) Give a set of generators for G, as well as a set of defining relations.

(b) What is the structure of G as an abstract group (is it cyclic, dihedral, alternating, symmetric, etc.)?

A-16 Let F be a finite field of characteristic $\neq 2$. Prove that $X^2 = -1$ has a solution in F if and only if $|F| \equiv 1 \mod 4$.

A-17 Let E be the splitting field over $\mathbb{Q}$ of $(X^2-2)(X^2-5)(X^2-7)$. Find an element α in E such that $E = \mathbb{Q}[\alpha]$. (You must prove that $E = \mathbb{Q}[\alpha]$.)

A-18 Let E be a Galois extension of F with Galois group S_n, $n > 1$ not prime. Let H_1 be the subgroup of S_n of elements fixing 1, and let H_2 be the subgroup generated by the cycle $(123\ldots n)$. Let $E_i = E^{H_i}$, $i = 1,2$. Find the degrees of E_1, E_2, $E_1 \cap E_2$, and E_1E_2 over F. Show that there exists a field M such that $F \subset M \subset E_2$, $M \neq F$, $M \neq E_2$, but that no such field exists for E_1.

A-19 Let ζ be a primitive 12th root of 1 over $\mathbb{Q}$. How many fields are there strictly between $\mathbb{Q}[\zeta^3]$ and $\mathbb{Q}[\zeta]$.

A-20 For the polynomial X^3-3, find explicitly its splitting field over $\mathbb{Q}$ and elements that generate its Galois group.

A-21 Let $E = \mathbb{Q}[\zeta]$, $\zeta^5 = 1$, $\zeta \neq 1$. Show that $i \notin E$, and that if $L = E[i]$, then -1 is a norm from L to E. Here $i = \sqrt{-1}$.

A-22 Let E be an extension field of F, and let Ω be an algebraic closure of E. Let $\sigma_1,\ldots,\sigma_n$ be distinct F-isomorphisms $E \to \Omega$.

(a) Show that $\sigma_1,\ldots,\sigma_n$ are linearly dependent over Ω.

(b) Show that $[E:F] \geq m$.

(c) Let F have characteristic $p > 0$, and let L be a subfield of Ω containing E and such that $a^p \in E$ for all $a \in L$. Show that each σ_i has a unique extension to a homomorphism $\sigma_i' : L \to \Omega$.

A-23 Identify the Galois group of the splitting field F of X^4-3 over $\mathbb{Q}$. Determine the number of quadratic subfields.

A-24 Let F be a subfield of a finite field E. Prove that the trace map $T = \mathrm{Tr}_{E/F}$ and the norm map $N = \mathrm{Nm}_{E/F}$ of E over F both map E *onto* F. (You may quote basic properties of finite fields and the trace and norm.)

A-25 Prove or disprove by counterexample.

(a) If L/F is an extension of fields of degree 2, then there is an automorphism σ of L such that F is the fixed field of σ.

(b) The same as (a) except that L is also given to be finite.

A-26 A finite Galois extension L of a field K has degree 8100. Show that there is a field F with $K \subset F \subset L$ such that $[F:K] = 100$.

A-27 An algebraic extension L of a field K of characteristic 0 is generated by an element θ that is a root of both of the polynomials $X^3 - 1$ and $X^4 + X^2 + 1$. Given that $L \neq K$, find the minimum polynomial of θ.

A-28 Let $F/\mathbb{Q}$ be a Galois extension of degree 3^n, $n \geq 1$. Prove that there is a chain of fields

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots F_n = F$$

such that for every i, $0 \leq i \leq n-1$, $[F_{i+1}:F_i] = 3$.

A-29 Let L be the splitting field over $\mathbb{Q}$ of an equation of degree 5 with distinct roots. Suppose that L has an automorphism that fixes three of these roots while interchanging the other two and also an automorphism $\alpha \neq 1$ of order 5.

(a) Prove that the group of automorphisms of L is the symmetric group on 5 elements.

(b) How many proper subfields of L are normal extensions of $\mathbb{Q}$? For each such field F, what is $[F:\mathbb{Q}]$?

A-30 If L/K is a separable algebraic field extension of finite degree d, show that the number of fields between K and L is at most $2^{d!}$. [This is far from best possible. See math.stackexchange.com, question 522976.]

A-31 Let K be the splitting field over $\mathbb{Q}$ of $X^5 - 1$. Describe the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of K over $\mathbb{Q}$, and show that K has exactly one subfield of degree 2 over $\mathbb{Q}$, namely, $\mathbb{Q}[\zeta + \zeta^4]$, $\zeta \neq 1$ a root of $X^5 - 1$. Find the minimum polynomial of $\zeta + \zeta^4$ over $\mathbb{Q}$. Find $\mathrm{Gal}(L/\mathbb{Q})$ when L is the splitting field over $\mathbb{Q}$ of

(a) $(X^2 - 5)(X^5 - 1)$;

(b) $(X^2 + 3)(X^5 - 1)$.

A-32 Let Ω_1 and Ω_2 be algebraically closed fields of transcendence degree 5 over $\mathbb{Q}$, and let $\alpha: \Omega_1 \to \Omega_2$ be a homomorphism (in particular, $\alpha(1) = 1$). Show that α is a bijection. (State carefully all theorems you use.)

A-33 Find the group of $\mathbb{Q}$-automorphisms of the field $k = \mathbb{Q}[\sqrt{-3}, \sqrt{-2}]$.

A-34 Prove that the polynomial $f(X) = X^3 - 5$ is irreducible over the field $\mathbb{Q}[\sqrt{7}]$. If L is the splitting field of $f(X)$ over $\mathbb{Q}[\sqrt{7}]$, prove that the Galois group of $L/\mathbb{Q}[\sqrt{7}]$ is isomorphic to S_3. Prove that there must exist a subfield K of L such that the Galois group of L/K is cyclic of order 3.

A-35 Identify the Galois group G of the polynomial $f(X) = X^5 - 6X^4 + 3$ over F, when (a) $F = \mathbb{Q}$ and when (b) $F = \mathbb{F}_2$. In each case, if E is the splitting field of $f(X)$ over F, determine how many fields K there are such that $E \supset K \supset F$ with $[K:F] = 2$.

A-36 Let K be a field of characteristic p, say with p^n elements, and let θ be the automorphism of K that maps every element to its pth power. Show that there exists an automorphism α of K such that $\theta\alpha^2 = 1$ if and only if n is odd.

A-37 Describe the splitting field and Galois group, over $\mathbb{Q}$, of the polynomial $X^5 - 9$.

A-38 Suppose that E is a Galois field extension of a field F such that $[E: F] = 5^3 \cdot (43)^2$. Prove that there exist fields K_1 and K_2 lying strictly between F and E with the following properties: (i) each K_i is a Galois extension of F; (ii) $K_1 \cap K_2 = F$; and (iii) $K_1 K_2 = E$.

A-39 Let $F = \mathbb{F}_p$ for some prime p. Let m be a positive integer not divisible by p, and let K be the splitting field of $X^m - 1$. Find $[K: F]$ and prove that your answer is correct.

A-40 Let F be a field of 81 elements. For each of the following polynomials $g(X)$, determine the number of roots of $g(X)$ that lie in F: $X^{80} - 1$, $X^{81} - 1$, $X^{88} - 1$.

A-41 Describe the Galois group of the polynomial $X^6 - 7$ over $\mathbb{Q}$.

A-42 Let K be a field of characteristic $p > 0$ and let $F = K(u, v)$ be a field extension of degree p^2 such that $u^p \in K$ and $v^p \in K$. Prove that K is not finite, that F is not a simple extension of K, and that there exist infinitely many intermediate fields $F \supset L \supset K$.

A-43 Find the splitting field and Galois group of the polynomial $X^3 - 5$ over the field $\mathbb{Q}[\sqrt{2}]$.

A-44 For every prime p, find the Galois group over $\mathbb{Q}$ of the polynomial $X^5 - 5p^4 X + p$.

A-45 Factorize $X^4 + 1$ over each of the finite fields (a) $\mathbb{F}_5$; (b) $\mathbb{F}_{25}$; and (c) $\mathbb{F}_{125}$. Find its splitting field in each case.

A-46 Let $\mathbb{Q}[\alpha]$ be a field of finite degree over $\mathbb{Q}$. Assume that there is a $q \in \mathbb{Q}$, $q \neq 0$, such that $|\rho(\alpha)| = q$ for all homomorphisms $\rho: \mathbb{Q}[\alpha] \to \mathbb{C}$. Show that the set of roots of the minimum polynomial of α is the same as that of q^2/α. Deduce that there exists an automorphism σ of $\mathbb{Q}[\alpha]$ such that

(a) $\sigma^2 = 1$ and

(b) $\rho(\sigma\gamma) = \overline{\rho(\gamma)}$ for all $\gamma \in \mathbb{Q}[\alpha]$ and $\rho: \mathbb{Q}[\alpha] \to \mathbb{C}$.

A-47 Let F be a field of characteristic zero, and let p be a prime number. Suppose that F has the property that all irreducible polynomials $f(X) \in F[X]$ have degree a power of p ($1 = p^0$ is allowed). Show that every equation $g(X) = 0$, $g \in F[X]$, is solvable by extracting radicals.

A-48 Let $K = \mathbb{Q}[\sqrt{5}, \sqrt{-7}]$ and let L be the splitting field over $\mathbb{Q}$ of $f(X) = X^3 - 10$.

(a) Determine the Galois groups of K and L over $\mathbb{Q}$.

(b) Decide whether K contains a root of f.

(c) Determine the degree of the field $K \cap L$ over $\mathbb{Q}$.

[Assume all fields are subfields of $\mathbb{C}$.]

A-49 Find the splitting field (over $\mathbb{F}_p$) of $X^{p^r} - X \in \mathbb{F}_p[X]$, and deduce that $X^{p^r} - X$ has an irreducible factor $f \in \mathbb{F}_p[X]$ of degree r. Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial that becomes equal to $f(X)$ when its coefficients are read modulo p. Show that $g(X)$ is irreducible in $\mathbb{Q}[X]$.

A-50 Let E be the splitting field of $X^3 - 51$ over $\mathbb{Q}$. List all the subfields of E, and find an element γ of E such that $E = \mathbb{Q}[\gamma]$.

A-51 Let $k = \mathbb{F}_{1024}$ be the field with 1024 elements, and let K be an extension of k of degree 2. Prove that there is a unique automorphism σ of K of order 2 which leaves k elementwise fixed and determine the number of elements of $K^\times$ such that $\sigma(x) = x^{-1}$.

A-52 Let F and E be finite fields of the same characteristic. Prove or disprove these statements:

(a) There is a ring homomorphism of F into E if and only if $|E|$ is a power of $|F|$.

(b) There is an injective group homomorphism of the multiplicative group of F into the multiplicative group of E if and only if $|E|$ is a power of $|F|$.

A-53 Let L/K be an algebraic extension of fields. Prove that L is algebraically closed if every polynomial over K factors completely over L.

A-54 Let K be a field, and let $M = K(X)$, X an indeterminate. Let L be an intermediate field different from K. Prove that M is finite-dimensional over L.

A-55 Let $\theta_1, \theta_2, \theta_3$ be the roots of the polynomial $f(X) = X^3 + X^2 - 9X + 1$.

(a) Show that the θ_i are real, nonrational, and distinct.

(b) Explain why the Galois group of $f(X)$ over $\mathbb{Q}$ must be either A_3 or S_3. Without carrying it out, give a brief description of a method for deciding which it is.

(c) Show that the rows of the matrix

$$\begin{pmatrix} 3 & 9 & 9 & 9 \\ 3 & \theta_1 & \theta_2 & \theta_3 \\ 3 & \theta_2 & \theta_3 & \theta_1 \\ 3 & \theta_3 & \theta_1 & \theta_2 \end{pmatrix}$$

are pairwise orthogonal; compute their lengths, and compute the determinant of the matrix.

A-56 Let E/K be a Galois extension of degree p^2q where p and q are primes, $q < p$ and q not dividing $p^2 - 1$. Prove that:

(a) there exist intermediate fields L and M such that $[L\colon K] = p^2$ and $[M\colon K] = q$;

(b) such fields L and M must be Galois over K; and

(c) the Galois group of E/K must be abelian.

A-57 Let ζ be a primitive 7th root of 1 (in $\mathbb{C}$).

(a) Prove that $1 + X + X^2 + X^3 + X^4 + X^5 + X^6$ is the minimum polynomial of ζ over $\mathbb{Q}$.

(b) Find the minimum polynomial of $\zeta + \frac{1}{\zeta}$ over $\mathbb{Q}$.

A-58 Find the degree over $\mathbb{Q}$ of the Galois closure K of $\mathbb{Q}[2^{\frac{1}{4}}]$ and determine the isomorphism class of $\mathrm{Gal}(K/\mathbb{Q})$.

A-59 Let p, q be distinct positive prime numbers, and consider the extension $K = \mathbb{Q}[\sqrt{p}, \sqrt{q}] \supset \mathbb{Q}$.

(a) Prove that the Galois group is isomorphic to $C_2 \times C_2$.

(b) Prove that every subfield of K of degree 2 over $\mathbb{Q}$ is of the form $\mathbb{Q}[\sqrt{m}]$ where $m \in \{p, q, pq\}$.

(c) Show that there is an element $\gamma \in K$ such that $K = \mathbb{Q}[\gamma]$.

APPENDIX **B**

Two-hour Examination

1. (a) Let σ be an automorphism of a field E. If $\sigma^4 = 1$ and

$$\sigma(\alpha) + \sigma^3(\alpha) = \alpha + \sigma^2(\alpha) \qquad \text{all } \alpha \in E,$$

show that $\sigma^2 = 1$.
(b) Let p be a prime number and let a, b be rational numbers such that $a^2 + pb^2 = 1$. Show that there exist rational numbers c, d such that $a = \frac{c^2 - pd^2}{c^2 + pd^2}$ and $b = \frac{2cd}{c^2 + pd^2}$. !!Check!!

2. Let $f(X)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[X]$, and let $g(X)$ be the resolvent cubic of f. What is the relation between the Galois group of f and that of g? Find the Galois group of f if

(a) $g(X) = X^3 - 3X + 1$;

(b) $g(X) = X^3 + 3X + 1$.

3. (a) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{F}_2[X]$ have, and what are their degrees.
(b) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{Q}[X]$ have, and what are their degrees?

4. Let E be the splitting field of $(X^5 - 3)(X^5 - 7) \in \mathbb{Q}[X]$. What is the degree of E over $\mathbb{Q}$? How many proper subfields of E are there that are not contained in the splitting fields of both $X^5 - 3$ and $X^5 - 7$?
[You may assume that 7 is not a 5th power in the splitting field of $X^5 - 3$.]

5. Consider an extension $\Omega \supset F$ of fields. Define $a \in \Omega$ to be *F-constructible* if it is contained in a field of the form

$$F[\sqrt{a_1}, \ldots, \sqrt{a_n}], \qquad a_i \in F[\sqrt{a_1}, \ldots, \sqrt{a_{i-1}}].$$

Assume Ω is a finite Galois extension of F and construct a field E, $F \subset E \subset \Omega$, such that every $a \in \Omega$ is E-constructible and E is minimal with this property.

6. Let Ω be an extension field of a field F. Show that every F-homomorphism $\Omega \to \Omega$ is an isomorphism provided:

(a) Ω is algebraically closed, and

(b) Ω has finite transcendence degree over F.

Can either of the conditions (i) or (ii) be dropped? (Either prove, or give a counterexample.)

You should prove all answers. You may use results proved in class or in the notes, but you should indicate clearly what you are using.

Possibly useful facts: The discriminant of $X^3 + aX + b$ is $-4a^3 - 27b^2$ and $2^8 - 1 = 255 = 3 \times 5 \times 17$.

APPENDIX **C**

Solutions to the Exercises

These solutions fall somewhere between hints and complete solutions. Students were expected to write out complete solutions.

1-1. Similar to Example 1.28.

1-2. Verify that 3 is not a square in $\mathbb{Q}[\sqrt{2}]$, and so $[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}] = 4$.

1-3. (a) Apply the division algorithm, to get $f(X) = q(X)(X-a)+r(X)$ with $r(X)$ constant, and put $X = a$ to find $r = f(a)$.
(c) Use that factorization in $F[X]$ is unique (or use induction on the degree of f).
(d) If G had two cyclic factors C and C' whose orders were divisible by a prime p, then G would have (at least) p^2 elements of order dividing p. This doesn't happen, and it follows that G is cyclic.
(e) The elements of order m in $F^\times$ are the roots of the polynomial $X^m - 1$, and so there are at most m of them. Hence every finite subgroup G of $F^\times$ satisfies the condition in (d).

1-4. Note that it suffices to construct $\alpha = \cos\frac{2\pi}{7}$, and that $[\mathbb{Q}[\alpha]:\mathbb{Q}] = \frac{7-1}{2} = 3$, and so its minimum polynomial has degree 3 (see Example 3.21). There is a standard method (once taught in high schools) for solving cubics using the equation

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

By "completing the cube", reduce the cubic to the form $X^3 - pX - q$. Then construct a square root a of $\frac{4p}{3}$, so that $a^2 = \frac{4p}{3}$. Let 3θ be the angle such that $\cos 3\theta = \frac{4q}{a^3}$, and use the angle trisector to construct $\cos\theta$. From the displayed equation, we find that $\alpha = a\cos\theta$ is a root of $X^3 - pX - q$.

1-5. Let f_1 be an irreducible factor of f in $E[X]$, and let (L,α) be a stem field for f_1 over E. Then $m|[L:F]$ because $L \supset E$ (1.20). But $f(\alpha) = 0$, and so $(F[\alpha],\alpha)$ is a stem field for f over F, which implies that $[F[\alpha]:F] = n$. Now $n|[L:F]$ because $L \supset F[\alpha]$. We deduce that $[L:F] = mn$ and $[L:E] = n$. But $[L:E] = \deg(f_1)$, and so $f_1 = f$.

1-6. The polynomials $f(X)-1$ and $f(X)+1$ have only finitely many roots, and so there exists an $n \in \mathbb{Z}$ such that $f(n) \neq \pm 1$. Let p be a prime dividing $f(n)$. Then $f(n) = 0$ modulo p, and so f has a root in $\mathbb{F}_p$. Thus it is not irreducible in $\mathbb{F}_p[X]$.

2-1. (a) is obvious, as is the "only if" in (b). For the "if" note that for any $a \in S(E)$, $a \notin F^2$, $E \approx F[X]/(X^2-a)$.

(c) Take $E_i = \mathbb{Q}[\sqrt{p_i}]$ with p_i the ith prime. Check that p_i is the only prime that becomes a square in E_i. For this use that $(a+b\sqrt{p})^2 \in \mathbb{Q} \implies 2ab = 0$.

(d) Every field of characteristic p contains (an isomorphic copy of) $\mathbb{F}_p$, and so we are looking at the quadratic extensions of $\mathbb{F}_p$. The homomorphism $a \mapsto a^2 : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ has kernel $\{\pm 1\}$, and so its image has index 2 in $\mathbb{F}_p^\times$. Thus the only possibility for $S(E)$ is $\mathbb{F}_p^\times$, and so there is at most one E (up to $\mathbb{F}_p$-isomorphism). To get one, take $E = F[X]/(X^2 - a)$, $a \notin \mathbb{F}_p^2$.

2-2. (a) If α is a root of $f(X) = X^p - X - a$ (in some splitting field), then the remaining roots are $\alpha + 1, \dots, \alpha + p - 1$, which obviously lie in whichever field contains α. Moreover, they are distinct. Suppose that, in $F[X]$,

$$f(X) = (X^r + a_1 X^{r-1} + \cdots + a_r)(X^{p-r} + \cdots), \quad 0 < r < p.$$

Then $-a_1$ is a sum of r of the roots of f, $-a_1 = r\alpha + d$ some $d \in \mathbb{Z} \cdot 1_F$, and it follows that $\alpha \in F$.

(b) As 0 and 1 are not roots of $X^p - X - 1$ in $\mathbb{F}_p$ it can't have p distinct roots in $\mathbb{F}_p$, and so (a) implies that $X^p - X - 1$ is irreducible in $\mathbb{F}_p[X]$ and hence also in $\mathbb{Z}[X]$ and $\mathbb{Q}[X]$ (see 1.18, 1.13).

2-3. Let α be the real 5th root of 2. Eisenstein's criterion shows that $X^5 - 2$ is irreducible in $\mathbb{Q}[X]$, and so $\mathbb{Q}[\sqrt[5]{2}]$ has degree 5 over $\mathbb{Q}$. The remaining roots of $X^5 - 2$ are $\zeta\alpha, \zeta^2\alpha, \zeta^3\alpha, \zeta^4\alpha$, where ζ is a primitive 5th root of 1. It follows that the subfield of $\mathbb{C}$ generated by the roots of $X^5 - 2$ is $\mathbb{Q}[\zeta, \alpha]$. The degree of $\mathbb{Q}[\zeta, \alpha]$ is 20, since it must be divisible by $[\mathbb{Q}[\zeta] : \mathbb{Q}] = 4$ and $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 5$.

2-4. It's $\mathbb{F}_p$ because $X^{p^m} - 1 = (X - 1)^{p^m}$. (Perhaps I meant $X^{p^m} - X$ — that would have been more interesting.)

2-5. If $f(X) = \prod (X - \alpha_i)^{m_i}$, $\alpha_i \neq \alpha_j$, then

$$f'(X) = \sum m_i \frac{f(X)}{X - \alpha_i}$$

and so $d(X) = \prod_{m_i > 1} (X - \alpha_i)^{m_i - 1}$. Therefore $g(X) = \prod (X - \alpha_i)$.

2-6. From (2.12) we know that either f is separable or $f(X) = f_1(X^p)$ for some polynomial f_1. Clearly f_1 is also irreducible. If f_1 is not separable, it can be written $f_1(X) = f_2(X^p)$. Continue in the way until you arrive at a separable polynomial. For the final statement, note that $g(X) = \prod (X - a_i)$, $a_i \neq a_j$, and so $f(X) = g(X^{p^e}) = \prod (X - \alpha_i)^{p^e}$ with $\alpha_i^{p^e} = a_i$.

3-1. Let σ and τ be automorphisms of $F(X)$ given by $\sigma(X) = -X$ and $\tau(X) = 1 - X$. Then σ and τ fix X^2 and $X^2 - X$ respectively, and so $\sigma\tau$ fixes $E \stackrel{\text{def}}{=} F(X) \cap F(X^2 - X)$. But $\alpha\tau X = 1 + X$, and so $(\sigma\tau)^m(X) = m + X$. Thus $\mathrm{Aut}(F(X)/E)$ is infinite, which implies that $[F(X) : E]$ is infinite (otherwise $F(X) = E[\alpha_1, \dots, \alpha_n]$; an E-automorphism of $F(X)$ is determined by its values on the α_i, and its value on α_i is a root of the minimum polynomial of α_i). If E contains a polynomial $f(X)$ of degree $m > 0$, then $[F(X) : E] \leq [F(X) : F(f(X))] = m$ — contradiction.

3-2. Since $1 + \zeta + \cdots + \zeta^{p-1} = 0$, we have $\alpha + \beta = -1$. If $i \in H$, then $iH = H$ and $i(G \smallsetminus H) = G \smallsetminus H$, and so α and β are fixed by H. If $j \in G \smallsetminus H$, then $jH = G \smallsetminus H$ and $j(G \smallsetminus H) = H$, and so $j\alpha = \beta$ and $j\beta = \alpha$. Hence $\alpha\beta \in \mathbb{Q}$, and α and β are the roots of $X^2 + X + \alpha\beta$. Note that

$$\alpha\beta = \sum_{i,j} \zeta^{i+j}, \quad i \in H, \quad j \in G \smallsetminus H.$$

How many times do we have $i+j=0$? If $i+j=0$, then $-1=i^{-1}j$, which is a nonsquare; conversely, if -1 is a nonsquare, take $i=1$ and $j=-1$ to get $i+j=0$. Hence

$$i+j=0 \text{ some } i\in H,\quad j\in G\smallsetminus H \iff -1 \text{ is a square mod } p \iff p\equiv -1 \mod 4.$$

If we do have a solution to $i+j=0$, we get all solutions by multiplying it through by the $\frac{p-1}{2}$ squares. So in the sum for $\alpha\beta$ we see 1 a total of $\frac{p-1}{2}$ times when $p\equiv 3 \mod 4$ and not at all if $p\equiv 1 \mod 4$. In either case, the remaining terms add to a rational number, which implies that each power of ζ occurs the same number of times. Thus for $p\equiv 1 \mod 4$, $\alpha\beta=-(\frac{p-1}{2})^2/(p-1)=\frac{p-1}{4}$; the polynomial satisfied by α and β is $X^2+X-\frac{p-1}{4}$, whose roots are $(-1\pm\sqrt{1+p-1})/2$; the fixed field of H is $\mathbb{Q}[\sqrt{p}]$. For $p\equiv -1 \mod 4$, $\alpha\beta=\frac{p-1}{2}+(-1)\left((\frac{p-1}{2})^2-\frac{p-1}{2}\right)/(p-1)=\frac{p-1}{2}-\frac{p-3}{4}=\frac{p+1}{4}$; the polynomial is $X^2+X+\frac{p-1}{4}$, with roots $(-1\pm\sqrt{1-p-1})/2$; the fixed field of H is $\mathbb{Q}[\sqrt{-p}]$.

3-3. (a) It is easy to see that M is Galois over $\mathbb{Q}$ with Galois group $\langle\sigma,\tau\rangle$:

$$\begin{cases}\sigma\sqrt{2}=-\sqrt{2}\\ \sigma\sqrt{3}=\sqrt{3}\end{cases}\qquad\begin{cases}\tau\sqrt{2}=\sqrt{2}\\ \tau\sqrt{3}=-\sqrt{3}\end{cases}.$$

(b) We have

$$\frac{\sigma\alpha^2}{\alpha^2}=\frac{2-\sqrt{2}}{2+\sqrt{2}}=\frac{(2-\sqrt{2})^2}{4-2}=\left(\frac{2-\sqrt{2}}{\sqrt{2}}\right)^2=(\sqrt{2}-1)^2,$$

i.e., $\sigma\alpha^2=((\sqrt{2}-1)\alpha)^2$. Thus, if $\alpha\in M$, then $\sigma\alpha=\pm(\sqrt{2}-1)\alpha$, and

$$\sigma^2\alpha=(-\sqrt{2}-1)(\sqrt{2}-1)\alpha=-\alpha;$$

as $\sigma^2\alpha=\alpha\neq 0$, this is impossible. Hence $\alpha\notin M$, and so $[E:\mathbb{Q}]=8$.
Extend σ to an automorphism (also denoted σ) of E. Again $\sigma\alpha=\pm(\sqrt{2}-1)\alpha$ and $\sigma^2\alpha=-\alpha$, and so $\sigma^2\neq 1$. Now $\sigma^4\alpha=\alpha$, $\sigma^4|M=1$, and so we can conclude that σ has order 4. After possibly replacing σ with its inverse, we may suppose that $\sigma\alpha=(\sqrt{2}-1)\alpha$.
Repeat the above argument with τ: $\frac{\tau\alpha^2}{\alpha^2}=\frac{3-\sqrt{3}}{3+\sqrt{3}}=\left(\frac{3-\sqrt{3}}{\sqrt{6}}\right)^2$, and so we can extend τ to an automorphism of L (also denoted τ) with $\tau\alpha=\frac{3-\sqrt{3}}{\sqrt{6}}\alpha$. The order of τ is 4.
Finally compute that

$$\sigma\tau\alpha=\frac{3-\sqrt{3}}{-\sqrt{6}}(\sqrt{2}-1)\alpha;\quad \tau\sigma\alpha=(\sqrt{2}-1)\frac{3-\sqrt{3}}{\sqrt{6}}\alpha.$$

Hence $\sigma\tau\neq\tau\sigma$, and $\mathrm{Gal}(E/\mathbb{Q})$ has two noncommuting elements of order 4. Since it has order 8, it must be the quaternion group.

3-5. Let $G=\mathrm{Aut}(E/F)$. Then E is Galois over E^G with Galois group G, and so $|G|=[E:E^G]$. Now $[E:F]=[E:E^G][E^G:F]=|G|[E^G:F]$.

4-1. The splitting field is the smallest field containing all mth roots of 1. Hence it is $\mathbb{F}_{p^n}$ where n is the smallest positive integer such that $m_0|p^n-1$, $m=m_0p^r$, where p is prime and does not divide m_0.

4-2. We have $X^4-2X^3-8X-3=(X^3+X^2+3X+1)(X-3)$, and $g(X)=X^3+X^2+3X+1$ is irreducible over $\mathbb{Q}$ (use 1.11), and so its Galois group is either A_3 or S_3. Either

check that its discriminant is not a square or, more simply, show by examining its graph that $g(X)$ has only one real root, and hence its Galois group contains a transposition (cf. the proof of 4.16).

4-3. Eisenstein's criterion shows that X^8-2 is irreducible over $\mathbb{Q}$, and so $[\mathbb{Q}[\alpha]:\mathbb{Q}]=8$ where α is a positive 8th root of 2. As usual for polynomials of this type, the splitting field is $\mathbb{Q}[\alpha,\zeta]$ where ζ is any primitive 8th root of 1. For example, ζ can be taken to be $\frac{1+i}{\sqrt{2}}$, which lies in $\mathbb{Q}[\alpha,i]$. It follows that the splitting field is $\mathbb{Q}[\alpha,i]$. Clearly $\mathbb{Q}[\alpha,i]\neq\mathbb{Q}[\alpha]$, because $\mathbb{Q}[\alpha]$, unlike i, is contained in $\mathbb{R}$, and so $[\mathbb{Q}[\alpha,i]:\mathbb{Q}[\alpha]]=2$. Therefore the degree is $2\times 8=16$.

4-4. Find an extension L/F with Galois group S_4, and let E be the fixed field of $S_3\subset S_4$. There is no subgroup strictly between S_n and S_{n-1}, because such a subgroup would be transitive and contain an $(n-1)$-cycle and a transposition, and so would equal S_n. We can take $E=L^{S_3}$. More specifically, we can take L to be the splitting field of X^4-X+2 over $\mathbb{Q}$ and E to be the subfield generated by a root of the polynomial (see 3.26).

4-5. Type: "Factor($X^{343}-X$) mod 7;" and discard the 7 factors of degree 1.

4-6. Type "galois($X^6+2X^5+3X^4+4X^3+5X^2+6X+7$);". It is the group $\mathrm{PGL}_2(\mathbb{F}_5)$ (group of invertible 2×2 matrices over $\mathbb{F}_5$ modulo scalar matrices) which has order 120. Alternatively, note that there are the following factorizations: mod 3, irreducible; mod 5 (deg 3)(deg 3); mod 13 (deg 1)(deg 5); mod 19, (deg 1)^2(deg 4); mod 61 (deg 1)^2(deg 2)^2; mod 79, (deg 2)^3. Thus the Galois group has elements of type:

$$6,\quad 3+3,\quad 1+5,\quad 1+1+4,\quad 1+1+2+2,\quad 2+2+2.$$

No element of type 2, 3, $3+2$, or $4+2$ turns up by factoring modulo any of the first 400 primes (or, so I have been told). This suggests it is the group $T14$ in the tables in Butler and McKay, which is indeed $\mathrm{PGL}_2(\mathbb{F}_5)$.

4-7. $\Longleftarrow$: Condition (a) implies that G_f contains a 5-cycle, condition (b) implies that $G_f\subset A_5$, and condition (c) excludes A_5. That leaves D_5 and C_5 as the only possibilities (see, for example, Jacobson, Basic Algebra I, p305, Ex 6). The derivative of f is $5X^4+a$, which has at most 2 real zeros, and so (from its graph) we see that f can have at most 3 real zeros. Thus complex conjugation acts as an element of order 2 on the splitting field of f, and this shows that we must have $G_f=D_5$.
$\Longrightarrow$: Regard D_5 as a subgroup of S_5 by letting it act on the vertices of a regular pentagon—all subgroups of S_5 isomorphic to D_5 look like this one. If $G_f=D_5$, then (a) holds because D_5 is transitive, (b) holds because $D_5\subset A_5$, and (c) holds because D_5 is solvable.

4-8. Suppose that f is irreducible of degree n. Then f has no root in a field $\mathbb{F}_{p^m}$ with $m<n$, which implies (a). However, every root α of f lies in $\mathbb{F}_{p^n}$, and so $\alpha^{p^n}-\alpha=0$. Hence $(X-\alpha)|(X^{p^n}-X)$, which implies (b) because f has no multiple roots.

Conversely, suppose that (a) and (b) hold. It follows from (b) that all roots of f lie in $\mathbb{F}_{p^n}$. Suppose that f had an irreducible factor g of degree $m<n$. Then every root of g generates $\mathbb{F}_{p^m}$, and so $\mathbb{F}_{p^m}\subset\mathbb{F}_{p^n}$. Consequently, m divides n, and so m divides n/p_i for some i. But then g divides both f and $X^{p^{n/p_i}}-X$, contradicting (a). Thus f is irreducible.

4-9. Let a_1,a_2 be conjugate nonreal roots, and let a_3 be a real root. Complex conjugation defines an element σ of the Galois group of f switching a_1 and a_2 and fixing a_3. On the other hand, because f is irreducible, its Galois group acts transitively on its roots, and so

there is a τ such that $\tau(a_3) = a_1$. Now

$$a_3 \overset{\tau}{\mapsto} a_1 \overset{\sigma}{\mapsto} a_2$$
$$a_3 \overset{\sigma}{\mapsto} a_3 \overset{\tau}{\mapsto} a_1.$$

This statement is false for reducible polynomials — consider for example $f(X) = (X^2 + 1)(X - 1)$.

5-1. For $a = 1$, this is the polynomial $\Phi_5(X)$, whose Galois group is cyclic of order 4.
For $a = 0$, it is $X(X^3 + X^2 + X + 1) = X(X + 1)(X^2 + 1)$, whose Galois group is cyclic of order 2.
For $a = -4$, it is $(X - 1)(X^3 + 2X^2 + 3X + 4)$. The cubic does not have $\pm 1, \pm 2$, or ± 4 as roots, and so it is irreducible in $\mathbb{Q}[X]$. Hence its Galois group is S_3 or A_3. But looking modulo 2, we see it contains a 2-cycle, so it must be S_3.
For any a, the resolvent cubic is

$$g(X) = X^3 - X^2 + (1 - 4a)X + 3a - 1.$$

Take $a = -1$. Then $f = X^4 + X^3 + X^2 + X - 1$ is irreducible modulo 2, and so it is irreducible in $\mathbb{Q}[X]$. We have $g = X^3 - X^2 + 5X - 4$, which is irreducible. Moreover $g' = 3X^2 - 2X + 5 = 3(X - \frac{1}{3})^2 + 4\frac{2}{3} > 0$ always, and so g has exactly one real root. Hence the Galois group of g is S_3, and therefore the Galois group of f is S_4. [In fact, 4 is the maximum number of integers giving distinct Galois groups: checking mod 2, we see there is a 2-cycle or a 4-cycle, and so $1, A_3, A_4, V_4$ are not possible. For D_8, a can't be an integer.]

5-2. We have $\mathrm{Nm}(a + ib) = a^2 + b^2$. Hence $a^2 + b^2 = 1$ if and only $a + ib = \frac{s+it}{s-it}$ for some $s, t \in \mathbb{Q}$ (Hilbert's Theorem 90). The rest is easy.

5-3. The degree $[\mathbb{Q}[\zeta_n]:\mathbb{Q}] = \varphi(n)$, ζ_n a primitive nth root of 1, and $\varphi(n) \to \infty$ as $n \to \infty$.

9-1. If some element centralizes the complex conjugation, then it must preserve the real numbers as a set. Now, since any automorphism of the real numbers preserves the set of squares, it must preserve the order; and hence be continuous. Since $\mathbb{Q}$ is fixed, this implies that the real numbers are fixed pointwise. It follows that any element which centralized the complex conjugation must be the identity or the complex conjugation itself. See mo121083, Andreas Thom.

A-1. (a) Need that $m|n$, because

$$n = [\mathbb{F}_{p^n}:\mathbb{F}_p] = [\mathbb{F}_{p^n}:\mathbb{F}_{p^m}] \cdot [\mathbb{F}_{p^m}:\mathbb{F}_p] = [\mathbb{F}_{p^n}:\mathbb{F}_{p^m}] \cdot m.$$

Use Galois theory to show there exists one, for example. (b) Only one; it consists of all the solutions of $X^{p^m} - X = 0$.

A-2. The polynomial is irreducible by Eisenstein's criterion. The polynomial has only one real root, and therefore complex conjugation is a transposition in G_f. This proves that $G_f \approx S_3$. The discriminant is $-1323 = -3^3 7^2$. Only the subfield $\mathbb{Q}[\sqrt{-3}]$ is normal over $\mathbb{Q}$. The subfields $\mathbb{Q}[\sqrt[3]{7}]$, $\mathbb{Q}[\zeta\sqrt[3]{7}]$ $\mathbb{Q}[\zeta^2\sqrt[3]{7}]$ are not normal over $\mathbb{Q}$. [The discriminant of $X^3 - a$ is $-27a^2 = -3(3a)^2$.]

A-3. The prime 7 becomes a square in the first field, but 11 does not: $(a + b\sqrt{7})^2 = a^2 + 7b^2 + 2ab\sqrt{7}$, which lies in $\mathbb{Q}$ only if $ab = 0$. Hence the rational numbers that become squares in $\mathbb{Q}[\sqrt{7}]$ are those that are already squares or lie in $7\mathbb{Q}^{\times 2}$.

A-4.(a) See Exercise 3.

(b) Let $F = \mathbb{F}_3[X]/(X^2+1)$. Modulo 3

$$X^8 - 1 = (X-1)(X+1)(X^2+1)(X^2+X+2)(X^2+2X+2).$$

Take α to be a root of X^2+X+2.

A-5. Since $E \neq F$, E contains an element $\frac{f}{g}$ with the degree of f or $g > 0$. Now

$$f(T) - \frac{f(X)}{g(X)}g(T)$$

is a nonzero polynomial having X as a root.

A-6. Use Eisenstein to show that $X^{p-1} + \cdots + 1$ is irreducible, etc. Done in class.

A-7. The splitting field is $\mathbb{Q}[\zeta,\alpha]$ where $\zeta^5 = 1$ and $\alpha^5 = 2$. It is generated by $\sigma = (12345)$ and $\tau = (2354)$, where $\sigma\alpha = \zeta\alpha$ and $\tau\zeta = \zeta^2$. The group has order 20. It is not abelian (because $\mathbb{Q}[\alpha]$ is not Galois over $\mathbb{Q}$), but it is solvable (its order is < 60).

A-8. (a) A homomorphism $\alpha\colon\mathbb{R} \to \mathbb{R}$ acts as the identity map on $\mathbb{Z}$, hence on $\mathbb{Q}$, and it maps positive real numbers to positive real numbers, and therefore preserves the order. Hence, for each real number a,

$$\{r \in \mathbb{Q} \mid a < r\} = \{r \in \mathbb{Q} \mid \alpha(a) < r\},$$

which implies that $\alpha(a) = a$.

(b) Choose a transcendence basis A for $\mathbb{C}$ over $\mathbb{Q}$. Because it is infinite, there is a bijection $\alpha\colon A \to A'$ from A onto a proper subset. Extend α to an isomorphism $\mathbb{Q}(A) \to \mathbb{Q}(A')$, and then extend it to an isomorphism $\mathbb{C} \to \mathbb{C}'$ where $\mathbb{C}'$ is the algebraic closure of $\mathbb{Q}(A')$ in $\mathbb{C}$.

A-9. The group $F^\times$ is cyclic of order 15. It has 3 elements of order dividing 3, 1 element of order dividing 4, 15 elements of order dividing 15, and 1 element of order dividing 17.

A-10. If E_1 and E_2 are Galois extensions of F, then E_1E_2 and $E_1 \cap E_2$ are Galois over F, and there is an exact sequence

$$1 \to \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F) \to \mathrm{Gal}(E_1 \cap E_2/F) \to 1.$$

In this case, $E_1 \cap E_2 = \mathbb{Q}[\zeta]$ where ζ is a primitive cube root of 1. The degree is 18.

A-11. Over $\mathbb{Q}$, the splitting field is $\mathbb{Q}[\alpha,\zeta]$ where $\alpha^6 = 5$ and $\zeta^3 = 1$ (because $-\zeta$ is then a primitive 6th root of 1). The degree is 12, and the Galois group is D_6 (generators (26)(35) and (123456)).

Over $\mathbb{R}$, the Galois group is C_2.

A-12. Let the coefficients of f be $a_1,\dots,a_n$ — they lie in the algebraic closure Ω of F. Let $g(X)$ be the product of the minimum polynomials over F of the roots of f in Ω.

Alternatively, the coefficients will lie in some finite extension E of F, and we can take the norm of $f(X)$ from $E[X]$ to $F[X]$.

A-13. If f is separable, $[E\colon F] = (G_f\colon 1)$, which is a subgroup of S_n. Etc..

A-14. $\sqrt{3}+\sqrt{7}$ will do.

A-15. The splitting field of X^4-2 is $E_1 = \mathbb{Q}[i,\alpha]$ where $\alpha^4 = 2$; it has degree 8, and Galois group D_4. The splitting field of X^3-5 is $E_2 = \mathbb{Q}[\zeta,\beta]$; it has degree 6, and Galois group

D_3. The Galois group is the product (they could only intersect in $\mathbb{Q}[\sqrt{3}]$, but $\sqrt{3}$ does not become a square in E_1).

A-16. The multiplicative group of F is cyclic of order $q-1$. Hence it contains an element of order 4 if and only if $4|q-1$.

A-17. Take $\alpha = \sqrt{2}+\sqrt{5}+\sqrt{7}$.

A-18. We have $E_1 = E^{H_1}$, which has degree n over F, and $E_2 = E^{<1\cdots n>}$, which has degree $(n-1)!$ over F, etc.. This is really a problem in group theory posing as a problem in field theory.

A-19. We have $\mathbb{Q}[\zeta] = \mathbb{Q}[i,\zeta']$ where ζ' is a primitive cube root of 1 and $\pm i = \zeta^3$ etc..

A-20. The splitting field is $\mathbb{Q}[\zeta, \sqrt[3]{3}]$, and the Galois group is S_3.

A-21. Use that

$$(\zeta+\zeta^4)(1+\zeta^2) = \zeta+\zeta^4+\zeta^3+\zeta$$

A-22. (a) is Dedekind's theorem. (b) is Artin's theorem 3.4. (c) is O.K. because $X^p - a^p$ has a unique root in Ω.

A-23. The splitting field is $\mathbb{Q}[i,\alpha]$ where $\alpha^4 = 3$, and the Galois group is D_4 with generators (1234) and (13) etc..

A-24. From Hilbert's theorem 90, we know that the kernel of the map $N\colon E^\times \to F^\times$ consists of elements of the form $\frac{\sigma\alpha}{\alpha}$. The map $E^\times \to E^\times$, $\alpha \mapsto \frac{\sigma\alpha}{\alpha}$, has kernel $F^\times$. Therefore the kernel of N has order $\frac{q^m-1}{q-1}$, and hence its image has order $q-1$. There is a similar proof for the trace — I don't know how the examiners expected you to prove it.

A-25. (a) is false—could be inseparable. (b) is true—couldn't be inseparable.

A-26. Apply the Sylow theorem to see that the Galois group has a subgroup of order 81. Now the Fundamental Theorem of Galois theory shows that F exists.

A-27. The greatest common divisor of the two polynomials over $\mathbb{Q}$ is X^2+X+1, which must therefore be the minimum polynomial for θ.

A-28. Theorem on p-groups plus the Fundamental Theorem of Galois Theory.

A-29. It was proved in class that S_p is generated by an element of order p and a transposition (4.15). There is only one F, and it is quadratic over $\mathbb{Q}$.

A-30. Let $L = K[\alpha]$. The splitting field of the minimum polynomial of α has degree at most $d!$, and a set with $d!$ elements has at most $2^{d!}$ subsets. [Of course, this bound is much too high: the subgroups are very special subsets. For example, they all contain 1 and they are invariant under $a \mapsto a^{-1}$.]

A-31. The Galois group is $(\mathbb{Z}/5\mathbb{Z})^\times$, which cyclic of order 4, generated by 2.

$$(\zeta+\zeta^4)+(\zeta^2+\zeta^3) = -1, \quad (\zeta+\zeta^4)(\zeta^2+\zeta^3) = -1.$$

(a) Omit.
(b) Certainly, the Galois group is a product $C_2 \times C_4$.

A-32. Let $a_1,\dots,a_5$ be a transcendence basis for $\Omega_1/\mathbb{Q}$. Their images are algebraically independent, therefore they are a maximal algebraically independent subset of Ω_2, and therefore they form a transcendence basis, etc..

A-33. $C_2 \times C_2$.

A-34. If $f(X)$ were reducible over $\mathbb{Q}[\sqrt{7}]$, it would have a root in it, but it is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. The discriminant is -675, which is not a square in $\mathbb{R}$, much less $\mathbb{Q}[\sqrt{7}]$.

A-35. (a) Should be $X^5 - 6X^4 + 3$. The Galois group is S_5, with generators (12) and (12345) — it is irreducible (Eisenstein) and (presumably) has exactly 2 nonreal roots. (b) It factors as $(X+1)(X^4+X^3+X^2+X+1)$. Hence the splitting field has degree 4 over $\mathbb{F}_2$, and the Galois group is cyclic.

A-36. This is really a theorem in group theory, since the Galois group is a cyclic group of order n generated by θ. If n is odd, say $n = 2m+1$, then $\alpha = \theta^m$ does.

A-37. It has order 20, generators (12345) and (2354).

A-38. Take K_1 and K_2 to be the fields corresponding to the Sylow 5 and Sylow 43 subgroups. Note that of the possible numbers $1, 6, 11, 16, 21, \ldots$ of Sylow 5-subgroups, only 1 divides 43. There are 1, 44, 87, ... subgroups of ....

A-39. See Exercise 14.

A-40. The group $F^\times$ is cyclic of order 80; hence 80, 1, 8.

A-41. It's D_6, with generators (26)(35) and (123456). The polynomial is irreducible by Eisenstein's criterion, and its splitting field is $\mathbb{Q}[\alpha, \zeta]$ where $\zeta \neq 1$ is a cube root of 1.

A-42. Example 5.5.

A-43. Omit.

A-44. It's irreducible by Eisenstein. Its derivative is $5X^4 - 5p^4$, which has the roots $X = \pm p$. These are the max and mins, $X = p$ gives negative; $X = -p$ gives positive. Hence the graph crosses the x-axis 3 times and so there are 2 imaginary roots. Hence the Galois group is S_5.

A-45. Its roots are primitive 8th roots of 1. It splits completely in $\mathbb{F}_{25}$. (a) $(X^2+2)(X^2+3)$.

A-46. $\rho(\alpha)\overline{\rho(\alpha)} = q^2$, and $\rho(\alpha)\rho(\frac{q^2}{\alpha}) = q^2$. Hence $\rho(\frac{q^2}{\alpha})$ is the complex conjugate of $\rho(\alpha)$. Hence the automorphism induced by complex conjugation is independent of the embedding of $\mathbb{Q}[\alpha]$ into $\mathbb{C}$.

A-47. The argument that proves the Fundamental Theorem of Algebra, shows that its Galois group is a p-group. Let E be the splitting field of $g(X)$, and let H be the Sylow p-subgroup. Then $E^H = F$, and so the Galois group is a p-group.

A-48. (a) $C_2 \times C_2$ and S_3. (b) No. (c). 1

A-49. Omit.

A-50. Omit.

A-51. $1024 = 2^{10}$. Want $\sigma x \cdot x = 1$, i.e., $Nx = 1$. They are the elements of the form $\frac{\sigma x}{x}$; have

$$1 \longrightarrow k^\times \longrightarrow K^\times \xrightarrow{x \mapsto \frac{\sigma x}{x}} K^\times.$$

Hence the number is $2^{11}/2^{10} = 2$.

A-52. Pretty standard. False; true.

A-53. Omit.

A-54. Similar to a previous problem.

A-55. Omit.

A-56. This is really a group theory problem disguised as a field theory problem.

A-57. (a) Prove it's irreducible by apply Eisenstein to $f(X+1)$. (b) See example worked out in class.

A-58. It's D_4, with generators (1234) and (12).

A-59. Omit.

SOLUTIONS FOR THE EXAM.

1. (a) Let σ be an automorphism of a field E. If $\sigma^4 = 1$ and

$$\sigma(\alpha)+\sigma^3(\alpha) = \alpha+\sigma^2(\alpha) \qquad \text{all } \alpha \in E,$$

show that $\sigma^2 = 1$.

If $\sigma^2 \neq 1$, then $1, \sigma, \sigma^2, \sigma^3$ are distinct automorphisms of E, and hence are linearly independent (Dedekind 5.14) — contradiction. [If $\sigma^2 = 1$, then the condition becomes $2\sigma = 2$, so either $\sigma = 1$ or the characteristic is 2 (or both).]
(b) Let p be a prime number and let a, b be rational numbers such that $a^2 + pb^2 = 1$. Show that there exist rational numbers c, d such that $a = \frac{c^2+pd^2}{c^2-pd^2}$ and $b = \frac{2cd}{c^2-pd^2}$.

Apply Hilbert's Theorem 90 to $\mathbb{Q}[\sqrt{p}]$ (or $\mathbb{Q}[\sqrt{-p}]$, depending how you wish to correct the sign).

2. Let $f(X)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[X]$, and let $g(X)$ be the resolvent cubic of f. What is the relation between the Galois group of f and that of g? Find the Galois group of f if

(a) $g(X) = X^3 - 3X + 1$;

(b) $g(X) = X^3 + 3X + 1$.

We have $G_g = G_f / G_f \cap V$, where $V = \{1, (12)(34), \ldots\}$. The two cubic polynomials are irreducible, because their only possible roots are ± 1. From their discriminants, one finds that the first has Galois group A_3 and the second S_3. Because $f(X)$ is irreducible, $4|(G_f : 1)$ and it follows that $G_f = A_4$ and S_4 in the two cases.

3. (a) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{F}_2[X]$ have, and what are their degrees?

Its roots are the nonzero elements of $\mathbb{F}_{2^8}$, which has subfields $\mathbb{F}_{2^4} \supset \mathbb{F}_{2^2} \supset \mathbb{F}_2$. There are $256 - 16$ elements not in $\mathbb{F}_{16}$, and their minimum polynomials all have degree 8. Hence there are 30 factors of degree 8, 3 of degree 4, and 1 each of degrees 2 and 1.
(b) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{Q}[X]$ have, and what are their degrees?

Obviously, $X^{255} - 1 = \prod_{d|255} \Phi_d = \Phi_1 \Phi_3 \Phi_5 \Phi_{15} \cdots \Phi_{255}$, and we showed in class that the Φ_d are irreducible. They have degrees $1, 2, 4, 8, 16, 32, 64, 128$.

4. Let E be the splitting field of $(X^5 - 3)(X^5 - 7) \in \mathbb{Q}[X]$. What is the degree of E over $\mathbb{Q}$? How many proper subfields of E are there that are not contained in the splitting fields of both $X^5 - 3$ and $X^5 - 7$?

The splitting field of X^5-3 is $\mathbb{Q}[\zeta,\alpha]$, which has degree 5 over $\mathbb{Q}[\zeta]$ and 20 over $\mathbb{Q}$. The Galois group of X^5-7 over $\mathbb{Q}[\zeta,\alpha]$ is (by ...) a subgroup of a cyclic group of order 5, and hence has order 1 or 5. Since 7 is not a 5th power in $\mathbb{Q}[\zeta,\alpha]$, it must be 5. Thus $[E:\mathbb{Q}]=100$, and

$$G=\mathrm{Gal}(E/\mathbb{Q})=(C_5\times C_5)\rtimes C_4.$$

We want the nontrivial subgroups of G not containing $C_5\times C_5$. The subgroups of order 5 of $C_5\times C_5$ are lines in $(\mathbb{F}_5)^2$, and hence $C_5\times C_5$ has $6+1=7$ proper subgroups. All are normal in G. Each subgroup of $C_5\times C_5$ is of the form $H\cap(C_5\times C_5)$ for exactly 3 subgroups H of G corresponding to the three possible images in $G/(C_5\times C_5)=C_4$. Hence we have 21 subgroups of G not containing $C_5\times C_5$, and 20 nontrivial ones. Typical fields: $\mathbb{Q}[\alpha]$, $\mathbb{Q}[\alpha,\cos\frac{2\pi}{5}]$, $\mathbb{Q}[\alpha,\zeta]$.
[You may assume that 7 is not a 5th power in the splitting field of X^5-3.]

5. Consider an extension $\Omega\supset F$ of fields. Define $\alpha\in\Omega$ to be *F-constructible* if it is contained in a field of the form

$$F[\sqrt{a_1},\dots,\sqrt{a_n}],\qquad a_i\in F[\sqrt{a_1},\dots,\sqrt{a_{i-1}}].$$

Assume Ω is a finite Galois extension of F and construct a field E, $F\subset E\subset\Omega$, such that every $a\in\Omega$ is E-constructible and E is minimal with this property.

Suppose E has the required property. From the primitive element theorem, we know $\Omega=E[a]$ for some a. Now a E-constructible $\implies$ $[\Omega:E]$ is a power of 2. Take $E=\Omega^H$, where H is the Sylow 2-subgroup of $\mathrm{Gal}(\Omega/F)$.

6. Let Ω be an extension field of a field F. Show that every F-homomorphism $\Omega\to\Omega$ is an isomorphism provided:

(a) Ω is algebraically closed, and

(b) Ω has finite transcendence degree over F.

Can either of the conditions (i) or (ii) be dropped? (Either prove, or give a counterexample.)

Let A be a transcendence basis for Ω/F. Because $\sigma:\Omega\to\Omega$ is injective, $\sigma(A)$ is algebraically independent over F, and hence (because it has the right number of elements) is a transcendence basis for Ω/F. Now $F[\sigma A]\subset\sigma\Omega\subset\Omega$. Because Ω is algebraic over $F[\sigma A]$ and $\sigma\Omega$ is algebraically closed, the two are equal. Neither condition can be dropped. E.g., $\mathbb{C}(X)\to\mathbb{C}(X)$, $X\mapsto X^2$. E.g., $\Omega=$ the algebraic closure of $\mathbb{C}(X_1,X_2,X_3,\dots)$, and consider an extension of the map $X_1\mapsto X_2$, $X_2\mapsto X_3$, ...

Index

algebra
  diagonalizable, 102
  étale, 102
algebra over F, 8
algebraic, 18, 19
algebraic closure, 24
  in a larger field, 25
algebraic integer, 11
algebraically closed, 24
algebraically dependent, 109
algebraically independent, 109
algorithm
  division, 9
  Euclid's, 10
  factoring a polynomial, 12
automorphism, 35

base
  neighbourhood, 92
basis
  separating transcendence, 116
  transcendence, 111
bound
  upper, 85

characteristic
  p, 9
  zero, 9
closure
  separable, 89
cohomology group, 70
commutative, 7
composite of fields, 15
conjugates, 38
constructible, 21, 43
cubic
  resolvent, 50
cyclotomic polynomial, 63

degree, 13
  of an algebra, 102
  separable, 39
directed, 98
discriminant, 47

Eisenstein's criterion, 12
element
  maximal, 85
  separable, 39
exponent, 72
extension
  abelian, 39
  algebraic, 18
  cyclic, 39
  finite, 13
  Galois, 37
  inseparable, 37
  normal, 37
  separable, 37
  simple, 15
  solvable, 39
  transcendental, 18
extension field, 13

F-algebra, 8
F-isomorphism, 27
F-homomorphism, 13
field, 8
  perfect, 32
  prime, 9
  stem, 17
fixed field, 36
Frobenius
  endomorphism, 9, 33
fundamental theorem
  of algebra, 12, 20, 24, 25, 61
  of Galois theory, 39

Galois, 92
Galois closure, 40
Galois correspondence, 97
Galois field, 54
Galois group, 38
  absolute, 93
  infinite, 93
  of a polynomial, 44
Gaussian numbers, 14
general polynomial, 77
group
  Cremona, 35
  profinite, 99
  topological, 91
group algebra, 66

homomorphism
  crossed, 69
  of F-algebras, 8
  of fields, 8

of rings, 7
principal crossed, 69

ideal, 7
integral domain, 7
invariants, 36
inverse limit, 98
inverse system, 98

Lemma
Gauss's, 11

module
G-, 69
multiplicity, 31

norm, 70, 79
normal basis, 66
normal closure, 40

ordering
partial, 85
total, 85

PARI, 6, 10, 13, 17, 18, 48, 51, 54, 56, 58, 63, 82
perfect field, 32
$\varphi(n)$, 63
polynomial
minimal, 18
monic, 10
primitive, 114
separable, 32
prime
Fermat, 23
primitive element, 59
primitive root of 1, 62

regular n-gon, 64
relatively prime, 101
ring, 7
root
multiple, 31
of a polynomial, 10
simple, 31

separable, 59
separably closed, 89
S_n, 44
solvable in radicals, 45
split, 28
splits, 24
splitting field, 28
subfield, 8
generated by subset, 15
subring, 7
generated by subset, 14
symmetric polynomial, 75
elementary, 75

Theorem
Artin's, 36

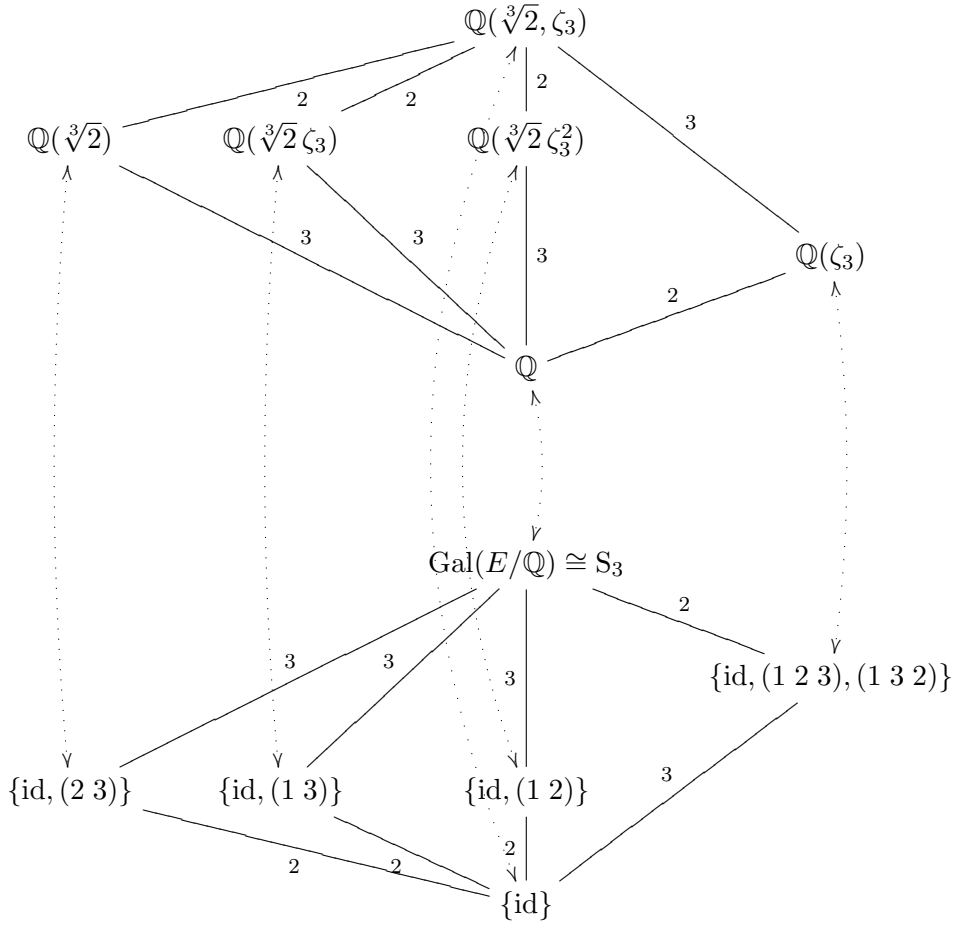
theorem
binomial in characteristic p, 9
Chinese remainder, 101
constructibility of n-gons, 64
constructible numbers, 21, 43
cyclotomic polynomials, 63
Dedekind, 55
Galois 1832, 45
Galois extensions, 38
independence of characters, 65
Liouville, 20
normal basis, 66
primitive element, 59
strong Nullstellensatz, 101
topology
Krull, 93, 117
trace, 79
transcendence degree, 112
transcendental, 18, 19

An Introduction to Galois Theory

Andrew Baker

[23/01/2013]

School of Mathematics & Statistics, University of Glasgow.
E-mail address: a.baker@maths.gla.ac.uk
URL: http://www.maths.gla.ac.uk/∼ajb



The Galois Correspondence for $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}$

Introduction: What is Galois Theory?

Much of early algebra centred around the search for explicit formulae for roots of polynomial equations in one or more unknowns. The solution of linear and quadratic equations in a single unknown was well understood in antiquity, while formulae for the roots of general real cubics and quartics was solved by the 16th century. These solutions involved complex numbers rather than just real numbers. By the early 19th century no general solution of a general polynomial equation 'by radicals' (*i.e.*, by repeatedly taking n-th roots for various n) was found despite considerable effort by many outstanding mathematicians. Eventually, the work of Abel and Galois led to a satisfactory framework for fully understanding this problem and the realization that the general polynomial equation of degree at least 5 could not always be solved by radicals. At a more profound level, the algebraic structure of *Galois extensions* is mirrored in the subgroups of their *Galois groups*, which allows the application of group theoretic ideas to the study of fields. This *Galois Correspondence* is a powerful idea which can be generalized to apply to such diverse topics as ring theory, algebraic number theory, algebraic geometry, differential equations and algebraic topology. Because of this, Galois theory in its many manifestations is a central topic in modern mathematics.

In this course we will focus on the following topics.

- The solution of polynomial equations over a field, including relationships between roots, methods of solutions and location of roots.
- The structure of finite and algebraic extensions of fields and their automorphisms.

We will study these in detail, building up a theory of algebraic extensions of fields and their automorphism groups and applying it to solve questions about roots of polynomial equations. The techniques we will meet can also be applied to study the following some of which may be met by people studying more advanced courses.

- Classic topics such as *squaring the circle*, *duplication of the cube*, *constructible numbers* and *constructible polygons*.
- Applications of Galois theoretic ideas in Number Theory, the study of differential equations and Algebraic Geometry.

There are many good introductory books on Galois Theory, some of which are listed in the Bibliography. In particular, [**2, 3, 8**] are all excellent sources and have many similarities to the present approach to the material.

Contents

Introduction: What is Galois Theory? ii

Chapter 1. Integral domains, fields and polynomial rings 1
Basic notions, convention, etc 1
1.1. Recollections on integral domains and fields 1
1.2. Polynomial rings 6
1.3. Identifying irreducible polynomials 12
1.4. Finding roots of complex polynomials of small degree 16
1.5. Automorphisms of rings and fields 19
Exercises on Chapter 1 23

Chapter 2. Fields and their extensions 27
2.1. Fields and subfields 27
2.2. Simple and finitely generated extensions 29
Exercises on Chapter 2 33

Chapter 3. Algebraic extensions of fields 35
3.1. Algebraic extensions 35
3.2. Splitting fields and Kronecker's Theorem 39
3.3. Monomorphisms between extensions 42
3.4. Algebraic closures 45
3.5. Multiplicity of roots and separability 48
3.6. The Primitive Element Theorem 52
3.7. Normal extensions and splitting fields 54
Exercises on Chapter 3 55

Chapter 4. Galois extensions and the Galois Correspondence 57
4.1. Galois extensions 57
4.2. Working with Galois groups 58
4.3. Subgroups of Galois groups and their fixed fields 60
4.4. Subfields of Galois extensions and relative Galois groups 61
4.5. The Galois Correspondence and the Main Theorem of Galois Theory 62
4.6. Galois extensions inside the complex numbers and complex conjugation 64
4.7. Galois groups of even and odd permutations 65
4.8. Kaplansky's Theorem 68
Exercises on Chapter 4 71

Chapter 5. Galois extensions for fields of positive characteristic 73
5.1. Finite fields 73

5.2. Galois groups of finite fields and Frobenius mappings 77
5.3. The trace and norm mappings 79
Exercises on Chapter 5 80

Chapter 6. A Galois Miscellany 83
6.1. A proof of the Fundamental Theorem of Algebra 83
6.2. Cyclotomic extensions 84
6.3. Artin's Theorem on linear independence of characters 88
6.4. Simple radical extensions 90
6.5. Solvability and radical extensions 92
6.6. Symmetric functions 96
Exercises on Chapter 6 97

Bibliography 101

CHAPTER 1

Integral domains, fields and polynomial rings

Basic notions, convention, etc

In these notes, a *ring* will always be a unital ring, *i.e.*, a ring with unity $1 \neq 0$. Most of the rings encountered will also be *commutative*. An *ideal* $I \lhd R$ will always mean a two-sided ideal. An ideal $I \lhd R$ in a ring R is *proper* if $I \neq R$, or equivalently if $I \subsetneq R$. Under a ring homomorphism $\varphi\colon R \longrightarrow S$, $1 \in R$ is sent to $1 \in S$, *i.e.*, $\varphi(1) = 1$.

1.1. Definition. Let $\varphi\colon R \longrightarrow S$ be a ring homomorphism.

- φ is a *monomorphism* if it is injective, *i.e.*, if for $r_1, r_2 \in R$,
$$\varphi(r_1) = \varphi(r_2) \quad \Longrightarrow \quad r_1 = r_2,$$
or equivalently if $\ker \varphi = \{0\}$.
- φ is an *epimorphism* if it is surjective, *i.e.*, if for every $s \in S$ there is an $r \in R$ with $\varphi(r) = s$.
- φ is an *isomorphism* if it is both a monomorphism and an epimorphism, *i.e.*, if it is invertible (in which case its inverse is also an isomorphism).

1.1. Recollections on integral domains and fields

The material in this section is standard and most of it should be familiar. Details may be found in [**3, 5**] or other books containing introductory ring theory. First we recall some important properties of elements in a ring.

1.2. Definition. Let R be a ring. An element $u \in R$ is a *unit* if it is *invertible*, *i.e.*, there is an element $v \in R$ for which
$$uv = 1 = vu.$$
We usually write u^{-1} for this element v, which is necessarily unique and is called the (*multiplicative*) *inverse* of u in R. We will denote the set of all invertible elements of R by $R^\times$ and note that it always forms a group under multiplication.

1.3. Definition. Let R be a commutative ring. Then a non-zero element $z \in R$ is a *zero-divisor* if there is a non-zero element $w \in R$ for which
$$zw = wz = 0.$$
A commutative ring R in which there are no zero-divisors is called an *integral domain* or an *entire ring*. This means that for $u, v \in R$,
$$uv = 0 \quad \Longrightarrow \quad u = 0 \text{ or } v = 0.$$

1.4. Example. The following rings are integral domains.

(i) The ring of integers, $\mathbb{Z}$.

(ii) If p is a prime, the ring of integers modulo p, $\mathbb{F}_p = \mathbb{Z}/p = \mathbb{Z}/(p)$.
(iii) The rings of rational numbers, $\mathbb{Q}$, real numbers, $\mathbb{R}$, and complex numbers, $\mathbb{C}$.
(iv) The polynomial ring $R[X]$, where R is an integral domain; in particular, the polynomial rings $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$ and $\mathbb{C}[X]$ are all integral domains.

1.5. Definition. Let $I \lhd R$ be a proper ideal in a commutative ring R.

- I is a *prime ideal* if for $u, v \in R$,

$$uv \in I \quad \Longrightarrow \quad u \in I \text{ or } v \in I.$$

- I is a *maximal ideal* R if whenever $J \lhd R$ is a proper ideal and $I \subseteq J$ then $J = I$.
- $I \lhd R$ is *principal* if

$$I = (p) = \{rp : r \in R\}$$

for some $p \in R$. Notice that if $p, q \in R$, then $(q) = (p)$ if and only if $q = up$ for some unit $u \in R$. We also write $p \mid x$ if $x \in (p)$.
- $p \in R$ is *prime* (or is *a prime*) if $(p) \lhd R$ is a prime ideal; this is equivalent to the requirement that whenever $p \mid xy$ with $x, y \in R$ then $p \mid x$ or $p \mid y$.
- R is a *principal ideal domain* if it is an integral domain and every ideal $I \lhd R$ is principal.
- A non-zero element $p \in R$ is *irreducible* (or is *an irreducible*) if for $u, v \in R$,

$$p = uv \quad \Longrightarrow \quad u \text{ or } v \text{ is a unit.}$$

1.6. Example. Every ideal $I \lhd \mathbb{Z}$ is principal, so $I = (n)$ for some $n \in \mathbb{Z}$ which we can always take to be non-negative, *i.e.*, $n \geqslant 0$. Hence $\mathbb{Z}$ is a principal ideal domain.

1.7. Proposition. *Let R be a commutative ring and $I \lhd R$ an ideal.*

(i) *The quotient ring R/I is an integral domain if and only if I is a prime ideal.*
(ii) *The quotient ring R/I is a field if and only if I is a maximal ideal.*

1.8. Example. If $n \geqslant 0$, the quotient ring $\mathbb{Z}/n = \mathbb{Z}/(n)$ is an integral domain if and only if n is a prime.

For any (not necessarily commutative) ring with unity there is an important ring homomorphism $\eta\colon \mathbb{Z} \longrightarrow R$ called the *unit* or *characteristic* homomorphism which is defined by

$$\eta(n) = n1 = \begin{cases} \underbrace{1 + \cdots + 1}_{n} & \text{if } n > 0, \\ -(\underbrace{1 + \cdots + 1}_{-n}) & \text{if } n < 0, \\ 0 & \text{if } n = 0. \end{cases}$$

Since $1 \in R$ is non-zero, $\ker \eta \lhd \mathbb{Z}$ is a proper ideal and using the Isomorphism Theorems we see that there is a quotient monomorphism $\overline{\eta}\colon \mathbb{Z}/\ker \eta \longrightarrow R$ which allows us to identify the quotient ring $\mathbb{Z}/\ker \eta$ with the image $\eta\mathbb{Z} \subseteq R$ as a subring of R. By Example 1.6, there is a unique non-negative integer $p \geqslant 0$ such that $\ker \eta = (p)$; this p is called the *characteristic* of R and denoted $\operatorname{char} R$.

1.9. Lemma. *If R is an integral domain, its characteristic* $\operatorname{char} R$ *is a prime.*

PROOF. Consider $p = \operatorname{char} R$. If $p = 0$ we are done. So suppose that $p > 0$. The quotient monomorphism $\overline{\eta}\colon \mathbb{Z}/\ker\eta \longrightarrow R$ identifies $\mathbb{Z}/\ker\eta$ with the subring $\operatorname{im}\overline{\eta} = \operatorname{im}\eta$ of the integral domain R. But every subring of an integral domain is itself an integral domain, hence $\mathbb{Z}/\ker\eta$ is an integral domain. Now by Proposition 1.7(i), $\ker\eta = (p)$ is prime ideal and so by Example 1.8, p is a prime. □

1.10. REMARK. When discussing a ring with unit R, we can consider it as containing as a subring of the form $\mathbb{Z}/(\operatorname{char} R)$ since the quotient homomorphism $\overline{\eta}\colon \mathbb{Z}/(\operatorname{char} R) \longrightarrow R$ gives an isomorphism $\mathbb{Z}/(\operatorname{char} R) \longrightarrow \operatorname{im}\eta$, allowing us to identify these rings. In particular, every integral domain contains as a subring either $\mathbb{Z} = \mathbb{Z}/(0)$ (if $\operatorname{char} R = 0$) or $\mathbb{Z}/(p)$ if $p = \operatorname{char} R > 0$ is a non-zero prime. This subring is sometimes called the *characteristic subring* of R. The rings $\mathbb{Z}$ and $\mathbb{Z}/n = \mathbb{Z}/(n)$ for $n > 0$ are often called *core rings*. When considering integral domains, the rings $\mathbb{Z}$ and $\mathbb{F}_p = \mathbb{Z}/p = \mathbb{Z}/(p)$ for $p > 0$ a prime are called *prime rings*.

Here is a useful and important fact about rings which contain a *finite* prime ring $\mathbb{F}_p$.

1.11. THEOREM (Idiot's Binomial Theorem). *Let R be a commutative ring containing $\mathbb{F}_p$ for some prime $p > 0$. If $u, v \in R$, then*

$$(u+v)^p = u^p + v^p.$$

PROOF. We have $p1 = 0$ in R, hence $pt = 0$ for any $t \in R$. The Binomial Expansion yields

$$(u+v)^p = u^p + \binom{p}{1}u^{p-1}v + \binom{p}{2}u^{p-2}v^2 + \cdots + \binom{p}{p-1}uv^{p-1} + v^p. \tag{1.1}$$

Now suppose that $1 \leqslant j \leqslant p-1$. Then we have

$$\binom{p}{j} = \frac{p\,(p-1)!}{j!\,(p-j)!} = p \times \frac{(p-1)!}{j!\,(p-j)!}.$$

There are no factors of p appearing in $(p-1)!$, $j!$ or $(p-j)!$, so since this number is an integer it must be divisible by p, *i.e.*,

$$p \mid \binom{p}{j}, \tag{1.2a}$$

or equivalently

$$\binom{p}{j} \equiv 0 \pmod{p}. \tag{1.2b}$$

Hence in R we have

$$\binom{p}{j}1 = 0.$$

Combining the divisibility conditions of (1.2) with the expansion of (1.1), we obtain the required equation in R,

$$(u+v)^p = u^p + v^p.$$ □

1.12. DEFINITION. A commutative ring $\Bbbk$ is a *field* if every non-zero element $u \in \Bbbk$ is a unit. This is equivalent to requiring that $\Bbbk^\times = \Bbbk - \{0\}$.

The familiar rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are all fields.

1.13. EXAMPLE. If $n \geqslant 1$, the quotient ring $\mathbb{Z}/n$ is a field if and only if n is a prime.

1.14. PROPOSITION. *Every field is an integral domain.*

PROOF. Let $\Bbbk$ be a field. Suppose that $u, v \in \Bbbk$ and $uv = 0$. If $u \neq 0$, we can multiply by u^{-1} to obtain

$$v = u^{-1}uv = 0,$$

hence $v = 0$. So at least one of u, v must be 0. □

1.15. LEMMA. *Let R be an integral domain. If $p \in R$ is a non-zero prime then it is irreducible.*

PROOF. Suppose that $p = uv$ for some $u, v \in R$. Then $p \mid u$ or $p \mid v$, and we might as well assume that $u = tp$ for some $t \in R$. Then $(1 - tv)p = 0$ and so $tv = 1$, showing that v is a unit with inverse t. □

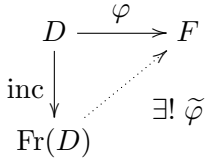
Now let D be an integral domain. A natural question to ask is whether D is isomorphic to a subring of a field. This is certainly true for the integers $\mathbb{Z}$ which are contained in the field of rational numbers $\mathbb{Q}$, and for a prime $p > 0$, the prime ring $\mathbb{F}_p$ is itself a field.

1.16. DEFINITION. The fields $\mathbb{Q}$ and $\mathbb{F}_p$ where $p > 0$ is a prime are the *prime fields*.

Of course, we can view $\mathbb{Z}$ as a subring of any subfield of the complex numbers so an answer to this question may not be unique! However, there is always a 'smallest' such field which is unique up to an isomorphism.

1.17. THEOREM. *Let D be an integral domain.*

(i) *There is a* field of fractions *of D, $\mathrm{Fr}(D)$, which contains D as a subring.*
(ii) *If $\varphi\colon D \longrightarrow F$ is a ring monomorphism into a field F, there is a unique homomorphism $\widetilde{\varphi}\colon \mathrm{Fr}(D) \longrightarrow F$ such that $\widetilde{\varphi}(t) = \varphi(t)$ for all $t \in D \subseteq \mathrm{Fr}(D)$.*



PROOF. (i) Consider the set

$$\mathrm{P}(D) = \{(a, b) : a, b \in D,\ b \neq 0\}.$$

Now introduce an equivalence relation $\sim$ on $\mathrm{P}(D)$, namely

$$(a', b') \sim (a, b) \quad \Longleftrightarrow \quad ab' = a'b.$$

Of course, it is necessary to check that this relation *is* an equivalence relation; this is left as an exercise. We denote the equivalence class of (a, b) by $[a, b]$ and the set of equivalence classes by $\mathrm{Fr}(D)$.

We define addition and multiplication on $\mathrm{Fr}(D)$ by

$$[a, b] + [c, d] = [ad + bc, bd], \quad [a, b][c, d] = [ac, bd].$$

We need to verify that these operations are well defined. For example, if $[a', b'] = [a, b]$ and $[c', d'] = [c, d]$, then

$$(a'd' + b'c')bd = a'd'bd + b'c'bd = ab'd'd + b'bcd' = (ad + bc)b'd',$$

and so $(a'd' + b'c', b'd') \sim (ad + bc, bd)$; hence addition is well defined. A similar calculation shows that $(a'c', b'd') \sim (ac, bd)$, so multiplication is also well defined. It is now straightforward to show that $\mathrm{Fr}(D)$ is a commutative ring with zero $0 = [0, 1]$ and unit $1 = [1, 1]$. In fact, as we will soon see, $\mathrm{Fr}(D)$ is a field.

Let $[a, b] \in \mathrm{Fr}(D)$. Then $[a, b] = [0, 1]$ if and only if $(0, 1) \sim (a, b)$ which is equivalent to requiring that $a = 0$; notice that for any $b \neq 0$, $[0, b] = [0, 1]$. We also have $[a, b] = [1, 1]$ if and only if $a = b$.

Now let $[a, b] \in \mathrm{Fr}(D)$ be non-zero, *i.e.*, $a \neq 0$. Then $b \neq 0$ and $[a, b], [b, a] \in \mathrm{Fr}(D)$ satisfy

$$[a, b][b, a] = [ab, ba] = [1, 1] = 1,$$

so $[a, b]$ has $[b, a]$ as an inverse. This shows that $\mathrm{Fr}(D)$ is a field.

We can view D as a subring of $\mathrm{Fr}(D)$ using the map

$$j \colon D \longrightarrow \mathrm{Fr}(D); \quad j(t) = [t, 1]$$

which is a ring homomorphism; it is easy to check that it is a monomorphism. Therefore we may identify $t \in D$ with $j(t) = [t, 1] \in \mathrm{Fr}(D)$ and D with the subring $\operatorname{im} j \subseteq \mathrm{Fr}(D)$.
(ii) Consider the function

$$\Phi \colon \mathrm{P}(D) \longrightarrow F; \quad \Phi(a, b) = \varphi(a)\varphi(b)^{-1}.$$

If $(a', b') \sim (a, b)$, then

$$\begin{aligned} \Phi(a', b') = \varphi(a')\varphi(b')^{-1} &= \varphi(a')\varphi(b)\varphi(b)^{-1}\varphi(b')^{-1} \\ &= \varphi(a'b)\varphi(b)^{-1}\varphi(b')^{-1} \\ &= \varphi(ab')\varphi(b')^{-1}\varphi(b)^{-1} \\ &= \varphi(a)\varphi(b')\varphi(b')^{-1}\varphi(b)^{-1} \\ &= \varphi(a)\varphi(b)^{-1} = \Phi(a, b), \end{aligned}$$

so Φ is constant on each equivalence class of $\sim$. Hence we may define the function

$$\widetilde{\varphi} \colon \mathrm{Fr}(D) \longrightarrow F; \quad \widetilde{\varphi}([a, b]) = \Phi(a, b).$$

It is now easy to verify that $\widetilde{\varphi}$ is a ring homomorphism which agrees with φ on $D \subseteq \mathrm{Fr}(D)$. □

The next three corollaries are left as an exercise.

1.18. Corollary. *If F is a field then $F = \mathrm{Fr}(F)$.*

1.19. Corollary. *If D is a subring of a field F, then $\mathrm{Fr}(D) \subseteq \mathrm{Fr}(F) = F$ and $\mathrm{Fr}(D)$ is the smallest subfield of F containing D.*

1.20. Corollary. *Let D_1 and D_2 be integral domains and let $\varphi \colon D_1 \longrightarrow D_2$ be a ring monomorphism. Then there is a unique induced ring homomorphism $\varphi_* \colon \mathrm{Fr}(D_1) \longrightarrow \mathrm{Fr}(D_2)$ which satisfies $\varphi_*(t) = \varphi(t)$ whenever $t \in D_1 \subseteq \mathrm{Fr}(D_1)$.*

$$\begin{array}{ccc} D_1 & \xrightarrow{\varphi} & D_2 \\ \downarrow{\scriptstyle \mathrm{inc}} & & \downarrow{\scriptstyle \mathrm{inc}} \\ \mathrm{Fr}(D_1) & \xrightarrow[\varphi_*]{} & \mathrm{Fr}(D_2) \end{array}$$

Moreover, this construction has the following properties.

- *If* $\varphi\colon D_1 \longrightarrow D_2$ *and* $\theta\colon D_2 \longrightarrow D_3$ *are monomorphisms between integral domains then* $\theta_* \circ \varphi_* = (\theta \circ \varphi)_*$ *as homomorphisms* $\mathrm{Fr}(D_1) \longrightarrow \mathrm{Fr}(D_3)$.
- *For any integral domain* D*, the identity homomorphism* $\mathrm{id}\colon D \longrightarrow D$ *induces the identity homomorphism* $(\mathrm{id})_* = \mathrm{id}\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$.

$$\begin{array}{ccccc} D_1 & \xrightarrow{\varphi} & D_2 & \xrightarrow{\theta} & D_3 \\ \downarrow{\scriptstyle \mathrm{inc}} & & \downarrow{\scriptstyle \mathrm{inc}} & & \downarrow{\scriptstyle \mathrm{inc}} \\ \mathrm{Fr}(D_1) & \xrightarrow[\varphi_*]{} & \mathrm{Fr}(D_2) & \xrightarrow[\theta_*]{} & \mathrm{Fr}(D_3) \end{array} \qquad \begin{array}{ccc} D & \xrightarrow{\mathrm{id}} & D \\ \downarrow{\scriptstyle \mathrm{inc}} & & \downarrow{\scriptstyle \mathrm{inc}} \\ \mathrm{Fr}(D) & \xrightarrow[\mathrm{id}_* = \mathrm{id}]{} & \mathrm{Fr}(D) \end{array}$$

1.21. Remarks. (a) When working with a field of fractions we usually adopt the familiar notation

$$\frac{a}{b} = a/b = [a, b]$$

for the equivalence class of (a, b). The rules for algebraic manipulation of such symbols are the usual ones for working with fractions, *i.e.*,

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}, \quad \frac{a_1}{b_1} \times \frac{a_2}{b_2} = \frac{a_1}{b_1}\,\frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}.$$

The field of fractions of an integral domain is sometimes called its *field of quotients*, however as the word quotient is also associated with quotient rings we prefer to avoid using that terminology. (b) Corollary 1.20 is sometimes said to imply that the construction of $\mathrm{Fr}(D)$ is *functorial* in the integral domain D.

1.2. Polynomial rings

Let R be a commutative ring. We will make frequent use of the *ring* $R[X]$ *of polynomials over* R *in an indeterminate* X. This consists of elements of form

$$p(X) = p_0 + p_1 X + \cdots + p_m X^m$$

where $m \geqslant 0$ and $p_0, p_1, \ldots, p_m \in R$; such $p(X)$ are called *polynomials*. Addition and multiplication in $R[X]$ are defined by

$$(p_0 + p_1 X + \cdots + p_m X^m) + (q_0 + q_1 X + \cdots + q_m X^m) = \\ (p_0 + q_0) + (p_1 + q_1)X + \cdots + (p_m + q_m)X^m,$$

and

$$(p_0 + p_1 X + \cdots + p_m X^m)(q_0 + q_1 X + \cdots + q_m X^m) = \\ (p_0 q_0) + (p_0 q_1 + p_1 q_0)X + \cdots + (p_0 q_m + p_1 q_{m-1} + \cdots + p_{m-1} q_1 + p_m q_0)X^{2m}.$$

Then $R[X]$ is a commutative ring with the constant polynomials 0 and 1 as its zero and unit. We identify $r \in R$ with the obvious constant polynomial; this allows us to view R as a subring of $R[X]$ and the inclusion function $\mathrm{inc}\colon R \longrightarrow R[X]$ is a monomorphism.

More generally, we inductively can define the ring of polynomials in n indeterminates $X_1, \ldots, X_n$ over R,

$$R[X_1, \ldots, X_n] = R[X_1, \ldots, X_{n-1}][X_n]$$

for $n \geqslant 1$. Again there is an inclusion monomorphism $\mathrm{inc}\colon R \longrightarrow R[X_1, \ldots, X_n]$ which sends each element of R to itself considered as a constant polynomial.

These polynomial rings have an important *universal property.*

1.22. THEOREM (Homomorphism Extension Property). *Let $\varphi\colon R \longrightarrow S$ be a ring homomorphism.*

(i) *For each $s \in S$ there is a unique ring homomorphism $\varphi_s\colon R[X] \longrightarrow S$ for which*
- $\varphi_s(r) = \varphi(r)$ *for all* $r \in R$,
- $\varphi_s(X) = s$.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \text{inc}}\downarrow & \nearrow_{\exists!\ \varphi_s} & \\ R[X] & & \end{array}$$

(ii) *For $n \geqslant 1$ and $s_1, \ldots, s_n \in S$, there is a unique ring homomorphism*

$$\varphi_{s_1,\ldots,s_n}\colon R[X_1, \ldots, X_n] \longrightarrow S$$

for which
- $\varphi_{s_1,\ldots,s_n}(r) = \varphi(r)$ *for all* $r \in R$,
- $\varphi_{s_1,\ldots,s_n}(X_i) = s_i$ *for* $i = 1, \ldots, n$.

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ {\scriptstyle \text{inc}}\downarrow & \nearrow_{\exists!\ \varphi_{s_1,\ldots,s_n}} & \\ R[X_1, \ldots, X_n] & & \end{array}$$

PROOF. (Sketch)
(i) For a polynomial $p(X) = p_0 + p_1X + \cdots + p_mX^m \in R[X]$, we define

$$\varphi_s(p(X)) = \varphi(p_0) + \varphi(p_1)s + \cdots + \varphi(p_m)s^m \in S. \tag{1.3}$$

It is then straightforward to check that φ_s is a ring homomorphism with the stated properties and moreover is the unique such homomorphism.
(ii) is proved by induction on n using (i). □

We will refer to $\varphi_{s_1,\ldots,s_n}$ as the *extension of φ by evaluation at $s_1, \ldots, s_n$*. It is standard to write

$$p(s_1, \ldots, s_n) = \varphi_{s_1,\ldots,s_n}(p(X_1, \ldots, X_n)).$$

An important special case occurs when we start with the identity homomorphism $\mathrm{id}\colon R \longrightarrow R$ and $r_1, \ldots, r_n \in R$; then we have the homomorphism

$$\varepsilon_{r_1,\ldots,r_n} = \mathrm{id}_{r_1,\ldots,r_n}\colon R[X_1, \ldots, X_n] \longrightarrow R.$$

Slightly more generally we may take the inclusion of a subring $\mathrm{inc}\colon R \longrightarrow S$ and $s_1, \ldots, s_n \in S$; then

$$\varepsilon_{s_1,\ldots,s_n} = \mathrm{inc}_{s_1,\ldots,s_n}\colon R[X_1, \ldots, X_n] \longrightarrow S$$

is called *evaluation at $s_1, \ldots, s_n$* and we denote its image by

$$R[s_1, \ldots, s_n] = \varepsilon_{s_1,\ldots,s_n}\, R[X_1, \ldots, X_n] \subseteq S.$$

Then $R[s_1, \ldots, s_n]$ is a subring of S, called the *subring generated by $s_1, \ldots, s_n$ over R.*

Here is an example illustrating how we will use such evaluation homomorphisms.

1.23. Example. Consider the inclusion homomorphism $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$. We have the evaluation at i homomorphism ε_i, for which $\varepsilon_i(X) = i$. We easily see that $\varepsilon_i\, \mathbb{Q}[X] \subseteq \mathbb{C}$ is a subring $\mathbb{Q}[i] \subseteq \mathbb{C}$ consisting of the complex numbers of form $a + bi$ with $a, b \in \mathbb{Q}$.

Notice that if we had used $-i$ instead of i, evaluation at $-i$, ε_{-i}, we would also have $\varepsilon_{-i}\, \mathbb{Q}[X] = \mathbb{Q}[i]$. These evaluation homomorphisms are related by complex conjugation since

$$\varepsilon_{-i}(p(X)) = \overline{\varepsilon_i(p(X))},$$

which is equivalent to the functional equation

$$\varepsilon_{-i} = (\overline{\ }) \circ \varepsilon_i\,.$$

Notice also that in these examples we have

$$\ker \varepsilon_{-i} = \ker \varepsilon_i = (X^2 + 1) \lhd \mathbb{Q}[X],$$

hence we also have

$$\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2 + 1).$$

In fact $(X^2 + 1)$ is actually a maximal ideal and so $\mathbb{Q}[i] \subseteq \mathbb{C}$ is a subfield; later we will write $\mathbb{Q}(i)$ for this subfield.

1.24. Proposition. *Let R be an integral domain.*

(i) *The ring $R[X]$ of polynomials in an indeterminate X over R is an integral domain.*
(ii) *The ring $R[X_1, \ldots, X_n]$ of polynomials in the indeterminates $X_1, \ldots, X_n$ over R is an integral domain.*

1.25. Corollary. *Let $\Bbbk$ be a field and $n \geqslant 1$. Then the polynomial ring $\Bbbk[X_1, \ldots, X_n]$ in the indeterminates $X_1, \ldots, X_n$ is an integral domain.*

As we will make considerable use of such rings we describe in detail some of their important properties. First we recall *long division* in a polynomial ring $\Bbbk[X]$ over a field $\Bbbk$; full details can be found in a basic course on commutative rings or any introductory book on this subject.

1.26. Theorem (Long Division). *Let $\Bbbk$ be a field. Let $f(X), d(X) \in \Bbbk[X]$ and assume that $d(X) \neq 0$ so that $\deg d(X) > 0$. Then there are unique polynomials $q(X), r(X) \in \Bbbk[X]$ for which*

$$f(X) = q(X)d(X) + r(X)$$

and either $\deg r(X) < \deg d(X)$ or $r(X) = 0$.

In the situation discussed in this result, the following names are often used. We refer to the process of finding $q(X)$ and $r(X)$ as *long division of $f(X)$ by $d(X)$*. Also,

$$f(X) = \text{the } \textit{dividend}, \quad d(X) = \text{the } \textit{divisor}, \quad q(X) = \text{the } \textit{quotient}, \quad r(X) = \text{the } \textit{remainder}.$$

1.27. Example. For $\Bbbk = \mathbb{Q}$, find the quotient and remainder when $f(X) = 6X^4 - 6X^3 + 3X^2 - 3X + 1$ is divided by $d(X) = 2X^2 + 1$.

SOLUTION. In the usual notation we have the following calculation.

$$\begin{array}{r|l} & 3X^2 - 3X \\ \hline 2X^2 + 1 & 6X^4 - 6X^3 + 3X^2 - 3X + 1 \\ & 6X^4 + 0X^3 + 3X^2 + 0X + 0 \\ \hline & -6X^3 + 0X^2 - 3X + 1 \\ & -6X^3 + 0X^2 - 3X + 0 \\ \hline & 1 \end{array}$$

Hence

$$6X^4 - 6X^3 + 3X^2 - 3X + 1 = (3X^2 - 3X)(2X^2 + 1) + 1,$$

giving $q(X) = 3X^2 - 3X$ and $r(X) = 1$. □

1.28. EXAMPLE. For $\Bbbk = \mathbb{F}_5$, find the quotient and remainder when $f(X) = 10X^5 + 6X^4 - 6X^3 + 3X^2 - 3X + 1$ is divided by $d(X) = 2X^2 + 1$.

SOLUTION. First notice that working modulo 5 we have

$$f(X) = 10X^5 + 6X^4 - 6X^3 + 3X^2 - 3X + 1 \equiv X^4 + 4X^3 + 3X^2 + 2X + 1 \pmod 5.$$

Notice also following multiplicative inverses in $\mathbb{F}_5$:

$$2^{-1} \equiv 3 \pmod 5, \quad 3^{-1} \equiv 2 \pmod 5, \quad 4^{-1} \equiv 4 \pmod 5.$$

We have the following calculation.

$$\begin{array}{r|l} & 3X^2 + 2X \\ \hline 2X^2 + 1 & 6X^4 + 4X^3 + 3X^2 + 2X + 1 \\ & 6X^4 + 0X^3 + 3X^2 + 0X + 0 \\ \hline & 4X^3 + 0X^2 + 2X + 1 \\ & 4X^3 + 0X^2 + 2X + 0 \\ \hline & 1 \end{array}$$

Hence

$$6X^4 - 6X^3 + 3X^2 - 3X + 1 \equiv (3X^2 + 2X)(2X^2 + 1) + 1 \pmod 5,$$

giving $q(X) = 3X^2 + 2X$ and $r(X) = 1$. □

An important consequence of Theorem 1.26 is the following which makes use of the *Euclidean Algorithm*.

1.29. COROLLARY. *Let $\Bbbk$ be a field and X an indeterminate. Let $f(X), g(X) \in \Bbbk[X]$ be non-zero. Then there are $a(X), b(X) \in \Bbbk[X]$ such that*

$$a(X)f(X) + b(X)g(X) = \gcd(f(X), g(X)).$$

Here the *greatest common divisor* $\gcd(f(X), g(X))$ of $f(X), g(X)$ is the monic polynomial of greatest degree which divides both of $f(X), g(X)$.

1.30. Proposition. *Let $\Bbbk$ be a field and X an indeterminate. Then a non-constant polynomial $p(X) \in \Bbbk[X]$ is irreducible if and only if it is a prime.*

Proof. By Lemma 1.15 we already know that $p(X)$ is irreducible if it is prime. So suppose that $p(X)$ is irreducible and that $p(X) \mid u(X)v(X)$ for $u(X), v(X) \in \Bbbk[X]$. Then by Corollary 1.29, there are $a(X), b(X) \in \Bbbk[X]$ such that

$$a(X)p(X) + b(X)u(X) = \gcd(p(X), u(X)).$$

But since $p(X)$ is irreducible, $\gcd(p(X), u(X)) = p(X)$ or $\gcd(p(X), u(X)) = 1$. In the latter case,

$$a(X)p(X) + b(X)u(X) = 1,$$

and multiplying through by $v(X)$ gives

$$a(X)p(X)v(X) + b(X)u(X)v(X) = v(X)$$

and so $p(X) \mid v(X)$. This shows that $p(X) \mid u(X)$ or $p(X) \mid v(X)$, and so $p(X)$ is prime. □

1.31. Theorem. *Let $\Bbbk$ be a field and X an indeterminate.*

(i) *Every ideal $I \lhd \Bbbk[X]$ is principal,* i.e., *$I = (h(X))$ for some $h(X) \in \Bbbk[X]$.*
(ii) *The ideal $(p(X)) \lhd \Bbbk[X]$ is prime if and only if $p(X) = 0$ or $p(X)$ is irreducible in $\Bbbk[X]$.*
(iii) *The quotient ring $\Bbbk[X]/(p(X))$ is an integral domain if and only if $p(X) = 0$ or $p(X)$ is irreducible in $\Bbbk[X]$.*
(iv) *The quotient ring $\Bbbk[X]/(p(X))$ is a field if and only if $p(X)$ is an irreducible in $\Bbbk[X]$.*

Proof. (i) Let $I \lhd \Bbbk[X]$ and assume that $I \neq (0)$. Then there must be at least one element of I with positive degree and so we can choose $h(X) \in I$ of minimal degree, say $d = \deg h(X)$.

Now let $p(X) \in I$. By Long Division, there are $q(X), r(X) \in \Bbbk[X]$ such that

$$p(X) = q(X)h(X) + r(X) \quad \text{and } \deg r(X) < d \text{ or } r(X) = 0.$$

Since $p(X)$ and $h(X)$ are in the ideal I, we also have

$$r(X) = p(X) - q(X)h(X) \in I.$$

If $r(X) \neq 0$, this would contradict the minimality of d, so we must have $r(X) = 0$, showing that $p(X) = q(X)h(X)$. Thus $I \subseteq (p(X)) \subseteq I$ and therefore $I = (p(X))$.

(ii) This follows from Proposition 1.30.

(iii) This follows from Proposition 1.7(i).

(iv) Since $\Bbbk[X]$ is an integral domain and not a field, it follows that if $\Bbbk[X]/(p(X))$ is a field then because it is an integral domain, $p(X)$ is an irreducible by (iii).

Suppose that $p(X)$ is irreducible (and hence is non-zero). Then for any $q(X) \in \Bbbk[X]$ with $q(X) \notin (p(X))$, by Corollary 1.29 we can find suitable $a(X), b(X) \in \Bbbk[X]$ for which

$$a(X)p(X) + b(X)q(X) = \gcd(p(X), q(X)).$$

But $\gcd(p(X), q(X)) = 1$ since $p(X)$ is irreducible, so

$$a(X)p(X) + b(X)q(X) = 1.$$

This shows that in the quotient ring $\Bbbk[X]/(p(X))$ the residue class of $q(X)$ has the residue class of $b(X)$ as its inverse. □

1.32. Remark. In connection with Theorem 1.31(i), notice that if $p(X) \in \Bbbk[X]$, then provided $d = \deg p(X) > 0$, we have for some $p_d \neq 0$,

$$p(X) = p_0 + p_1 X + \cdots + p_d X^d = p_d q(X),$$

where

$$q(X) = p_d^{-1} p_0 + p_d^{-1} p_1 X + \cdots + p_d^{-1} p_{d-1} X^{d-1} + X^d.$$

This easily implies that as ideals of $\Bbbk[X]$, $(p(X)) = (q(X))$. So we can always find a monic polynomial as the generator of a given ideal, and this monic polynomial is unique.

1.33. Proposition (Unique Factorization Property). *Every non-constant polynomial $f(x) \in \Bbbk[X]$ has a factorization*

$$f(x) = c p_1(X) \cdots p_k(X),$$

where $c \in \Bbbk$, and $p_1(X), \ldots, p_k(X) \in \Bbbk[X]$ are irreducible monic polynomials. Moreover, c is unique and the sequence of polynomials $p_1(X), \ldots, p_k(X)$ is unique apart from the order of the terms.

Proof. (Sketch)
Existence is proved by induction on the degree of $f(X)$ and begins with the obvious case $\deg f(X) = 1$. If $\deg f(X) > 1$, then either $f(X)$ is already irreducible, or $f(X) = f_1(X) f_2(X)$ with both factors of positive degree, and therefore $\deg f_j(X) < \deg f(X)$. This gives the inductive step.

To prove uniqueness, suppose that

$$p_1(X) \cdots p_k(X) = q_1(X) \cdots q_\ell(X)$$

where $p_i(X), q_j(X) \in \Bbbk[X]$ are irreducible monic polynomials. Then by Proposition 1.30, each $p_i(X)$ is prime, hence divides one of the $q_j(X)$, hence must equal it. By reordering we can assume that $p_i(X) = q_i(X)$ and $k \leqslant \ell$. After cancelling common factors we obtain

$$q_{k+1}(X) \cdots q_\ell(X) = 1,$$

and so we see that $k = \ell$. □

1.34. Corollary. *Suppose that $f(X) \in \Bbbk[X]$ factors into linear factors*

$$f(X) = c(X - u_1) \cdots (X - u_d),$$

where $u_1, \ldots, u_d \in \Bbbk$. Then the sequence of roots $u_1, \ldots, u_d$ is unique apart from the order. In particular, if $v_1, \ldots, v_r$ are the distinct roots, then

$$f(X) = c(X - v_1)^{m_1} \cdots (X - v_r)^{m_r},$$

where $m_i > 0$ and this factorization is unique apart from the order of the pairs (v_i, m_i).

1.35. Corollary. *The number of distinct roots of a non-constant polynomial $f(X) \in \Bbbk[X]$ is at most* $\deg f(X)$.

1.36. Definition. If $\Bbbk$ is a field and X an indeterminate, then the field of fractions of $\Bbbk[X]$ is the *field of rational functions*, $\Bbbk(X)$. The elements of $\Bbbk(X)$ are fractions of the form

$$\frac{a_0 + a_1 X + \cdots + a_m X^m}{b_0 + b_1 X + \cdots + b_n X^n}$$

with $a_i, b_j \in \Bbbk$ and $b_0 + b_1 X + \cdots + b_n X^n \neq 0$.

1.3. Identifying irreducible polynomials

When $\Bbbk$ is a field, we will need some effective methods for deciding when a polynomial in $\Bbbk[X]$ is irreducible.

Let us consider factorisation of polynomials over $\mathbb{Q}$. If $f(X) \in \mathbb{Z}[X]$ then we can also consider $f(X)$ as an element of $\mathbb{Q}[X]$. If $R = \mathbb{Z}$ or $\mathbb{Q}$, we say that $f(X)$ has a *proper factorisation over* R if $f(X) = g(X)h(X)$ for some $g(X), h(X) \in R[X]$ with $\deg g(X) > 0$ and $\deg h(X) > 0$.

1.37. Proposition (Gauss's Lemma). *Let $f(X) \in \mathbb{Z}[X]$. Then $f(X)$ has a proper factorisation over $\mathbb{Z}$ if and only it has a proper factorisation over $\mathbb{Q}$.*

So to find factors of $f(X)$ it is sufficient to look for factors in $\mathbb{Z}[X]$. Our next result is a special case of the *Eisenstein Irreducibility Test*. The version here is slightly more general than the more usual one which corresponds to taking $s = 0$.

1.38. Proposition (Eisenstein Test). *Let $f(X) \in \mathbb{Z}[X]$ and $s \in \mathbb{Z}$. Choose $a_i \in \mathbb{Z}$ so that*

$$f(X) = a_0 + a_1(X - s) + \cdots + a_{d-1}(X - s)^{d-1} + a_d(X - s)^d,$$

where $d = \deg f(X)$. Suppose that $p > 0$ is a prime for which the following three conditions hold:

- $a_k \equiv 0 \pmod{p}$ *for $k = 0, \ldots, d-1$;*
- $a_0 \not\equiv 0 \pmod{p^2}$;
- $a_d \not\equiv 0 \pmod{p}$.

Then $f(X)$ is irreducible in $\mathbb{Q}[X]$ and hence also in $\mathbb{Z}[X]$.

1.39. Example. Let $p \geqslant 2$ be a prime. Then the polynomial

$$\Phi_p(X) = 1 + X + \cdots + X^{p-1} \in \mathbb{Z}[X]$$

is irreducible in $\mathbb{Q}[X]$ and hence also in $\mathbb{Z}[X]$.

Proof. Working in $\mathbb{Z}[X]$,

$$\begin{aligned}
\Phi_p(X)(X-1) &= (1 + X + \cdots + X^{p-1})(X-1) \\
&= X^p - 1 \\
&= (1 + (X-1))^p - 1 \\
&= \sum_{k=1}^{p} \binom{p}{k} (X-1)^k \\
&\equiv (X-1)^p \pmod{p},
\end{aligned}$$

since by (1.2a), p divides

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}$$

when $k = 1, \ldots, p-1$. Hence

$$\Phi_p(X) \equiv (X-1)^{p-1} \pmod{p}$$

Also,

$$\binom{p}{1} = p \not\equiv 0 \pmod{p^2},$$

giving

$$\Phi_p(X) = (X-1)^{p-1} + c_{p-2}(X-1)^{p-2} + \cdots + c_1(X-1) + c_0 \tag{1.4}$$

with $c_r \equiv 0 \pmod{p}$ and $c_0 = p$. So the Eisenstein Test can be applied here with $s = 1$ to show that $\Phi_p(X)$ is irreducible in $\mathbb{Z}[X]$. □

1.40. Example. As examples we have the irreducible polynomials

$$\begin{aligned}
\Phi_2(X) &= 1 + X, \\
\Phi_3(X) &= 1 + X + X^2, \\
\Phi_5(X) &= 1 + X + X^2 + X^3 + X^4, \\
\Phi_7(X) &= 1 + X + X^2 + X^3 + X^4 + X^5 + X^6, \\
\Phi_{11}(X) &= 1 + X + X^2 + X^3 + X^4 + X^5 + X^6 + X^7 + X^8 + X^9 + X^{10}.
\end{aligned}$$

These are examples of the *cyclotomic polynomials* $\Phi_n(X) \in \mathbb{Z}[X]$ which are defined for all $n \geqslant 1$ by

$$X^n - 1 = \prod_{d|n} \Phi_d(X), \tag{1.5a}$$

where the product is taken over all the positive divisors of n (including 1 and n). For example,

$$\begin{aligned}
X^2 - 1 &= (X-1)(X+1) = \Phi_1(X)\Phi_2(X), \\
X^3 - 1 &= (X-1)(X^2+X+1) = \Phi_1(X)\Phi_3(X), \\
X^4 - 1 &= (X-1)(X+1)(X^2+1) = \Phi_1(X)\Phi_2(X)\Phi_4(X), \\
X^5 - 1 &= (X-1)(X^4+X^3+X^2+X+1) = \Phi_1(X)\Phi_5(X), \\
X^6 - 1 &= (X-1)(X+1)(X^2+X+1)(X^2-X+1) = \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_6(X), \\
X^{12} - 1 &= (X-1)(X+1)(X^2+X+1)(X^2+1)(X^2-X+1)(X^4-X^2+1) \\
&= \Phi_1(X)\Phi_2(X)\Phi_3(X)\Phi_4(X)\Phi_6(X)\Phi_{12}(X).
\end{aligned}$$

Cyclotomic polynomials can be computed recursively using Equation (1.5a). If we know $\Phi_k(X)$ for $k < n$, then

$$\Phi_n(X) = \frac{X^n - 1}{\displaystyle\prod_{\substack{d|n \\ d<n}} \Phi_d(X)}. \tag{1.5b}$$

The degree of $\Phi_n(X)$ involves a function of n probably familiar from elementary Number Theory.

1.41. Definition. The *Euler function* $\varphi\colon \mathbb{N} \longrightarrow \mathbb{N}$ is defined by

$$\begin{aligned}
\varphi(n) &= \text{number of } k = 1, \ldots, n \text{ for which } \gcd(n,k) = 1 \\
&= |(\mathbb{Z}/n)^\times| = \text{number of units in } \mathbb{Z}/n \\
&= \text{number of generators of the cyclic group } \mathbb{Z}/n.
\end{aligned}$$

In particular, if $p \geqslant 2$ is a prime then $\varphi(p) = p - 1$. Of course, $\varphi(1) = 1$.

It can be shown that for each natural number n,

$$\sum_{d|n} \varphi(d) = n. \tag{1.6}$$

Notice that we can inductively determine $\varphi(n)$ using this equation. For example, if p and q are *distinct* primes, then

$$\varphi(pq) = pq - (\varphi(p) + \varphi(q) + \varphi(1)) = pq - (p-1) - (q-1) - 1 = (p-1)(q-1).$$

It is also true that whenever m, n are coprime, *i.e.*, when $\gcd(m,n) = 1$,

$$\varphi(mn) = \varphi(m)\varphi(n). \tag{1.7}$$

Thus if $n = p_1^{r_1} \cdots p_s^{r_s}$ where $p_1 < p_2 < \cdots < p_s$ are the prime factors of n and $r_j > 0$, then

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_s^{r_s}). \tag{1.8}$$

Furthermore, if p is a prime and $r > 0$, then

$$\varphi(p^r) = (p-1)p^{r-1}. \tag{1.9}$$

Notice that as a result, $\varphi(n)$ is even when $n > 2$.

1.42. Remark. For those who know about the *Möbius function* μ (which takes values $0, \pm 1$) and *Möbius inversion*, the latter can be used to solve Equation (1.6) for φ, giving

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}. \tag{1.10}$$

Similarly, the formulae of (1.5) lead to

$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)}. \tag{1.11}$$

So for example, if p, q are distinct primes, then using standard properties of μ,

$$\begin{aligned} \Phi_{pq}(X) &= (X^{pq}-1)^{\mu(1)}(X^{pq/p}-1)^{\mu(p)}(X^{pq/q}-1)^{\mu(q)}(X^{pq/pq}-1)^{\mu(pq)} \\ &= (X^{pq}-1)(X^q-1)^{-1}(X^p-1)^{-1}(X-1) = \frac{(X^{pq}-1)(X-1)}{(X^q-1)(X^p-1)}. \end{aligned}$$

Recall that an element ζ of a field K is a *primitive n-th root of unity* if

$$\min\{k : 1 \leqslant k \text{ and } \zeta^k = 1\} = n.$$

We think of $\zeta_n = e^{2\pi i/n}$ as the *standard complex primitive n-th root of unity.* Then every complex n-th root of unity has the form $\zeta_n^k = e^{2\pi ik/n}$ for $k = 0, 1, \ldots, n-1$.

1.43. Theorem. *For each $n \geqslant 1$, the cyclotomic polynomial $\Phi_n(X)$ is irreducible in $\mathbb{Q}[X]$ and hence in $\mathbb{Z}[X]$. The complex roots of $\Phi_n(X)$ are the primitive n-th roots of unity,*

$$\zeta_n^k = e^{2\pi ik/n} \quad (0 \leqslant k \leqslant n-1,\ \gcd(k,n) = 1).$$

and the number of these is $\deg \Phi_n(X) = \varphi(n)$. *Hence,*

$$\Phi_n(X) = \prod_{\substack{t=1,\ldots,n-1 \\ \gcd(t,n)=1}} (X - \zeta_n^t).$$

Proof. We will give a reformulation and proof of this in Theorem 6.2. □

1.44. Example. For $n = 6$ we have

$$\zeta_6 = e^{2\pi i/6} = e^{\pi i/3} = \frac{1}{2} + \frac{\sqrt{3}}{2} i.$$

Then $\varphi(6) = 2$ and

$$\Phi_6(X) = X^2 - X + 1 = (X - \zeta_6)(X - \zeta_6^5).$$

It is also worth recording a related general result on cyclic groups.

1.45. Proposition. *Let $n \geqslant 1$ and $C = \langle g \rangle$ be a cyclic group of order n and a generator g. Then an element $g^r \in C$ is a generator if and only if $\gcd(r, n) = 1$; the number of such elements of C is $\varphi(n)$.*

This leads to a useful group theoretic result.

1.46. Lemma. *Let G be a finite group satisfying the following condition:*

- *For each $n \geqslant 1$, there are at most n solutions of $x^n = \iota$ in G.*

Then G is cyclic and in particular is abelian.

Proof. Let $\theta_G(d)$ denote the number of elements in G of order d. By Lagrange's Theorem, $\theta_G(d) = 0$ unless d divides $|G|$. Since

$$G = \bigcup_{d||G|} \{g \in G : |g| = d\},$$

we have

$$|G| = \sum_{d||G|} \theta_G(d).$$

Recall the Euler φ-function satisfies Equation (1.6), hence

$$|G| = \sum_{d||G|} \varphi(d).$$

Combining these we obtain

$$\sum_{d||G|} \theta_G(d) = \sum_{d||G|} \varphi(d). \tag{1.12}$$

Let d be a divisor of $|G|$. By Proposition 1.45, for each element $g \in G$ of order d, the cyclic subgroup $\langle g \rangle \leqslant G$ has $\varphi(d)$ generators, each of order d. As there are at most d such elements g in G, this gives $\theta_G(d) \leqslant \varphi(d)$. So

$$\sum_{d||G|} \theta_G(d) \leqslant \sum_{d||G|} \varphi(d).$$

Now if $\theta_G(d) < \varphi(d)$ for some d, we would have a *strict* inequality in place of Equation (1.12). Hence $\theta_G(d) = \varphi(d)$ for all d. In particular, there are $\varphi(|G|)$ elements of order $|G|$, hence there must be an element of order $|G|$, so G is cyclic. □

The above results for polynomials over $\mathbb{Q}$ and $\mathbb{Z}$ have analogues over the field of fractions $\Bbbk(T)$ and polynomial ring $\Bbbk[T]$, where $\Bbbk$ is a field.

A polynomial $f(X) \in \Bbbk[T][X]$ is an element of $\Bbbk(T)[X]$. If $R = \Bbbk[T]$ or $\Bbbk(T)$, we say that $f(X)$ has a *proper factorisation over R* if $f(X) = g(X)h(X)$ for some $g(X), h(X) \in R[X]$ with $\deg g(X) > 0$ and $\deg h(X) > 0$.

1.47. Proposition (Gauss's Lemma). *Let $f(X) \in \Bbbk[T][X]$. Then $f(X)$ has a proper factorisation over $\Bbbk[T]$ if and only it has a proper factorisation over $\Bbbk(T)$.*

Here is another version of the *Eisenstein Test*; again we state a version which is slightly more general than the usual one which corresponds to the case where $s = 0$.

1.48. Proposition (Eisenstein Test). *Let $f(X) \in \Bbbk[T][X]$ and $s \in \Bbbk[T]$. Choose $a_i \in \Bbbk[T]$ so that*

$$f(X) = a_0 + a_1(X - s) + \cdots + a_{d-1}(X - s)^{d-1} + a_d(X - s)^d,$$

where $d = \deg f(X)$. Suppose that $p(T) \in \Bbbk[T]$ is an irreducible for which the following three conditions hold:

- $a_k \equiv 0 \pmod{p(T)}$ *for $k = 0, \ldots, d-1$;*
- $a_0 \not\equiv 0 \pmod{p(T)^2}$*;*
- $a_d \not\equiv 0 \pmod{p(T)}$.

Then $f(X)$ is irreducible in $\Bbbk(T)[X]$ and hence also in $\Bbbk[T][X]$.

1.49. Example. Let $\Bbbk$ be a field. Then the polynomial $X^n - T$ is irreducible in $\Bbbk(T)[X]$.

1.4. Finding roots of complex polynomials of small degree

♡♠♣♢ In this section we work within the complex numbers and take $\Bbbk \subseteq \mathbb{C}$. In practice we will usually have $\Bbbk = \mathbb{R}$ or $\Bbbk = \mathbb{C}$.

For monic linear (degree 1) or quadratic (degree 2) polynomials, methods of finding roots are very familiar. Let us consider the cases of cubic (degree 3) and quartic (degree 4) polynomials.

Cubic polynomials: Cardan's method. The following 16th century method of finding roots of cubics is due to Jerôme Cardan who seems to have obtained some preliminary versions from Niccolò Tartaglia by somewhat disreputable means! For historical details see [**2, 3**].

A monic cubic

$$f(X) = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$$

can be transformed into one with no quadratic term by a change of variables $X \longmapsto X - a_2/3$ giving

$$g(X) = f(X - a_2/3) = X^3 - \left(a_1 - \frac{1}{3}a_2^2\right)X + \left(a_0 - \frac{a_1a_2}{3} + \frac{2a_2^3}{27}\right) \in \mathbb{C}[X].$$

Clearly finding the roots of $f(X)$ is equivalent to finding those of $g(X)$, so we may as well assume that we want to find the complex roots of

$$f(X) = X^3 + pX + q \in \mathbb{C}[X].$$

Suppose that $x \in \mathbb{C}$ is a root of $f(X)$, *i.e.*,

$$x^3 + px + q = 0. \tag{1.13}$$

If we introduce $u \in \mathbb{C}$ for which

$$x = u - \frac{p}{3u},$$

then

$$\left(u - \frac{p}{3u}\right)^3 + p\left(u - \frac{p}{3u}\right) + q = 0$$

and so

$$u^3 - \frac{p^3}{27u^3} + q = 0,$$

hence

$$u^6 + qu^3 - \frac{p^3}{27} = 0.$$

Solving for u^3 we obtain

$$u^3 = -\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}},$$

where $\sqrt{q^2 + \frac{4p^3}{27}}$ denotes one of the complex square roots of the discriminant of the quadratic equation

$$U^2 + qU - \frac{p^3}{27} = 0.$$

Now if we take u to be a cube root of one of the complex numbers

$$-\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}$$

we obtain the desired root of $f(X)$ as $x = u - p/3u$. Notice that we have a choice of 2 values for u^3 and for each of these a choice of 3 values for u, differing by factors of the form ω^r for $r = 0, 1, 2$ where $\omega = e^{2\pi i/3}$ is a primitive cube root of 1. However, since

$$\frac{1}{-q + \sqrt{q^2 + \frac{4p^3}{27}}} = \frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{q^2 - (q^2 + 4p^3/27)} = -27\frac{\left(-q - \sqrt{q^2 + \frac{4p^3}{27}}\right)}{4p^3},$$

it is easy to verify that there are in fact only 3 choices of the root x which we can write symbolically as

$$x = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}} \tag{1.14}$$

or more precisely as

$$x = \sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}} - \frac{p}{3\sqrt[3]{-\frac{q}{2} + \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}}}. \tag{1.15}$$

1.50. Example. Find the complex roots of the polynomial

$$f(X) = X^3 + 3X - 10 \in \mathbb{R}[X].$$

Solution. Applying the method above, we reduce to the quadratic equation

$$U^2 - 10U - 1 = 0$$

whose roots are $5 \pm \sqrt{26} \in \mathbb{R}$. Notice that $5 + \sqrt{26} > 0$ and $5 - \sqrt{26} < 0$; we also have

$$5 - \sqrt{26} = \frac{-1}{5 + \sqrt{26}}.$$

Now $5 + \sqrt{26}$ has the complex cube roots

$$\sqrt[3]{5 + \sqrt{26}},\ \sqrt[3]{5 + \sqrt{26}}\,\omega,\ \sqrt[3]{5 + \sqrt{26}}\,\omega^2.$$

Here we have $x = u - 1/u$, so the 3 complex roots of $f(X)$ are

$$\left(\sqrt[3]{5+\sqrt{26}} - \frac{1}{\sqrt[3]{5+\sqrt{26}}} \right) \omega^r \quad (r = 0, 1, 2).$$

Notice that one of these is real, namely

$$\sqrt[3]{5+\sqrt{26}} - \frac{1}{\sqrt[3]{5+\sqrt{26}}} = \frac{\left(\sqrt[3]{5+\sqrt{26}}\right)^2 - 1}{\sqrt[3]{5+\sqrt{26}}}.$$ □

Quartic polynomials: Ferrari's method. The following method of finding roots of quartics was publicised by Cardan who attributed it to his student Lodovicio Ferrari.

A general monic quartic polynomial

$$f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$$

can be transformed into one with no cubic term by a change of variables $X \longmapsto X - a_2/3$ giving

$$g(X) = f(X - a_3/4) =$$
$$Y^4 + \left(a_2 - \frac{3}{8}a_3^2\right)Y^2 + \left(\frac{1}{8}a_3^3 - \frac{1}{2}a_2a_3 + a_1\right)Y - \left(\frac{1}{16}a_2a_3^2 - \frac{3}{256}a_3^4 + \frac{1}{4}a_1a_3 + a_0\right).$$

Clearly finding the roots of $f(X)$ is equivalent to finding those of $g(X)$, so we may as well assume that we want to find the complex roots of

$$f(X) = X^4 + pX^2 + qX + r \in \mathbb{C}[X].$$

Suppose that x is a root and introduce numbers y, z such that $z = x^2 + y$ (we will fix the values of these later). Then

$$\begin{aligned} z^2 &= x^4 + 2x^2y + y^2 \\ &= -px^2 - qx - r + 2x^2y + y^2 \\ &= (2y - p)x^2 - qx + y^2 - r. \end{aligned}$$

Now choose y to make the last quadratic expression in x a square,

$$(2y - p)x^2 - qx + (y^2 - r) = (Ax + B)^2. \tag{1.16}$$

This can be done by requiring the vanishing of the discriminant

$$q^2 - 4(2y - p)(y^2 - r) = 0. \tag{1.17}$$

Notice that if $y = p/2$ then we would require $q = 0$ and then

$$f(X) = X^4 + pX^2 + r = (X^2)^2 + p(X^2) + r = 0$$

can be solved by solving

$$Z^2 + pZ + r = 0.$$

Since Equation (1.17) is a cubic in y, we can use the method of solution of cubics to find a root $y = t$ say. Then for Equation (1.16) we have

$$(x^2 + t)^2 = (Ax + B)^2,$$

whence

$$x^2 = -t \pm (Ax + B).$$

Thus taking the two square roots of the right hand side we obtain 4 values for x, which we write symbolically as

$$x = \pm\sqrt{-t \pm (Ax + B)}.$$

1.51. Remark. In the case of cubic and quartic polynomials over $\mathbb{C}$ we can obtain all the roots by repeatedly taking square or cube roots (or *radicals*). Consequently such polynomials are said to be *solvable by radicals*. Later we will see that this is not true in general for polynomials of degree at least 5; this is one of the great early successes of this theory.

1.5. Automorphisms of rings and fields

1.52. Definition. Let R be a ring and $R_0 \subseteq R$ a subring.

- An *automorphism of* R is a ring isomorphism $\alpha\colon R \longrightarrow R$. The set of all such automorphisms is denoted $\mathrm{Aut}(R)$.
- An *automorphism of* R *over* R_0 is a ring isomorphism $\alpha\colon R \longrightarrow R$ for which $\alpha(r) = r$ whenever $r \in R_0$. The set of all automorphisms of R over R_0 is denoted $\mathrm{Aut}_{R_0}(R)$.

1.53. Proposition. *For a ring R with a subring $R_0 \subseteq R$, $\mathrm{Aut}(R)$ and $\mathrm{Aut}_{R_0}(R)$ form groups under composition of functions.*

Proof. The composition $\alpha \circ \beta$ of two automorphisms $\alpha, \beta\colon R \longrightarrow R$ is also an automorphism of R as is the inverse of α. The identity function $\mathrm{id} = \mathrm{id}_R\colon R \longrightarrow R$ is an automorphism. Hence $\mathrm{Aut}(R)$ forms a group under composition. The argument for $\mathrm{Aut}_{R_0}(R)$ is similar. □

1.54. Proposition. *Let R be one of the core rings $\mathbb{Z}$ or $\mathbb{Z}/n$ with $n > 1$. Then*

(i) *The only automorphism of R is the identity,* i.e., $\mathrm{Aut}(R) = \{\mathrm{id}\}$.

(ii) *If S is a ring containing a core ring R and $\alpha \in \mathrm{Aut}(S)$, then α restricts to the identity on R,* i.e., *$\alpha(r) = r$ for all $r \in R$. Hence,* $\mathrm{Aut}(S) = \mathrm{Aut}_R(S)$.

Proof. (i) For such a core ring R, every element has the form $k1$ for some $k \in \mathbb{Z}$. For an automorphism α of R,

$$\begin{aligned}
\alpha(k1) &= \begin{cases} \underbrace{\alpha(1) + \cdots + \alpha(1)}_{k} & \text{if } k > 0, \\ -(\underbrace{\alpha(1) + \cdots + \alpha(1)}_{-k}) & \text{if } k < 0, \\ \alpha(0) & \text{if } k = 0 \end{cases} \\
&= \begin{cases} \underbrace{1 + \cdots + 1}_{k} & \text{if } k > 0, \\ -(\underbrace{1 + \cdots + 1}_{-k}) & \text{if } k < 0, \\ 0 & \text{if } k = 0 \end{cases} \\
&= k1.
\end{aligned}$$

Thus $\alpha = \mathrm{id}$.

(ii) For $\alpha \in \mathrm{Aut}(S)$, $\alpha(1) = 1$ and a similar argument to that for (i) shows that $\alpha(r) = r$ for all $r \in R$. □

1.55. Proposition. *Let D be an integral domain and $\alpha\colon D \longrightarrow D$ be an automorphism. Then the induced homomorphism gives an automorphism $\alpha_*\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$.*

Proof. Given α, the induced homomorphism $\alpha_*\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$ exists and we need to show it has an inverse. The inverse automorphism $\alpha^{-1}\colon D \longrightarrow D$ also gives rise to an induced homomorphism $(\alpha^{-1})_*\colon \mathrm{Fr}(D) \longrightarrow \mathrm{Fr}(D)$. Since $\alpha^{-1} \circ \alpha = \mathrm{id} = \alpha \circ \alpha^{-1}$, we can apply Corollary 1.20 to show that

$$(\alpha^{-1})_* \circ (\alpha)_* = \mathrm{id} = (\alpha)_* \circ (\alpha^{-1})_*.$$

Hence $(\alpha)_*$ is invertible with inverse $(\alpha^{-1})_*$. □

1.56. Corollary. *There is a monomorphism of groups*

$$(\ )_*\colon \mathrm{Aut}(D) \longrightarrow \mathrm{Aut}(\mathrm{Fr}(D)); \quad \alpha \longmapsto \alpha_*.$$

1.57. Example. The field of fractions of the ring of integers $\mathbb{Z}$ is the field of rationals $\mathbb{Q}$. The homomorphism

$$(\ )_*\colon \mathrm{Aut}(\mathbb{Z}) \longrightarrow \mathrm{Aut}(\mathbb{Q}); \quad \alpha \longmapsto \alpha_*$$

is an isomorphism and hence $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$.

Combining this example with Proposition 1.54(ii) we obtain another useful result.

1.58. Proposition. *Let $\Bbbk$ be one of the prime fields $\mathbb{Q}$ or $\mathbb{F}_p$ with $p > 0$ prime. If R is a ring containing $\Bbbk$ as a subring, then every automorphism of R restricts to the identity on $\Bbbk$,* i.e., $\mathrm{Aut}(R) = \mathrm{Aut}_{\Bbbk}(R)$.

Recalling Definition 1.36, we have an example which shows that the monomorphism of Corollary 1.56 need not be an epimorphism. Here we take $D = \mathbb{Q}[X]$ and $\mathrm{Fr}(\mathbb{Q}[X]) = \mathbb{Q}(X)$.

1.59. Example. The homomorphism

$$(\ )_*\colon \mathrm{Aut}(\mathbb{Q}[X]) \longrightarrow \mathrm{Aut}(\mathbb{Q}(X)); \quad \alpha \longmapsto \alpha_*$$

is a monomorphism but it is not an epimorphism since there is an automorphism

$$\gamma\colon \mathbb{Q}(X) \longrightarrow \mathbb{Q}(X); \quad \gamma(f(X)) = f(1/X)$$

which sends $X \in \mathbb{Q}[X] \subseteq \mathbb{Q}(X)$ to $1/X \notin \mathbb{Q}[X]$ and so does not restrict to an automorphism of $\mathbb{Q}[X]$.

Let $\Bbbk$ be a field. The group of invertible 2×2 matrices over $\Bbbk$ is the 2×2 *general linear group over* $\Bbbk$,

$$\mathrm{GL}_2(\Bbbk) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} : a_{ij} \in \Bbbk,\ a_{11}a_{22} - a_{12}a_{21} \neq 0 \right\}$$

The scalar matrices form a normal subgroup

$$\mathrm{Scal}_2(\Bbbk) = \{\mathrm{diag}(t,t) : t \in \Bbbk,\ t \neq 0\} \lhd \mathrm{GL}_2(\Bbbk).$$

The quotient group is called the 2×2 *projective general linear group over* $\Bbbk$,

$$\mathrm{PGL}_2(\Bbbk) = \mathrm{GL}_2(\Bbbk)/\,\mathrm{Scal}_2(\Bbbk).$$

Notice that $\mathrm{GL}_2(\Bbbk)$ has another interesting subgroup called the *affine subgroup*,

$$\mathrm{Aff}_1(\Bbbk) = \left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} : a, b \in \Bbbk,\ a \neq 0 \right\} \leqslant \mathrm{GL}_2(\Bbbk).$$

1.60. Example. Let $\Bbbk$ be a field and X an indeterminate. Then $\mathrm{Aut}_{\Bbbk}(\Bbbk[X])$ and hence $\mathrm{Aut}_{\Bbbk}(\Bbbk(X))$, contains a subgroup isomorphic to $\mathrm{Aff}_1(\Bbbk)$. In fact, $\mathrm{Aut}_{\Bbbk}(\Bbbk[X]) \cong \mathrm{Aff}_1(\Bbbk)$.

Proof. We begin by showing that to each affine matrix

$$A = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} \in \mathrm{Aff}_1(\Bbbk)$$

there is an associated automorphism $\alpha_A \colon \Bbbk[X] \longrightarrow \Bbbk[X]$.

For this we use the element $aX + b \in \Bbbk[X]$ together with the extension result of Theorem 1.22(i) to obtain a homomorphism $\alpha_A \colon \Bbbk[X] \longrightarrow \Bbbk[X]$ with $\alpha_A(X) = aX + b$. Using the inverse matrix

$$A^{-1} = \begin{bmatrix} a^{-1} & -a^{-1}b \\ 0 & 1 \end{bmatrix}$$

we similarly obtain a homomorphism $\alpha_{A^{-1}} \colon \Bbbk[X] \longrightarrow \Bbbk[X]$ for which

$$\alpha_{A^{-1}}(X) = a^{-1}X - a^{-1}b.$$

Using the same line of argument as in the proof of Proposition 1.55 (or doing a direct calculation) we see that $\alpha_{A^{-1}}$ is the inverse of α_A an so $\alpha_A \in \mathrm{Aut}_{\Bbbk}(\Bbbk[X])$. It is straightforward to check that for $A_1, A_2 \in \mathrm{Aff}_1(\Bbbk)$,

$$\alpha_{A_2A_1} = \alpha_{A_1} \circ \alpha_{A_2},$$

(note the order!) hence there is a homomorphism of groups

$$\mathrm{Aff}_1(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk[X]); \quad A \longmapsto \alpha_{A^{-1}},$$

which is easily seen to be a monomorphism. Composing with $(\ )_*$ we see that there is a monomorphism $\mathrm{Aff}_1(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$. In fact, this is also an epimorphism and we leave the proof of this as an exercise. □

1.61. Example. Let $\Bbbk$ be a field and X an indeterminate. Then

(i) $\mathrm{Aut}_{\Bbbk}(\Bbbk(X))$ contains a subgroup isomorphic to $\mathrm{PGL}_2(\Bbbk)$.
(ii) In fact, $\mathrm{Aut}_{\Bbbk}(\Bbbk(X)) \cong \mathrm{PGL}_2(\Bbbk)$.

Proof. (i) We begin by showing that to each invertible matrix

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathrm{GL}_2(\Bbbk)$$

there is an associated automorphism $\alpha^A \colon \Bbbk(X) \longrightarrow \Bbbk(X)$.

We begin by choosing the element $(a_{11}X + a_{12})/(a_{21}X + a_{22}) \in \Bbbk(X)$ and then using Theorem 1.22(i) to obtain a homomorphism $\Bbbk[X] \longrightarrow \Bbbk(X)$ that sends X to $(a_{11}X+a_{12})/(a_{21}X+a_{22})$. By applying $(\ )_*$ to this we obtain a homomorphism (known as a *fractional linear transformation*) $\alpha^A \colon \Bbbk(X) \longrightarrow \Bbbk(X)$ for which

$$\alpha^A(X) = \frac{a_{11}X + a_{12}}{a_{21}X + a_{22}}.$$

Again we find that

$$\alpha^{A_2A_1} = \alpha^{A_1} \circ \alpha^{A_2}.$$

There is an associated homomorphism of groups $\mathrm{GL}_2(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$ sending A to $\alpha^{A^{-1}}$. However, this is not an injection in general since for each scalar matrix $\mathrm{diag}(t,t)$,

$$\alpha^{\mathrm{diag}(t,t)}(X) = \frac{tX}{t} = X,$$

showing that $\alpha^{\mathrm{diag}(t,t)}$ is the identity function.

In fact it is easy to see that $\mathrm{Scal}_2(\Bbbk) \lhd \mathrm{GL}_2(\Bbbk)$ is the kernel of this homomorphism. Therefore passing to the quotient $\mathrm{PGL}_2(\Bbbk) = \mathrm{GL}_2(\Bbbk)/\mathrm{Scal}_2(\Bbbk)$ we obtain a monomorphism $\mathrm{PGL}_2(\Bbbk) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$. There is one case where $\mathrm{Scal}_2(\Bbbk)$ is the trivial group, namely $\Bbbk = \mathbb{F}_2$.

(ii) To show that every automorphism of $\Bbbk(X)$ is a fractional linear transformation is less elementary. We give a sketch proof for the case of $\Bbbk = \mathbb{C}$; actually this argument can be modified to work for any *algebraically closed* field, but an easy argument then shows the general case.

Let $\alpha \in \mathrm{Aut}_{\mathbb{C}}(\mathbb{C}(X))$. There is an associated rational (hence meromorphic) function f given by $z \longmapsto f(z)$, where $\alpha(X) = f(X)$, defined on $\mathbb{C}$ with the poles of f deleted. If we write

$$f(X) = \frac{p(X)}{q(X)}$$

where $p(X), q(X) \in \mathbb{C}[X]$ have no common factors of positive degree, then the *order* of $f(X)$ is

$$\operatorname{ord} f = \max\{\deg p(X), \deg q(X)\}.$$

Now let $c \in \mathbb{C}$. Then the number of solutions counted with algebraic multiplicity of the equation $f(z) = c$ turns out to be $\operatorname{ord} f$. Also, if $\deg p(X) \leqslant \deg q(X)$ then the number of poles of f counted with algebraic multiplicity is also $\operatorname{ord} f$. Finally, if $\deg p(X) > \deg q(X)$ then we can write

$$f(X) = p_1(X) + \frac{p_0(X)}{q(X)},$$

where $p_0(X), p_1(X) \in \mathbb{C}[X]$ and $\deg p_0(X) < \deg q(X)$. Then the number of poles of f counted with algebraic multiplicity is

$$\deg p_1(X) + \operatorname{ord} \frac{p_0}{q}.$$

Now it is easy to see that since α is invertible so is the function f. But this can only happen if the function f is injective which means that all of these numbers must be 1, hence $\operatorname{ord} f = 1$. Thus

$$f(X) = \frac{aX + b}{cX + d} \neq \text{constant}$$

and the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ must be invertible. □

Clearly not every fractional linear transformation $\alpha^A \colon \Bbbk(X) \longrightarrow \Bbbk(X)$ maps polynomials to polynomials so $(\ )_* \colon \mathrm{Aut}_{\Bbbk}(\Bbbk[X]) \longrightarrow \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$ is not an epimorphism.

Now we turn to a more familiar field $\mathbb{R}$, the real numbers.

1.62. Proposition. *The only automorphism of the field $\mathbb{R}$ is the identity function, hence* $\mathrm{Aut}(\mathbb{R}) = \{\mathrm{id}\}$.

PROOF. First we note that $\mathbb{Q} \subseteq \mathbb{R}$ is a subring and if $\alpha \in \mathrm{Aut}(\mathbb{R})$ then $\alpha(q) = q$ for $q \in \mathbb{Q}$ by Example 1.57.

We recall from Analysis that the rational numbers are *dense* in the real numbers in the sense that each $r \in \mathbb{R}$ can be expressed as a limit $r = \lim_{n\to\infty} q_n$, where $q_n \in \mathbb{Q}$. Then for a continuous function $f\colon \mathbb{R} \longrightarrow \mathbb{R}$, its value at r depends on its values on $\mathbb{Q}$ since

$$f(r) = f(\lim_{n\to\infty} q_n) = \lim_{n\to\infty} f(q_n).$$

We will show that an automorphism $\alpha \in \mathrm{Aut}(\mathbb{R})$ is continuous.

First recall that for $x, y \in \mathbb{R}$,

$$x < y \iff 0 < y - x \iff y - x = t^2 \text{ for some non-zero } t \in \mathbb{R}.$$

Now for $\alpha \in \mathrm{Aut}(\mathbb{R})$ and $s \in \mathbb{R}$, we have $\alpha(s^2) = \alpha(s)^2$. Hence,

$$x < y \Longrightarrow \alpha(y) - \alpha(x) = \alpha(t)^2 \text{ for some non-zero } t \in \mathbb{R} \Longrightarrow \alpha(x) < \alpha(y).$$

So α preserves order and fixes rational numbers.

Now let $x \in \mathbb{R}$ and $\varepsilon > 0$. Then we can choose a rational number q such that $0 < q \leqslant \varepsilon$. Taking $\delta = q$ we find that for $y \in \mathbb{R}$ with $|y - x| < \delta$ (*i.e.*, $-\delta < y - x < \delta$) we have

$$-\delta = \alpha(-\delta) < \alpha(y) - \alpha(x) < \alpha(\delta) = \delta,$$

hence

$$|\alpha(y) - \alpha(x)| < \delta \leqslant \varepsilon.$$

This shows that α is continuous at x.

Thus every automorphism of $\mathbb{R}$ is continuous function which fixes all the rational numbers, hence it must be the identity function. □

1.63. REMARK. If we try to determine $\mathrm{Aut}(\mathbb{C})$ the answer turns out to be much more complicated. It is easy to see that complex conjugation $\overline{(\ )}\colon \mathbb{C} \longrightarrow \mathbb{C}$ is an automorphism of $\mathbb{C}$ and fixes every real number, *i.e.*, $\overline{(\ )} \in \mathrm{Aut}_{\mathbb{R}}(\mathbb{C})$; in fact, $\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\mathrm{id}, \overline{(\ )}\}$. However, it is *not* true that every $\alpha \in \mathrm{Aut}(\mathbb{C})$ fixes every real number! The automorphism group $\mathrm{Aut}(\mathbb{C})$ is actually enormous but it is hard to find an explicit element other than id and $\overline{(\ )}$. Note that given an automorphism $\alpha \in \mathrm{Aut}(\mathbb{C})$, the composition $\alpha \circ \overline{(\ )} \circ \alpha^{-1}$ is also self inverse, so there are many elements of order 2 in the group $\mathrm{Aut}(\mathbb{C})$.

Exercises on Chapter 1

1-1. Let R be a ring. Show that

$$\{n \in \mathbb{Z} : n > 0 \text{ and } n1 = 0\} = \{n \in \mathbb{Z} : n > 0 \text{ and } nr = 0 \text{ for all } r \in R\}.$$

Deduce that if $\mathrm{char}\, R > 0$ then these sets are non-empty and

$$\mathrm{char}\, R = \min\{n \in \mathbb{Z} : n > 0 \text{ and } nr = 0 \text{ for all } r \in R\}.$$

1-2. Let R be an integral domain.

(a) Show that every subring $S \subseteq R$ is also an integral domain. What is the relationship between $\mathrm{char}\, S$ and $\mathrm{char}\, R$?

(b) If R is a field, give an example to show that a subring of R need not be a field.

1-3. For each of the following rings R, find the characteristic $\operatorname{char} R$ and the characteristic subring of R. Determine which of these rings is an integral domain. In (b) and (c), A is an arbitrary commutative ring.

(a) Any subring $R \subseteq \mathbb{C}$.
(b) The polynomial ring $R = A[X]$.
(c) The ring of $n \times n$ matrices over A,

$$R = \operatorname{Mat}_n(A) = \left\{ \begin{bmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{bmatrix} : a_{ij} \in A \right\}.$$

1-4. If R is a commutative ring with unit containing the prime field $\mathbb{F}_p$ for some prime $p > 0$, show that the function $\varphi\colon R \longrightarrow R$ given by $\varphi(t) = t^p$, defines a ring homomorphism. Give examples to show that φ need not be surjective or injective.

1-5. Let R and S be rings with unity and $Q \lhd S$ a prime ideal.

(a) If $\varphi\colon R \longrightarrow S$ is a ring homomorphism, show that

$$\varphi^{-1}Q = \{r \in R : \varphi(r) \in Q\} \subseteq R$$

is a prime ideal of R.
(b) If $R \subseteq S$ is a subring, show that $Q \cap R$ is a prime ideal of R.
(c) If the word 'prime' is replaced by 'maximal' throughout, are the results in parts (a) and (b) still true? [*Hint: look for a counterexample.*]
(d) If $R \subseteq S$ is a subring and $P \lhd R$ is a maximal ideal, suppose that $Q \lhd S$ is a prime ideal for which $P \subseteq Q$. Show that $Q \cap R = P$.

1-6. Let $\Bbbk$ be a field, R be a ring with unit and let $\varphi\colon \Bbbk \longrightarrow R$ be a ring homomorphism. Show that φ is a monomorphism.

1-7. Consider the sets

$$\mathbb{Z}(i) = \{u + vi : u, v \in \mathbb{Z}\} \subseteq \mathbb{C}, \quad \mathbb{Q}(i) = \{u + vi : u, v \in \mathbb{Q}\} \subseteq \mathbb{C}.$$

(a) Show that $\mathbb{Z}(i)$ and $\mathbb{Q}(i)$ are subrings of $\mathbb{C}$. Also show that $\mathbb{Z}(i)$ is an integral domain, $\mathbb{Q}(i)$ is a field and $\mathbb{Z}(i)$ is a subring of $\mathbb{Q}(i)$.
(b) Show that the inclusion homomorphism $\operatorname{inc}\colon \mathbb{Z}(i) \longrightarrow \mathbb{Q}(i)$ extends to a monomorphism $\operatorname{inc}_*\colon \operatorname{Fr}(\mathbb{Z}(i)) \longrightarrow \mathbb{Q}(i)$.
(c) Show that inc_* is an isomorphism, so $\operatorname{Fr}(\mathbb{Z}(i)) = \mathbb{Q}(i)$.

1-8. Let R be a commutative ring.

(a) If $a, b \in R$, show that there is a unique ring homomorphism $\psi_{a,b}\colon R[X] \longrightarrow R[X]$ for which $\psi_{a,b}(r) = r$ if $r \in R$ and $\psi_{a,b}(X) = aX + b$. If $c, d \in R$, determine $\psi_{a,b} \circ \psi_{c,d}$. If a is a unit, show that $\psi_{a,b}$ is an isomorphism and find its inverse.
(b) Now suppose that $R = \Bbbk$ is a field and $a, b \in \Bbbk$ with $a \neq 0$. Prove the following.
  (i) If $f(X) \in \Bbbk[X]$, the $\deg \psi_{a,b}(f(X)) = \deg f(X)$.
  (ii) If $p(X) \in \Bbbk[X]$ is a prime then so is $\psi_{a,b}(p(X))$.

(iii) If $p(X) \in \Bbbk[X]$ is an irreducible then so is $\psi_{a,b}(p(X))$.

1-9. Let $\Bbbk$ be a field and $\Bbbk[[X]]$ be the set consisting of all power series

$$\sum_{k=0}^{\infty} a_k X^k = a_0 + a_1 X + \cdots + a_k X^k + \cdots ,$$

with $a_k \in \Bbbk$.

(a) Show that this can be made into an integral domain containing $\Bbbk[X]$ as a subring by defining addition and multiplication in the obvious way.
(b) Show that $\sum_{k=0}^{\infty} a_k X^k \in \Bbbk[[X]]$ is a unit if and only if $a_0 \neq 0$.
(c) Show that $\mathrm{Fr}(\Bbbk[[X]])$ consists of all *finite-tailed Laurent series*

$$\sum_{k=\ell}^{\infty} a_k X^k = a_\ell X^\ell + a_{\ell+1} X^{\ell+1} + \cdots + a_k X^k + \cdots$$

for some $\ell \in \mathbb{Z}$ and $a_{\Bbbk} \in \Bbbk$.

1-10. Taking $\Bbbk = \mathbb{Q}$, find the quotient and remainder when performing long division of $f(X) = 6X^4 - 6X^3 + 3X^2 - 3X - 2$ by $d(X) = 2X^3 + X + 3$.

1-11. Taking $\Bbbk = \mathbb{F}_3$, find the quotient and remainder when performing long division of $f(X) = 2X^3 + 2X^2 + X + 1$ by $d(X) = 2X^3 + 2X$.

1-12. Let $p > 0$ be a prime. Suppose that $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ with $p \nmid a_n$ and that $\overline{f(X)} \in \mathbb{F}_p[X]$ denotes the polynomial obtained by reducing the coefficients of $f(X)$ modulo p. If $\overline{f(X)}$ is irreducible, show that $f(X)$ is irreducible. Which of the following polynomials in $\mathbb{Z}[X]$ is irreducible?

$$X^3 - X + 1,\ X^3 + 2X + 1,\ X^3 + X - 1,\ X^5 - X + 1,\ X^5 + X - 1,\ 5X^3 - 10X + X^2 - 2.$$

1-13. Find generators for each of the following ideals:

$$I_1 = \{f(X) \in \mathbb{Q}[X] : f(i) = 0\} \lhd \mathbb{Q}[X], \qquad I_2 = \{f(X) \in \mathbb{Q}[X] : f(\sqrt{2}\, i) = 0\} \lhd \mathbb{Q}[X],$$
$$I_3 = \{f(X) \in \mathbb{Q}[X] : f(\sqrt{2}) = 0\} \lhd \mathbb{Q}[X], \qquad I_4 = \{f(X) \in \mathbb{R}[X] : f(\sqrt{2}) = 0\} \lhd \mathbb{R}[X],$$
$$I_5 = \{f(X) \in \mathbb{R}[X] : f(\sqrt{2}\, i) = 0\} \lhd \mathbb{R}[X], \qquad I_6 = \{f(X) \in \mathbb{R}[X] : f(\zeta_3) = 0\} \lhd \mathbb{R}[X].$$

1-14. Consider the inclusion $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$ and its extension to $\varepsilon_{\sqrt{2}}\colon \mathbb{Q}[X] \longrightarrow \mathbb{C}$. Determine the image $\varepsilon_{\sqrt{2}}\, \mathbb{Q}[X] \subseteq \mathbb{C}$. What is $\varepsilon_{-\sqrt{2}}\, \mathbb{Q}[X] \subseteq \mathbb{C}$? Find $\ker \varepsilon_{\sqrt{2}} \lhd \mathbb{Q}[X]$ and $\ker \varepsilon_{-\sqrt{2}} \lhd \mathbb{Q}[X]$; are these maximal ideals?

1-15. Let $\omega = (-1 + \sqrt{3}i)/2 \in \mathbb{C}$. Consider the inclusion $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$ and its extension to $\varepsilon_\omega\colon \mathbb{Q}[X] \longrightarrow \mathbb{C}$. Determine the image $\varepsilon_\omega\, \mathbb{Q}[X] \subseteq \mathbb{C}$. Determine $\ker \varepsilon_\omega \lhd \mathbb{Q}[X]$ and decide whether it is maximal. Find another evaluation homomorphism with the same kernel and image.

1-16. Consider the inclusion $\mathrm{inc}\colon \mathbb{Q} \longrightarrow \mathbb{C}$ and its extension to $\varepsilon_\alpha\colon \mathbb{Q}[X] \longrightarrow \mathbb{C}$ where α is one of the 4 complex roots of the polynomial $f(X) = X^4 - 2 \in \mathbb{Q}[X]$. Determine the image $\varepsilon_\alpha\, \mathbb{Q}[X] \subseteq \mathbb{C}$ and the ideal $\ker \varepsilon_\alpha \lhd \mathbb{Q}[X]$; is the latter ideal maximal? What happens if α is replaced by one of the other roots of $f(X)$?

Repeat this problem starting with the inclusion of the real numbers into the complex numbers $\mathrm{inc}\colon \mathbb{R} \longrightarrow \mathbb{C}$ and $\varepsilon_\alpha\colon \mathbb{R}[X] \longrightarrow \mathbb{C}$.

1-17. Use Cardan's method to find the complex roots of the polynomial

$$f(X) = X^3 - 9X^2 + 21X - 5.$$

1-18. Consider the real numbers

$$\alpha = \sqrt[3]{10+\sqrt{108}} + \sqrt[3]{10-\sqrt{108}}, \quad \beta = \sqrt[3]{1+\frac{2}{3}\sqrt{\frac{7}{3}}} + \sqrt[3]{1-\frac{2}{3}\sqrt{\frac{7}{3}}}.$$

Find rational cubic polynomials $f(X)$ and $g(X)$ for which $f(\alpha) = 0 = g(\beta)$. Hence determine these real numbers.

1-19. Prove the final part of Example 1.60 by showing that there is an isomorphism of groups $\mathrm{Aff}_1(\Bbbk) \cong \mathrm{Aut}_{\Bbbk}(\Bbbk[X])$.

1-20. Let $\Bbbk$ be any field. Consider the 6 automorphisms $\alpha_j \colon \Bbbk(X) \longrightarrow \Bbbk(X)$ $(j = 1, \ldots, 6)$ defined by

$$\begin{aligned} &\alpha_1(f(X)) = f(X), && \alpha_2(f(X)) = f(1-X), && \alpha_3(f(X)) = f(1/X), \\ &\alpha_4(f(X)) = f((X-1)/X), && \alpha_5(f(X)) = f(1/(1-X)), && \alpha_6(f(X)) = f(X/(X-1)). \end{aligned}$$

Show that the set consisting of these elements is a subgroup $\Gamma_{\Bbbk} \leqslant \mathrm{Aut}_{\Bbbk}(\Bbbk(X))$ isomorphic to the symmetric group S_3. When $\Bbbk = \mathbb{F}_2$, show that $\Gamma_{\Bbbk} \cong \mathrm{GL}_2(\Bbbk)$.

1-21. Determine the cyclotomic polynomial $\Phi_{20}(X)$.

1-22. Let $p > 0$ be a prime.

(a) Show that for $k \geqslant 1$, the cyclotomic polynomial $\Phi_{p^k}(X)$ satisfies

$$\Phi_{p^k}(X) = \Phi_p(X^{p^{k-1}})$$

and has as its complex roots the primitive p^k-th roots of 1.

(b) Show that $\Phi_{p^k}(X) \in \mathbb{Q}[X]$ is irreducible.

(c) Generalize part (a) to show that if $n = p_1^{r_1} \cdots p_k^{r_k}$ is the prime power factorization of n with the p_i being distinct primes and $r_i > 0$, then

$$\Phi_n(X) = \Phi_{p_1 \cdots p_k}(X^{p_1^{r_1-1} \cdots p_k^{r_k-1}}).$$

1-23. For $n \geqslant 2$, show that

$$X^{\varphi(n)} \Phi_n(X^{-1}) = \Phi_n(X).$$

1-24. Show that for $n \geqslant 1$, $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$.
Find expressions for $\zeta_5 + \zeta_5^{-1}$ and $\zeta_5^2 + \zeta_5^{-2}$ in terms of $\cos(2\pi/5)$. Hence find a rational polynomial which has $\cos(2\pi/5)$ as a root.

1-25. Let $p > 0$ be a prime and K be a field with $\mathrm{char}\, K = p$.

(a) Show that if $\zeta \in K$ is a p-th root of 1 then $\zeta = 1$. Deduce that if $m, n > 0$ and $p \nmid n$, then every np^m-th root of 1 in K is an n-th root of 1.

(b) If $a \in K$, show that the polynomial $X^p - a \in K[X]$ has either no roots or exactly one root in K.

CHAPTER 2

Fields and their extensions

2.1. Fields and subfields

2.1. Definition. Let K and L be fields and suppose that $K \subseteq L$ is a subring. Then we say that K is a *subfield* of L; L is also said to be an *extension* (*field*) of K. We write $K \leqslant L$ or L/K to indicate this, and write $K < L$ if K is a proper subfield of L, *i.e.*, if $K \neq L$.

An important fact about an extension of fields L/K is that L is a K-vector space whose addition is the addition in the field L while scalar multiplication is defined by

$$u \cdot x = ux \quad (u \in K,\ x \in L).$$

2.2. Definition. We will call $\dim_K L$ the *degree* or *index* of the extension L/K and use the notation $[L : K] = \dim_K L$. An extension of fields L/K is *finite* (*dimensional*) if $[L : K] < \infty$, otherwise it is *infinite* (*dimensional*).

2.3. Example. Show that the extension $\mathbb{C}/\mathbb{R}$ is finite, while $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$ are both infinite.

Solution. We have

$$\mathbb{C} = \{x + yi : x, y \in \mathbb{R}\},$$

so $1, i$ span $\mathbb{C}$ as a vector space over $\mathbb{R}$. Since $i \notin \mathbb{R}$, these elements are also linearly independent over $\mathbb{R}$ and therefore they form a basis, whence $[\mathbb{C} : \mathbb{R}] = 2$. The infiniteness of $\mathbb{R}/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$ are consequences of the fact that any finite dimensional vector space over $\mathbb{Q}$ is *countable*, however $\mathbb{R}$ and $\mathbb{C}$ are uncountable. A basis for the $\mathbb{Q}$-vector space $\mathbb{R}$ is known as a *Hamel basis*. □

2.4. Example. Consider the extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ where

$$\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} : x, y \in \mathbb{Q}\}.$$

Show that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

Solution. The elements $1, \sqrt{2}$ clearly span the $\mathbb{Q}$-vector space $\mathbb{Q}(\sqrt{2})$. Now recall that $\sqrt{2} \notin \mathbb{Q}$. If the elements $1, \sqrt{2}$ were linearly dependent we would have $u + v\sqrt{2} = 0$ for some $u, v \in \mathbb{Q}$ not both zero; in fact it is easy to see that we would then also have u, v both non-zero. Thus we would have

$$\sqrt{2} = -\frac{u}{v} \in \mathbb{Q},$$

which we know to be false. Hence $1, \sqrt{2}$ are linearly independent and so form a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. □

If we have two extensions L/K and M/L then it is a straightforward to verify that $K \leqslant M$ and so we have another extension M/K.

2.5. Definition. Given two extensions L/K and M/L, we say that L/K is a *subextension of* M/K and sometimes write $L/K \leqslant M/K$.

2.6. THEOREM. *Let L/K be a subextension of M/K.*

(i) *If one or both of the dimensions $[L : K]$ or $[M : L]$ is infinite then so is $[M : K]$.*

(ii) *If the dimensions $[L : K]$ and $[M : L]$ are both finite then so is $[M : K]$ and*

$$[M : K] = [M : L]\,[L : K].$$

PROOF. (i) If $[M : K]$ is finite, choose a basis $m_1, \ldots, m_r$ of M over K. Now any element $u \in M$ can be expressed as

$$u = t_1 m_1 + \cdots + t_r m_r,$$

where $t_1, \ldots, t_r \in K$; but since $K \subseteq L$, this means that $m_1, \ldots, m_r$ spans M over L and so $[M : L] < \infty$. Also L is a K-vector subspace of the finite dimensional K-vector space M, hence $[L : K] < \infty$.

(ii) Setting $r = [L : K]$ and $s = [M : L]$, choose a basis $\ell_1, \ldots, \ell_r$ of L over K and a basis $m_1, \ldots, m_s$ of M over L.

Now let $v \in M$. Then there are elements $y_1, \ldots, y_s \in L$ for which

$$v = y_1 m_1 + \cdots + y_s m_s.$$

But each y_j can be expressed in the form

$$y_j = x_{1j}\ell_1 + \cdots + x_{rj}\ell_r$$

for suitable $x_{ij} \in K$. Hence,

$$v = \sum_{j=1}^{s} \left(\sum_{i=1}^{r} x_{ij}\ell_i \right) m_j = \sum_{j=1}^{s} \sum_{i=1}^{r} x_{ij}(\ell_i m_j),$$

where each coefficient x_{ij} is in K. Thus the elements $\ell_i m_j$ $(i = 1, \ldots, r,\ j = 1, \ldots, s)$ span the K-vector space M.

Now suppose that for some $t_{ij} \in K$ we have

$$\sum_{j=1}^{s} \sum_{i=1}^{r} t_{ij}(\ell_i m_j) = 0.$$

On collecting terms we obtain

$$\sum_{j=1}^{s} \left(\sum_{i=1}^{r} t_{ij}\ell_i \right) m_j = 0,$$

where each coefficient $\sum_{i=1}^{r} t_{ij}\ell_i$ is in L. By the linear independence of the m_j over L, this means that for each j,

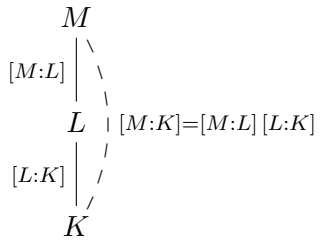
$$\sum_{i=1}^{r} t_{ij}\ell_i = 0.$$

By the linear independence of the ℓ_i over K, each $t_{ij} = 0$.

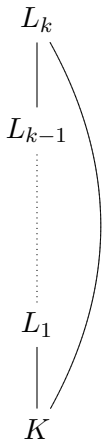
Hence the $\ell_i m_j$ form a basis of M over K and so

$$[M : K] = rs = [M : L]\,[L : K]. \qquad \square$$

We will often indicate subextensions in diagrammatic form where larger fields always go above smaller ones and the information on the lines indicates dimensions



We often suppress 'composite' lines such as the dashed one. Such *towers of extensions* are our main objects of study. We can build up sequences of extensions and form towers of arbitrary length. Thus, if $L_1/K,\ L_2/L_1, \dots,\ L_k/L_{k-1}$ is a such a sequence of extensions, there is a diagram



2.2. Simple and finitely generated extensions

2.7. Definition. Let F be a field and $K \leqslant F$. Given elements $u_1, \dots, u_r \in F$ we set

$$K(u_1, \dots, u_r) = \bigcap_{\substack{K \leqslant L \leqslant F \\ u_1, \dots, u_r \in L}} L$$

which is the smallest subfield in F that contains K and the elements $u_1, \dots, u_r$. The extension $K(u_1, \dots, u_r)/K$ is said to be *generated* by the elements $u_1, \dots, u_r$; we also say that $K(u_1, \dots, u_r)/K$ is a *finitely generated* extension of K. An extension of the form $K(u)/K$ is called a *simple extension of K with generator u*.

We can extend this to the case of an infinite sequence $u_1, \dots, u_r, \dots$ in F and denote by $K(u_1, \dots, u_r, \dots) \leqslant F$ the smallest extension field of K containing all the elements u_r.

It can be shown that

(2.1) $K(u_1, \dots, u_r) =$

$$\left\{ \frac{f(u_1, \dots, u_r)}{g(u_1, \dots, u_r)} \in F : f(X_1, \dots, X_r), g(X_1, \dots, X_r) \in K[X_1, \dots, X_r],\ g(u_1, \dots, u_r) \neq 0 \right\}.$$

Reordering the u_i does not change $K(u_1, \dots, u_n)$.

2.8. Proposition. *Let $K(u)/K$ and $K(u,v)/K(u)$ be simple extensions. Then*

$$K(u,v) = K(u)(v) = K(v)(u).$$

More generally,

$$K(u_1,\dots,u_n) = K(u_1,\dots,u_{n-1})(u_n)$$

and this is independent of the order of the sequence $u_1,\dots,u_n$.

2.9. Theorem. *For a simple extension $K(u)/K$, exactly one of the following conditions holds.*

(i) *The evaluation at u homomorphism $\varepsilon_u\colon K[X] \longrightarrow K(u)$ is a monomorphism and on passing to the fraction field gives an isomorphism $(\varepsilon_u)_*\colon K(X) \longrightarrow K(u)$. In this case, $K(u)/K$ is infinite and u is said to be* transcendental over K.

(ii) *The evaluation at u homomorphism $\varepsilon_u\colon K[X] \longrightarrow K(u)$ has a non-trivial kernel $\ker\varepsilon_u = (p(X))$ where $p(X) \in K[X]$ is an irreducible monic polynomial of positive degree and the quotient homomorphism $\widetilde{\varepsilon}_u\colon K[X]/(p(X)) \longrightarrow K(u)$ is an isomorphism. In this case $K(u)/K$ is finite with $[K(u):K] = \deg p(X)$ and u is said to be* algebraic over K.

Proof. (i) If $\ker\varepsilon_u = (0)$, all that needs checking is that $(\varepsilon_u)_*$ is an epimorphism; but as u is in the image of $(\varepsilon_u)_*$ this is obvious.
(ii) When $\ker\varepsilon_u \neq (0)$, Theorem 1.31(iv) implies that the image of ε_u is a subfield of $K(u)$ and since it contains u it must equal $K(u)$. Hence $\widetilde{\varepsilon}_u$ is an isomorphism. Using Long Division, we find that every element of $K[X]/(p(X))$ can be uniquely expressed as a coset of the form

$$f(X) + (p(X)),$$

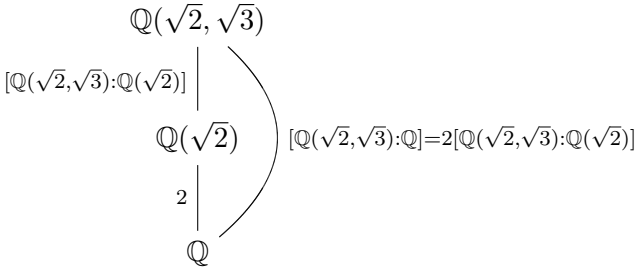
where $\deg f(X) < \deg p(X)$. Hence every element of $K[X]/(p(X))$ can be uniquely expressed as a linear combination over K of the d cosets

$$1 + (p(X)),\ X + (p(X)),\ X^2 + (p(X)),\dots,\ X^{d-1} + (p(X)),$$

where $d = \deg p(X)$. Via the isomorphism $\widetilde{\varepsilon}_u$ under which $\widetilde{\varepsilon}_u(X^k + (p(X))) = u^k$, we see that the elements $1, u, \dots, u^{d-1}$ form a basis for $K(u)$ over K. □

2.10. Example. For the extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ we have $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$.

Proof. By Example 2.4 we know that $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$. We have the following tower of extensions.



We will show that $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$.

Notice that if $u \in \mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ then $u = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}(\sqrt{2})$, so $1, \sqrt{3}$ span $\mathbb{Q}(\sqrt{2},\sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. But if these are linearly dependent then $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Writing

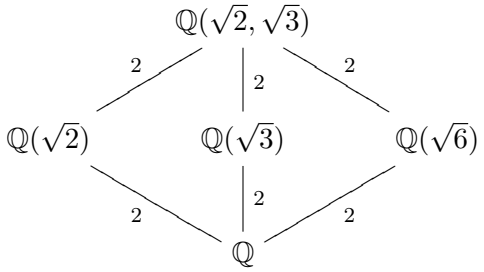
$$\sqrt{3} = v + w\sqrt{2}$$

with $v, w \in \mathbb{Q}$, we find that

$$v^2 + 2w^2 + 2vw\sqrt{2} = 3 \in \mathbb{Q},$$

and hence $2vw\sqrt{2} \in \mathbb{Q}$. The possibilities $v = 0$ or $w = 0$ are easily ruled out, while $v, w \neq 0$ would implies that $\sqrt{2} \in \mathbb{Q}$ which is false. So $1, \sqrt{3}$ are linearly independent over $\mathbb{Q}(\sqrt{2})$ and therefore form a basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. This shows that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$ and so $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = 4$. □

2.11. Remark. There are some other subfields of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ which are conveniently displayed in the following diagram.



One idea in the verification of Example 2.10 can be extended to provide a useful general result whose proof is left as an exercise.

2.12. Proposition. *Let $p_1, \ldots, p_n$ be a sequence of distinct primes $p_i > 0$. Then*

$$\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}).$$

Hence $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})] = 2$ and $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

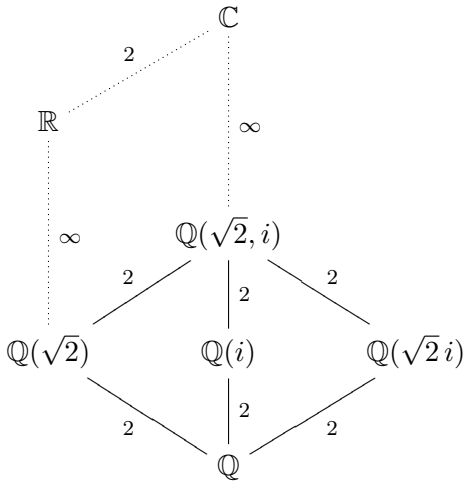
2.13. Example. For the extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ we have $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$.

Proof. We know that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Also, $i \notin \mathbb{Q}(\sqrt{2})$ since i is not real and $\mathbb{Q}(\sqrt{2}) \leqslant \mathbb{R}$. Since $i^2 + 1 = 0$, we have $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2})(i)$ and $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = 2$. Using the formula

$$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}],$$

we obtain $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. □

This example also has several other subfields, with only $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, i) \cap \mathbb{R}$ being a subfield of $\mathbb{R}$.



2.14. Example. For $n \geqslant 1$, let $E_n = \mathbb{Q}(2^{1/n}) \leqslant \mathbb{R}$, where $2^{1/n} \in \mathbb{R}$ denotes the positive real n-th root of 2.

(i) Show that $[E_n : \mathbb{Q}] = n$.
(ii) If $m \geqslant 1$ with $m \mid n$, show that $E_m \leqslant E_n$ and determine $[E_n : E_m]$.
(iii) If m, n are coprime, show that $E_{mn} = \mathbb{Q}(2^{1/m}, 2^{1/n})$.

Solution. (i) Consider the evaluation homomorphism $\varepsilon_{2^{1/n}} \colon \mathbb{Q}[X] \longrightarrow E_n$. Applying the Eisenstein Test 1.38 using the prime 2 to the polynomial $X^n - 2 \in \mathbb{Z}[X]$, we find that

$$\ker \varepsilon_{2^{1/n}} = (X^n - 2) \lhd \mathbb{Q}[X],$$

and the induced homomorphism $\widetilde{\varepsilon}_{2^{1/n}} \colon \mathbb{Q}[X]/(X^n - 2) \longrightarrow E_n$ is an isomorphism. Hence $[E_n : \mathbb{Q}] = n$.
(ii) Since n/m is an integer,

$$2^{1/m} = (2^{1/n})^{n/m} \in E_n,$$

so

$$E_m = \mathbb{Q}(2^{1/m}) \subseteq E_n.$$

By Theorem 2.6 we have

$$n = [E_n : \mathbb{Q}] = [E_n : E_m]\,[E_m : \mathbb{Q}] = m[E_n : E_m],$$

whence $[E_n : E_m] = n/m$.
(iii) By (ii) we have $E_m \leqslant E_{mn}$ and $E_n \leqslant E_{mn}$, hence $\mathbb{Q}(2^{1/m}, 2^{1/n}) \leqslant E_{mn}$. As $\gcd(m, n) = 1$, there are integers r, s for which $rm + sn = 1$ and so

$$\frac{1}{mn} = \frac{rm + sn}{mn} = \frac{r}{n} + \frac{s}{m}.$$

This shows that

$$2^{1/mn} = (2^{1/n})^r (2^{1/m})^s \in \mathbb{Q}(2^{1/m}, 2^{1/n}),$$

whence $E_{mn} \leqslant \mathbb{Q}(2^{1/m}, 2^{1/n})$. Combining these inclusions we obtain $E_{mn} = \mathbb{Q}(2^{1/m}, 2^{1/n})$. $\square$

Exercises on Chapter 2

2-1. Let $p \in \mathbb{N}$ be an prime. Show that the extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ has $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

2-2. Let $p, q > 0$ be distinct primes. Show that $[\mathbb{Q}(\sqrt{p}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$.

2-3. Prove Proposition 2.12 by induction on n.

2-4. Let K a field with $\operatorname{char} K \neq 2$ and suppose that L/K is an extension. If $a, b \in K$ are distinct, suppose that $u, v \in L$ satisfy $u^2 = a$ and $v^2 = b$. Show that $K(u, v) = K(u + v)$. [*Hint: first show that* $u \pm v \neq 0$ *and deduce that* $u - v \in K(u+v)$*; then show that* $u, v \in K(u+v)$.]

2-5. Show that $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

2-6. Show that $[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = 4$. Find the three subfields $L \leqslant \mathbb{Q}(\sqrt{3}, i)$ with $[L : \mathbb{Q}] = 2$ and display their relationship in a diagram, indicating which ones are subfields of $\mathbb{R}$.

2-7. Let $\zeta_5 = e^{2\pi i/5} \in \mathbb{C}$.

(a) Explain why $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$.

(b) Show that $\cos(2\pi/5),\ \sin(2\pi/5)\, i \in \mathbb{Q}(\zeta_5)$.

(c) Show that for $t \in \mathbb{R}$,

$$\cos 5t = 16\cos^5 t - 20\cos^3 t + 5\cos t.$$

(d) Show that the numbers $\cos(2k\pi/5)$ with $k = 0, 1, 2, 3, 4$ are roots of the polynomial

$$f(X) = 16X^5 - 20X^3 + 5X - 1 = (X - 1)(4X^2 + 2X - 1)^2$$

and deduce that $[\mathbb{Q}(\cos(2\pi/5)) : \mathbb{Q}] = 2$.

(e) Display the relationship between the fields $\mathbb{Q}$, $\mathbb{Q}(\cos(2\pi/5))$, and $\mathbb{Q}(\zeta_5)$ in a suitable diagram.

2-8. This question is for those who like lots of calculation or using Maple. Let $\zeta_7 = e^{2\pi i/7} \in \mathbb{C}$.

(a) Explain why $[\mathbb{Q}(\zeta_7) : \mathbb{Q}] = 6$.

(b) Show that $\cos(2\pi/7),\ \sin(2\pi/7)\, i \in \mathbb{Q}(\zeta_7)$.

(c) Show

$$\cos 7t = 64\cos^7 t - 112\cos^5 t + 56\cos^3 t - 7\cos t.$$

Show that the numbers $\cos(2k\pi/7)$ with $k = 0, 1, \ldots, 6$ are roots of the polynomial

$$f(X) = 64X^7 - 112X^5 + 56X^3 - 7X - 1 = (X - 1)(8X^3 + 4X^2 - 4X - 1)^2$$

and deduce that $[\mathbb{Q}(\cos(2\pi/7)) : \mathbb{Q}] = 3$.

(d) Show that $\sin(2\pi/7)\, i$ is a root of

$$g(X) = 64X^7 + 112X^5 + 56X^3 + 7X = X(64X^6 + 112X^4 + 56X^2 + 7)$$

and that $64X^6 + 112X^4 + 56X^2 + 7 \in \mathbb{Q}[X]$ is irreducible. What is $[\mathbb{Q}(\sin(2\pi/7)\, i) : \mathbb{Q}]$?

(e) Display the relationship between the fields $\mathbb{Q}$, $\mathbb{Q}(\cos(2\pi/7))$, $\mathbb{Q}(\sin(2\pi/7)\, i)$ and $\mathbb{Q}(\zeta_7)$ in a diagram.

(f) Is $i \in \mathbb{Q}(\zeta_7)$?

2-9. In this question we continue to consider the situation described in Example 2.14.

(a) Show that

$$\mathrm{Aut}_{\mathbb{Q}}(E_n) = \begin{cases} \{\mathrm{id}\} & \text{if } n \text{ is odd,} \\ \{\mathrm{id}, \tau_n\} \cong \mathbb{Z}/2 & \text{if } n \text{ is even,} \end{cases}$$

where τ_n has composition order 2.

(b) Let $E = \bigcup_{n \geqslant 1} E_n \leqslant \mathbb{R}$. Show that $\mathrm{Aut}_{\mathbb{Q}}(E) = \{\mathrm{id}\}$.

(c) Display the 6 subfields of E_{12} in a diagram.

(d) Which of the subfields in part (c) contain the element $2^{1/2} + 2^{1/3}$?

CHAPTER 3

Algebraic extensions of fields

3.1. Algebraic extensions

Let L/K be an extension of fields. From Theorem 2.9(ii), recall the following notion.

3.1. Definition. An element $t \in L$ is *algebraic over* K if there is a non-zero polynomial $p(X) \in K[X]$ for which $p(t) = 0$.

Notice in particular that for an element $t \in K$, the polynomial $p(X) = X - t \in K[X]$ satisfies $p(t) = 0$, so t is algebraic over K.

Theorem 2.9 allows us to characterize algebraic elements in other ways.

3.2. Proposition. *Let $t \in L$. Then the following conditions are equivalent.*

(i) *t is algebraic over K.*
(ii) *The evaluation homomorphism $\varepsilon_t \colon K[X] \longrightarrow L$ has non-trivial kernel.*
(iii) *The extension $K(t)/K$ is finite dimensional.*

3.3. Definition. If $t \in L$ is algebraic over K then by Proposition 3.2,

$$\ker \varepsilon_t = (\operatorname{minpoly}_{K,t}(X)) \neq (0),$$

where $\operatorname{minpoly}_{K,t}(X) \in K[X]$ is an irreducible monic polynomial called the *minimal polynomial of t over K*. The degree of $\operatorname{minpoly}_{K,t}(X)$ is called the *degree of t over K* and is denoted $\deg_K t$.

3.4. Proposition. *If $t \in L$ is algebraic over K then*

$$[K(t) : K] = \deg \operatorname{minpoly}_{K,t}(X) = \deg_K t.$$

Proof. This follows from Theorem 2.9(ii). □

3.5. Remark. Suppose that $t \in L$ is algebraic over K and that $p(X) \in \ker \varepsilon_t$ with $\deg p(X) = \deg \operatorname{minpoly}_{K,t}(X)$. Then $\operatorname{minpoly}_{K,t}(X) \mid p(X)$ and so

$$p(X) = u \operatorname{minpoly}_{K,t}(X)$$

for some $u \in K$. In particular, when $p(X)$ is monic,

$$p(X) = \operatorname{minpoly}_{K,t}(X).$$

We will often use this without further comment.

3.6. Example. Consider $\mathbb{C}/\mathbb{Q}$. The minimal polynomial of $\sqrt{2} \in \mathbb{C}$ over $\mathbb{Q}$ is

$$\operatorname{minpoly}_{\mathbb{Q},\sqrt{2}}(X) = X^2 - 2.$$

PROOF. Clearly $X^2-2 \in \ker \varepsilon_{\sqrt{2}}$ since $(\sqrt{2})^2-2=0$. By Example 2.4,

$$\deg \operatorname{minpoly}_{\mathbb{Q},\sqrt{2}}(X) = [\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2,$$

hence

$$\operatorname{minpoly}_{\mathbb{Q},\sqrt{2}}(X) = X^2-2. \qquad \square$$

3.7. EXAMPLE. Consider $\mathbb{C}/\mathbb{Q}$. The minimal polynomial of $i \in \mathbb{C}$ over $\mathbb{Q}$ is X^2+1.

PROOF. Clearly $X^2+1 \in \ker \varepsilon_i$ since $i^2+1=0$. As $[\mathbb{Q}(i):\mathbb{Q}]=2$, we have

$$\operatorname{minpoly}_{\mathbb{Q},i}(X) = X^2+1. \qquad \square$$

3.8. EXAMPLE. Consider $\mathbb{C}/\mathbb{Q}$. Find the minimal polynomial of the primitive 6-th root of unity, $\zeta_6 \in \mathbb{C}$ over $\mathbb{Q}$.

SOLUTION. Recall from Example 1.44 that ζ_6 is a root of the irreducible cyclotomic polynomial

$$\Phi_6(X) = X^2 - X + 1.$$

Then $\Phi_6(X) \in \ker \varepsilon_{\zeta_6}$ so $\operatorname{minpoly}_{\mathbb{Q},\zeta_6}(X) \mid \Phi_6(X)$. Since $\Phi_6(X)$ is irreducible and monic, we must have

$$\operatorname{minpoly}_{\mathbb{Q},\zeta_6}(X) = \Phi_6(X)$$

and so $\deg_{\mathbb{Q}} \zeta_6 = 2$. $\square$

3.9. EXAMPLE. Consider $\mathbb{C}/\mathbb{Q}$. Find the minimal polynomial of $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$.

SOLUTION. Notice that

$$\sqrt{3}-\sqrt{2} = \frac{(\sqrt{3}-\sqrt{2})(\sqrt{3}+\sqrt{2})}{(\sqrt{3}+\sqrt{2})} = \frac{1}{\sqrt{2}+\sqrt{3}} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

So we have

$$\sqrt{2} = \frac{1}{2}\Big((\sqrt{2}+\sqrt{3}) - (\sqrt{3}-\sqrt{2})\Big) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}),$$
$$\sqrt{3} = \frac{1}{2}\Big((\sqrt{2}+\sqrt{3}) + (\sqrt{3}-\sqrt{2})\Big) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}),$$

hence $\mathbb{Q}(\sqrt{2},\sqrt{3}) \leqslant \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \leqslant \mathbb{Q}(\sqrt{2},\sqrt{3})$ we must have

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

Referring to Example 2.10 we see that

$$\deg_{\mathbb{Q}}(\sqrt{2}+\sqrt{3}) = 4.$$

Let us find a non-zero polynomial in $\ker \varepsilon_{\sqrt{2}+\sqrt{3}} \lhd \mathbb{Q}[X]$.

Referring to Example 2.10 or Proposition 2.12 we see that $\sqrt{2}+\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, hence

$$\deg_{\mathbb{Q}(\sqrt{2})}(\sqrt{2}+\sqrt{3}) = 2.$$

One polynomial in $\ker \varepsilon_{\sqrt{2}+\sqrt{3}} \lhd \mathbb{Q}(\sqrt{2})[X]$ is

$$(X-(\sqrt{2}+\sqrt{3}))(X-(\sqrt{2}-\sqrt{3})) = X^2 - 2\sqrt{2}X - 1.$$

Since this is monic and of degree 2,

$$\operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),\sqrt{2}+\sqrt{3}}(X) = X^2 - 2\sqrt{2}X - 1.$$

Similarly,

$$\operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),-\sqrt{2}+\sqrt{3}}(X) = X^2 + 2\sqrt{2}X - 1.$$

Consider

$$\begin{aligned} p(X) &= \operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),\sqrt{2}+\sqrt{3}}(X) \operatorname{minpoly}_{\mathbb{Q}(\sqrt{2}),-\sqrt{2}+\sqrt{3}}(X) \\ &= (X^2 - 2\sqrt{2}X - 1)(X^2 + 2\sqrt{2}X - 1) \\ &= X^4 - 10X^2 + 1. \end{aligned}$$

Then $p(\sqrt{2}+\sqrt{3}) = 0$ so $p(X) \in \ker \varepsilon_t$. Since $\deg p(X) = 4$ and $p(X)$ is monic, we have

$$\operatorname{minpoly}_{\mathbb{Q},\sqrt{2}+\sqrt{3}}(X) = X^4 - 10X^2 + 1. \qquad \square$$

3.10. Definition. Let L/K be a finite extension. An element $u \in L$ for which $L = K(u)$ is called a *primitive element* for the extension L/K. If L/K such a primitive element exists, then L/K is called a *simple extension.*

Later we will see that when $\operatorname{char} K = 0$ every finite extension L/K has a primitive element, hence every such extension is simple.

3.11. Lemma. *Let L/K be a finite extension and $u \in L$. Then u is a primitive element for L/K if and only if $\deg_K u = [L : K]$.*

Proof. $K(u) \subseteq L$ is a finite dimensional K-vector subspace. Then $K(u) = L$ if and only $\dim_K K(u) = \dim_K L$. Since $\deg_K u = \dim_K K(u)$ and $[L : K] = \dim_K L$ the result follows. $\square$

Sometimes the minimal polynomial of an element in an extension is introduced in a different but equivalent way.

3.12. Proposition. *Let $t \in L$ be algebraic over K. Then*

$$\mathfrak{I}(t) = \{f(X) \in K[X] : f(t) = 0\} \subseteq K[X]$$

is an ideal which is principal and has an irreducible monic generator $q(X) \in K[X]$. In fact, $q(X) = \operatorname{minpoly}_{K,t}(X)$.

Proof. It is easy to see that $\mathfrak{I}(t) \lhd K[X]$ and therefore $\mathfrak{I}(t) = (q(X))$ for some monic generator $q(X)$. To see that $q(X)$ is irreducible, suppose that $q(X) = q_1(X)q_2(X)$ with $\deg q_i(X) < \deg q(X)$. Now as $q_1(t)q_2(t) = 0$, we must have $q_1(t) = 0$ or $q_2(t) = 0$, hence $q_1(X) \in \mathfrak{I}(t)$ or $q_2(X) \in \mathfrak{I}(t)$. These possibilities give $q(X) \mid q_1(X)$ or $q(X) \mid q_2(X)$ and so $\deg q(X) \leqslant \deg q_1(X)$ or $\deg q(X) \leqslant \deg q_2(X)$, contradicting the above assumption that $\deg q_i(X) < \deg q(X)$.

The irreducible monic polynomial $\operatorname{minpoly}_{K,t}(X)$ is in $\mathfrak{I}(t)$ so $q(X) \mid \operatorname{minpoly}_{K,t}(X)$ and therefore $q(X) = \operatorname{minpoly}_{K,t}(X)$. $\square$

The next Lemma will often be useful.

3.13. Lemma. *Let L/K be an extension and suppose that $u_1, \ldots, u_n \in L$ are algebraic. Then $K(u_1, \ldots, u_n)/K$ is a finite extension.*

Proof. Use induction on n together with Proposition 2.8 and Theorem 2.6(ii). $\square$

We now come to an important notion for extensions.

3.14. Definition. The extension L/K is *algebraic* or L is *algebraic over* K if every element $t \in L$ is algebraic over K.

3.15. Proposition. *Let L/K be a finite extension. Then L/K is algebraic.*

Proof. Let $t \in L$. Since the K-vector space L is finite dimensional, when viewed as elements of this vector space, the powers $1, t, \ldots, t^n, \ldots$ must be linearly dependent over K. Hence for suitable coefficients $c_j \in K$ not all zero and some $m \geqslant 1$ we have

$$c_0 + c_1 t + \cdots + c_m t^m = 0.$$

But this means that t is algebraic over K. □

3.16. Proposition. *Let M/L and L/K be algebraic extensions. Then the extension M/K is algebraic.*

Proof. Let $u \in M$. Then u is algebraic over L, so there is a polynomial

$$p(X) = p_0 + p_1 X + \cdots + p_m X^m \in L[X]$$

of positive degree with $p(u) = 0$. By Lemma 3.13, the extension $K(p_0, \ldots, p_m)/K$ is finite and so is $K(p_0, \ldots, p_m, u)/K(p_0, \ldots, p_m)$. By Theorem 2.6(ii), $K(p_0, \ldots, p_m, u)/K$ is finite, so by Proposition 3.15, u is algebraic over K. □

3.17. Definition. For an extension L/K, let

$$L^{\mathrm{alg}} = \{t \in L : t \text{ is algebraic over } K\} \subseteq L.$$

3.18. Proposition. *For an extension L/K, L^{alg} is a subfield containing K and L^{alg}/K is algebraic.*

Proof. Clearly $K \subseteq L^{\mathrm{alg}}$. We must show that $L^{\mathrm{alg}} \leqslant L$.

Let $u, v \in L^{\mathrm{alg}}$. Then by Lemma 3.13, $K(u, v)/K$ is a finite dimensional extension, hence every element of $K(u, v)$ is algebraic over K. In particular, $u + v$ and uv are in $K(u, v)$ and if $u \neq 0$, u^{-1} is also in $K(u, v)$. Therefore $u + v$, uv and u^{-1} are all algebraic over K. □

3.19. Example. In the extension $\mathbb{C}/\mathbb{Q}$ we can consider $\mathbb{C}^{\mathrm{alg}} \leqslant \mathbb{C}$ which is called the subfield of *algebraic numbers*. Similarly, in the extension $\mathbb{R}/\mathbb{Q}$ the subfield

$$\mathbb{R}^{\mathrm{alg}} = \mathbb{C}^{\mathrm{alg}} \cap \mathbb{R} \leqslant \mathbb{C}$$

consists of all the *real algebraic numbers*. Elements of $\mathbb{C} - \mathbb{C}^{\mathrm{alg}}$ are called *transcendental* complex numbers; examples are e and π. The sets $\mathbb{C}^{\mathrm{alg}}$ and $\mathbb{R}^{\mathrm{alg}}$ are both countable, whereas $\mathbb{C}$ and $\mathbb{R}$ are uncountable, so there are in fact many more transcendental numbers but it can be hard to determine whether a given number is transcendental or not. A more usual notation for $\mathbb{C}^{\mathrm{alg}}$ is $\overline{\mathbb{Q}}$ since this is the *algebraic closure* of $\mathbb{Q}$ which will be discussed later. When dealing with algebraic extensions of $\mathbb{Q}$ we will usually work with subfields of $\overline{\mathbb{Q}} = \mathbb{C}^{\mathrm{alg}}$.

We end this section with a technical result.

3.20. Proposition. *Let $K(u)/K$ be a finite simple extension. Then there are only finitely many subextensions $F/K \leqslant K(u)/K$.*

PROOF. Consider the minimal polynomial $\mathrm{minpoly}_{K,u}(X) \in K[X]$. Now for any subextension $F/K \leqslant K(u)/K$ we can also consider

$$\mathrm{minpoly}_{F,u}(X) = c_0 + c_1 X + \cdots + c_{k-1}X^{k-1} + X^k \in F[X],$$

which divides $\mathrm{minpoly}_{K,u}(X)$ in $F[X]$. The Unique Factorization Property 1.33 implies that $\mathrm{minpoly}_{K,u}(X)$ has only finitely many monic divisors in $K(u)[X]$, so there are only a finite number of possibilities for $\mathrm{minpoly}_{F,u}(X)$. Now consider $F_0 = K(c_0, c_1, \ldots, c_{k-1})$, the extension field of K generated by the coefficients of $\mathrm{minpoly}_{F,u}(X)$. Then $F_0 \leqslant F$ and so $\mathrm{minpoly}_{F,u}(X) \in F_0[X]$ is irreducible since it is irreducible in $F[X]$; hence $\mathrm{minpoly}_{F,u}(X) = \mathrm{minpoly}_{F_0,u}(X)$. We have

$$[K(u) : F] = \deg \mathrm{minpoly}_{F,u}(X) = \deg \mathrm{minpoly}_{F_0,u}(X) = [K(u) : F_0],$$

hence $F = F_0$.

This shows that there are only finitely many subextensions $F/K \leqslant K(u)/K$, each of which has the form $K(a_0, a_1, \ldots, a_{\ell-1})$, where

$$a_0 + a_1 X + \cdots + a_{\ell-1}X^{\ell-1} + X^\ell \in K(u)[X]$$

is a factor of $\mathrm{minpoly}_{K,u}(X)$ in $K(u)[X]$. □

3.2. Splitting fields and Kronecker's Theorem

We can now answer a basic question. Let K be a field and $p(X) \in K[X]$ be a polynomial of positive degree.

3.21. QUESTION. Is there an extension field L/K for which $p(X)$ has a root in L?

A stronger version of this question is the following.

3.22. QUESTION. Is there an extension field E/K for which $p(X)$ factorizes into linear factors in $E[X]$?

3.23. DEFINITION. $p(X) \in K[X]$ *splits in* E/K or *over* E if it factorizes into linear factors in $E[X]$.

Of course, if we have such a field E then the distinct roots $u_1, \ldots, u_k$ of $p(X)$ in E generate a subfield $K(u_1, \ldots, u_k) \leqslant E$ which is the smallest subfield of E that answers Question 3.22.

3.24. DEFINITION. Such a minimal extension of K is called a *splitting field* of $p(X)$ over K and we will sometimes denote it by $K(p(X))$ or K_p.

We already know how to answer Question 3.21.

3.25. THEOREM (Kronecker's Theorem: first version). *Let K be a field and $p(X) \in K[X]$ be a polynomial of positive degree. Then there is a finite extension L/K for which $p(X)$ has a root in L.*

PROOF. We begin by factorizing $p(X) \in K[X]$ into irreducible monic factors $q_j(X)$ together with a constant factor c:

$$p(X) = cq_1(X) \cdots q_r(X).$$

Now for any j we can form the quotient field $K[x]/(q_j(X))$ which is a finite dimensional (simple) extension of K and in which the coset $X + (q_j(X))$ satisfies the equation

$$q_j(X + (q_j(X))) = 0 + (q_j(X)).$$

Hence $p(X)$ has a root in $K[x]/(q_j(X))$.

Of course, this construction is only interesting if $q_j(X)$ to has degree bigger than 1 since a linear polynomial already has a root in K. □

To answer Question 3.22 we iterate this construction. Namely, having found one root u_1 in an extension L_1/K we discard the linear factor $X - u_1$ and consider the polynomial

$$p_1(X) = \frac{p(X)}{X - u_1} \in L_1[X].$$

We can repeat the argument to form a finite extension of L_1 (and hence of K) containing a root of $p_1(X)$ and so on. At each stage we either already have another root in L_1 or we need to enlarge the field to obtain one.

3.26. Theorem (Kronecker's Theorem: second version). *Let K be a field and $p(X) \in K[X]$ be a polynomial of positive degree. Then there is a finite extension E/K which is a splitting field of $p(X)$ over K.*

In practise we often have extension fields 'lying around in nature' containing roots and we can work inside of these. When working over $\mathbb{Q}$ (or any other subfield of $\mathbb{C}$) we can always find roots in $\mathbb{C}$ by the Fundamental Theorem of Algebra. We then refer to a subfield of $\mathbb{C}$ which is a splitting field as *the splitting subfield*.

3.27. Example. Find a splitting field $E/\mathbb{Q}$ for $p(X) = X^4 - 4$ over $\mathbb{Q}$ and determine $[E : \mathbb{Q}]$.

Solution. Notice that

$$p(X) = (X^2 - 2)(X^2 + 2),$$

so first we adjoin the roots $\pm\sqrt{2}$ of $(X^2 - 2)$ to form $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$ which gives an extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ of degree 2.

Next consider the polynomial $X^2 + 2 \in \mathbb{Q}(\sqrt{2})[X]$. The complex roots of $X^2 + 2$ are $\pm\sqrt{2}i$ and these are not real, so this polynomial is irreducible in $\mathbb{Q}(\sqrt{2})[X]$. Hence we need to consider $\mathbb{Q}(\sqrt{2}, \sqrt{2}i) = \mathbb{Q}(\sqrt{2}, i)$ and the extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}(\sqrt{2})$ which has degree 2.

$$\begin{array}{c} \mathbb{C} \\ \vdots \\ \infty \\ \mathbb{Q}(\sqrt{2}, i) \\ \text{adjoin roots of } X^2 + 2 \;\Big|\; 2 \\ \mathbb{Q}(\sqrt{2}) \\ \text{adjoin roots of } X^2 - 2 \;\Big|\; 2 \\ \mathbb{Q} \end{array}$$

Thus the splitting subfield of $p(X)$ over $\mathbb{Q}$ in $\mathbb{C}$ is $\mathbb{Q}(\sqrt{2}, i)$ and $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. □

Of course we could have started by first adjoining roots of X^2+2 and then adjoining roots of X^2-2, thus giving the tower

$$\begin{array}{c} \mathbb{C} \\ \vdots \\ \infty \\ \vdots \\ \mathbb{Q}(\sqrt{2},i) \\ \text{adjoin roots of } X^2-2 \;\Big|\; 2 \\ \mathbb{Q}(\sqrt{2}i) \\ \text{adjoin roots of } X^2+2 \;\Big|\; 2 \\ \mathbb{Q} \end{array}$$

An important point is that if a splitting field exists inside of a given extension field F/K, it is unique as a subfield of F.

3.28. Proposition. *Let F/K be an extension field and $p(X) \in K[X]$. If $E_1, E_2 \leqslant F$ are splitting subfields for $p(X)$ over K then $E_1 = E_2$.*

Proof. Let $u_1, \ldots, u_k \in F$ be the distinct roots of $p(X)$ in F. By definition, $K(u_1, \ldots, u_k)$ is the smallest subfield containing K and all the u_j. But $K(u_1, \ldots, u_k)$ must be contained in any splitting subfield, so $E_1 = K(u_1, \ldots, u_k) = E_2$. □

Since we will frequently encounter quadratic polynomials we record a useful result on roots of such polynomials. Recall that $p(X) = aX^2 + bX + c \in K[X]$ is *quadratic* if $a \neq 0$ and its *discriminant* is

$$\Delta = b^2 - 4ac \in K.$$

The proof of the next result is the standard one which works provided 2 has an inverse in K, *i.e.*, when $\operatorname{char} K \neq 2$.

3.29. Proposition. *Let K be a field of characteristic different from 2. Then the quadratic polynomial $p(X) = aX^2 + bX + c \in K[X]$ has*

- *no roots in K if Δ is not a square in K;*
- *one root $-b/(2a) = -(2a)^{-1}b$ if $\Delta = 0$;*
- *two distinct roots*

$$\frac{-b+\delta}{2a} = (2a)^{-1}(-b+\delta), \quad \frac{-b-\delta}{2a} = (2a)^{-1}(-b-\delta),$$

if $\Delta = \delta^2$ for some non-zero $\delta \in K$.

In particular, the splitting field of $p(X)$ over K is K if Δ is a square in K and $K(\delta)$ otherwise, where δ is one of the two square roots of Δ in some extension of K such as the algebraic closure $\overline{K}$ which we will introduce in Section 3.4.

3.30. Example. Find a splitting field $E/\mathbb{Q}$ for $p(X) = X^3 - 2$ over $\mathbb{Q}$ and determine $[E : \mathbb{Q}]$.

Solution. By the Eisenstein Test 1.38, $p(X)$ is irreducible over $\mathbb{Q}$. One root of $p(X)$ is $\sqrt[3]{2} \in \mathbb{R}$ so we adjoin this to $\mathbb{Q}$ to form an extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ of degree 3. Now

$$p(X) = (X - \sqrt[3]{2})(X^2 + \sqrt[3]{2}X + (\sqrt[3]{2})^2)$$

and the second factor has the non-real complex roots $\sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2$ lying in the extension $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}(\sqrt[3]{2})$ of degree 2. So the splitting subfield of X^3-2 in $\mathbb{C}$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ with $[\mathbb{Q}(\sqrt[3]{2},\zeta_3):\mathbb{Q}]=6$.

An alternative strategy would have been to adjoin one of the other roots $\sqrt[3]{2}\,\zeta_3$ or $\sqrt[3]{2}\,\zeta_3^2$ first. We could also have begun by adjoining ζ_3 to form the extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$, but none of the roots of $p(X)$ lie in this field so the extension $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}(\zeta_3)$ of degree 3 is obtained by adjoining one and hence all of the roots.

Figure 3.1 shows all the subfields of the extension $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}$. □

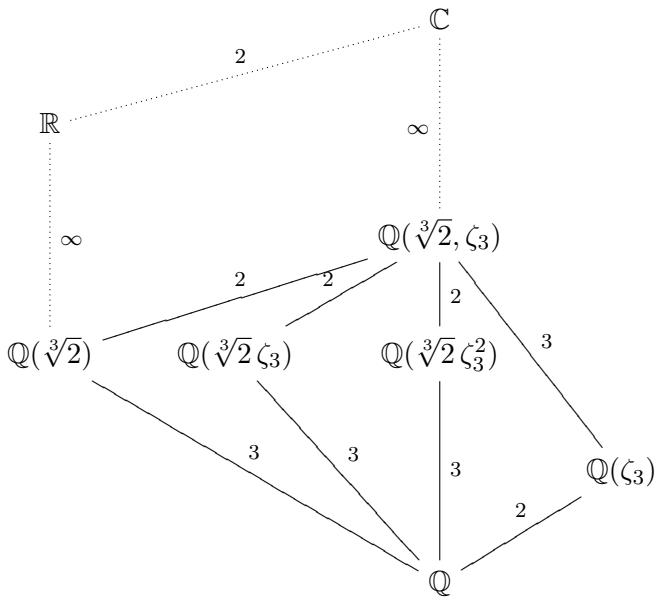


FIGURE 3.1. The subfields of $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}$

3.3. Monomorphisms between extensions

3.31. DEFINITION. For extensions F/K and L/K, let $\mathrm{Mono}_K(L,F)$ denote the set of all monomorphisms $L \longrightarrow F$ which fix the elements of K.

3.32. REMARK. We always have $\mathrm{Aut}_K(F) \subseteq \mathrm{Mono}_K(F,F)$ and $\mathrm{Mono}_K(F,F)$ is closed under composition but is not always a group since elements are not necessarily invertible. If F/K is finite, then we do have $\mathrm{Mono}_K(F,F) = \mathrm{Aut}_K(F)$ since every injective K-linear transformation is surjective and so invertible.

We will also use the following notation.

3.33. DEFINITION. Let F/K be an extension and $p(X) \in K[X]$. Set

$$\mathrm{Roots}(p,F) = \{u \in F : p(u) = 0\},$$

the set of roots of $p(X)$ in F. This is always a finite set which may of course be empty, which happens precisely when $p(X)$ has no root in F.

Suppose that $p(X) \in K[X]$ is an irreducible polynomial which we might as well assume is monic, and let F/K be an extension. Then if $t \in F$ is a root of $p(X)$, the evaluation homomorphism $\varepsilon_t \colon K[X] \longrightarrow F$ factors through the quotient monomorphism $\widetilde{\varepsilon}_t \colon K[X]/(p(X)) \longrightarrow F$ whose image is $K(t) \leqslant F$. Of course, there is one such monomorphism for each root of $p(X)$ in F. If we fix one such root t_0 and identify $K[X]/(p(X))$ with $K(t_0)$ via $\widetilde{\varepsilon}_{t_0}$, then each root of $p(X)$ in F gives rise to a monomorphism $\varphi_t = \widetilde{\varepsilon}_t \circ \widetilde{\varepsilon}_{t_0}^{-1} \colon K(t_0) \longrightarrow F$ for which $\varphi_t(t_0) = t$.

$$\begin{array}{ccccc} & & \overset{\varphi_t = \widetilde{\varepsilon}_t \circ \widetilde{\varepsilon}_{t_0}^{-1}}{\frown} & & \\ K(t_0) & \underset{\cong}{\overset{\widetilde{\varepsilon}_{t_0}}{\longleftarrow}} & K[X]/(p(X)) & \xrightarrow{\widetilde{\varepsilon}_t} & F \end{array}$$

Notice that if $\varphi \colon K[X]/(p(X)) \longrightarrow F$ is any homomorphism extending the identity function on K, then the coset $X + (p(X))$ must be sent by φ to a root of $p(X)$ in F, hence every such homomorphism arises this way. This discussion is summarized in the following result.

3.34. Proposition. *Let F/K be a field extension. Let $p(X) \in K[X]$ be an irreducible polynomial with $t_0 \in F$ be a root of $p(X)$. Then there is a bijection*

$$\mathrm{Roots}(p, F) \longleftrightarrow \mathrm{Mono}_K(K(t_0), F)$$

given by $t \longleftrightarrow \varphi_t$, where $\varphi_t \colon K(t_0) \longrightarrow F$ has the effect $\varphi_t(t_0) = t$.

3.35. Example. Show that $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C})$ has two elements.

Solution. We have $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[X]/(X^2 - 2)$ where $X^2 - 2$ is irreducible over $\mathbb{Q}$. Hence the $\mathbb{Q}$-monomorphisms we want send $\sqrt{2}$ to $\pm\sqrt{2}$ which are the complex roots of $X^2 - 2$. In fact both possibilities occur, giving monomorphisms $\mathrm{id}, \alpha \colon \mathbb{Q}(\sqrt{2}) \longrightarrow \mathbb{C}$, where

$$\alpha(a + b\sqrt{2}) = a - b\sqrt{2}.$$

We can replace $\mathbb{C}$ by $\mathbb{Q}(\sqrt{2})$ to obtain

$$\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{C}) = \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2})) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{2})).$$

We will see that this is not always true. □

3.36. Example. Show that $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{C})$ has 3 elements but $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}))$ contains only the identity function.

Solution. Here $\mathrm{minpoly}_{\mathbb{Q}, \sqrt[3]{2}}(X) = X^3 - 2$ and there are 3 complex roots $\sqrt[3]{2}$, $\sqrt[3]{2}\,\zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$. As two of these roots are not real, $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}))$ contains only the identity since $\mathbb{Q}(\sqrt[3]{2}) \leqslant \mathbb{R}$.

Each of the above roots corresponds to one of the subfields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\,\zeta_3)$ or $\mathbb{Q}(\sqrt[3]{2}\,\zeta_3^2)$ of $\mathbb{C}$ and there are 3 monomorphisms $\alpha_0, \alpha_1, \alpha_2 \colon \mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{C}$ given by

$$\begin{aligned} \alpha_0(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2, \\ \alpha_1(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + b\sqrt[3]{2}\,\zeta_3 + c(\sqrt[3]{2})^2\,\zeta_3^2, \\ \alpha_2(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) &= a + b\sqrt[3]{2}\,\zeta_3^2 + c(\sqrt[3]{2})^2\,\zeta_3. \end{aligned}$$

These mappings have images

$$\alpha_0\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}), \quad \alpha_1\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}\,\zeta_3), \quad \alpha_2\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}\,\zeta_3^2).$$ □

3.37. PROPOSITION. *Let F/K and L/K be extensions.*

(i) *For $p(X) \in K[X]$, each monomorphism $\alpha \in \mathrm{Mono}_K(L, F)$ restricts to a function $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, F)$ which is an injection.*

(ii) *If $\alpha \in \mathrm{Mono}_K(L, L)$, then $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, L)$ is a bijection.*

PROOF. (i) For $u \in \mathrm{Roots}(p, L)$ we have

$$p(\alpha(u)) = \alpha(p(u)) = \alpha(0) = 0,$$

so α maps $\mathrm{Roots}(p, L)$ into $\mathrm{Roots}(p, F)$. Since α is an injection its restriction to $\mathrm{Roots}(p, L) \subseteq L$ is also an injection.
(ii) From (i), $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, L)$ is an injective function from a finite set to itself, hence it is also surjective by the Pigeon Hole Principle. Thus $\alpha_p\colon \mathrm{Roots}(p, L) \longrightarrow \mathrm{Roots}(p, L)$ is a bijection. □

Part (ii) says that any automorphism of L/K permutes the set of roots in L of a polynomial $p(X) \in K[X]$. This gives us a strong hold on the possible automorphisms. In the case of finite, or more generally algebraic, extensions it is the key to understanding the automorphism group and this is a fundamental insight of Galois Theory.

3.38. EXAMPLE. Determine $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C})$.

SOLUTION. We have already met the extension $\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ in Example 3.30 and we will make use of information from there. We build up the list of monomorphisms in stages.

First consider monomorphisms that fix $\sqrt[3]{2}$ and hence fix the subfield $\mathbb{Q}(\sqrt[3]{2})$. These form the subset

$$\mathrm{Mono}_{\mathbb{Q}(\sqrt[3]{2})}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}) \subseteq \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}).$$

We know that $\mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathbb{Q}(\sqrt[3]{2})(\zeta_3)$ and that ζ_3 is a root of the irreducible cyclotomic polynomial $\Phi_3(X) = X^2 + X + 1 \in \mathbb{Q}(\sqrt[3]{2})[X]$. So there are two monomorphisms id, α_0 fixing $\mathbb{Q}(\sqrt[3]{2})$, where α_0 has the effect

$$\alpha_0\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2} \\ \zeta_3 & \longmapsto & \zeta_3^2 \end{pmatrix}.$$

Next we consider monomorphisms that send $\sqrt[3]{2}$ to $\sqrt[3]{2}\,\zeta_3$. This time we have 2 distinct ways to extend to elements of $\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{Q}(\sqrt[3]{2}, \zeta_3))$ since again we can send ζ_3 to either ζ_3 or ζ_3^2. The possibilities are

$$\alpha_1\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3 \\ \zeta_3 & \longmapsto & \zeta_3 \end{pmatrix}, \quad \alpha_1'\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3 \\ \zeta_3 & \longmapsto & \zeta_3^2 \end{pmatrix}.$$

Finally we consider monomorphisms that send $\sqrt[3]{2}$ to $\sqrt[3]{2}\,\zeta_3^2$. There are again two possibilities

$$\alpha_2\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3^2 \\ \zeta_3 & \longmapsto & \zeta_3 \end{pmatrix}, \quad \alpha_2'\colon \begin{pmatrix} \sqrt[3]{2} & \longmapsto & \sqrt[3]{2}\,\zeta_3^2 \\ \zeta_3 & \longmapsto & \zeta_3^2 \end{pmatrix}.$$

These are all 6 of the required monomorphisms. It is also the case here that

$$\mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{C}) = \mathrm{Mono}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3), \mathbb{Q}(\sqrt[3]{2}, \zeta_3)) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)),$$

so these form a group. It is a nice exercise to show that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) \cong \mathrm{S}_3$, the symmetric group on 3 objects. It is also worth remarking that $|\,\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3))| = [\mathbb{Q}(\sqrt[3]{2}, \zeta_3) : \mathbb{Q}]$. □

We end this section with another useful result.

3.39. Proposition. *Let L/K be an extension and $\alpha \in \mathrm{Mono}_K(L,L)$. Then α restricts to an automorphism $\alpha^{\mathrm{alg}}\colon L^{\mathrm{alg}} \longrightarrow L^{\mathrm{alg}}$.*

Proof. Suppose that $u \in L^{\mathrm{alg}}$, say $p(u) = 0$ for some $p(X) \in K[X]$ of positive degree. Then

$$p(\alpha(u)) = \alpha(p(u)) = \alpha(0) = 0,$$

so α maps $L^{\mathrm{alg}} \subseteq L$ into itself and therefore gives rise to a restriction $\alpha^{\mathrm{alg}}\colon L^{\mathrm{alg}} \longrightarrow L^{\mathrm{alg}}$ which is also a monomorphism. We must show that α^{alg} is a bijection by showing it is surjective.

Let $v \in L^{\mathrm{alg}}$ and suppose that $q(v) = 0$ for some $q(X) \in K[X]$ of positive degree. Now $\mathrm{Roots}(q,L) \neq \emptyset$ since it contains v, and it is also finite. Then $\alpha_q\colon \mathrm{Roots}(q,L) \longrightarrow \mathrm{Roots}(q,L)$ is a bijection by Proposition 3.37(ii), hence $v = \alpha_q(w) = \alpha(w)$ for some $w \in \mathrm{Roots}(q,L) \subseteq L^{\mathrm{alg}}$. This shows that $v \in \mathrm{im}\,\alpha$ and so α^{alg} is surjective. □

3.4. Algebraic closures

An important property of the complex numbers is that $\mathbb{C}$ is *algebraically closed*.

3.40. Theorem (Fundamental Theorem of Algebra for $\mathbb{C}$). *Every non-constant polynomial $p(X) \in \mathbb{C}[X]$ has a root in $\mathbb{C}$.*

3.41. Corollary. *Every non-constant polynomial $p(X) \in \mathbb{C}[X]$ has a factorization*

$$p(X) = c(X - u_1)\cdots(X - u_d),$$

where $c, u_1, \ldots, u_d \in \mathbb{C}$ and this is unique apart from the order of the roots u_j.

It is natural to pose the following question.

3.42. Question. Let K be a field. Is there an algebraically closed field F containing K?

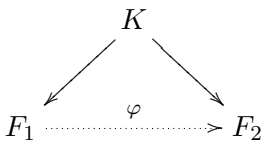
By taking F^{alg} we might as well ask that such a field be algebraic over K.

3.43. Definition. Let K be a field. An extension F/K is called an *algebraic closure of K* if F is algebraic over K and is algebraically closed.

3.44. Theorem. *Let K be a field.*

(i) *There is an algebraic closure of K.*

(ii) *Let F_1 and F_2 be algebraic closures of K. Then there is an isomorphism $\varphi\colon F_1 \longrightarrow F_2$ which fixes the elements of K.*



Hence algebraic closures are essentially unique.

Proof. See [**3**] for a proof using *Zorn's Lemma* (see Axiom 3.48) which is logically equivalent to the *Axiom of Choice*. □

Because of the uniqueness we usually fix some choice of algebraic closure of K and write $\overline{K}$ or $K^{\text{alg cl}}$, referring to it as *the* algebraic closure of K. We are already familiar with the example $\overline{\mathbb{C}} = \mathbb{C}$. There are some immediate consequences of Theorem 3.44. We will temporarily write $E_1 \doteq E_2$ to indicate that for extensions E_1/K and E_2/K there is an isomorphism $E_1 \longrightarrow E_2$ fixing the elements of K.

3.45. Proposition. *Let K be a field.*

(i) *If L/K is an algebraic extension, then $\overline{L} \doteq \overline{K}$.*
(ii) *If L/K is an extension, then so is $\overline{L}/K$ and $(\overline{L})^{\text{alg}} \doteq \overline{K}$.*

Proof. (i) By Proposition 3.16, every element of $\overline{L}$ is algebraic over K. Since $\overline{L}$ is algebraically closed it is an algebraic closure of K.
(ii) Every non-constant polynomial in $(\overline{L})^{\text{alg}}[X]$ has a root in $\overline{L}$; indeed, by Proposition 3.16, all of its roots are in fact algebraic over K since $(\overline{L})^{\text{alg}}$ is algebraic over K. Hence these roots lie in $(\overline{L})^{\text{alg}}$, which shows that it is algebraically closed. □

For example, we have $\overline{\mathbb{Q}} = \mathbb{C}^{\text{alg}}$ and $\overline{\mathbb{R}} = \mathbb{C}$.

There is a stronger result than Theorem 3.44(ii), the Monomorphism Extension Theorem, which we will find useful. Again the proof uses Zorn's Lemma which we state below. First we need some definitions.

3.46. Definition. A *partially ordered set* $(X, \preccurlyeq)$ consists of a set X and a binary relation $\preccurlyeq$ such that whenever $x, y, z \in X$,

- $x \preccurlyeq x$;
- if $x \preccurlyeq y$ and $y \preccurlyeq z$ then $x \preccurlyeq z$;
- if $x \preccurlyeq y$ and $y \preccurlyeq x$ then $x = y$.

$(X, \preccurlyeq)$ is *totally ordered* if for every pair $x, y \in X$, at least one of $x \preccurlyeq y$ or $y \preccurlyeq x$ is true.

3.47. Definition. Let $(X, \preccurlyeq)$ be a partially ordered set and $Y \subseteq X$.

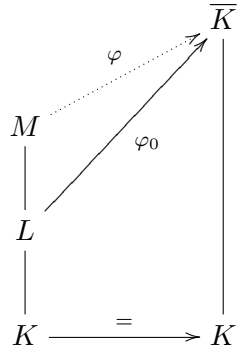
- $\overline{y} \in X$ is an *upper bound for Y* if for every $y \in Y$, $y \preccurlyeq \overline{y}$.
- An element $x \in X$ is a *maximal element of X* if

$$x \preccurlyeq y \quad \Longrightarrow \quad y = x.$$

3.48. Axiom (Zorn's Lemma). *Let $(X, \preccurlyeq)$ be a partially ordered set in which every totally ordered subset has an upper bound. Then X has a maximal element.*

3.49. Theorem (Monomorphism Extension Theorem). *Let M/K be an algebraic extension and $L/K \leqslant M/K$. Suppose that $\varphi_0 \colon L \longrightarrow \overline{K}$ is a monomorphism fixing the elements of K.*

Then there is an extension of φ_0 to a monomorphism $\varphi\colon M \longrightarrow \overline{K}$.



PROOF. We consider the set X consisting of all pairs (F, θ), where $F/L \leqslant M/L$ and $\theta\colon F \longrightarrow \overline{K}$ extends φ_0. We order X using the relation $\preccurlyeq$ for which $(F_1, \theta_1) \preccurlyeq (F_2, \theta_2)$ whenever $F_1 \leqslant F_2$ and θ_2 extends θ_1. Then $(X, \preccurlyeq)$ is a partially ordered set.

Suppose that $Y \subseteq X$ is a totally ordered subset. Let

$$\widetilde{F} = \bigcup_{(F,\theta)\in Y} F.$$

Then $\widetilde{F}/L \leqslant M/L$. Also there is a function $\widetilde{\theta}\colon \widetilde{F} \longrightarrow \overline{K}$ defined by

$$\widetilde{\theta}(u) = \theta(u)$$

whenever $u \in F$ for $(F, \theta) \in Y$. It is straightforward to check that if $u \in F'$ for $(F', \theta') \in Y$ then

$$\theta'(u) = \theta(u),$$

so $\widetilde{\theta}$ is well-defined. Then for every $(F, \theta) \in Y$ we have $(F, \theta) \preccurlyeq (\widetilde{F}, \widetilde{\theta})$, so $(\widetilde{F}, \widetilde{\theta})$ is an upper bound for Y. By Zorn's Lemma there must be a maximal element of X, (M_0, θ_0).

Suppose that $M_0 \neq M$, so there is an element $u \in M$ for which $u \notin M_0$. Since M is algebraic over K it is also algebraic over M_0, hence u is algebraic over M_0. If

$$\operatorname{minpoly}_{M_0,u}(X) = a_0 + \cdots + a_{n-1}X^{n-1} + X^n,$$

then the polynomial

$$f(X) = \theta_0(a_0) + \cdots + \theta_0(a_{n-1})X^{n-1} + X^n \in (\theta_0 M_0)[X]$$

is also irreducible and so it has a root v in $\overline{K}$ (which is also an algebraic closure of $\theta_0 M_0 \leqslant \overline{K}$). The Homomorphism Extension Property 1.22 of the polynomial ring $M_0[X]$ applied to the monomorphism $\theta_0\colon M_0 \longrightarrow \overline{K}$ yields a homomorphism $\theta_0'\colon M_0[X] \longrightarrow \overline{K}$ extending θ_0 and for which $\theta_0'(u) = v$. This factors through the quotient ring $M_0[X]/(\operatorname{minpoly}_{M_0,u}(X))$ to give a monomorphism $\theta_0''\colon M_0(u) \longrightarrow \overline{K}$ extending θ_0. But then $(M_0, \theta_0) \preccurlyeq (M_0(u), \theta_0'')$ and $(M_0, \theta_0) \neq (M_0(u), \theta_0'')$, contradicting the maximality of (M_0, θ_0). Hence $M_0 = M$ and so we can take $\varphi = \theta_0$. □

3.50. EXAMPLE. Let $u \in \overline{K}$ and suppose that $p(X) = \operatorname{minpoly}_{K,u}(X) \in K[X]$. Then for any other root of $p(X)$, $v \in \overline{K}$ say, there is a monomorphism $\varphi_v\colon K(u) \longrightarrow \overline{K}$ with $\varphi_v(u) = v$. This extends to a monomorphism $\varphi\colon \overline{K} \longrightarrow \overline{K}$.

3.51. DEFINITION. Let $u, v \in \overline{K}$. Then v is *conjugate to u over K* or is a *conjugate of u over K* if there is a monomorphism $\varphi\colon \overline{K} \longrightarrow \overline{K}$ fixing K for which $v = \varphi(u)$.

3.52. Lemma. *If $u, v \in \overline{K}$, then v is conjugate to u over K if and only if* $\operatorname{minpoly}_{K,u}(v) = 0$.

Proof. Suppose that $v = \varphi(u)$ for some $\varphi \in \operatorname{Mono}_K(\overline{K}, \overline{K})$. If

$$\operatorname{minpoly}_{K,u}(X) = a_0 + a_1 X + \cdots + a_{d-1}X^{d-1} + X^d,$$

then

$$a_0 + a_1 u + \cdots + a_{d-1}u^{d-1} + u^d = 0$$

and so

$$a_0 + a_1 v + \cdots + a_{d-1}v^{d-1} + v^d = \varphi(a_0 + a_1 u + \cdots + a_{d-1}u^{d-1} + u^d) = 0.$$

The converse follows from Example 3.50. □

3.5. Multiplicity of roots and separability

Let K be a field. Suppose that $f(X) \in K[X]$ and $u \in K$ is a root of $f(X)$, *i.e.*, $f(u) = 0$. Then we can factor $f(X)$ as $f(X) = (X - u)f_1(X)$ for some $f_1(X) \in K[X]$.

3.53. Definition. If $f_1(u) = 0$ then u is a *multiple* or *repeated root* of $f(X)$. If $f_1(u) \neq 0$ then u is a *simple root* of $f(X)$.

We need to understand more clearly when an irreducible polynomial has a multiple root since this turns out to be important in what follows. Consider the *formal derivative on* $K[X]$, *i.e.*, the function $\partial\colon K[X] \longrightarrow K[X]$ given by

$$\partial(f(X)) = f'(X) = a_1 + 2a_2 X + \cdots + da_d X^{d-1},$$

where $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$ with $a_j \in K$.

3.54. Proposition. *The formal derivative $\partial\colon K[X] \longrightarrow K[X]$ has the following properties.*

(i) *∂ is K-linear.*

(ii) *∂ is a* derivation, i.e., *for $f(X), g(X) \in K[X]$,*

$$\partial(f(X)g(X)) = \partial(f(X))g(X) + f(X)\partial(g(X)).$$

(iii) *If* $\operatorname{char} K = 0$, *then* $\ker \partial = K$ *and ∂ is surjective.*

(iv) *If* $\operatorname{char} K = p > 0$, *then*

$$\ker \partial = \{h(X^p) : h(X) \in K[X]\}$$

and $\operatorname{im} \partial$ *is spanned by the monomials X^k with $p \nmid (k+1)$.*

Proof. (i) This is routine.

(ii) By K-linearity, it suffices to verify this for the case where $f(X) = X^r$ and $g(X) = X^s$ with $r, s \geqslant 0$. But then

$$\partial(X^{r+s}) = (r+s)X^{r+s-1} = rX^{r-1}X^s + sX^r X^{s-1} = \partial(X^r)X^s + X^r\partial(X^s).$$

(iii) If $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_d X^d$ then

$$\partial(f(X)) = 0 \quad \Longleftrightarrow \quad a_1 = 2a_2 = \cdots = da_d = 0.$$

So $\partial(f(X)) = 0$ if and only if $f(X) = a_0 \in K$. It is also clear that every polynomial $g(X) \in K[X]$ has the form $g(X) = \partial(f(X))$ where $f(X)$ is an anti-derivative of $g(X)$.

(iv) For a monomial X^m, $\partial(X^m) = mX^{m-1}$ and this is zero if and only if $p \mid m$. Using this we see that

$$\partial(a_0 + a_1X + a_2X^2 + \cdots + a_dX^d) = 0 \quad \iff \quad a_m = 0 \text{ whenever } p \nmid m.$$

Also, $\operatorname{im}\partial$ is spanned by the monomials X^k for which $\partial(X^{k+1}) \neq 0$, which are the ones with $p \nmid (k+1)$. □

We now apply the formal derivative to detect multiple roots.

3.55. Proposition. *Let $f(X) \in K[X]$ have a root $u \in L$ for some extension L/K. Then u is a multiple root of $f(X)$ if and only if $f(X)$ and $f'(X)$ have a common factor of positive degree in $K[X]$ which vanishes at u.*

Proof. Working in $L[X]$, let $f(X) = (X-u)f_1(X)$. Then

$$f'(X) = f_1(X) + (X-u)f_1'(X),$$

so $f'(u) = f_1(u)$. Hence u is a multiple root if and only if $f(X)$ and $f'(X)$ have a common factor in $L[X]$ (and hence in $K[X]$ by Proposition 3.12) and which vanishes at u. □

3.56. Corollary. *If $f(X)$ is irreducible in $K[X]$ then a root u is a multiple root if and only if $f'(X) = 0$. In particular, this can only happen if* $\operatorname{char} K > 0$.

3.57. Corollary. *If* $\operatorname{char} K = 0$ *and $f(X)$ is irreducible in $K[X]$, then every root of $f(X)$ is simple.*

3.58. Example. For $n \geqslant 1$, show that each of the roots of $f(X) = X^n - 1$ in $\mathbb{C}$ is simple.

Solution. We have $f'(X) = \partial(X^n - 1) = nX^{n-1}$, so for any root ζ of $f(X)$,

$$f'(\zeta) = n\zeta^{n-1} \neq 0.$$ □

3.59. Example. Show that $2i$ is a multiple root of $f(X) = X^4 + 8X^2 + 16$.

Solution. We have $f'(X) = 4X^3 + 16X$. Using Long Division and the Euclidean Algorithm we find that $\gcd(f(X), f'(X)) = X^2 + 4$, where $2i$ is also a root of $X^2 + 4$. Hence $2i$ is a multiple root of $f(X)$. In fact, $X^4 + 8X^2 + 16 = (X^2 + 4)^2$, so this is obvious. □

3.60. Example. Let $p > 0$ be a prime and suppose that $L/\mathbb{F}_p$ is an extension. Show that each of the roots of $f(X) = X^p - 1$ in L is multiple.

Solution. We have $f'(X) = \partial(X^p - 1) = pX^{p-1} = 0$, so if ζ is any root of $f(X)$ then $f'(\zeta) = 0$. In fact, 1 is the *only* root of $X^p - 1$ since this polynomial factorises (essentially uniquely) as

$$X^p - 1 = (X-1)^p$$

because of the Idiot's Binomial Theorem 1.11 and the Unique Factorization Property 1.33. □

3.61. Definition. An irreducible polynomial $p(X) \in K[X]$ is *separable over K* if every root of $p(X)$ in an extension L/K is simple. By Corollary 3.56, this is equivalent to requiring that $p'(X) \neq 0$. If $u \in L$ is a multiple root of $p(X)$, then the *multiplicity of u in $p(X)$* is the maximum m such that$p(X) = (X-u)^m q(X)$ for some $q(X) \in L[X]$.

3.62. Proposition. *Let K be a field and let $\overline{K}$ be an algebraic closure. If the irreducible polynomial $p(X) \in K[X]$ has distinct roots $u_1, \ldots, u_k \in \overline{K}$, then the multiplicities of the u_j are equal. Hence in $\overline{K}[X]$,*

$$p(X) = c(X - u_1)^m \cdots (X - u_k)^m,$$

where $c \in K$ and $m \geqslant 1$.

Proof. Let $u \in \overline{K}$ be a root of $p(X)$ and suppose that it has multiplicity m, so we can write $p(X) = (X - u)^m p_1(X)$ where $p_1(X) \in K(u)[X]$ and $p_1(u) \neq 0$.

Now let $v \in \overline{K}$ be any other root of $p(X)$. By Proposition 3.34, there is a monomorphism $\varphi_v \colon K(u) \longrightarrow \overline{K}$ for which $\varphi_v(u) = v$. When $p(X)$ is viewed as an element of $K(u)[X]$, the coefficients of $p(X)$ are fixed by φ_v. Then

$$\varphi_v((X - u)^m p_1(X)) = (X - u)^m p_1(X),$$

and so

$$(X - v)^m \widetilde{p}_1(X) = (X - u)^m p_1(X),$$

where $\widetilde{p}_1(X) \in \overline{K}[X]$ is obtained applying φ_v to the coefficients of $p_1(X)$. Now by Corollary 1.34, $(X - v)^m$ must divide $p_1(X)$ in $\overline{K}[X]$, and therefore the multiplicity of v must be at least m. Interchanging the rôles of u and v we find that the multiplicities of u and v are in fact equal. □

3.63. Corollary. *Let K be a field and let $\overline{K}$ be an algebraic closure. If the irreducible polynomial $p(X) \in K[X]$ has distinct roots $u_1, \ldots, u_k \in \overline{K}$ which are all simple then in $\overline{K}[X]$,*

$$p(X) = c(X - u_1) \cdots (X - u_k),$$

where $c \in K$ and $k = \deg p(X)$.

3.64. Corollary. *Let K be a field and let $u \in \overline{K}$. Then the number of distinct conjugates of u is*

$$\frac{\deg \operatorname{minpoly}_{K,u}(X)}{m},$$

where m is the multiplicity of u in $\operatorname{minpoly}_{K,u}(X)$.

3.65. Definition. An algebraic element $u \in L$ in an extension L/K is *separable* if its minimal polynomial $\operatorname{minpoly}_{K,u}(X) \in K[X]$ is separable.

3.66. Definition. An algebraic extension L/K is called *separable* if every element of L is separable over K.

3.67. Example. An algebraic extension L/K of a field of characteristic 0 is separable by Corollary 3.57.

3.68. Definition. Let L/K be a finite extension. The *separable degree of L over K* is

$$(L : K) = |\operatorname{Mono}_K(L, \overline{K})|.$$

3.69. Lemma. *For a finite simple extension $K(u)/K$,*

$$(K(u) : K) = |\operatorname{Roots}(\operatorname{minpoly}_{K,u}, \overline{K})|.$$

If $K(u)/K$ is separable, then $[K(u) : K] = (K(u) : K)$.

PROOF. This follows from Proposition 3.34 applied to the case $L = \overline{K}$. □

Any finite extension L/K can be built up from a succession of simple extensions

$$K(u_1)/K,\ K(u_1,u_2)/K(u_1),\cdots,L = K(u_1,\ldots,u_k)/K(u_1,\ldots,u_{k-1}). \tag{3.1}$$

So we can use the following to compute $(L:K) = (K(u_1,\ldots,u_k):K)$.

3.70. PROPOSITION. *Let L/K and M/L be finite extensions. Then*

$$(M:K) = (M:L)(L:K).$$

PROOF. For $\alpha \in \mathrm{Mono}_K(M,\overline{K})$ let $\alpha_L \in \mathrm{Mono}_K(L,\overline{K})$ be its restriction to L. By the Monomorphism Extension Theorem 3.49, each element of $\mathrm{Mono}_K(L,\overline{K})$ extends to a monomorphism $M \longrightarrow \overline{K}$, so every element $\beta \in \mathrm{Mono}_K(L,\overline{K})$ has the form $\beta = \alpha_L$ for some $\alpha \in \mathrm{Mono}_K(M,\overline{K})$. Since $(L:K) = |\,\mathrm{Mono}_K(L,\overline{K})|$, we need to show that the number of such α is always $(M:L) = |\,\mathrm{Mono}_L(M,\overline{K})|$.

So given $\beta \in \mathrm{Mono}_K(L,\overline{K})$, choose any extension to a monomorphism $\widetilde{\beta}\colon \overline{K} \longrightarrow \overline{K}$; by Proposition 3.39, $\widetilde{\beta}$ is an automorphism. Of course, restricting to $M \leqslant \overline{K}$ we obtain a monomorphism $M \longrightarrow \overline{K}$. Now for any extension $\beta'\colon M \longrightarrow \overline{K}$ of β we can form the composition $\widetilde{\beta}^{-1} \circ \beta'\colon M \longrightarrow \overline{K}$; notice that if $u \in L$, then

$$\widetilde{\beta}^{-1} \circ \beta'(u) = \widetilde{\beta}^{-1}(\beta(u)) = u,$$

hence $\widetilde{\beta}^{-1} \circ \beta' \in \mathrm{Mono}_L(M,\overline{K})$. Conversely, each $\gamma \in \mathrm{Mono}_L(M,\overline{K})$ gives rise to a monomorphism $\widetilde{\beta} \circ \gamma\colon M \longrightarrow \overline{K}$ which extends β. In effect, this shows that there is a bijection

$$\big\{\text{extensions of } \beta \text{ to monomorphism a } M \longrightarrow \overline{K}\big\} \longleftrightarrow \mathrm{Mono}_L(M,\overline{K}),$$

so $(M:L) = |\,\mathrm{Mono}_L(M,\overline{K})|$ agrees with the number of extensions of β to a monomorphism $M \longrightarrow \overline{K}$. Therefore we have the desired formula $(M:K) = (M:L)(L:K)$. □

3.71. COROLLARY. *Let L/K be a finite extension. Then $(L:K) \mid [L:K]$.*

PROOF. If L/K is a simple extension then by Propositions 3.62 and 3.34 we know that this is true. The general result follows by building up L/K as a sequence of simple extensions as in (3.1) and then using Theorem 2.6(ii) which gives

$$[L:K] = [K(u_1):K]\,[K(u_1,u_2):K(u_1)]\cdots[K(u_1,\ldots,u_k):K(u_1,\ldots,u_{k-1})].$$

For each k, $(K(u_1,\ldots,u_k):K(u_1,\ldots,u_{k-1}))$ divides $[K(u_1,\ldots,u_k):K(u_1,\ldots,u_{k-1})]$, so the desired result follows. □

3.72. PROPOSITION. *Let L/K be a finite extension. Then L/K is separable if and only if $(L:K) = [L:K]$.*

PROOF. Suppose that L/K is separable. If $K \leqslant E \leqslant L$, then for any $u \in L$, u is algebraic over E, and in the polynomial ring $E[X]$ we have $\mathrm{minpoly}_{E,u}(X) \mid \mathrm{minpoly}_{K,u}(X)$. As $\mathrm{minpoly}_{K,u}(X)$ is separable, so is $\mathrm{minpoly}_{E,u}(X)$, and therefore L/E is separable. Clearly E/K is also separable. We have $(L:K) = (L:E)\,(E:K)$ and $[L:K] = [L:E]\,[E:K]$, so to

verify that $(L:K) = [L:K]$ it suffices to show that $(L:E) = [L:E]$ and $(E:K) = [E:K]$. Expressing L/K in terms of a sequence of simple extensions as in (3.1), we have

$$(L:K) = (K(u_1):K)\cdots(L:K(u_1,\ldots,u_{k-1})),$$
$$[L:K] = [K(u_1):K]\cdots[L:K(u_1,\ldots,u_{k-1})].$$

Now we can apply Lemma 3.69 to each of these intermediate separable simple extensions to obtain $(L:K) = [L:K]$.

For the converse, suppose that $(L:K) = [L:K]$. We must show that for each $u \in L$, u is separable. For the extensions $K(u)/K$ and $L/K(u)$ we have $(L:K) = (L:K(u))\,(K(u):K)$ and $[L:K] = [L:K(u)]\,[K(u):K]$. By Corollary 3.71, there are some positive integers r, s for which $[L:K(u)] = r(L:K(u))$ and $[K(u):K] = s(K(u):K)$. Hence

$$(L:K(u))(K(u):K) = rs(L:K(u))(K(u):K),$$

which can only happen if $r = s = 1$. Thus $(K(u):K) = [K(u):K]$ and so u is separable. □

3.73. Proposition. *Let L/K and M/L be finite extensions. Then M/K is separable if and only if L/K and M/L are separable.*

Proof. If M/K is separable then $[M:K] = (M:K)$ and so by Proposition 3.70,

$$[M:L][L:K] = (M:L)(L:K).$$

This can only happen if $[M:L] = (M:L)$ and $[L:K] = (L:K)$, since $(M:L) \leqslant [M:L]$ and $(L:K) \leqslant [L:K]$. By Proposition 3.72 this implies that L/K and M/L are separable.

Conversely, if L/K and M/L are separable then $[M:L] = (M:L)$ and $[L:K] = (L:K)$, hence

$$[M:K] = [M:L][L:K] = (M:L)(L:K) = (M:K).$$

Therefore M/K is separable. □

3.6. The Primitive Element Theorem

Recall from Definition 3.10 that a finite extension L/K is simple if there is an element $u \in L$ for which $L = K(u)$, and such an element is called a primitive element.

3.74. Theorem (Primitive Element Theorem). *Let L/K be a finite separable extension. Then L has a primitive element, hence L/K is a simple extension.*

Proof. The case where K is a finite field will be dealt with in Proposition 5.16. So we will assume that K is infinite.

Since L is built up from a sequence of simple extensions it suffices to consider the case $L = K(u,v)$. Let $p(X), q(X) \in K[X]$ be the minimal polynomials of u and v over K. Suppose that the distinct roots of $p(X)$ in $\overline{K}$ are $u = u_1,\ldots,u_r$, while the distinct roots of $q(X)$ are $v = v_1,\ldots,v_s$. By the separability assumption, $r = \deg p(X)$ and $s = \deg q(X)$.

Since K is infinite, we can choose an element $t \in K$ for which

$$t \neq \frac{u - u_i}{v_j - v}$$

whenever $j \neq 1$. Then taking $w = u + tv \in L$, we find that $w \neq u_i + tv_j$ whenever $j \neq 1$. Define the polynomial (of degree r)

$$h(X) = p(w - tX) \in K(w)[X] \subseteq L[X].$$

Then $h(v) = p(u) = 0$, but $h(v_j) \neq p(u_i) = 0$ for any $j \neq 1$ by construction of t, so none of the other v_j is a zero of $h(X)$.

Now since the polynomials $h(X), q(X) \in K(w)[X]$ have exactly one common root in $\overline{K}$, namely v, by separability their greatest common divisor in $K(w)[X]$ is a linear polynomial which must be $X - v$, hence $v \in K(w)$ and so $u = w - tv \in K(w)$. This shows that $K(u, v) \leqslant K(w)$ and therefore $K(w) = K(u, v)$. □

3.75. Corollary. *Let L/K be a finite extension of a field of characteristic 0. Then L has a primitive element.*

Proof. Since $\mathbb{Q} \leqslant K$, K is infinite and by Example 3.67 L/K is separable. □

To find a primitive element we can always use the method suggested by the proof of Theorem 3.74, however a 'try it and see' approach will often be sufficient.

3.76. Example. Find a primitive element for the extension $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$.

Solution. Consider $\sqrt{3} + i$. Then working over the subfield $\mathbb{Q}(\sqrt{3}) \leqslant \mathbb{Q}(\sqrt{3}, i)$ we find that $i \notin \mathbb{Q}(\sqrt{3}) \leqslant \mathbb{R}$ and

$$(X - (\sqrt{3} + i))(X - (\sqrt{3} - i)) = X^2 - 2\sqrt{3}X + 4 \in \mathbb{Q}(\sqrt{3})[X],$$

hence

$$X^2 - 2\sqrt{3}X + 4 = \operatorname{minpoly}_{\mathbb{Q}(\sqrt{3}), \sqrt{3}+i}(X).$$

Now taking

$$(X^2 - 2\sqrt{3}X + 4)(X^2 + 2\sqrt{3}X + 4) = X^4 - 4X^2 + 16 \in \mathbb{Q}[X],$$

we see that $\operatorname{minpoly}_{\mathbb{Q}, \sqrt{3}+i}(X) \mid (X^4 - 4X^2 + 16)$ in $\mathbb{Q}[X]$. Notice that

$$(\sqrt{3} + i)^{-1} = \frac{(\sqrt{3} - i)}{(\sqrt{3} + i)(\sqrt{3} - i)} = \frac{(\sqrt{3} - i)}{3 + 1} = \frac{1}{4}(\sqrt{3} - i) \in \mathbb{Q}(\sqrt{3} + i),$$

since $(\sqrt{3} + i)^{-1} \in \mathbb{Q}(\sqrt{3} + i)$. Hence

$$\sqrt{3} = \frac{1}{2}((\sqrt{3} + i) + (\sqrt{3} - i)), \quad i = \frac{1}{2}((\sqrt{3} + i) - (\sqrt{3} - i)),$$

are both in $\mathbb{Q}(\sqrt{3} + i)$, showing that $\mathbb{Q}(\sqrt{3}, i) \leqslant \mathbb{Q}(\sqrt{3} + i)$ and so $\mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(\sqrt{3} + i)$. Thus we must have $\deg \operatorname{minpoly}_{\mathbb{Q}, \sqrt{3}+i}(X) = 4$, and so $\operatorname{minpoly}_{\mathbb{Q}, \sqrt{3}+i}(X) = X^4 - 4X^2 + 16$. □

There is a general phenomenon illustrated by Example 3.76.

3.77. Proposition. *Let $u \in \overline{K}$ be separable over K. Then*

$$\operatorname{minpoly}_{K,u}(X) = (X - \alpha_1(u)) \cdots (X - \alpha_d(u)),$$

where $\alpha_1, \ldots, \alpha_d$ are the elements of $\operatorname{Mono}_K(K(u), \overline{K})$. In particular, the polynomial

$$(X - \alpha_1(u)) \cdots (X - \alpha_d(u)) \in \overline{K}[X]$$

is in $K[X]$ and is irreducible therein.

PROOF. Since $K(u)$ is separable then by Lemma 3.52,

$$d = \deg \operatorname{minpoly}_{K,u}(X) = [K(u) : K] = (K(u) : K). \qquad \square$$

In Example 3.76 we have

$$[\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4.$$

There are four monomorphisms $\alpha_k \colon \mathbb{Q}(\sqrt{3}, i) \longrightarrow \mathbb{Q}(\sqrt{3}, i)$ given by

$$\alpha_1 = \mathrm{id}, \quad \alpha_2 = \begin{pmatrix} \sqrt{3} & \longmapsto & \sqrt{3} \\ i & \longmapsto & -i \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} \sqrt{3} & \longmapsto & -\sqrt{3} \\ i & \longmapsto & i \end{pmatrix}, \quad \alpha_4 = \begin{pmatrix} \sqrt{3} & \longmapsto & -\sqrt{3} \\ i & \longmapsto & -i \end{pmatrix}.$$

Then

$$\alpha_2(\sqrt{3} + i) = (\sqrt{3} - i), \quad \alpha_3(\sqrt{3} + i) = (-\sqrt{3} + i), \quad \alpha_4(\sqrt{3} + i) = (-\sqrt{3} - i),$$

so

$$(X - \sqrt{3} - i)(X - \sqrt{3} + i)(X + \sqrt{3} - i)(X + \sqrt{3} + i) = X^4 - 4X^2 + 16 \in \mathbb{Q}[X].$$

Hence this polynomial is irreducible. So we have $[\mathbb{Q}(\sqrt{3}+i) : \mathbb{Q}] = 4$ and $\mathbb{Q}(\sqrt{3}+i) = \mathbb{Q}(\sqrt{3}, i)$.

3.7. Normal extensions and splitting fields

Let $\overline{K}$ be an algebraic closure for the field K and let $E/K \leqslant \overline{K}/K$ be a finite extension. If $\varphi \in \mathrm{Mono}_K(E, \overline{K})$, then by Remark 3.32, $\varphi E = E$ if and only if $\varphi E \leqslant E$.

3.78. DEFINITION. E/K is *normal* if $\varphi E = E$ for every $\varphi \in \mathrm{Mono}_K(E, \overline{K})$.

3.79. REMARK. If E/K is a normal extension then whenever an irreducible polynomial $p(X) \in K[X]$ has a root in E, it splits in E since by Lemma 3.52 each pair of roots of $p(X)$ is conjugate over K and one can be mapped to the other by a monomorphism $\overline{K} \longrightarrow \overline{K}$ which must map E into itself.

3.80. THEOREM. *A finite extension E/K is normal if and only if it is a splitting field over K for some polynomial $f(X) \in K[X]$.*

PROOF. Suppose that E/K is normal. Then there is a sequence of extensions

$$K \leqslant K(u_1) \leqslant K(u_1, u_2) \leqslant \cdots \leqslant K(u_1, \ldots, u_n) = E$$

Construct a polynomial by taking

$$f(X) = \operatorname{minpoly}_{K,u_1}(X) \operatorname{minpoly}_{K,u_2}(X) \cdots \operatorname{minpoly}_{K,u_n}(X).$$

Then by Remark 3.79, $f(X)$ splits in E. Also, E is generated by some of the roots of $f(X)$. Hence E is a splitting field for $f(X)$ over K.

Now suppose that E is a splitting field for $g(X) \in K[X]$, so that $E = K(v_1, \ldots, v_k)$, where $v_1, \ldots, v_k$ are the distinct roots of $g(X)$ in E. Now any monomorphism $\theta \in \mathrm{Mono}_K(E, \overline{K})$ must map these roots to $\theta(v_1), \ldots, \theta(v_k)$ which are also roots of $g(X)$ and therefore lie in E (see Proposition 3.34). Since θ permutes the roots v_j, we have

$$\theta E = \theta K(v_1, \ldots, v_k) = K(\theta(v_1), \ldots, \theta(v_k)) = K(v_1, \ldots, v_k) = E. \qquad \square$$

3.81. COROLLARY. *Let E/L and L/K be finite extensions. If E/K is normal then E/L is normal.*

PROOF. If E is the splitting field of a polynomial $f(X) \in K[X]$ over K, then E is the splitting field of $f(X)$ over L. □

These result makes it easy to recognize a normal extension since it is sufficient to describe it as a splitting field for *some* polynomial over K. In Chapter 4 we will see that separable normal extensions play a central rôle in Galois Theory, indeed these are known as *Galois extensions*.

Exercises on Chapter 3

3-1. Prove Proposition 3.2.

3-2. Finding splitting subfields $E \leqslant \mathbb{C}$ over $\mathbb{Q}$ and determine $[E : \mathbb{Q}]$ for each of the following polynomials.

$p_1(X) = X^4 - X^2 + 1, \quad p_2(X) = X^6 - 2, \quad p_3(X) = X^4 + 2, \quad p_4(X) = X^4 + 5X^3 + 10X^2 + 10X + 5.$

[*Hint: for $p_4(X)$, consider $p_4(Y-1) \in \mathbb{Q}[Y]$.*]

3-3. Prove that $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)) \cong \mathrm{S}_3$, the symmetric group on 3 elements, as claimed in the solution of Example 3.38. [*Hint: work out the effect of each automorphism on the three roots of the polynomial $X^3 - 2$.*]

3-4. Let $\Bbbk$ be a field of characteristic $\mathrm{char}\,\Bbbk = p > 0$ and $\Bbbk(T)$ be the field of rational functions in T over $\Bbbk$. Show that the polynomial $g(X) = X^p - T \in \Bbbk(T)[X]$ is irreducible and has a multiple root in $\overline{\Bbbk(T)}$. How does $g(X)$ factor in $\overline{\Bbbk(T)}[X]$?

3-5. Find primitive elements for the extensions $\mathbb{Q}(\sqrt{5}, \sqrt{10})/\mathbb{Q}$, $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt{3}, i)/\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{3}, i)/\mathbb{Q}$, in each case finding it minimal polynomial over $\mathbb{Q}$. [*Hint: look for elements of high degree over $\mathbb{Q}$, or use the method of proof of Theorem 3.74.*]

3-6. Prove the following converse of Proposition 3.20:

Let L/K be a finite extension. If there are only finitely many subextensions $F/K \leqslant L/K$, then L/K is simple, i.e., *$L = K(w)$ for some $w \in L$.*

[*Hint: First deal with the case where $L = K(u, v)$, then use induction on n to prove the general case $L = K(u_1, \ldots, u_n)$.*]

3-7. Let K be a field. Show that every quadratic (*i.e.*, of degree 2) extension E/K is normal. Is such an extension always separable?

3-8. Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of odd degree greater than 1 and having only one real root $u \in \mathbb{R}$. Show that $\mathbb{Q}(u)/\mathbb{Q}$ is not a normal extension.

CHAPTER 4

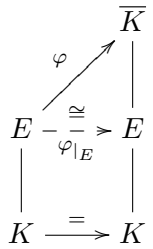
Galois extensions and the Galois Correspondence

In this Chapter we will study the structure of *Galois extensions* and their associated *Galois groups*, in particular we will explain how these are related through the *Galois Correspondence*. Throughout the chapter, let K be a field.

4.1. Galois extensions

4.1. Definition. A finite extension E/K is a (*finite*) *Galois extension* if it is both normal and separable.

From Section 3.5 we know that for such a Galois extension E/K, $[E : K] = (E : K)$ and also every monomorphism $\varphi \in \mathrm{Mono}_K(E, \overline{K})$ maps E into itself, hence restricts to an automorphism of E which will be denoted $\varphi_{|E}$.



Also, by the Monomorphism Extension Theorem 3.49, every automorphism $\alpha \in \mathrm{Aut}_K(E)$ extends to a monomorphism $E \longrightarrow \overline{K}$ fixing elements of K. So there is a bijection

$$\mathrm{Mono}_K(E, \overline{K}) \longleftrightarrow \mathrm{Aut}_K(E)$$

and we have

$$|\mathrm{Aut}_K(E)| = (E : K) = [E : K]. \tag{4.1}$$

4.2. Definition. For a finite Galois extension E/K, the group

$$\mathrm{Gal}(E/K) = \mathrm{Aut}_K(E)$$

is called the *Galois group of the extension* or the *Galois group of E over K*. The elements of $\mathrm{Gal}(E/K)$ are called (*Galois*) *automorphisms* of E/K.

Notice that Equation (4.1) implies

$$|\mathrm{Gal}(E/K)| = (E : K) = [E : K]. \tag{4.2}$$

We can also reformulate the notion of conjugacy introduced in Definition 3.51.

4.3. Definition. Let E/K a finite Galois extension and $u, v \in E$. Then v is *conjugate to u* if there is a $\varphi \in \mathrm{Gal}(E/K)$ for which $v = \varphi(u)$; we also say that v is a *conjugate of u*.

It is easy to see that for $u, v \in \overline{K}$, there is a finite Galois extension E/K in which v is a conjugate of u if and only v is a conjugate of u over K in the old sense. Here is a slightly different way to understand this. First notice that every element $\varphi \in \mathrm{Aut}_K(\overline{K}, \overline{K})$ restricts to a monomorphism $E \longrightarrow \overline{K}$ whose image is contained in E, hence gives rise to an automorphism $\varphi_E \colon E \longrightarrow E$. Similarly, if F/K is any finite normal extension with $E \leqslant F$, every automorphism $\theta \colon F \longrightarrow F$ restricts to an automorphism $\theta_E^F \colon E \longrightarrow E$. The proof of the next result is left as an exercise.

4.4. Proposition. *If E/K is a finite Galois extension, then the function*

$$\mathrm{Aut}_K(\overline{K}, \overline{K}) \longrightarrow \mathrm{Aut}_K(E, E); \quad \varphi \longmapsto \varphi_E$$

is a surjective group homomorphism. If $F/K \leqslant \overline{K}/K$ is any finite normal extension with $E \leqslant F$ then there is a surjective group homomorphism

$$\mathrm{Aut}_K(F, F) \longrightarrow \mathrm{Aut}_K(E, E); \quad \theta \longmapsto \theta_E^F.$$

Furthermore, for $\varphi \in \mathrm{Aut}_K(\overline{K}, \overline{K})$ we have

$$(\varphi_F)_E^F = \varphi_E.$$

4.2. Working with Galois groups

Let E/K be a finite Galois extension. Then we know that E is a splitting field for some polynomial over K since E/K is normal. We also know that E is a simple extension of K since E/K is separable. Hence E is a splitting field for the minimal polynomial of any primitive element for E/K; this minimal polynomial has degree $[E : K]$. It is often convenient to use these facts to interpret elements of the Galois group as permutations of the roots of some polynomial which splits over E.

4.5. Example. Describe the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ as a subgroup of the group of permutations of the roots of $(X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$.

Solution. We have

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]\,[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4,$$

and the following non-trivial elements of the Galois group together with the element identity $\alpha_1 = \mathrm{id}$:

$$\alpha_2 = \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ \sqrt{3} & \longmapsto & \sqrt{3} \\ -\sqrt{3} & \longmapsto & -\sqrt{3} \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} \sqrt{2} & \longmapsto & \sqrt{2} \\ -\sqrt{2} & \longmapsto & -\sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ -\sqrt{3} & \longmapsto & \sqrt{3} \end{pmatrix}, \quad \alpha_4 = \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ \sqrt{3} & \longmapsto & -\sqrt{3} \\ -\sqrt{3} & \longmapsto & \sqrt{3} \end{pmatrix}.$$

Writing the roots in the list $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ and numbering them from 1 to 4, these automorphisms correspond to the following permutations in S_4 expressed in cycle notation:

$$\alpha_2 \longleftrightarrow (1\ 2), \quad \alpha_3 \longleftrightarrow (3\ 4), \quad \alpha_4 \longleftrightarrow (1\ 2)(3\ 4). \qquad \square$$

4.6. Example. Using a primitive element u for the extension, describe the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ as a subgroup of the group of permutations of the roots of $\mathrm{minpoly}_{\mathbb{Q},u}(X) \in \mathbb{Q}[X]$.

SOLUTION. We have $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ and the conjugates of $u = \sqrt{2}+\sqrt{3}$ are $\pm\sqrt{2}\pm\sqrt{3}$. Listing these as

$$\sqrt{2}+\sqrt{3},\ \sqrt{2}-\sqrt{3},\ -\sqrt{2}+\sqrt{3},\ -\sqrt{2}-\sqrt{3},$$

and after numbering them accordingly, we find the correspondences

$$\alpha_2 \longleftrightarrow (1\ 3)(2\ 4), \quad \alpha_3 \longleftrightarrow (1\ 2)(3\ 4), \quad \alpha_4 \longleftrightarrow (1\ 4)(2\ 3). \qquad \square$$

Next we summarize the properties of Galois groups that can be deduced from what we have established so far. Recall that for an extension F/K and a polynomial $f(X) \in K[X]$, $\mathrm{Roots}(f,F)$ denotes the set of roots of $f(X)$ in F.

4.7. RECOLLECTION. Recall that an action of a group G on a set X is *transitive* if for every pair of elements $x, y \in X$, there is an element $g \in G$ such that $y = gx$ (so there is only one orbit); the action is *faithful* or *effective* if for every non-identity element $h \in G$, there is an element $z \in X$ such that $hz \neq z$.

4.8. THEOREM. *Let E/K be a finite Galois extension. Suppose that E is the splitting field of a separable irreducible polynomial $f(X) \in K[X]$ of degree n. Then the following are true.*

(i) $\mathrm{Gal}(E/K)$ *acts transitively and faithfully on* $\mathrm{Roots}(f,E)$.
(ii) $\mathrm{Gal}(E/K)$ *can be identified with a subgroup of the group of permutations of* $\mathrm{Roots}(f,E)$. *If we order the roots $u_1,\dots,u_n$ then* $\mathrm{Gal}(E/K)$ *can be identified with a subgroup of* S_n.
(iii) $|\mathrm{Gal}(E/K)|$ *divides $n!$ and is divisible by n.*

As we have seen in Examples 4.5 and 4.6, in practise it is often easier to use a not necessarily irreducible polynomial to determine and work with a Galois group.

4.9. EXAMPLE. The Galois extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ has degree $[\mathbb{Q}(\zeta_8):\mathbb{Q}] = 4$ and it has the following automorphisms apart from the identity:

$$\alpha\colon \zeta_8 \longmapsto \zeta_8^3, \quad \beta\colon \zeta_8 \longmapsto \zeta_8^5, \quad \gamma\colon \zeta_8 \longmapsto \zeta_8^7.$$

If we list the roots of the minimal polynomial

$$\mathrm{minpoly}_{\mathbb{Q},\zeta}(X) = \Phi_8(X) = X^4+1$$

in the order $\zeta_8, \zeta_8^3, \zeta_8^5, \zeta_8^7$, we find that these automorphisms correspond to the following permutations in S_4:

$$\alpha \longleftrightarrow (1\ 2)(3\ 4), \quad \beta \longleftrightarrow (1\ 3)(2\ 4), \quad \gamma \longleftrightarrow (1\ 4)(2\ 3).$$

So the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q})$ corresponds to

$$\{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \leqslant \mathrm{S}_4.$$

Noticing that

$$\zeta_8 = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i,$$

we easily find that $\sqrt{2}, i \in \mathbb{Q}(\zeta_8)$; hence $\mathbb{Q}(\sqrt{2},i) \leqslant \mathbb{Q}(\zeta_8)$. Since $[\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = 4$, we have $\mathbb{Q}(\sqrt{2},i) = \mathbb{Q}(\zeta_8)$. Notice that $\mathbb{Q}(\sqrt{2},i)$ is the splitting field of $f(X) = (X^2-2)(X^2+1)$ over

$\mathbb{Q}$. Now list the roots of $f(X)$ in the order $\sqrt{2}, -\sqrt{2}, i, -i$, and observe that

$$\alpha\colon \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ i & \longmapsto & -i \\ -i & \longmapsto & i \end{pmatrix} \longleftrightarrow (1\ 2)(3\ 4), \qquad \beta\colon \begin{pmatrix} \sqrt{2} & \longmapsto & -\sqrt{2} \\ -\sqrt{2} & \longmapsto & \sqrt{2} \\ i & \longmapsto & i \\ -i & \longmapsto & -i \end{pmatrix} \longleftrightarrow (1\ 2),$$

$$\gamma\colon \begin{pmatrix} \sqrt{2} & \longmapsto & \sqrt{2} \\ -\sqrt{2} & \longmapsto & -\sqrt{2} \\ i & \longmapsto & -i \\ -i & \longmapsto & i \end{pmatrix} \longleftrightarrow (3\ 4).$$

In this description, the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q})$ corresponds to the subgroup

$$\{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\} \leqslant \mathrm{S}_4.$$

While it can be hard to determine Galois groups in general, special arguments can sometimes be exploited.

4.10. Example. Suppose that $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$ is an irreducible cubic and that $f(X)$ has only one real root. Then $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{S}_3$.

Proof. Let $u_1 \in \mathbb{R}$ be the real root of $f(X)$ and let u_2, u_3 be the remaining complex roots. Then $\mathbb{Q}(f(X)) = \mathbb{Q}(u_1, u_2, u_3)$ and in fact $[\mathbb{Q}(f(X)) : \mathbb{Q}] = 6$ since $[\mathbb{Q}(f(X)) : \mathbb{Q}] \mid 6$ and $u_2 \notin \mathbb{Q}(u_1) \leqslant \mathbb{R}$. Hence $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q})$ is isomorphic to a subgroup of S_3 and so $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{S}_3$ since the orders agree. We also have $\mathbb{Q}(f(X)) \cap \mathbb{R} = \mathbb{Q}(u_1)$.

The Galois group $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q})$ contains an element of order 3 which corresponds to a 3-cycle when viewed as a permutation of the roots u_1, u_2, u_3; we can assume that this is $(1\ 2\ 3)$. It also contains an element of order 2 obtained by restricting complex conjugation to $\mathbb{Q}(f(X))$; this fixes u_1 and interchanges u_2, u_3, so it corresponds to the transposition $(2\ 3)$. □

4.11. Remark. Such examples occur when the cubic polynomial $f(X)$ has local maximum and minimum at real values c_+ and c_- with $f(c_+), f(c_-) > 0$ or $f(c_+), f(c_-) < 0$. This happens for example with $f(X) = X^3 - 3X + 3$ which has local extrema at ± 1 and $f(1) = 1$, $f(-1) = 5$.

Given a Galois extension E/K, we will next study subextensions $L/K \leqslant E/K$ and subgroups $\Gamma \leqslant \mathrm{Gal}(E/K)$, focusing on the relationship between objects of these types.

4.3. Subgroups of Galois groups and their fixed fields

Let E/K a Galois extension and suppose that $\Gamma \leqslant \mathrm{Gal}(E/K)$. Consider the subset of elements of E fixed by Γ,

$$E^\Gamma = \{u \in E : \forall \gamma \in \Gamma,\ \gamma(u) = u\}.$$

4.12. Lemma. *$E^\Gamma \leqslant E$ is a subfield of E containing K.*

Proof. For $u, v \in E^\Gamma$ and $\gamma \in \Gamma$,

$$\gamma(u + v) = \gamma(u) + \gamma(v) = u + v, \quad \gamma(uv) = \gamma(u)\gamma(v) = uv.$$

Also, if $u \neq 0$,

$$\gamma(u^{-1}) = \gamma(u)^{-1} = u^{-1}.$$

Finally, if $t \in K$ then $\gamma(t) = t$, so $K \leqslant E^\Gamma$. □

4.13. Definition. $E^\Gamma \leqslant E$ is the *fixed subfield of* Γ.

By Proposition 3.73, the extensions E/E^Γ and E^Γ/K are separable. E/E^Γ is also normal, so this is a Galois extension; we will identify its Galois group. Notice that

$$[E : E^\Gamma] = (E : E^\Gamma) = |\operatorname{Gal}(E/E^\Gamma)|.$$

Now each element of $\operatorname{Gal}(E/E^\Gamma)$ is also an element of $\operatorname{Gal}(E/K)$ and $\operatorname{Gal}(E/E^\Gamma) \leqslant \operatorname{Gal}(E/K)$. Notice that by definition $\Gamma \leqslant \operatorname{Gal}(E/E^\Gamma)$, so Lagrange's Theorem implies that $|\Gamma|$ divides $|\operatorname{Gal}(E/E^\Gamma)|$. In fact we have

4.14. Proposition. *For* $\Gamma \leqslant \operatorname{Gal}(E/K)$*, we have* $\operatorname{Gal}(E/E^\Gamma) = \Gamma$ *and the equations*

$$[E : E^\Gamma] = |\operatorname{Gal}(E/E^\Gamma)| = |\Gamma|, \quad [E^\Gamma : K] = \frac{|\operatorname{Gal}(E/K)|}{|\Gamma|}.$$

Proof. We know that E/E^Γ is separable, so by the Primitive Element Theorem 3.74 it is simple, say $E = E^\Gamma(u)$. Now let the distinct elements of Γ be $\gamma_1 = \mathrm{id}, \gamma_2, \ldots, \gamma_h$, where $h = |\Gamma|$. Consider the polynomial of degree h

$$f(X) = (X - u)(X - \gamma_2(u)) \cdots (X - \gamma_h(u)) \in E[X].$$

Notice that $f(X)$ is unchanged by applying any γ_k to its coefficients since the roots $\gamma_j(u)$ are permuted by γ_k. Hence, $f(X) \in E^\Gamma[X]$. This shows that

$$[E : E^\Gamma] = [E^\Gamma(u) : E^\Gamma] \leqslant h = |\Gamma|.$$

Since $\Gamma \leqslant \operatorname{Gal}(E/E^\Gamma)$, we also have

$$h = |\Gamma| \leqslant |\operatorname{Gal}(E/E^\Gamma)| = [E : E^\Gamma].$$

Combining these two inequalities we obtain

$$[E : E^\Gamma] = |\operatorname{Gal}(E/E^\Gamma)| = |\Gamma| = h$$

and therefore $\Gamma = \operatorname{Gal}(E/E^\Gamma)$. □

4.4. Subfields of Galois extensions and relative Galois groups

Let E/K a Galois extension and suppose that $L/K \leqslant E/K$ (*i.e.*, $K \leqslant L \leqslant E$). Then E/L is also a Galois extension whose Galois group $\operatorname{Gal}(E/L)$ is sometimes called the *relative Galois group of the pair of extensions* E/K *and* L/K. The following is immediate.

4.15. Lemma. *The relative Galois group of the pair of extensions* $L/K \leqslant E/K$ *is a subgroup of* $\operatorname{Gal}(E/K)$, i.e., $\operatorname{Gal}(E/L) \leqslant \operatorname{Gal}(E/K)$*, and its order is* $|\operatorname{Gal}(E/L)| = [E : L]$.

4.16. Proposition. *Let* $L/K \leqslant E/K$*. Then* $L = E^{\operatorname{Gal}(E/L)}$.

Proof. Clearly $L \leqslant E^{\operatorname{Gal}(E/L)}$. Suppose that $u \in E - L$. By Theorem 4.8(i), there is an automorphism $\theta \in \operatorname{Gal}(E/L)$ such that $\theta(u) \neq u$, hence $u \notin E^{\operatorname{Gal}(E/L)}$. This shows that $E^{\operatorname{Gal}(E/L)} \leqslant L$ and therefore $E^{\operatorname{Gal}(E/L)} = L$. □

We need to understand when $\operatorname{Gal}(E/L) \leqslant \operatorname{Gal}(E/K)$ is actually a normal subgroup. The next result explains the connection between the two uses of the word *normal* which both ultimately derive from their use in Galois theory.

4.17. Proposition. *Let E/K be a finite Galois extension and $L/K \leqslant E/K$.*

(i) *The relative Galois group* $\mathrm{Gal}(E/L)$ *of the pair of extensions $L/K \leqslant E/K$ is a normal subgroup of* $\mathrm{Gal}(E/K)$ *if and only if L/K is a normal extension.*

(ii) *If L/K is normal and hence a Galois extension, then there is a group isomorphism*

$$\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L) \xrightarrow{\cong} \mathrm{Gal}(L/K); \quad \alpha\,\mathrm{Gal}(E/L) \longmapsto \alpha_{|_L}.$$

Proof. (i) Suppose that $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/K)$, *i.e.*, for all $\alpha \in \mathrm{Gal}(E/L)$ and $\beta \in \mathrm{Gal}(E/K)$, we have $\beta\alpha\beta^{-1} \in \mathrm{Gal}(E/L)$. Now if $u \in L$, then for any $\gamma \in \mathrm{Gal}(E/K)$ and $\alpha \in \mathrm{Gal}(E/L)$, $\gamma(u) \in E$ satisfies

$$\alpha\gamma(u) = \gamma(\gamma^{-1}\alpha\gamma(u)) = \gamma(u),$$

since $\gamma^{-1}\alpha\gamma \in \mathrm{Gal}(E/L)$; hence $\gamma(u) \in E^{\mathrm{Gal}(E/L)} = L$. By the Monomorphism Extension Theorem 3.49, every monomorphism $L \longrightarrow \overline{K}$ fixing K extends to a monomorphism $E \longrightarrow \overline{K}$ which must have image E, so the above argument shows that L/K is normal.

Conversely, if L/K is normal, then for every $\varphi \in \mathrm{Gal}(E/K)$ and $v \in L$, $\varphi(v) \in L$, so for every $\theta \in \mathrm{Gal}(E/L)$, $\theta(\varphi(v)) = \varphi(v)$ and therefore

$$\varphi^{-1}\theta\varphi(v) = v.$$

This shows that $\varphi^{-1}\theta\varphi \in \mathrm{Gal}(E/L)$. Hence for every $\varphi \in \mathrm{Gal}(E/K)$,

$$\varphi\,\mathrm{Gal}(E/L)\varphi^{-1} = \mathrm{Gal}(E/L),$$

which shows that $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/K)$.

(ii) If $\alpha \in \mathrm{Gal}(E/K)$, then $\alpha L = L$ since L/K is normal. Hence we can restrict α to an automorphism of L,

$$\alpha_{|_L} : L \longrightarrow L; \quad \alpha_{|_L}(u) = \alpha(u).$$

Then $\alpha_{|_L}$ is the identity function on L if and only if $\alpha \in \mathrm{Gal}(E/L)$. It is easy to see that the function

$$\mathrm{Gal}(E/K) \longrightarrow \mathrm{Gal}(L/K); \quad \alpha \longmapsto \alpha_{|_L}$$

is a group homomorphism whose kernel is $\mathrm{Gal}(E/L)$. Thus we obtain an injective homomorphism

$$\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L) \longrightarrow \mathrm{Gal}(L/K)$$

for which

$$|\,\mathrm{Gal}(E/K)/\mathrm{Gal}(E/L)| = \frac{[E:K]}{[E:L]} = [L:K] = |\,\mathrm{Gal}(L/K)|.$$

Hence this homomorphism is an isomorphism. □

4.5. The Galois Correspondence and the Main Theorem of Galois Theory

We are now almost ready to state our central result which describes the *Galois Correspondence* associated with a finite Galois extension. We will use the following notation. For a finite Galois extension E/K, let

$$\mathcal{S}(E/K) = \text{the set of all subgroups of } \mathrm{Gal}(E/K);$$
$$\mathcal{F}(E/K) = \text{the set of all subextensions } L/K \text{ of } E/K.$$

Each of these sets is ordered by inclusion. Since every subgroup of a finite group is a finite subset of a finite set, $\mathcal{S}(E/K)$ is also a finite set. Define two functions by

$$\Phi_{E/K}\colon \mathcal{F}(E/K) \longrightarrow \mathcal{S}(E/K); \quad \Phi_{E/K}(L) = \mathrm{Gal}(E/L),$$
$$\Theta_{E/K}\colon \mathcal{S}(E/K) \longrightarrow \mathcal{F}(E/K); \quad \Theta_{E/K}(\Gamma) = E^{\Gamma}.$$

4.18. Theorem (Main Theorem of Galois Theory). *Let E/K be a finite Galois extension. Then the functions $\Phi_{E/K}$ and $\Theta_{E/K}$ are mutually inverse bijections which are order-reversing.*

$$\mathcal{F}(E/K) \underset{\Theta_{E/K}}{\overset{\Phi_{E/K}}{\rightleftarrows}} \mathcal{S}(E/K)$$

Under this correspondence, normal subextensions of E/K correspond to normal subgroups of $\mathrm{Gal}(E/K)$ and vice versa.

Proof. We know from Proposition 4.16 that for an extension L/K in $\mathcal{F}(E/K)$,

$$\Theta_{E/K}(\Phi_{E/K}(L)) = \Theta_{E/K}(\mathrm{Gal}(E/L)) = E^{\mathrm{Gal}(E/L)} = L.$$

Also, by Proposition 4.14 for $H \in \mathcal{S}(E/K)$ we have

$$\Phi_{E/K}(\Theta_{E/K}(\Gamma)) = \Phi_{E/K}(E^{\Gamma}) = \mathrm{Gal}(E/E^{\Gamma}) = \Gamma.$$

This shows that $\Phi_{E/K}$ and $\Theta_{E/K}$ are mutually inverse and so are inverse bijections.

Let $L_1/K,\ L_2/K \in \mathcal{F}(E/K)$ satisfy $L_1/K \leqslant L_2/K$. Then $\mathrm{Gal}(E/L_2) \leqslant \mathrm{Gal}(E/L_1)$ since $L_1 \subseteq L_2$ and so if $\alpha \in \mathrm{Gal}(E/L_2)$ then α fixes every element of L_1. Hence $\Phi_{E/K}(L_2) \leqslant \Phi_{E/K}(L_1)$ and so $\Phi_{E/K}$ reverses order.

Similarly, if $\Gamma_1, \Gamma_2 \in \mathcal{S}(E/K)$ and $\Gamma_1 \leqslant \Gamma_2$, then $E^{\Gamma_2} \leqslant E^{\Gamma_1}$ since if $w \in E^{\Gamma_2}$ then it is fixed by every element of Γ_1 (as Γ_1 is a subset of Γ_2). Hence $\Theta_{E/K}$ reverses order. □

There is an immediate consequence of the Main Theorem 4.18 which is closely related to Proposition 3.20.

4.19. Corollary. *Let E/K be a finite Galois extension. Then there are only finitely many subextensions $L/K \leqslant E/K$.*

Proof. Since the set $\mathcal{S}(E/K)$ is finite, so is $\mathcal{F}(E/K)$. □

When dealing with a finite Galois extension E/K, we indicate the subextensions in a diagram with a line going upwards indicating an inclusion. We can also do this with the subgroups of the Galois group $\mathrm{Gal}(E/K)$ with labels indicating the index of the subgroups. In effect, the Galois Correspondence inverts these diagrams.

4.20. Example. Figure 4.1 shows the Galois Correspondence for the extension of Example 3.30.

As noted at the end of Example 3.38, the Galois group here is $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}) \cong \mathrm{S}_3$. It is useful to make this isomorphism explicit. First take the 3 roots of the polynomial $X^3 - 2$ for which E is the splitting field over $\mathbb{Q}$; these are $\sqrt[3]{2}, \sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\,\zeta_3^2$ which we number in the order they are listed. Then the monomorphisms $\mathrm{id}, \alpha_0, \alpha_1, \alpha_1', \alpha_2, \alpha_2'$ extend to automorphisms of E, each of which permutes these 3 roots in the following ways given by cycle notation:

$$\alpha_0 = (2\ 3), \quad \alpha_1 = (1\ 2\ 3), \quad \alpha_1' = (1\ 2), \quad \alpha_2 = (1\ 3\ 2), \quad \alpha_2' = (1\ 3).$$

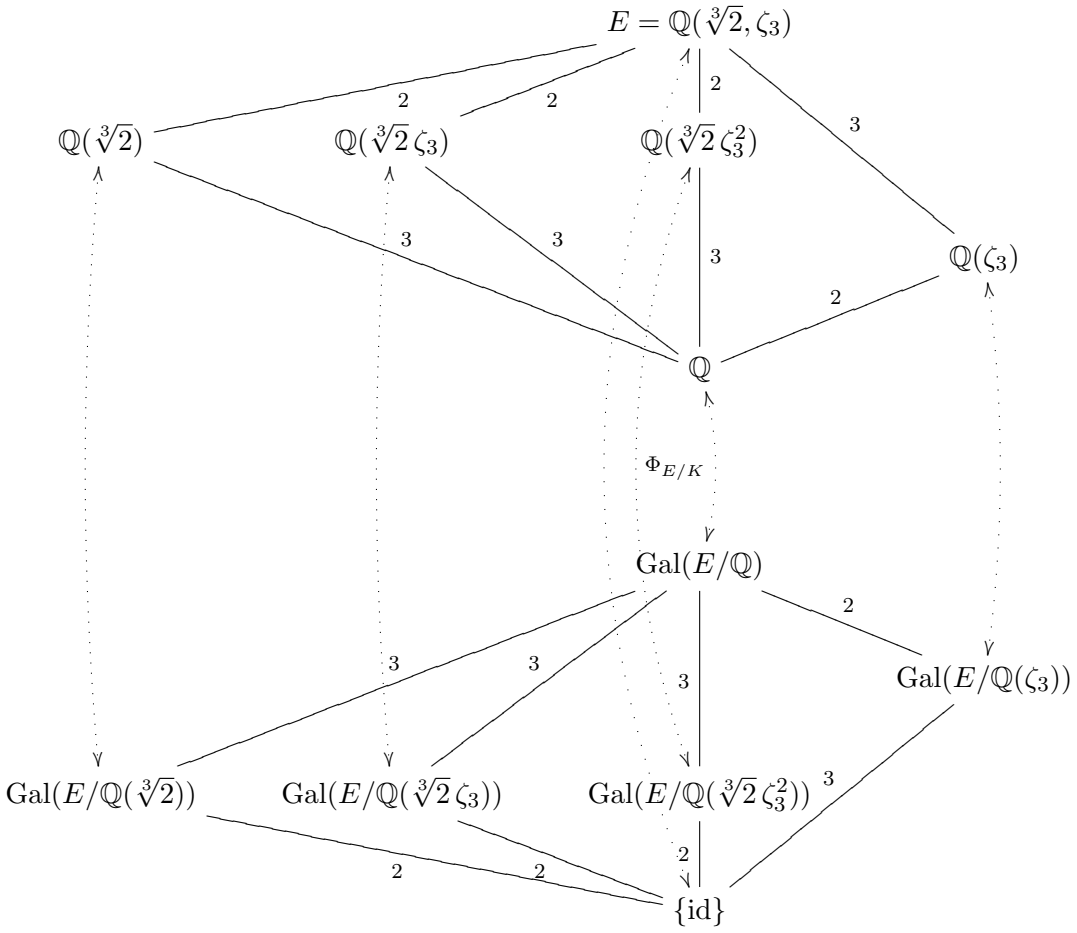


FIGURE 4.1. The Galois Correspondence for $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$

We find that

$$\mathrm{Gal}(E/\mathbb{Q}(\zeta_3)) = \{\mathrm{id}, \alpha_1, \alpha_2\} \cong \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}, \qquad \mathrm{Gal}(E/\mathbb{Q}(\sqrt[3]{2})) = \{\mathrm{id}, \alpha_0\} \cong \{\mathrm{id}, (2\ 3)\},$$
$$\mathrm{Gal}(E/\mathbb{Q}(\sqrt[3]{2}\,\zeta_3)) = \{\mathrm{id}, \alpha_2'\} \cong \{\mathrm{id}, (1\ 3)\}, \qquad \mathrm{Gal}(E/\mathbb{Q}(\sqrt[3]{2}\,\zeta_3^2)) = \{\mathrm{id}, \alpha_1'\} \cong \{\mathrm{id}, (1\ 2)\}.$$

Notice that $\{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\} \lhd \mathrm{S}_3$ and so $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is a normal extension. Of course $\mathbb{Q}(\zeta_3)$ is the splitting field of $X^3 - 1$ over $\mathbb{Q}$.

4.6. Galois extensions inside the complex numbers and complex conjugation

When working with Galois extensions contained in the complex numbers it is often useful to make use of complex conjugation as an element of a Galois group. Let $E/\mathbb{Q}$ be a finite Galois extension with $E/\mathbb{Q} \leqslant \mathbb{C}/\mathbb{Q}$. Setting $E_{\mathbb{R}} = \mathbb{R} \cap E$, we have $\mathbb{Q} \leqslant E_{\mathbb{R}} \leqslant E$.

4.21. PROPOSITION. *Complex conjugation* $\overline{(\ )}\colon \mathbb{C} \longrightarrow \mathbb{C}$ *restricts to an automorphism of* E *over* $\mathbb{Q}$, $\overline{(\ )}_{E/\mathbb{Q}}\colon E \longrightarrow E$. *Furthermore,*

(i) $\overline{(\ )}_{E/\mathbb{Q}}$ *agrees with the identity function if and only if* $E_{\mathbb{R}} = E$.

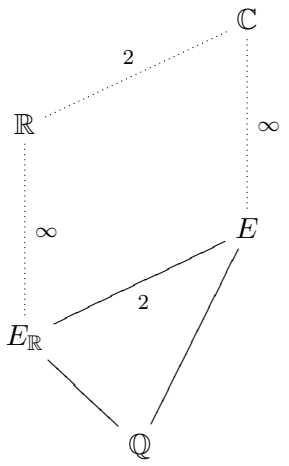
(ii) *If* $E_{\mathbb{R}} \neq E$, *then*

$$\left\langle \overline{(\ )}_{E/\mathbb{Q}} \right\rangle = \{\mathrm{id}, \overline{(\ )}_{E/\mathbb{Q}}\} \cong \mathbb{Z}/2,$$

hence, $E_{\mathbb{R}} = E^{\left\langle \overline{(\ )}_{E/\mathbb{Q}} \right\rangle}$ *and* $[E : E_{\mathbb{R}}] = 2$.

PROOF. Let $u \in E$. As $E/\mathbb{Q}$ is normal, $\mathrm{minpoly}_{\mathbb{Q},u}(X) \in \mathbb{Q}[X]$ splits over E, so all of its complex roots lie in E. But $\overline{(\ )}$ permutes the roots of this minimal polynomial. Therefore $\overline{(\ )}$ maps E into itself.
(i) For $z \in \mathbb{C}$, $\overline{z} = z$ if and only if $z \in \mathbb{R}$.
(ii) Here $|\langle \overline{(\ )}_{E/\mathbb{Q}} \rangle| = 2$, and

$$E^{\langle \overline{(\ )}_{E/\mathbb{Q}} \rangle} = \{u \in E : \overline{u} = u\} = E_{\mathbb{R}}.$$



□

We will usually write $\overline{(\ )}$ rather than $\overline{(\ )}_{E/\mathbb{Q}}$ when no confusion seems likely to result.

4.22. EXAMPLE. Consider the cyclotomic extension $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ where

$$\zeta_8 = e^{\pi i/4} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} i.$$

From Example 4.9 we know that

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{2}, i), \quad [\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4,$$

and we easily see that

$$\mathbb{Q}(\zeta_8)_{\mathbb{R}} = \mathbb{Q}(\sqrt{2}).$$

4.7. Galois groups of even and odd permutations

We have seen that for a monic separable polynomial $f(X) \in K[X]$ of degree n, the Galois group of its splitting field E over K can naturally be thought of as a subgroup of the symmetric group S_n, where we view the latter as permuting the roots of $f(X)$. It is reasonable to ask when $\mathrm{Gal}(E/K) \leqslant \mathrm{A}_n$ rather than just $\mathrm{Gal}(E/K) \leqslant \mathrm{S}_n$.

We first recall an interpretation of the *sign* of a permutation $\sigma \in \mathrm{S}_n$, $\operatorname{sgn} \sigma = \pm 1$. For each pair i, j with $1 \leqslant i < j \leqslant n$, exactly one of the inequalities $\sigma(i) < \sigma(j)$ or $\sigma(j) < \sigma(i)$ must hold and the ratio $(\sigma(j) - \sigma(i))/(j - i)$ is either positive or negative. It is easily verified that the right-hand side of the following equation must have value ± 1 and so

$$\operatorname{sgn} \sigma = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}. \tag{4.3}$$

Note that this is sometimes used as the definition of $\operatorname{sgn} \sigma$.

Suppose that $f(X)$ factorizes over E as

$$f(X) = (X - u_1)\cdots(X - u_n) = \prod_{i=1}^{n}(X - u_i).$$

Here $u_1, \ldots, u_n \in E$ are the roots of $f(X)$; as we have assumed that $f(X)$ is separable, the u_i are distinct.

4.23. Definition. The *discriminant* of $f(X)$ is

$$\operatorname{Discr}(f(X)) = \prod_{1\leqslant i<j\leqslant n} (u_j - u_i)^2 \in E.$$

Notice that $\operatorname{Discr}(f(X)) \neq 0$ since $u_i \neq u_j$ if $i \neq j$.

4.24. Remark. There is an explicit formula for computing $\operatorname{Discr}(f(X))$ is terms of its coefficients. For polynomials

$$p(X) = a_0 + a_1X + \cdots + a_mX^m, \quad q(X) = b_0 + b_1X + \cdots + b_nX^n,$$

their *resultant* is the $(m+n)\times(m+n)$ determinant (with n rows of a_i's and m rows of b_i's)

$$\operatorname{Res}(p(X), q(X)) = \begin{vmatrix} a_0 & a_1 & \ldots\ldots & a_m & 0 & \ldots\ldots\ldots\ldots\ldots\ldots & 0 \\ 0 & a_0 & a_1 & \ldots\ldots & a_m & 0 & \ldots\ldots\ldots\ldots\ldots\ldots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ldots\ldots\ldots\ldots\ldots\ldots & 0 & a_0 & a_1 & \ldots\ldots & a_m \\ b_0 & b_1 & \ldots\ldots & b_n & 0 & \ldots\ldots\ldots\ldots\ldots\ldots & 0 \\ 0 & b_0 & b_1 & \ldots\ldots & b_n & 0 & \ldots\ldots\ldots\ldots\ldots\ldots & 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ 0 & \ldots\ldots\ldots\ldots\ldots\ldots & 0 & b_0 & b_1 & \ldots\ldots & b_n \end{vmatrix}. \tag{4.4}$$

In particular, if $f(X)$ is monic with $\deg f(X) = n$,

$$\operatorname{Discr}(f(X)) = (-1)^{n(n-1)/2}\operatorname{Res}(f(X), f'(X)). \tag{4.5}$$

So for example,

$$\begin{aligned}\operatorname{Discr}(X^3 + pX + q) &= (-1)^3\operatorname{Res}(X^3 + pX + q, 3X^2 + p) \\ &= (-1)\begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix} = -4p^3 - 27q^2.\end{aligned}$$

Here are some low degree examples of discriminants obtained with the aid of Maple.

$n = 2$: $$\operatorname{Discr}(a_0 + a_1X + X^2) = -4a_0 + a_1^2.$$

$n = 3$: $$\operatorname{Discr}(a_0 + a_1X + a_2X^2 + X^3) = -27a_0^2 + 18a_0a_1a_2 + a_1^2a_2^2 - 4a_2^3a_0 - 4a_1^3.$$

$n = 4$: $$\begin{aligned}\operatorname{Discr}(a_0 + a_1X + a_2X^2 + a_3X^3 + X^4) &= 18a_3a_1^3a_2 - 6a_3^2a_1^2a_0 - 192a_3a_1a_0^2 - 27a_1^4 \\ &+ 144a_2a_3^2a_0^2 + 144a_0a_1^2a_2 + 256a_0^3 - 4a_3^3a_1^3 - 128a_2^2a_0^2 + 16a_2^4a_0 - 4a_2^3a_1^2 \\ &+ 18a_3^3a_1a_2a_0 - 80a_3a_1a_2^2a_0 - 27a_3^4a_0^2 + a_2^2a_3^2a_1^2 - 4a_2^3a_3^2a_0.\end{aligned}$$

$$
\begin{aligned}
n=5:\quad \operatorname{Discr}(a_0+a_1X+a_2X^2+a_3X^3+a_4X^4+X^5) &= 2250a_4a_3^2a_0^3 - 36a_0a_4^3a_1^3 - 128a_3^2a_1^4 \\
&+ 2000a_0^2a_3a_1^2 - 900a_1a_3^3a_0^2 - 2500a_0^3a_4a_1 - 50a_0^2a_4^2a_1^2 - 900a_4a_2^3a_0^2 - 27a_4^4a_1^4 - 3750a_3a_2a_0^3 \\
&+ 356{a_3}^2{a_2}^2a_4a_1a_0 + 560a_3a_2^2a_4^2a_0^2 - 2050a_3a_2a_0^2a_4a_1 - 80a_3^2a_2a_4{a_1}^3 + 825a_3^2a_2^2a_0^2 \\
&+ 16a_3^3a_2^3a_0 + 2000a_2a_4^2a_0^3 - 6a_2^2a_4^2a_1^3 - 128a_2^2a_4^4a_0^2 + 16a_2^4a_4^3a_0 - 4a_2^3a_4^3a_1^2 - 630{a_3}^3a_2a_4{a_0}^2 \\
&+ 108a_3^5a_0^2 + 108a_2^5a_0 - 746a_3a_2a_0a_4{a_1}^2{a_1}^2 - 27a_2^4a_1^2 + 256a_4^5a_0^3 - 4a_3^3a_2^2a_1^2 + 144a_3a_2^2a_1^3 \\
&+ 144a_4^2a_1^4a_3 + 3125a_0^4 + 256a_1^5 - 72a_3^4a_2a_1a_0 + 18a_3a_2a_3^3a_4^3a_1^3 + 560a_3^2a_2a_0a_1^2 + 16a_3^4a_1^3 \\
&+ 18a_3{a_2}^3a_4a_1{}^2 - 72a_3{a_2}^4a_4a_0 + 144{a_3}^2a_2{a_4}^3{a_0}^2 - 192{a_4}^4a_1a_3a_0{}^2 - 630a_3{a_2}^3a_1a_0 \\
&+ 24{a_2}^3{a_4}^2a_1a_0 + {a_3}^2{a_2}^2{a_4}^2{a_1}^2 - 6{a_4}^3{a_1}^2{a_3}^2a_0 - 80a_3{a_2}^2{a_4}^3a_1a_0 - 4{a_3}^2{a_2}^3{a_4}^2a_0 \\
&+ 2250a_1a_2^2a_0^2 - 1600a_3a_4^3a_0^3 - 192a_4a_1^4a_2 - 1600a_0a_1^3a_2 - 4a_3^3a_1^3a_4^2 - 27a_3^4a_4^2a_0^2 \\
&+ 1020{a_4}^2{a_3}^2{a_0}^2a_1 + 18{a_3}^3a_2{a_4}^2a_0a_1 + 160a_2{a_4}^3{a_0}^2a_1 + 144a_2{a_4}^4a_0{a_1}^2 \\
&+ 24a_4{a_1}^2{a_3}^3a_0 + 1020a_0a_4{a_2}^2{a_1}^2 + 160a_0a_4{a_1}^3a_3.
\end{aligned}
$$

So for example,

$$\operatorname{Discr}(X^5+a_4X^4+a_0) = a_0^3(3125a_0+256a_4^5), \quad \operatorname{Discr}(X^5+a_1X+a_0) = 256a_1^5+3125a_0^4.$$

4.25. Proposition. *For every* $\sigma \in \operatorname{Gal}(E/K)$,

$$\sigma(\operatorname{Discr}(f(X))) = \operatorname{Discr}(f(X)).$$

Hence $\operatorname{Discr}(f(X)) \in E^{\operatorname{Gal}(E/K)} = K$.

Proof. For $\sigma \in \operatorname{Gal}(E/K) \leqslant \mathrm{S}_n$, we have

$$\sigma(\operatorname{Discr}(f(X))) = \prod_{1\leqslant i<j\leqslant n} (u_{\sigma(j)} - u_{\sigma(i)})^2 = \left(\prod_{1\leqslant i<j\leqslant n} (u_{\sigma(j)} - u_{\sigma(i)}) \right)^2.$$

Now for each pair i, j with $i < j$,

$$\sigma(u_j - u_i) = u_{\sigma(j)} - u_{\sigma(i)},$$

and by Equation (4.3)

$$\prod_{1\leqslant i<j\leqslant n} (u_{\sigma(j)} - u_{\sigma(i)}) = \operatorname{sgn}\sigma \prod_{1\leqslant i<j\leqslant n} (u_j - u_i) = (\pm 1) \prod_{1\leqslant i<j\leqslant n} (u_j - u_i). \tag{4.6}$$

Hence $\sigma(\operatorname{Discr}(f(X))) = \operatorname{Discr}(f(X))$. Since $E^{\operatorname{Gal}(E/K)} = K$, we have $\operatorname{Discr}(f(X)) \in K$. □

Now let

$$\delta(f(X)) = \prod_{1\leqslant i<j\leqslant n} (u_j - u_i) \in E.$$

Then $\delta(f(X))^2 = \operatorname{Discr}(f(X))$, so the square roots of $\operatorname{Discr}(f(X))$ are $\pm\delta(f(X))$. Now consider the effect of $\sigma \in \operatorname{Gal}(E/K)$ on $\delta(f(X)) \in E$. By Equation (4.6),

$$\sigma(\delta(f(X))) = \operatorname{sgn}\sigma\, \delta(f(X)) = \pm\delta(f(X)).$$

If $\delta(f(X)) \in K$, this means that $\operatorname{sgn}\sigma = 1$. On the other hand, if $\delta(f(X)) \notin K$ then

$$K(\delta(f(X))) = E^{\operatorname{Gal}(E/K)\cap \mathrm{A}_n}.$$

Of course $|\operatorname{Gal}(E/K)/\operatorname{Gal}(E/K)\cap \mathrm{A}_n| = 2$.

4.26. Proposition. *The Galois group* $\mathrm{Gal}(E/K) \leqslant \mathrm{S}_n$ *is contained in* A_n *if and only if* $\mathrm{Discr}(f(X))$ *is a square in* K.

4.27. Example. For the polynomials of Examples 6.40 and 6.42 we obtain

$$\begin{aligned}
\mathrm{Discr}(X^5 - 35X^4 + 7) &= -4611833296875 = -3^3 \cdot 5^6 \cdot 7^4 \cdot 29 \cdot 157, \\
\delta(X^5 - 35X^4 + 7) &= \pm 5^3 \cdot 3 \cdot 7^2 \cdot \sqrt{3 \cdot 29 \cdot 157}\, i = \pm 18375\sqrt{13659}\, i \notin \mathbb{Q}; \\
\mathrm{Discr}(X^5 + 20X + 16) &= 1024000000 = 2^{16} \cdot 5^6, \\
\delta(X^5 + 20X + 16) &= \pm 2^8 5^3 \in \mathbb{Q}.
\end{aligned}$$

4.8. Kaplansky's Theorem

In this section we give a detailed account of the Galois theory of irreducible rational polynomials $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$. The following result describes the Galois groups that occur and the proof introduces some useful computational techniques.

4.28. Theorem (Kaplansky's Theorem). *Let* $f(X) = X^4 + aX^2 + b \in \mathbb{Q}[X]$ *be irreducible.*

(i) *If* b *is a square in* $\mathbb{Q}$ *then* $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$.
(ii) *If* $b(a^2 - 4b)$ *is a square in* $\mathbb{Q}$ *then* $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathbb{Z}/4$.
(iii) *If neither* b *nor* $b(a^2 - 4b)$ *is a square in* $\mathbb{Q}$ *then* $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{D}_8$.

Proof. Let $g(X) = X^2 + aX + b \in \mathbb{Q}[X]$. Notice that $g(X)$ must be irreducible since otherwise $f(X)$ would factorize, hence $(a^2 - 4b)$ is not a square in $\mathbb{Q}$. Setting $d = (a^2 - 4b) \in \mathbb{Q}$ and taking δ to be a square root of d (so $\delta \notin \mathbb{Q}$), we find that the roots of $g(X)$ are $(-a \pm \delta)/2 \notin \mathbb{Q}$. Then the roots of $f(X)$ are $\pm u, \pm v$, where

$$u^2 = \frac{(-a + \delta)}{2}, \quad v^2 = \frac{(-a - \delta)}{2},$$

so the splitting field of $f(X)$ over $\mathbb{Q}$ is $E = \mathbb{Q}(u, v)$ which contains the quadratic extension $\mathbb{Q}(\delta)/\mathbb{Q}$. Since $\deg f(X) = 4$, we also have $4 \mid [E : \mathbb{Q}]$. In fact, since E is obtained by at most 3 successive quadratic extensions we also have $[E : \mathbb{Q}] \mid 8$.
(i) We have

$$(uv)^2 = u^2 v^2 = \frac{a^2 - d}{4} = \frac{4b}{4} = b,$$

hence uv is a square root of b which is in $\mathbb{Q}$. Setting $c = uv \in \mathbb{Q}$, we find that $v = c/u \in \mathbb{Q}(u)$. This shows that $E = \mathbb{Q}(u)$ and we have the following Galois tower.

$$\begin{array}{c} E = \mathbb{Q}(u) \\ \Big| \, 2 \\ \mathbb{Q}(\delta) \\ \Big| \, 2 \\ \mathbb{Q} \end{array}$$

In particular $[E : \mathbb{Q}] = 4 = |\mathrm{Gal}(E/\mathbb{Q})|$. Notice that for the Galois extension $\mathbb{Q}(\delta)/\mathbb{Q}$ there must be a normal subgroup $N \lhd \mathrm{Gal}(E/\mathbb{Q})$ with

$$\mathbb{Q}(\delta) = E^N, \quad \mathrm{Gal}(\mathbb{Q}(\delta)/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q})/N.$$

Hence there is an element $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ for which $\sigma(\delta) = -\delta$. This element must also have the effects $\sigma(u) = \pm v$ and $\sigma(v) = \pm u$. Given u we might as well choose v so that $\sigma(u) = v$. There is also an element $\tau \in N$ for which $\tau(u) = -u$ and we also have $\tau(v) = -v$. Notice that if $\sigma(v) = -u$ then easy calculation shows that

$$\tau\sigma(v) = \sigma\tau(v) = u, \quad \tau\sigma(\delta) = \sigma\tau(\delta) = -\delta,$$

hence we might as assume that $\sigma(v) = u$ since if necessary we can replace our original choice by $\tau\sigma$.

We now have

$$\sigma(u) = \frac{c}{u}, \quad \tau(u) = -u, \quad \tau\sigma(u) = \sigma\tau(u) = -\frac{c}{u}.$$

These satisfy

$$\sigma^2 = \tau^2 = (\sigma\tau)^2 = \mathrm{id} = \text{the identity}, \quad \sigma\tau = \tau\sigma.$$

This shows that

$$\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\} \cong \mathbb{Z}/2 \times \mathbb{Z}/2 = \text{the Klein 4-group}.$$

(ii) If bd is a square in $\mathbb{Q}$, then

$$(uv\delta)^2 = u^2v^2d = bd,$$

which is a square in $\mathbb{Q}$, so we can write $uv\delta = c \in \mathbb{Q}$ or equivalently $v = c/(u\delta) \in \mathbb{Q}(u)$ since $\mathbb{Q}(\delta) \leqslant \mathbb{Q}(u)$. This shows that $E = \mathbb{Q}(u, v) = \mathbb{Q}(u)$ and again we have a Galois tower

$$\begin{array}{c} E = \mathbb{Q}(u) \\ \Big| \, 2 \\ \mathbb{Q}(\delta) \\ \Big| \, 2 \\ \mathbb{Q} \end{array}$$

with $[E : \mathbb{Q}] = 4 = |\,\mathrm{Gal}(E/\mathbb{Q})|$.

Since $\mathbb{Q}(\delta)/\mathbb{Q}$ is Galois there is an element $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ with $\sigma(\delta) = -\delta$ and this has the effect $\sigma(u) = \pm v$; given u we might as well choose v so that $\sigma(u) = v$. Notice that

$$\sigma(v) = \frac{c}{\sigma(u\delta)} = -\frac{c}{v\delta} = -u,$$

so $\sigma^2(u) = -u$. This shows that

$$\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2\sigma^3\} \cong \mathbb{Z}/4 = \text{a cyclic group of order 4}.$$

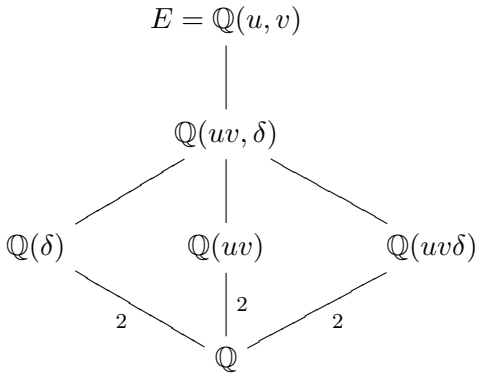
(iii) Suppose that d, b and bd are not squares in $\mathbb{Q}$. By an easy calculation we find that $(uv)^2 = b$, so $uv \in E$ is a square root of b in E. Suppose that $uv \in \mathbb{Q}(\delta)$; then $uv = p + q\delta$ for some $p, q \in \mathbb{Q}$. By squaring we obtain

$$b = (p^2 + q^2d) + 2pq\delta,$$

and so $pq = 0$. We cannot have $q = 0$ since this would imply that b was a square in $\mathbb{Q}$; if $p = 0$ then $b = q^2d$ and so $bd = (qd)^2$, implying that bd was a square in $\mathbb{Q}$. Thus we have $\mathbb{Q}(uv) \cap \mathbb{Q}(\delta) = \mathbb{Q}$. A similar discussion shows that

$$\mathbb{Q}(uv\delta) \cap \mathbb{Q}(\delta) = \mathbb{Q} = \mathbb{Q}(uv\delta) \cap \mathbb{Q}(uv).$$

So we have a Galois tower which includes the following subfields.



Choose

$$\alpha \in \mathrm{Gal}(E/\mathbb{Q}(uv)) \leqslant \mathrm{Gal}(E/\mathbb{Q})$$

so that $\alpha(\delta) = -\delta$. By renaming $-v$ to v if necessary, we may assume that $v = \alpha(u)$ and so $u = \alpha(v)$. Notice that $\alpha^2 = \mathrm{id}$.

Choose

$$\beta \in \mathrm{Gal}(E/\mathbb{Q}(\delta)) \leqslant \mathrm{Gal}(E/\mathbb{Q})$$

with $\beta(uv) = -uv$. We must have either $\beta(u) = -u$ or $\beta(v) = -v$, so by interchanging $\pm\delta$ if necessary we can assume that $\beta(u) = -u$ and $\beta(v) = v$. Notice that $\beta^2 = \mathrm{id}$.

Choose

$$\gamma \in \mathrm{Gal}(E/\mathbb{Q}(\delta, uv)) \leqslant \mathrm{Gal}(E/\mathbb{Q})$$

so that $\gamma(u) = -u$. Then we must have $\gamma(v) = -v$ since $\gamma(uv) = uv$. Notice that $\gamma^2 = \mathrm{id}$.

Setting $\sigma = \alpha\beta$ we find $\sigma(u) = -v$ and $\sigma(v) = u$. Then $\sigma^2 = \gamma$ and σ has order 4. Also,

$$\alpha\sigma\alpha = \beta\sigma\beta = \sigma^{-1}.$$

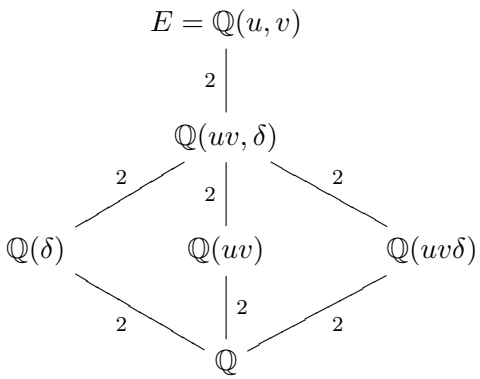
The eight elements

$$\mathrm{id}, \sigma, \gamma, \sigma^{-1}, \alpha, \alpha\sigma, \alpha\gamma, \alpha\sigma^{-1}$$

form a group isomorphic to the dihedral group of order 8, D_8. Therefore we have

$$\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{D}_8,$$

and $[E : \mathbb{Q}] = 8$. The corresponding Galois tower is



□

4.29. Example. We have the following Galois groups:

$$\mathrm{Gal}(\mathbb{Q}(X^4+1)/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2; \quad \mathrm{Gal}(\mathbb{Q}(X^4+4X^2+2)/\mathbb{Q}) \cong \mathbb{Z}/4;$$
$$\mathrm{Gal}(\mathbb{Q}(X^4+2X^2+2)/\mathbb{Q}) \cong \mathrm{D}_8\,.$$

Exercises on Chapter 4

4-1. If $f(X) \in K[X]$ is a separable polynomial, prove that the splitting field of $f(X)$ over K is a finite Galois extension of K.

4-2. Let K be a field for which $\mathrm{char}\, K \neq 2, 3$ and suppose that $f(X) \in K[x]$ is a cubic polynomial.

(a) Show that there $u, v \in \overline{K}$ with $u \neq 0$ such that $f(uX+v) = X^3 + aX + b$ for some $a, b \in \overline{K}$. If $f(X)$ is monic, deduce that $a, b \in K$; under what conditions is this always true?

(b) If $g(X) = X^3 + aX + b \in K[x]$ is irreducible and $E = K(g(X))$ is its splitting field over K, explain why $\mathrm{Gal}(E/K)$ is isomorphic to one of the groups S_3 or A_3.

(c) Continuing with the notation and assumptions of (b), suppose that w_1, w_2, w_3 are the distinct roots of $g(X)$ in E and let

$$\Delta = (w_1 - w_2)^2(w_2 - w_3)^2(w_1 - w_3)^2 \in E.$$

Show that

$$\Delta = -4b^3 - 27a^2,$$

and hence $\Delta \in K$. If $\delta = (w_1 - w_2)(w_3 - w_3)(w_1 - w_3)$, show that

$$\mathrm{Gal}(E/K) \cong \begin{cases} \mathrm{A}_3 & \text{if } \delta \in K, \\ \mathrm{S}_3 & \text{if } \delta \notin K. \end{cases}$$

[*Hint: Consider* $K(\delta) \leqslant E$ *and the effect on the element* δ *of even and odd permutations in* $\mathrm{Gal}(E/K) \leqslant \mathrm{S}_3$.]

4-3. Show that $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$ is irreducible over $\mathbb{Q}$, and show that its discriminant is a square in $\mathbb{Q}$. Prove that the Galois group of $f(X)$ over $\mathbb{Q}$ is cyclic.

4-4. This is a revision exercise on finite groups of small order.

(a) Show that every non-abelian finite group has order at least 6.

(b) Let D_8 be the dihedral group with the eight elements

$$\iota, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$$

satisfying

$$\alpha^4 = \iota, \quad \beta^2 = \iota, \quad \beta\alpha\beta = \alpha^{-1} = \alpha^3.$$

Find all the normal subgroups of D_8.

4-5. Use Kaplansky's Theorem 4.28 to find the Galois group of the splitting field E of the polynomial $X^4 + 3 \in \mathbb{Q}[X]$ over $\mathbb{Q}$. Determine all the subextensions $F \leqslant E$ for which $F/\mathbb{Q}$ is Galois.

4-6. Find the Galois groups for each of the following extensions:
$\mathbb{Q}(X^3 - 10)/\mathbb{Q}$; $\mathbb{Q}(\sqrt{2})(X^3 - 10)/\mathbb{Q}(\sqrt{2})$; $\mathbb{Q}(\sqrt{3}\,i)(X^3 - 10)/\mathbb{Q}(\sqrt{3}\,i)$;
$\mathbb{Q}(\sqrt{23}\,i)(X^3 - X - 1)/\mathbb{Q}(\sqrt{23}\,i)$; $K(X^3 - X - 1)/K$ for $K = \mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{5}\,i)$, $\mathbb{Q}(i)$.

4-7. Let $p > 0$ be a prime. Let K be a field with $\operatorname{char} K \neq p$. Suppose that $0 \neq a \in K$ and $f(X) = X^p - a \in K[X]$. Let L/K where L is a splitting field for $f(X)$ over K.

(a) Show that $f(X)$ has p distinct roots in L. If $u \in L$ is one such root, describe the remaining roots and show that L contains p distinct p-th roots of 1.

(b) Suppose that K contains p distinct p-th roots of 1. Show that either $f(X)$ is irreducible over K or it factors into p distinct linear factors over K.

(c) Suppose that the only p-th root of 1 in K is 1. Show that either $f(X)$ is irreducible over K or it has a root in K.

4-8. Let K be a field of characteristic $\operatorname{char} K = p$ where $p > 0$ is a prime. Suppose that $0 \neq a \in K$ and $f(X) = X^p - a \in K[X]$. Show that if $f(X)$ has no root in K then it is irreducible over K.

4-9. (a) Verify that the resultant of Definition 4.24 satisfies the following identities:

$$\begin{aligned}
\operatorname{Res}(p(X), q(X) + X^r p(X)) &= \operatorname{Res}(p(X), q(X)),\\
\operatorname{Res}(p(X) + X^s q(X), q(X)) &= \operatorname{Res}(p(X), q(X)),\\
\operatorname{Res}(q(X), p(X)) &= (-1)^{mn} \operatorname{Res}(p(X), q(X)),\\
\operatorname{Res}(aq(X), bp(X)) &= a^n b^m \operatorname{Res}(p(X), q(X)),
\end{aligned}$$

where $a, b \in K$, $r \leqslant n$ and $s \leqslant n$.
(b) Deduce that $\operatorname{Res}(p(X), q(X)) = 0$ if and only if $\gcd(p(X), q(X)) \neq 1$.
(c) Show that for a non-constant polynomial $f(X)$, $\operatorname{Res}(f(X), f'(X)) = 0$ if and only if $f(X)$ has no multiple roots in any extension field of K.

CHAPTER 5

Galois extensions for fields of positive characteristic

In this chapter we will investigate extensions of fields of positive characteristic, especially finite fields. A thorough account of finite fields and their applications can be found in [**6**].

Throughout this chapter we will assume that K is a field of prime characteristic $p = \operatorname{char} K > 0$, containing the prime subfield $\mathbb{F}_p$.

5.1. Finite fields

If K is a finite field, then K is an $\mathbb{F}_p$-vector space. Our first goal is to count the elements of K. Here is a more general result.

5.1. Lemma. *Let F be a finite field with q elements and let V be an F-vector space. Then $\dim_F V < \infty$ if and only if V is finite in which case $|V| = q^{\dim_F V}$.*

Proof. If $d = \dim_F V < \infty$, then for a basis $v_1, \dots, v_d$ we can express each element $v \in V$ uniquely in the form $v = t_1 v_1 + \cdots + t_d v_d$, where $t_1, \dots, t_d \in F$. Clearly there are exactly q^d such expressions, so $|V| = q^d$.

Conversely, if V is finite then any basis has finitely many elements and so $\dim_F V < \infty$. □

5.2. Corollary. *Let F be a finite field and E/F an extension. Then E is finite if and only if E/F is finite and then $|E| = |F|^{[E:F]}$.*

5.3. Corollary. *Let K be a finite field. Then $K/\mathbb{F}_p$ is finite and $|K| = p^{[K:\mathbb{F}_p]}$.*

Our next task is to show that for each power p^d there is a finite field with p^d elements. We start with the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$ and consider the polynomial

$$\Theta_{p^d}(X) = X^{p^d} - X \in \mathbb{F}_p[X].$$

Notice that $\Theta'_{p^d}(X) = -1$, hence by Proposition 3.55 every root of $\Theta_{p^d}(X)$ in $\overline{\mathbb{F}}_p$ is simple. Therefore by Corollary 1.35 $\Theta_{p^d}(X)$ must have exactly p^d distinct roots in $\overline{\mathbb{F}}_p$, say $0, u_1, \dots, u_{p^d-1}$. Then in $\overline{\mathbb{F}}_p[X]$ we have

$$X^{p^d} - X = X(X - u_1) \cdots (X - u_{p^d-1}),$$

and each root is separable over $\mathbb{F}_p$. Let

$$\mathbb{F}_{p^d} = \{u \in \overline{\mathbb{F}}_p : \Theta_{p^d}(u) = 0\} \subseteq \overline{\mathbb{F}}_p, \quad \mathbb{F}^0_{p^d} = \{u \in \mathbb{F}_{p^d} : u \neq 0\}.$$

Notice that $u \in \mathbb{F}^0_{p^d}$ if and only if $u^{p^d-1} = 1$.

5.4. Proposition. *For each $d \geqslant 1$, $\mathbb{F}_{p^d}$ is a finite subfield of $\overline{\mathbb{F}}_p$ with p^d elements and $\mathbb{F}^0_{p^d} = \mathbb{F}^\times_{p^d}$. Furthermore, the extension $\mathbb{F}_{p^d}/\mathbb{F}_p$ is a separable splitting field.*

PROOF. If $u, v \in \mathbb{F}_{p^d}$ then by the Idiot's Binomial Theorem 1.11,

$$(u+v)^{p^d} - (u+v) = (u^{p^d} + v^{p^d}) - (u+v) = (u^{p^d} - u) + (v^{p^d} - v) = 0,$$
$$(uv)^{p^d} - uv = u^{p^d} v^{p^d} - uv = uv - uv = 0.$$

Furthermore, if $u \neq 0$ then $u^{p^d-1} = 1$ and so u has multiplicative inverse u^{p^d-2}. Hence $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$. Notice that $\mathbb{F}_p \leqslant \mathbb{F}_{p^d}$, so $\mathbb{F}_{p^d}/\mathbb{F}_p$ is a finite extension. In any field the non-zero elements are always invertible, hence $\mathbb{F}^0_{p^d} = \mathbb{F}^\times_{p^d}$. □

5.5. DEFINITION. The finite subfield $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$ is called the *Galois field of order* p^d.

The notation $\mathrm{GF}(p^d)$ is often used in place of $\mathbb{F}_{p^d}$. Of course, $\mathbb{F}_{p^1} = \mathrm{GF}(p^1) = \mathrm{GF}(p) = \mathbb{F}_p$ and $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$.

5.6. PROPOSITION. *Let* $d \geqslant 1$.

(i) $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$ *is the splitting subfield for each of the polynomials* $X^{p^d} - X$ *and* $X^{p^d-1} - 1$ *over* $\mathbb{F}_p$.
(ii) $\mathbb{F}_{p^d} \leqslant \overline{\mathbb{F}}_p$ *is the unique subfield with* p^d *elements.*
(iii) *If* F *is any field with* p^d *elements then there is a monomorphism* $F \longrightarrow \overline{\mathbb{F}}_p$ *with image* $\mathbb{F}_{p^d}$, *hence* $F \cong \mathbb{F}_{p^d}$.

PROOF. (i) As $\mathbb{F}_{p^d}$ consists of exactly the roots of $\Theta_{p^d}(X)$ in $\overline{\mathbb{F}}_p$, it is the splitting subfield. The non-zero elements of $\mathbb{F}_{p^d}$ are the roots of $X^{p^d-1} - 1$, so $\mathbb{F}_{p^d}$ is also the splitting subfield for this polynomial.
(ii) Let $F \leqslant \overline{\mathbb{F}}_p$ have p^d elements. Notice that the non-zero elements of F form a group $F^\times$ under multiplication. This group is abelian and has $p^d - 1$ elements, so by Lagrange's Theorem, each element $u \in F^\times$ has order dividing $p^d - 1$, therefore $u^{p^d-1} = 1$ and so $u^{p^d} = u$. But this means every element of F is a root of $\Theta_{p^d}(X)$ and so $F \leqslant \mathbb{F}_{p^d}$; equality follows since these subfields both have p^d elements.
(iii) Apply the Monomorphism Extension Theorem 3.49 for $K = L = \mathbb{F}_p$ and $M = F$. By (ii), the image of the resulting monomorphism must be $\mathbb{F}_{p^d}$, therefore $F \cong \mathbb{F}_{p^d}$. □

It is worth noting the following consequence of this result and the construction of $\mathbb{F}_{p^d}$.

5.7. COROLLARY. *Let* K *be a finite field of characteristic* p. *Then* $K/\mathbb{F}_p$ *is a finite Galois extension.*

5.8. EXAMPLE. Consider the polynomial $X^4 - X \in \mathbb{F}_2[X]$. By inspection, in the ring $\mathbb{F}_2[X]$ we find that

$$X^4 - X = X^4 + X = X(X^3 + 1) = X(X+1)(X^2 + X + 1).$$

Now $X^2 + X + 1$ has no root in $\mathbb{F}_2$ so it must be irreducible in $\mathbb{F}_2[X]$. Its splitting field is a quadratic extension $\mathbb{F}_2(w)/\mathbb{F}_2$ where w is one of the roots of $X^2 + X + 1$, the other being $w + 1$ since the sum of the roots is the coefficient of X. This tells us that every element of $\mathbb{F}_4 = \mathbb{F}_2(w)$ can be uniquely expressed in the form $a + bw$ with $a, b \in \mathbb{F}_2$. To calculate products we use the fact that $w^2 = w + 1$, so for $a, b, c, d \in \mathbb{F}_2$ we have

$$(a + bw)(c + dw) = ac + (ad + bc)w + bdw^2 = (ac + bd) + (ad + bc + bd)w.$$

5.9. Example. Consider the polynomial $X^9 - X \in \mathbb{F}_3[X]$. Let us find an irreducible polynomial of degree 2 in $\mathbb{F}_3[X]$. Notice that X^2+1 has no root in $\mathbb{F}_3$, hence $X^2+1 \in \mathbb{F}_3[X]$ is irreducible; so if $u \in \overline{\mathbb{F}}_3$ is a root of X^2+1 then $\mathbb{F}_3(u)/\mathbb{F}_3$ has degree 2 and $\mathbb{F}_3(u) = \mathbb{F}_9$. Every element of $\mathbb{F}_9$ can be uniquely expressed in the form $a + bu$ with $a, b \in \mathbb{F}_3$. Multiplication is carried out using the relation $u^2 = -1 = 2$.

By inspection, in the ring $\mathbb{F}_3[X]$ we find that

$$X^9 - X = X(X^8 - 1) = (X^3 - X)(X^2 + 1)(X^2 + X - 1)(X^2 - X - 1).$$

So $X^2 + X - 1$ and $X^2 - X - 1$ are also quadratic irreducibles in $\mathbb{F}_3[X]$. We can find their roots in $\mathbb{F}_9$ using the quadratic formula since in $\mathbb{F}_3$ we have $2^{-1} = (-1)^{-1} = -1$. The discriminant of $X^2 + X - 1$ is

$$1 - 4(-1) = 5 = 2 = u^2,$$

so its roots are $(-1)(-1 \pm u) = 1 \pm u$. Similarly, the discriminant of $X^2 - X - 1$ is

$$1 - 4(-1) = 5 = 2 = u^2$$

and its roots are $(-1)(1 \pm u) = -1 \pm u$. Then we have

$$\mathbb{F}_9 = \mathbb{F}_3(u) = \mathbb{F}_3(1 \pm u) = \mathbb{F}_3(-1 \pm u).$$

There are two issues we can now clarify.

5.10. Proposition. *Let $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ be two Galois fields of characteristic p. Then $\mathbb{F}_{p^m} \leqslant \mathbb{F}_{p^n}$ if and only if $m \mid n$.*

Proof. If $\mathbb{F}_{p^m} \leqslant \mathbb{F}_{p^n}$, then by Corollary 5.2,

$$p^n = (p^m)^{[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]} = p^{m[\mathbb{F}_{p^n}:\mathbb{F}_{p^m}]},$$

so $m \mid n$.

If $m \mid n$, write $n = km$ with $k \geqslant 1$. Then for $u \in \mathbb{F}_{p^m}$ we have $u^{p^m} = u$, so

$$u^{p^n} = u^{p^{mk}} = (u^{p^m})^{p^{m(k-1)}} = u^{p^{m(k-1)}} = \cdots = u^{p^m} = u.$$

Hence $u \in \mathbb{F}_{p^n}$ and therefore $\mathbb{F}_{p^m} \leqslant \mathbb{F}_{p^n}$. □

This means that we can think of the Galois fields $\mathbb{F}_{p^n}$ as ordered by divisibility of n. The diagram of subfields for $\mathbb{F}_{p^{24}}$ can be seen in Figure 5.1 which shows extensions with no intermediate subextensions.

5.11. Theorem. *The algebraic closure of $\mathbb{F}_p$ is the union of all the Galois fields of characteristic p,*

$$\overline{\mathbb{F}}_p = \bigcup_{n \geqslant 1} \mathbb{F}_{p^n}.$$

Furthermore, each element $u \in \overline{\mathbb{F}}_p$ is separable over $\mathbb{F}_p$.

Proof. Let $u \in \overline{\mathbb{F}}_p$. Then u is algebraic over $\mathbb{F}_p$ and the extension $\mathbb{F}_p(u)/\mathbb{F}_p$ is finite. Hence by Corollary 5.2, $\mathbb{F}_p(u) \leqslant \overline{\mathbb{F}}_p$ is a finite subfield. Proposition 5.10 now implies that $\mathbb{F}_p(u) = \mathbb{F}_{p^n}$ for some n. The separability statement follows from Corollary 5.7. □

We will require a useful fact about Galois fields.

5.12. Proposition. *The group of units $\mathbb{F}_{p^d}^\times$ in $\mathbb{F}_{p^d}$ is cyclic.*

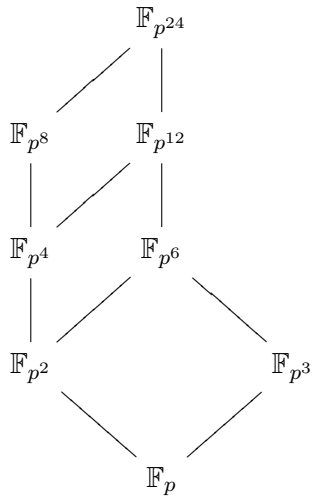


FIGURE 5.1. The subfields of $\mathbb{F}_{p^{24}}$

This is a special case of a more general result about arbitrary fields.

5.13. PROPOSITION. *Let K be a field. Then every finite subgroup $U \leqslant K^\times$ is cyclic.*

PROOF. Use Corollary 1.35 and Lemma 1.46. □

5.14. DEFINITION. $w \in \mathbb{F}_{p^d}^\times$ is called a *primitive root* if it is a primitive (p^d-1)-th root of unity, *i.e.*, its order in the group $\mathbb{F}_{p^d}^\times$ is (p^d-1), hence $\langle w\rangle = \mathbb{F}_{p^d}^\times$.

5.15. REMARK. Unfortunately the word *primitive* has two confusingly similar uses in the context of finite fields. Indeed, some authors use the term *primitive element* for what we have called a *primitive root*, but that conflicts with our usage, although as we will in the next result, every primitive root is indeed a primitive element in our sense!

5.16. PROPOSITION. *The extension of Galois fields $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ is simple,* i.e., *$\mathbb{F}_{p^{nd}} = \mathbb{F}_{p^d}(u)$ for some $u \in \mathbb{F}_{p^{nd}}$.*

PROOF. By Proposition 5.12, $\mathbb{F}_{p^{nd}}$ has a primitive root w say. Then every element of $\mathbb{F}_{p^{nd}}$ can be expressed as a polynomial in w, so $\mathbb{F}_{p^{nd}} \leqslant \mathbb{F}_{p^d}(w) \leqslant \mathbb{F}_{p^{nd}}$. This implies that $\mathbb{F}_{p^{nd}} = \mathbb{F}_{p^d}(w)$. □

5.17. REMARK. This completes the proof of the Primitive Element Theorem 3.74 which we had previously only established for infinite fields.

5.18. EXAMPLE. In Example 5.8 we find that $\mathbb{F}_4 = \mathbb{F}_2(w)$ has the two primitive roots w and $w+1$.

5.19. EXAMPLE. In Example 5.9 we have $\mathbb{F}_9 = \mathbb{F}_3(u)$ and $\mathbb{F}_9^\times$ is cyclic of order 8. Since $\varphi(8) = 4$, there are four primitive roots and these are the roots of the polynomials X^2+X-1 and X^2-X-1 which we found to be $\pm 1 \pm u$.

We record a fact that is very important in Number Theory.

5.20. PROPOSITION. *Let $p > 0$ be an odd prime.*

(i) *If $p \equiv 1 \pmod 4$, the polynomial $X^2+1 \in \mathbb{F}_p[X]$ has two roots in $\mathbb{F}_p$.*

(ii) *If* $p \equiv 3 \pmod 4$ *the polynomial* $X^2+1 \in \mathbb{F}_p[X]$ *is irreducible, so* $\mathbb{F}_{p^2} \cong \mathbb{F}_p[X]/(X^2+1)$.

PROOF. (i) We have $4 \mid (p-1) = |\mathbb{F}_p^\times|$, so if $u \in \mathbb{F}_p^\times$ is a generator of this cyclic group, the order of $u^{|\mathbb{F}_p^\times|/4}$ is 4, hence this is a root of X^2+1 (the other root is $-u^{|\mathbb{F}_p^\times|/4}$).
(ii) If $v \in \mathbb{F}_p$ is a root of X^2+1 then v has order 4 in $\mathbb{F}_p^\times$. But then $4 \mid (p-1) = |\mathbb{F}_p^\times|$, which is impossible since $p-1 \equiv 2 \pmod 4$. □

Here is a generalization of Proposition 5.20.

5.21. PROPOSITION. $\mathbb{F}_{p^d}$ *contains a primitive* n*-th root of unity if and only if* $p^d \equiv 1 \pmod n$ *and* $p \nmid n$.

5.2. Galois groups of finite fields and Frobenius mappings

Consider an extension of Galois fields $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$. By Proposition 5.6(i), Corollary 5.7 and Proposition 3.73, this extension is Galois and

$$|\operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})| = [\mathbb{F}_{p^{nd}} : \mathbb{F}_{p^d}] = n.$$

We next introduce an important element of the Galois group $\operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$.

5.22. DEFINITION. The (*relative*) *Frobenius mapping* for the extension $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$ is the function $\mathrm{F}_d\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ given by $\mathrm{F}_d(t) = t^{p^d}$.

5.23. PROPOSITION. *The relative Frobenius mapping* $\mathrm{F}_d\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ *is an automorphism of* $\mathbb{F}_{p^{nd}}$ *that fixes the elements of* $\mathbb{F}_{p^d}$, *so* $\mathrm{F}_d \in \operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d})$. *The order of* F_d *is* n, *so* $\operatorname{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}) = \langle \mathrm{F}_d \rangle$, *the cyclic group generated by* F_d.

PROOF. For $u, v \in \mathbb{F}_{p^{nd}}$, we have the identities

$$\mathrm{F}_d(u+v) = (u+v)^{p^d} = u^{p^d} + v^{p^d}, \quad \mathrm{F}_d(uv) = (uv)^{p^d} = u^{p^d} v^{p^d},$$

so F_d is a ring homomorphism. Also, for $u \in \mathbb{F}_{p^d}$ we have

$$\mathrm{F}_d(u) = u^{p^d} = u,$$

so F_d fixes the elements of $\mathbb{F}_{p^d}$. To see that F_d is an automorphism, notice that the composition power $\mathrm{F}_d^n = \mathrm{F}_d \circ \cdots \circ \mathrm{F}_d$ (with n factors) satisfies

$$\mathrm{F}_d^n(t) = t^{p^{nd}} = t$$

for all $t \in \mathbb{F}_{p^{nd}}$, hence $\mathrm{F}_d^n = \mathrm{id}$. Then F_d is invertible with inverse $\mathrm{F}_d^{-1} = \mathrm{F}_d^{n-1}$. This also shows that the order of F_d in the group $\operatorname{Aut}_{\mathbb{F}_{p^d}}(\mathbb{F}_{p^{nd}})$ is at most n. Suppose the order is k with $k \leqslant n$; then every element $u \in \mathbb{F}_{p^{nd}}$ satisfies the equation $\mathrm{F}_d^k(u) = u$ which expands to $u^{p^{kd}} = u$, hence $u \in \mathbb{F}_{p^{kd}}$. But this can only be true if $k = n$. □

Frobenius mappings exist on the algebraic closure $\overline{\mathbb{F}}_p$. For $d \geqslant 1$, consider the function

$$\mathrm{F}_d\colon \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p\,; \quad \mathrm{F}_d(t) = t^{p^d}.$$

5.24. PROPOSITION. *Let* $d \geqslant 1$.

(i) $\mathrm{F}_d\colon \overline{\mathbb{F}}_p \longrightarrow \overline{\mathbb{F}}_p$ *is an automorphism of* $\overline{\mathbb{F}}_p$ *which fixes the elements of* $\mathbb{F}_{p^d}$. *In fact for* $u \in \overline{\mathbb{F}}_p$, $\mathrm{F}_d(u) = u$ *if and only if* $u \in \mathbb{F}_{p^d}$.

(ii) *The restriction of* F_d *to the Galois subfield* $\mathbb{F}_{p^{dn}}$ *agrees with the relative Frobenius mapping* $\mathrm{F}_d\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$.

(ii) *If* $k \geqslant 1$, *then* $\mathrm{F}_d^k = \mathrm{F}_{kd}$. *Hence in the automorphism group* $\mathrm{Aut}_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$, F_d *has infinite order, so* $\mathrm{Aut}_{\mathbb{F}_{p^d}}(\overline{\mathbb{F}}_p)$ *is infinite.*

PROOF. This is left as an exercise. □

The Frobenius mapping $\mathrm{F} = \mathrm{F}_1$ is often called the *absolute Frobenius mapping* since it exists as an element of each of the groups $\mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ and $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n}) = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ for every $n \geqslant 1$.

In $\mathrm{Gal}(\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}) = \langle \mathrm{F}_d \rangle$, for each k with $k \mid n$ there is the cyclic subgroup $\langle \mathrm{F}_d^k \rangle$ of order $|\langle \mathrm{F}_d^k \rangle| = n/k$.

5.25. PROPOSITION. *For* $k \mid n$, *the fixed subfield of* $\langle \mathrm{F}_d^k \rangle$ *in* $\mathbb{F}_{p^{nd}}$ *is* $\mathbb{F}_{p^{nd}}^{\langle \mathrm{F}_d^k \rangle} = \mathbb{F}_{p^{dk}}$.

$$
\begin{array}{c}
\mathbb{F}_{p^{nd}} \\
\Big| \; n/k \\
\mathbb{F}_{p^{nd}}^{\langle \mathrm{F}_d^k \rangle} = \mathbb{F}_{p^{dk}} \\
\Big| \; k \\
\mathbb{F}_{p^d}
\end{array}
$$

PROOF. For $u \in \mathbb{F}_{p^{nd}}$ we have $\mathrm{F}_d^k(u) = u^{p^{dk}}$, hence $\mathrm{F}_d^k(u) = u$ if and only if $u \in \mathbb{F}_{p^{dk}}$. □

Figure 5.2 shows the subgroup diagram corresponding to the lattice of subfields of $\mathbb{F}_{p^{24}}$ shown in Figure 5.1.

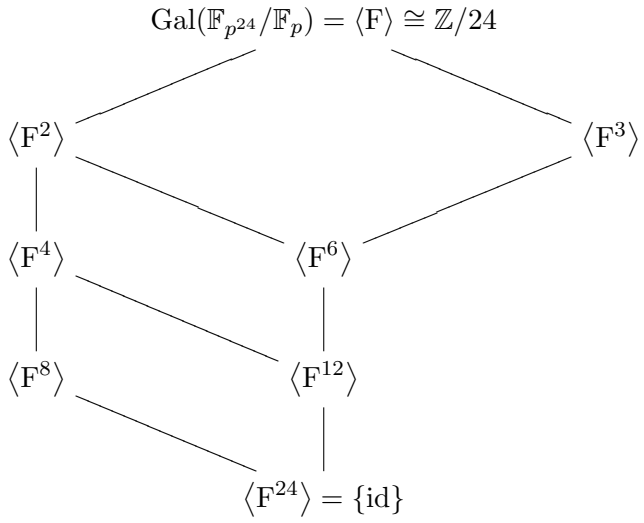


FIGURE 5.2. The subgroups of the Galois groups of $\mathbb{F}_{p^{24}}/\mathbb{F}_p$

5.3. The trace and norm mappings

For an extension of Galois fields $\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}$, consider the function $\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^{nd}}$ defined by

$$\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = u + u^{p^d} + u^{p^{2d}} + \cdots + u^{p^{(n-1)d}} = u + \mathrm{F}_d(u) + \mathrm{F}_{2d}(u) + \cdots + \mathrm{F}_{(n-1)d}(u).$$

Notice that

$$\begin{aligned}\mathrm{F}_d(\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u)) &= u^{p^d} + u^{p^{2d}} + u^{p^{3d}} + \cdots + u^{p^{nd}} \\ &= u^{p^d} + u^{p^{2d}} + u^{p^{3d}} + \cdots + u^{p^{(n-1)d}} + u = \mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u).\end{aligned}$$

So by Proposition 5.24(i), $\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) \in \mathbb{F}_{p^d}$. If we modify $\mathrm{T}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ to have codomain $\mathbb{F}_{p^d}$, we obtain the *relative trace*

$$\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}\colon \mathbb{F}_{p^{nd}} \longrightarrow \mathbb{F}_{p^d}; \quad \mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = u + u^{p^d} + u^{p^{2d}} + \cdots + u^{p^{(n-1)d}}.$$

5.26. Proposition. *The relative trace* $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ *is a surjective* $\mathbb{F}_{p^d}$*-linear mapping and whose kernel is an* $\mathbb{F}_{p^d}$*-vector subspace of dimension* $n-1$.

Proof. Clearly $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ is additive. For $t \in \mathbb{F}_{p^d}$ we have $t^{p^d} = t$, so $\mathbb{F}_{p^d}$-linearity follows from the formula

$$tu + (tu)^{p^d} + (tu)^{p^{2d}} + \cdots + (tu)^{p^{(n-1)d}} = tu + tu^{p^d} + tu^{p^{2d}} + \cdots + tu^{p^{(n-1)d}}.$$

To see that $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ is surjective, notice that $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = 0$ if and only if u is a root of the polynomial

$$X + X^{p^d} + X^{p^{2d}} + \cdots + X^{p^{(n-1)d}} \in \mathbb{F}_{p^d}[X]$$

which has degree $p^{(n-1)d}$ and so has at most $p^{(n-1)d} < p^{nd}$ roots in $\mathbb{F}_{p^{nd}}$. This means that $\ker \mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ cannot be the whole of $\mathbb{F}_{p^{nd}}$. $\mathrm{Tr}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ is surjective since its codomain has dimension 1. □

There is a multiplicative version of this construction. Consider the function

$$\mathrm{N}\colon \mathbb{F}_{p^{nd}}^{\times} \longrightarrow \mathbb{F}_{p^{nd}}^{\times}$$

for which

$$\mathrm{N}(u) = uu^{p^d}u^{p^{2d}}\cdots u^{p^{(n-1)d}} = u\,\mathrm{F}_d(u)\,\mathrm{F}_{2d}(u)\cdots\mathrm{F}_{(n-1)d}(u).$$

Then we have

$$\begin{aligned}\mathrm{F}_d(\mathrm{N}(u)) &= u^{p^d}u^{p^{2d}}u^{p^{3d}}\cdots u^{p^{nd}} \\ &= u^{p^d}u^{p^{2d}}u^{p^{3d}}\cdots u^{p^{(n-1)d}}u \\ &= uu^{p^d}u^{p^{2d}}u^{p^{3d}}\cdots u^{p^{(n-1)d}} \\ &= \mathrm{N}(u).\end{aligned}$$

So by Proposition 5.24(i), $\mathrm{N}(u) \in \mathbb{F}_{p^d}$. By redefining the codomain we obtain the *relative norm*

$$\mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}\colon \mathbb{F}_{p^{nd}}^{\times} \longrightarrow \mathbb{F}_{p^d}^{\times}; \quad \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}(u) = uu^{p^d}u^{p^{2d}}\cdots u^{p^{(n-1)d}}.$$

5.27. Proposition. *The relative norm* $\mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ *is a surjective group homomorphism.*

PROOF. Multiplicativity is obvious. The kernel of $\mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}$ consists of the roots in $\mathbb{F}_{p^{nd}}$ of the polynomial

$$X^{1+p^d+\cdots+p^{(n-1)d}} - 1 \in \mathbb{F}_{p^d}[X],$$

so

$$|\ker \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}| \leqslant 1 + p^d + \cdots + p^{(n-1)d} = \frac{p^{nd}-1}{p^d-1}.$$

Hence

$$|\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}| = \frac{p^{nd}-1}{|\ker \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}|} \geqslant p^d - 1.$$

Since $\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}} \leqslant \mathbb{F}_{p^d}^\times$, we also have

$$|\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}}| \leqslant p^d - 1,$$

therefore

$$\operatorname{im} \mathrm{Norm}_{\mathbb{F}_{p^{nd}}/\mathbb{F}_{p^d}} = \mathbb{F}_{p^d}^\times. \qquad \square$$

Exercises on Chapter 5

5-1. Show that Proposition 5.13 also applies to an integral domain in place of a field.

5-2. What happens to Theorem 5.20 if we try to take $p = 2$.

5-3. Let $f(X) \in \mathbb{F}_{p^d}[X]$ be an irreducible polynomial with $\deg f(X) = n$. Find the splitting field of $f(X)$. Deduce that for any other irreducible polynomial $g(X) \in \mathbb{F}_{p^d}[X]$ with $\deg g(X) = n$, the splitting fields of $f(X)$ and $g(X)$ over $\mathbb{F}_{p^d}$ agree.

5-4. Find the smallest Galois fields containing all the roots of the following polynomials, in each case find a primitive root of this Galois field:

(a) $X^8 - 1 \in \mathbb{F}_{41}[X]$; (b) $X^8 - 1 \in \mathbb{F}_5[X]$; (c) $X^8 - 1 \in \mathbb{F}_{11}[X]$; (d) $X^8 - 1 \in \mathbb{F}_2[X]$.

5-5. Let $w \in \mathbb{F}_{p^d}^\times$ be a primitive root. If $\ell < d$, show that $w \notin \mathbb{F}_{p^\ell}^\times$. Deduce that $\deg_{\mathbb{F}_p} w = d$ and $d \mid \varphi(p^d - 1)$.

5-6. Let $p > 0$ be a prime. Suppose that $d \geqslant 1$, and $K/\mathbb{F}_{p^d}$ is an extension. For $a \in K$, let $g_a(X) = X^{p^d} - X - a \in K[X]$.

(a) If the polynomial $g_a(X)$ is irreducible over K, show that the splitting field E of $g_a(X)$ over K is separable and $\mathrm{Gal}(E/K) \cong \mathbb{F}_{p^d}$. [*Hint: show that if $u \in E$ is a root of $g_a(X)$ in an extension E/K, then so is $u + t$ for every $t \in \mathbb{F}_p$.*]

(b) If $d = 1$, show that $g_a(X)$ is irreducible over K if and only if it has no root in K.

(c) If K is a finite field and $d > 1$, explain why $g_a(X)$ can never be irreducible over K.

5-7. Let p be an odd prime, $d \geqslant 1$ and write $q = p^d$.

(a) Consider $\{\pm 1\} = \{1, -1\}$ as a group under multiplication. Show that there is a unique group homomorphism $\lambda_q \colon \mathbb{F}_q^\times \longrightarrow \{\pm 1\}$ which is characterized by the requirement that for every $u \in \mathbb{F}_q^\times$, $\lambda_q(u) = 1$ if and only if $u = v^2$ for some $v \in \mathbb{F}_q^\times$. Is λ_q always surjective?

(b) Consider the set of all squares in $\mathbb{F}_q$,

$$\Sigma_q = \{u^2 \in \mathbb{F}_q : u \in \mathbb{F}_q\} \subseteq \mathbb{F}_q.$$

Show that the number of elements of Σ_q is $|\Sigma_q| = (q+1)/2$. Deduce that if $t \in \mathbb{F}_q$ then the set

$$t - \Sigma_q = \{t - u^2 \in \mathbb{F}_q : u \in \mathbb{F}_q\}$$

has $|t - \Sigma_q| = (q+1)/2$ elements.

(c) If $t \in \mathbb{F}_q$, show that

$$|\Sigma_q \cap (t - \Sigma_q)| \geqslant 1.$$

Deduce that every element of $\mathbb{F}_q$ is either a square or can be written as the sum of two squares.

(d) Deduce that the equation $x^2 + y^2 + z^2 = 0$ has at least one non-trivial solution in $\mathbb{F}_q$.

(e) What can you say about the case $p = 2$?

CHAPTER 6

A Galois Miscellany

In this chapter we will explore some miscellaneous topics in Galois Theory. Historically, Galois Theory has always been an important tool in Number Theory and Algebra, stimulating the development of subjects such as Group Theory, Ring Theory and such diverse areas as Differential Equations, Complex Analysis and Algebraic Geometry. Many of the ideas introduced in this chapter are of great importance in these and other mathematical areas.

6.1. A proof of the Fundamental Theorem of Algebra

We will prove the *Fundamental Theorem of Algebra* for the complex numbers $\mathbb{C}$. This proof is essentially due to Gauss but he did not use the historically more recent Sylow theory. It is interesting to compare the proof below with others which use the topology of the plane and circle or Complex Analysis; our proof only uses the connectivity of the real line (via the Intermediate Value Theorem) together with explicit calculations in $\mathbb{C}$ involving square roots.

6.1. Theorem (The Fundamental Theorem of Algebra). *The field of complex numbers $\mathbb{C}$ is algebraically closed and $\overline{\mathbb{R}} = \mathbb{C}$.*

Proof. We know that $[\mathbb{C} : \mathbb{R}] = 2$, so $\mathbb{C}/\mathbb{R}$ is algebraic. Let $p(X) \in \mathbb{C}[X]$ be irreducible. Then any root u of $p(X)$ in the algebraic closure $\overline{\mathbb{C}}$ is algebraic over $\mathbb{R}$, so in $\mathbb{C}[X]$ we have $p(X) \mid \operatorname{minpoly}_{\mathbb{R},u}(X)$. The splitting field of $p(X)$ over $\mathbb{C}$ is contained in the splitting field E of $\operatorname{minpoly}_{\mathbb{R},u}(X)(X^2+1)$ over $\mathbb{R}$. Since $\mathbb{C} \leqslant E$, we have $2 \mid [E : \mathbb{R}]$ and so $2 \mid |\operatorname{Gal}(E/\mathbb{R})|$.

Now consider a 2-Sylow subgroup $P \leqslant \operatorname{Gal}(E/\mathbb{R})$ and recall that $|\operatorname{Gal}(E/\mathbb{R})|/|P|$ is odd. For the fixed subfield of P, we have

$$[E^P : \mathbb{R}] = \frac{|\operatorname{Gal}(E/\mathbb{R})|}{|P|},$$

which shows that $E^P/\mathbb{R}$ has odd degree. The Primitive Element Theorem 3.74 allows us to write $E^P = \mathbb{R}(v)$ for some v whose minimal polynomial over $\mathbb{R}$ must also have odd degree. But by the Intermediate Value Theorem, every real polynomial of odd degree has a real root, so irreducibility implies that v has degree 1 over $\mathbb{R}$ and therefore $E^P = \mathbb{R}$. This shows that $\operatorname{Gal}(E/\mathbb{R}) = P$, hence $\operatorname{Gal}(E/\mathbb{R})$ is a 2-group.

As $\mathbb{C}/\mathbb{R}$ is a Galois extension, we can consider the normal subgroup $\operatorname{Gal}(E/\mathbb{C}) \triangleleft \operatorname{Gal}(E/\mathbb{R})$ for which $|\operatorname{Gal}(E/\mathbb{R})| = 2\,|\operatorname{Gal}(E/\mathbb{C})|$. We must show that $|\operatorname{Gal}(E/\mathbb{C})| = 1$, so suppose not. From the theory of 2-groups, there is a normal subgroup $N \triangleleft \operatorname{Gal}(E/\mathbb{C})$ of index 2, so we can consider the Galois extension $E^N/\mathbb{C}$ of degree 2. But from known properties of $\mathbb{C}$ (see Proposition 3.29), every quadratic $aX^2 + bX + c \in \mathbb{C}[X]$ has complex roots (because we can find square roots of every complex number). So we cannot have an irreducible quadratic polynomial in $\mathbb{C}[X]$. Therefore $|\operatorname{Gal}(E/\mathbb{C})| = 1$ and $E = \mathbb{C}$. □

6.2. Cyclotomic extensions

We begin by discussing the situation for *cyclotomic extensions* over $\mathbb{Q}$ using material discussed in Section 1.3. Let $\zeta_n = e^{2\pi i/n}$, the standard primitive n-th root of 1 in $\mathbb{C}$. In Theorem 1.43, it was claimed that the irreducible polynomial over $\mathbb{Q}$ which has ζ_n as a root was the n-th cyclotomic polynomial

$$\Phi_n(X) = \prod_{\substack{t=1,\dots,n-1 \\ \gcd(t,n)=1}} (X - \zeta_n^t).$$

6.2. Theorem. *Let $n \geqslant 2$. Then*

- $\mathbb{Q}(\zeta_n) = \mathbb{Q}[X]/(\Phi_n(X))$;
- $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$;
- $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$, *where the element $t_n \in (\mathbb{Z}/n)^\times$ acts on $\mathbb{Q}(\zeta_n)$ by $t_n \cdot \zeta_n = \zeta_n^t$.*

Proof. Since the complex roots of $\Phi_n(X)$ are the powers ζ_n^t with $t = 1, \dots, n-1$ and $\gcd(t, n) = 1$, $\mathbb{Q}(\zeta_n)$ is the splitting field of $\Phi_n(X)$ over $\mathbb{Q}$ and indeed $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n^t)$ whenever t has the above properties and so ζ_n^t is a primitive n-th root of unity. The main step in the proof is to show that $\Phi_n(X) \in \mathbb{Z}[X]$ is irreducible. To do this we will show that every power ζ_n^t as above is actually a Galois conjugate of ζ_n over $\mathbb{Q}$, therefore

$$\Phi_n(X) = \mathrm{minpoly}_{\mathbb{Q},\zeta_n}(X) = \mathrm{minpoly}_{\mathbb{Q},\zeta_n^t}(X)$$

and hence $\Phi_n(X)$ is irreducible.

Consider

$$\mathbb{Z}(\zeta_n) = \{a_0 + a_1\zeta_n + \cdots + a_r\zeta_n^r : r \geqslant 0,\ a_j \in \mathbb{Z}\} \subseteq \mathbb{Q}(\zeta_n).$$

Then $\mathbb{Z}(\zeta_n)$ is a subring of $\mathbb{Q}(\zeta_n)$ and so is an integral domain. Its group of units contains the cyclic subgroup $\langle\zeta_n\rangle$ of order n.

Let $p > 0$ be a prime which does not divide n. Let $P \lhd \mathbb{Z}(\zeta_n)$ be a maximal ideal which contains p; then the quotient ring $\mathbb{Z}(\zeta_n)/P$ is a field of characteristic p. In fact, it is a finite field, say $\mathbb{F}_{p^d}$ for some d. Let $\pi\colon \mathbb{Z}(\zeta_n) \longrightarrow \mathbb{F}_{p^d}$ be the quotient homomorphism.

Inside the group of units of $\mathbb{Z}(\zeta_n)$ is the subgroup of powers of ζ_n, $\langle\zeta_n\rangle \leqslant \mathbb{Z}(\zeta_n)^\times$; this is a cyclic subgroup of order n. We claim that when restricted to $\langle\zeta_n\rangle$, π gives an injective group homomorphism, $\pi'\colon \langle\zeta_n\rangle \longrightarrow \mathbb{F}_{p^d}^\times$. To see this, suppose that $\pi'(\zeta_n^r) = 1$ for some $r = 1, 2, \dots, n-1$; then $\zeta_n^r - 1 \in P$. By elementary Group Theory we can assume that $r \mid n$ and so $p \nmid r$. On factoring we have

$$(\zeta_n - 1)(\zeta_n^{r-1} + \cdots + \zeta_n + 1) \equiv (\zeta_n - 1)r \pmod{P},$$

so $\zeta_n - 1 \in P$ or $r \in P$ since maximal ideals are prime. But $\mathbb{Z} \cap P = (p)$ and so $r \notin P$, hence $\zeta_n - 1 \in P$. Recalling that

$$\zeta_n^{n-1} + \cdots + \zeta_n + 1 = 0,$$

we see that $n \in P$ and hence $p \mid n$, thus contradicting our original assumption on n. So π' is injective.

Writing $\overline{u} = \pi'(u)$, we can consider the effect of the absolute Frobenius map $\mathrm{F}\colon \mathbb{F}_{p^d} \longrightarrow \mathbb{F}_{p^d}$ on $\overline{\zeta}_n^t = \overline{\zeta_n^t}$,

$$\mathrm{F}(\overline{\zeta}_n^t) = (\overline{\zeta}_n^t)^p = \overline{\zeta_n^{tp}}.$$

This shows that in the Galois extension $\mathbb{F}_{p^d}/\mathbb{F}_p$, $\overline{\zeta}_n^t$ is conjugate to $\overline{\zeta_n^{tp}}$; by iterating this we find that $\overline{\zeta}_n^t$ is conjugate to every power of the form $\overline{\zeta_n^{tp^k}}$.

Now let $t = 1, \ldots, n-1$ and $\gcd(t, n) = 1$. Suppose there is a factorization

$$\Phi_n(X) = f(X)\,\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(X)$$

for some monic polynomial $f(X) \in \mathbb{Z}[X]$ and $f(\zeta_n^t) = 0$. Consider the prime power factorization $t = p_1^{r_1} \cdots p_m^{r_m}$, where the p_j are primes with $2 \leqslant p_1 < \cdots < p_m$ and $r_j \geqslant 1$ with. Since $\gcd(t, n) = 1$ we also have $p_j \nmid n$ s.

Now consider a maximal ideal $P_1 \lhd \mathbb{Z}[\zeta_n]$ containing p_1. Reducing modulo P_1 and working in the resulting extension $\mathbb{F}_{p_1^{d_1}}/\mathbb{F}_{p_1}$, we find that $\overline{\zeta}_n$ is conjugate to $\overline{\zeta}_n^{p_1^{r_1}}$. By separability and the fact that the reduction map $\pi_1 \colon \mathbb{Z}[\zeta_n] \longrightarrow \mathbb{F}_{p_1^{d_1}}$ is injective on the powers of ζ_n, we find that $\overline{f(\zeta_n^{p_1^{r_1}})} \neq 0$ and so $f(\zeta_n^{p_1^{r_1}}) \neq 0$ in $\mathbb{Z}[\zeta_n]$. This shows that $\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^{p_1^{r_1}}) = 0$ and so $\zeta_n^{p_1^{r_1}}$ is conjugate to ζ_n.

Repeating this argument starting with $\zeta_n^{p_1^{r_1}}$ and using the prime p_2 we find that

$$\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^{p_1^{r_1}p_2^{r_2}}) = 0$$

and so $\zeta_n^{p_1^{r_1}p_2^{r_2}}$ is conjugate to ζ_n. Continuing in this fashion, for each $j = 1, \ldots, m$ we have

$$\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^{p_1^{r_1}p_2^{r_2}\cdots p_j^{r_j}}) = 0$$

and so $\zeta_n^{p_1^{r_1}\cdots p_j^{r_j}}$ is conjugate to ζ_n. When $j = m$, this shows that $\mathrm{minpoly}_{\mathbb{Q},\zeta_n}(\zeta_n^t) = 0$. Hence ζ_n^t is conjugate to ζ_n in the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. □

6.3. Theorem. *For $n > 2$, consider the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ where $\zeta_n = e^{2\pi i/n}$. Then $\mathbb{Q}(\zeta_n)_{\mathbb{R}} \neq \mathbb{Q}(\zeta_n)$. Furthermore,*

$$\mathbb{Q}(\zeta_n)_{\mathbb{R}} = \mathbb{Q}(\zeta_n)^{\langle(\overline{\ })\rangle} = \mathbb{Q}(\zeta_n + \overline{\zeta}_n) = \mathbb{Q}(\cos(2\pi/n)),$$

and

$$[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}] = \frac{\varphi(n)}{2}.$$

Proof. Recall that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}/n^\times,$$

where the residue class of r acts by sending ζ_n to ζ_n^r. Complex conjugation corresponds to the residue class of $-1 \equiv n-1 \pmod{n}$. Making use of the identities

$$e^{\theta i} = \cos\theta + \sin\theta\, i, \quad \cos\theta = \frac{1}{2}(e^{\theta i} + e^{-\theta i}),$$

we obtain

$$\cos(2\pi/n) = \frac{1}{2}(\zeta_n + \overline{\zeta}_n) = \frac{1}{2}(\zeta_n + \zeta_n^{-1}).$$

Complex conjugation fixes each of the real numbers $\cos(2\pi k/n)$ for $k = 1, 2, \ldots, n-1$. The residue class of r acts by sending $\cos(2\pi/n)$ to $\cos(2\pi r/n)$; it is elementary to show that $\cos(2\pi r/n) \neq \cos(2\pi/n)$ unless $r \equiv 1 \pmod{n}$. Hence

$$\langle(\overline{\ })\rangle = \{\mathrm{id}, (\overline{\ })\} = \mathrm{Gal}(\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q}).$$

Thus we have

$$\mathbb{Q}(\zeta_n)^{\langle(\overline{\ })\rangle} = \mathbb{Q}(\cos(2\pi/n)),$$

and so $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}] = \varphi(n)/2$. Notice that ζ_n is a root of the polynomial

$$X^2 - 2\cos(2\pi/n)X + 1 \in \mathbb{Q}(\cos(2\pi/n))[X],$$

so we also have

$$\operatorname{minpoly}_{\mathbb{Q}(\cos(2\pi/n)),\zeta_n}(X) = X^2 - 2\cos(2\pi/n)X + 1. \tag{6.1}$$

□

6.4. Example. We have

$$[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}] = \varphi(24) = 8$$

and

$$\operatorname{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Proof. By Theorem 1.43 we have $[\mathbb{Q}(\zeta_{24}) : \mathbb{Q}] = 8$. Also,

$$\zeta_{24}^6 = i, \quad \zeta_{24}^3 = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i, \quad \zeta_{24}^8 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

and all of these numbers are in $\mathbb{Q}(\zeta_{24})$, hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) \leqslant \mathbb{Q}(\zeta_{24})$. It is easy to check that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) : \mathbb{Q}] = 8,$$

which implies that

$$\mathbb{Q}(\zeta_{24}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}, i).$$

Using this we find that

$$\operatorname{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q}) \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2.$$

We also have $\cos(2\pi/24) = \cos(\pi/12) \in \mathbb{Q}(\zeta_{24})$. Since

$$\cos(2\pi/12) = \cos(\pi/6) = \frac{\sqrt{3}}{2},$$

we have

$$2\cos^2(\pi/12) - 1 = \frac{\sqrt{3}}{2}$$

and so

$$4\cos^4(\pi/12) - 4\cos^2(\pi/12) + 1 = \frac{3}{4},$$

giving

$$16\cos^4(\pi/12) - 16\cos^2(\pi/12) + 1 = 0.$$

Then

$$16X^4 - 16X^2 + 1 = 16\operatorname{minpoly}_{\mathbb{Q},\cos(\pi/12)}(X).$$

Note that case (i) of Kaplansky's Theorem 4.28 applies to the polynomial $\operatorname{minpoly}_{\mathbb{Q},\cos(\pi/12)}(X)$.

For this example, $\operatorname{Gal}(\mathbb{Q}(\zeta_{24})/\mathbb{Q})$ has $2^3 - 1 = 7$ subgroups of each of the orders 2 and 4; it is an interesting exercise to find them all together with their fixed subfields. □

6.5. Remark. The minimal polynomial for $\cos(\pi/12)$ can also be found as follows. We have $\Phi_{24}(\zeta_{24}) = 0$, hence since

$$\Phi_{24}(X) = X^8 - X^4 + 1,$$

we obtain

$$\zeta_{24}^8 - \zeta_{24}^4 + 1 = 0.$$

Then after multiplying by ζ_{24}^{-4} we have

$$\zeta_{24}^4 - 1 + \zeta_{24}^{-4} = 0,$$

giving

$$(\zeta_{24}^4 + \zeta_{24}^{-4}) - 1 = 0.$$

Now

$$(\zeta_{24} + \zeta_{24}^{-1})^4 = (\zeta_{24}^4 + \zeta_{24}^{-4}) + 4(\zeta_{24}^2 + \zeta_{24}^{-2}) + 6,$$

hence

$$\zeta_{24}^4 + \zeta_{24}^{-4} = (\zeta_{24} + \zeta_{24}^{-1})^4 - 4(\zeta_{24}^2 + \zeta_{24}^{-2}) - 6.$$

Similarly,

$$(\zeta_{24} + \zeta_{24}^{-1})^2 = \zeta_{24}^2 + \zeta_{24}^{-2} + 2,$$

so

$$\zeta_{24}^2 + \zeta_{24}^{-2} = (\zeta_{24} + \zeta_{24}^{-1})^2 - 2.$$

Combining these we have

$$(\zeta_{24} + \zeta_{24}^{-1})^4 - 4(\zeta_{24} + \zeta_{24}^{-1})^2 + 1 = 0,$$

and so

$$16\cos^4(\pi/12) - 16\cos^2(\pi/12) + 1 = 0.$$

This method will work for any n where $\varphi(n)$ is even, *i.e.*, when $n > 2$.

6.6. Remark. The polynomial that expresses $\cos n\theta$ as a polynomial in $\cos\theta$ is the n-th *Chebsyhev polynomial of the first kind* $\mathrm{T}_n(X) \in \mathbb{Z}[X]$. Here are the first few of these polynomials:

$$\mathrm{T}_2(X) = 2X^2 - 1, \qquad \mathrm{T}_3(X) = 4X^3 - 3X,$$
$$\mathrm{T}_4(X) = 8X^4 - 8X^2 + 1, \qquad \mathrm{T}_5(X) = 16X^5 - 20X^3 + 5X,$$
$$\mathrm{T}_6(X) = 32X^6 - 48X^4 + 18X^2 - 1, \qquad \mathrm{T}_7(X) = 64X^7 - 112X^5 + 56X^3 - 7X.$$

These form a system of *orthogonal polynomials* which can be computed in Maple using the command `orthopoly[T](n,X)`.

Now let K be a field with characteristic $\operatorname{char} K \nmid n$. The polynomial $\Phi_n(X)$ has integer coefficients, so we can view it as an element of $K[X]$ since either $\mathbb{Q} \leqslant K$ or $\mathbb{F}_p \leqslant K$ and we can reduce the coefficients modulo p. In either case it can happen that $\Phi_n(X)$ factors in $K[X]$. However, we can still describe the splitting field of $X^n - 1$ over K and its Galois group.

6.7. Theorem. *If* $\operatorname{char} K \nmid n$, *then the splitting field of* $X^n - 1$ *over* K *is* $K(\zeta)$, *where* $\zeta \in \overline{K}$ *is a primitive* n*-th root of unity. The Galois group* $\mathrm{Gal}(K(\zeta)/K)$ *is isomorphic to a subgroup of* $(\mathbb{Z}/n)^\times$, *hence it is abelian with order dividing* $\varphi(n)$.

PROOF. Working in $\overline{K}$, we know that $\Phi_n(\zeta) = 0$, hence the roots of $\mathrm{minpoly}_{K,\zeta}(X) \in K[X]$ are primitive roots of 1. So $X^n - 1$ splits over $K(\zeta)$ and each element $\alpha \in \mathrm{Gal}(K(\zeta)/K)$ has the action $\alpha(\zeta) = \zeta^{r_\alpha}$, where $\gcd(r_\alpha, n) = 1$. Hence $\mathrm{Gal}(K(\zeta)/K)$ is isomorphic to a subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n)^\times$ which implies that it is abelian and its order divides $\varphi(n)$. □

6.8. REMARK. When $p = \mathrm{char}\, K > 0$, this Galois group only depends on the largest subfield of K which is algebraic over $\mathbb{F}_p$. For example, if $K = \mathbb{F}_{p^d}(T)$ then the value of d is the crucial factor. The precise outcome can be determined with the aid of Proposition 5.21.

6.9. EXAMPLE. We have the following splitting fields and Galois groups.

(i) The splitting field of $X^4 - 1$ over $\mathbb{F}_3(T)$ is $\mathbb{F}_9(T)$ and

$$\mathrm{Gal}(\mathbb{F}_9(T)/\mathbb{F}_3(T)) \cong (\mathbb{Z}/4)^\times \cong \mathbb{Z}/2.$$

(ii) By Proposition 5.20, $X^4 - 1$ splits over $\mathbb{F}_5(T)$ and the Galois group $\mathrm{Gal}(\mathbb{F}_5(T)/\mathbb{F}_5(T))$ is trivial.

PROOF. (i) By Proposition 5.20, $X^4 - 1$ is separable over $\mathbb{F}_3(T)$ and has irreducible factors $(X - 1)$, $(X + 1)$ and $(X^2 + 1)$. The splitting field of $(X^2 + 1)$ over $\mathbb{F}_3$ is $\mathbb{F}_9 = \mathbb{F}_3(\zeta)$, where $\zeta^2 + 1 = 0$, so $(X^2 + 1)$ splits over $\mathbb{F}_9(T)$. Also,

$$\mathrm{Gal}(\mathbb{F}_9/\mathbb{F}_3) \cong (\mathbb{Z}/4)^\times \cong \mathbb{Z}/2,$$

with generator σ satisfying $\sigma(\zeta) = \zeta^{-1} = -\zeta$. This generator clearly extends to an automorphism of $\mathbb{F}_9(T)$ which fixes T.
(ii) By Proposition 5.20, $X^4 - 1$ splits over $\mathbb{F}_5$. □

6.3. Artin's Theorem on linear independence of characters

Let G be a group and K a field.

6.10. DEFINITION. A group homomorphism $\chi\colon G \longrightarrow K^\times$ is called a *character of G with values in K*.

6.11. EXAMPLE. Given any ring homomorphism $\varphi\colon R \longrightarrow K$ we obtain a character of $R^\times$ in K by restricting φ to a map $\chi_\varphi\colon R^\times \longrightarrow K^\times$.

6.12. EXAMPLE. Given an automorphism $\alpha\colon K \longrightarrow K$, $\chi_\alpha\colon K^\times \longrightarrow K^\times$ is a character of $K^\times$ in K.

6.13. EXAMPLE. Let E/K be a Galois extension and $\sigma \in \mathrm{Gal}(E/K)$. Then $\chi_\sigma\colon E^\times \longrightarrow E^\times$ is a character.

6.14. DEFINITION. Let $\chi_1, \ldots, \chi_n$ be characters of a group G in a field K. Then $\chi_1, \ldots, \chi_n$ are *linearly independent* if for $t_1, \ldots, t_n \in K$,

$$t_1\chi_1 + \cdots + t_n\chi_n = 0 \quad \Longrightarrow \quad t_1 = \cdots = t_n = 0.$$

If $\chi_1, \ldots, \chi_n$ are not linearly independent then they are *linearly dependent*.

In this definition, the functional equation means that for all $g \in G$,

$$t_1\chi_1(g) + \cdots + t_n\chi_n(g) = 0.$$

6.15. Theorem (Artin's Theorem). *Let $\chi_1, \ldots, \chi_n$ be distinct characters of a group G in a field K. Then $\chi_1, \ldots, \chi_n$ are linearly independent.*

Proof. We proceed by induction on n. For $n = 1$ the result is easily verified. For the inductive assumption, suppose that it holds for any $n \leqslant k$.

Let $\chi_1, \ldots, \chi_{k+1}$ be a set of $k+1$ distinct characters for which there are $t_1, \ldots, t_{k+1} \in K$ not all zero and such that

$$t_1\chi_1 + \cdots + t_{k+1}\chi_{k+1} = 0. \tag{6.2}$$

If one of the t_i is zero, say $t_r = 0$, then $\chi_1, \ldots, \chi_{r-1}, \chi_{r+1}, \ldots, \chi_{k+1}$ is linearly dependent, contradicting the inductive assumption. Hence all of the t_i must be non-zero. As $\chi_1 \neq \chi_2$, there must be an element $g_0 \in G$ for which $\chi_1(g_0) \neq \chi_2(g_0)$. So for all $g \in G$, Equation (6.2) applied to $g_0 g$ yields

$$t_1\chi_1(g_0g) + \cdots + t_{k+1}\chi_{k+1}(g_0g) = 0,$$

and therefore since $\chi_j(g_0g) = \chi_j(g_0)\chi_j(g)$, we see that

$$t_1\chi_1(g_0)\chi_1 + \cdots + t_{k+1}\chi_{k+1}(g_0)\chi_{k+1} = 0.$$

Multiplying Equation (6.2) by $\chi_1(g_0)$ and subtracting gives

$$t_2(\chi_2(g_0) - \chi_1(g_0))\chi_2 + t_3(\chi_3(g_0) - \chi_1(g_0))\chi_3 + \cdots + t_{k+1}(\chi_{k+1}(g_0) - \chi_1(g_0))\chi_{k+1} = 0,$$

in which the coefficient $t_2(\chi_2(g_0) - \chi_1(g_0))$ is not zero. Hence $\chi_2, \ldots, \chi_{k+1}$ is linearly dependent, again contradicting the inductive assumption. So $\chi_1, \ldots, \chi_{k+1}$ is linearly independent, which demonstrates the inductive step. □

6.16. Corollary. *Suppose that $\alpha_1, \ldots, \alpha_n$ are distinct automorphisms of the field K. Let $t_1, \ldots, t_n \in K$ be a sequence of elements, not all of which are 0. Then there is a $z \in K$ for which*

$$t_1\alpha_1(z) + \cdots + t_n\alpha_n(z) \neq 0.$$

Hence the K-linear transformation $t_1\alpha_1 + \cdots + t_n\alpha_n \colon K \longrightarrow K$ is non-trivial.

6.17. Corollary. *Let E/K be a finite Galois extension of degree n and let $\alpha_1, \ldots, \alpha_n$ be the distinct elements of $\mathrm{Gal}(E/K)$. Then the function $\alpha_1 + \cdots + \alpha_n \colon E \longrightarrow E$ is a non-trivial K-linear transformation whose image is contained in K. Hence the associated K-linear transformation*

$$\mathrm{Tr}_{E/K} \colon E \longrightarrow K; \quad \mathrm{Tr}_{E/K}(x) = \alpha_1(x) + \cdots + \alpha_n(x)$$

is surjective.

The function $\mathrm{Tr}_{E/K} \colon E \longrightarrow K$ is called the *trace mapping* of E/K.

Proof. First note that for $x \in E$ and $\gamma \in \mathrm{Gal}(E/K)$,

$$\gamma(\alpha_1(x) + \cdots + \alpha_n(x)) = \gamma\alpha_1(x) + \cdots + \gamma\alpha_n(x) = \alpha_1(x) + \cdots + \alpha_n(x),$$

since the list $\gamma\alpha_1, \ldots, \gamma\alpha_n$ is the same as $\alpha_1, \ldots, \alpha_n$ apart from its order. Hence,

$$\alpha_1(x) + \cdots + \alpha_n(x) \in E^{\mathrm{Gal}(E/K)} = K.$$

The rest of the statement follows directly from Corollary 6.16. □

Suppose that E/K is a finite Galois extension with cyclic Galois group $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ of order n. For each $u \in E^\times$, the element $u\sigma(u)\cdots\sigma^{n-1}(u) \in E$ satisfies

$$\sigma(u\sigma(u)\cdots\sigma^{n-1}(u)) = \sigma(u)\cdots\sigma^{n-1}(u)\sigma^n(u) = \sigma(u)\cdots\sigma^{n-1}(u)u,$$

hence in $u\sigma(u)\cdots\sigma^{n-1}(u) \in E^{\langle\sigma\rangle} = K$. Now using this we define a group homomorphism

$$\mathrm{N}_{E/K}\colon E^\times \longrightarrow K^\times; \quad \mathrm{N}_{E/K}(u) = u\sigma(u)\cdots\sigma^{n-1}(u).$$

$\mathrm{N}_{E/K}$ is called the *norm mapping* for E/K and generalizes the norm mapping for finite fields of Section 5.3.

There is another homomorphism

$$\delta_{E/K}\colon E^\times \longrightarrow E^\times; \quad \delta_{E/K}(u) = u\sigma(u)^{-1}.$$

Notice that for $u \in E^\times$,

$$\mathrm{N}_{E/K}(\delta_{E/K}(u)) = (u\sigma(u)^{-1})(\sigma(u)\sigma^2(u)^{-1}\cdots\sigma^{n-1}(u)\sigma^n(u)^{-1}) = 1,$$

since $\sigma^n(u) = u$. So $\operatorname{im}\delta_{E/K} \leqslant \ker \mathrm{N}_{E/K}$. Our next result is an important generalization of Proposition 5.27.

6.18. Theorem (Hilbert's Theorem 90). *Let E/K be a finite Galois extension with cyclic Galois group $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ of order n. Then $\operatorname{im}\delta_{E/K} = \ker \mathrm{N}_{E/K}$. Explicitly, if $u \in E^\times$ and $u\,\sigma(u)\cdots\sigma^{n-1}(u) = 1$, then there is a $v \in E^\times$ such that $u = v\sigma(v)^{-1}$.*

Proof. Let $u \in \ker \mathrm{N}_{E/K}$.

The characters $\sigma^k\colon E^\times \longrightarrow E^\times$ with $k = 0, 1, \ldots, n-1$ are distinct and linearly independent by Artin's Theorem 6.15. Consider the function

$$\mathrm{id} + u\sigma + u\sigma(u)\sigma^2 + \cdots + u\sigma(u)\cdots\sigma^{n-2}(u)\sigma^{n-1}\colon E^\times \longrightarrow E.$$

This cannot be identically zero, so for some $w \in E$, the element

$$v = w + u\sigma(w) + u\sigma(u)\sigma^2(w) + \cdots + u\sigma(u)\cdots\sigma^{n-2}(u)\sigma^{n-1}(w)$$

is non-zero. Notice that

$$u\sigma(v) = u\sigma(w) + u\sigma(u)\sigma^2(w) + u\sigma(u)\sigma^2(u)\sigma^3(w) + \cdots + u\sigma(u)\sigma^2(u)\cdots\sigma^{n-1}(u)\sigma^n(w) = v,$$

since

$$u\sigma(u)\sigma^2(u)\cdots\sigma^{n-1}(u)\sigma^n(w) = w.$$

Thus we have $u = v\sigma(v)^{-1}$ as required. □

6.4. Simple radical extensions

In this section we will investigate splitting fields of polynomials of the form $X^n - a$, where $\mathrm{char}\, K \nmid n$. We call these *simple radical extensions* and later in Definition 6.33 we introduce a more general notion of *radical extension*.

6.19. Proposition. *Let $f(X) = X^n - a \in K[X]$ be irreducible and separable over K. Then the splitting field of $f(X)$ over K has the form $K(u, \zeta)$, where u is a root of $f(X)$ and ζ is a primitive n-th root of 1.*

6.20. Corollary. *If K contains a primitive n-th root of 1, ζ, then the splitting field of $f(X) = X^n - a$ over K has the form $K(u)$, where u is a root of $f(X)$. The Galois group* $\mathrm{Gal}(K(u)/K)$ *is cyclic of order n with a generator σ for which $\sigma(u) = \zeta u$.*

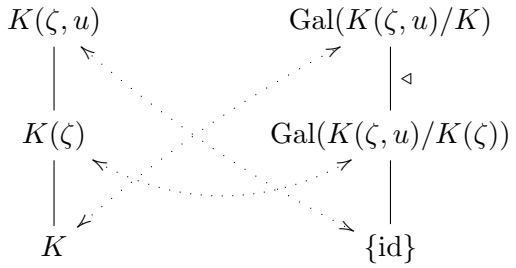
In the more general situation of Proposition 6.19,

$$\{\mathrm{id}\} \lhd \mathrm{Gal}(K(\zeta,u)/K(\zeta)) \lhd \mathrm{Gal}(K(\zeta,u)/K),$$

where $\mathrm{Gal}(K(\zeta,u)/K(\zeta))$ is cyclic and

$$\mathrm{Gal}(K(\zeta)/K)) \cong \mathrm{Gal}(K(\zeta,u)/K))/\,\mathrm{Gal}(K(\zeta,u)/K(\zeta))$$

is abelian. The Galois Correspondence identifies the following towers of subfields and subgroups.



6.21. Definition. Let K be a field with $\mathrm{char}\, K \nmid n$ and which contains a primitive n-th root of 1, ζ say. Then L/K is a *simple n-Kummer extension* if $L = K(u)$ where $u^n = a$ for some $a \in K$. L/K is an (*iterated*) *n-Kummer extension* if $L = K(u_1, \ldots, u_k)$ where $u_1^n = a_1,\ \ldots,\ u_k^n = a_k$ for some elements $a_1, \ldots, a_k \in K$.

Note that in this definition we do not require the polynomials $X^n - a_j \in K[X]$ to be irreducible.

6.22. Proposition. *Let $K(u)/K$ be a simple n-Kummer extension. Then $K(u)/K$ is a Galois extension and* $\mathrm{Gal}(K(u)/K)$ *is cyclic with order dividing n.*

Proof. Suppose that $u^n = a \in K$. Then in $\overline{K}[X]$ we have

$$X^n - a = (X-u)(X-\zeta u)\cdots(X-\zeta^{n-1}u).$$

Clearly the roots of $X^n - a$ are distinct and so $K(u)/K$ is separable over K; in fact, $K(u)$ is a splitting field of $X^n - a$ over K. This means that $K(u)/K$ is Galois.

For each $\alpha \in \mathrm{Gal}(K(u)/K)$ we have $\alpha(u) = \zeta^{r_\alpha} u$ for some $r_\alpha = 0, 1 \ldots, n-1$. Notice that for $\beta \in \mathrm{Gal}(K(u)/K)$,

$$\beta\alpha(u) = \beta(\zeta^{r_\alpha}u) = \zeta^{r_\alpha}\beta(u) = \zeta^{r_\alpha}\zeta^{r_\beta}u = \zeta^{r_\alpha + r_\beta}u,$$

and so $r_{\beta\alpha} = r_\alpha + r_\beta$. Hence the function

$$\rho\colon\ \mathrm{Gal}(K(u)/K) \longrightarrow \langle\zeta\rangle\,; \quad \rho(\alpha) = \zeta^{r_\alpha},$$

is a group homomorphism. As $\langle\zeta\rangle$ is cyclic of order n, Lagrange's Theorem implies that the image of ρ has order dividing n. Since every element of $\mathrm{Gal}(K(u)/K)$ is determined by its effect on u, ρ is injective, hence $|\,\mathrm{Gal}(K(u)/K)|$ divides n. In fact, $\mathrm{Gal}(K(u)/K)$ is cyclic since every subgroup of a cyclic group is cyclic. □

6.23. Example. Let $n \geqslant 1$ and $q \in \mathbb{Q}$. Then $\mathbb{Q}(\zeta_n, \sqrt[n]{q})/\mathbb{Q}(\zeta_n)$ is a simple n-Kummer extension.

6.24. Example. $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(i)$ is a simple 4-Kummer extension with $\mathrm{Gal}(\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}(i))$ cyclic of order 2.

Proof. We have $(\sqrt{2})^4 - 4 = 0$, but

$$X^4 - 4 = (X^2 - 2)(X^2 + 2),$$

and

$$X^2 - 2 = \mathrm{minpoly}_{\mathbb{Q}(i),\sqrt{2}}(X).$$

The corresponding group homomorphism $\rho\colon \mathrm{Gal}(\mathbb{Q}(i)(\sqrt{2})/\mathbb{Q}(i)) \longrightarrow \langle i\rangle$ has image

$$\mathrm{im}\,\rho = \{1,-1\} \leqslant \langle i\rangle\,. \qquad \square$$

Here is a converse to Proposition 6.22.

6.25. Proposition. *Suppose that* $\mathrm{char}\,K \nmid n$ *and there is an element* $\zeta \in K$ *which is a primitive* n*-th root of unity. If* E/K *is a finite Galois extension with cyclic Galois group of order* n*, then there is an element* $a \in E$ *such that* $E = K(a)$ *and* a *is a root of a polynomial of the form* $X^n - b$ *with* $b \in K$*. Hence* E/K *is a simple* n*-Kummer extension.*

Proof. We have

$$\mathrm{N}_{E/K}(\zeta^{-1}) = \zeta^{-n} = 1,$$

so by Hilbert's Theorem 6.18, there is an element $a \in E$ for which $\zeta^{-1} = a\sigma(a)^{-1}$. Then $\sigma(a) = \zeta a$ and the elements $\sigma^k(a) = \zeta^k a$ for $k = 0, 1, \ldots, n-1$ are distinct, so they must be the n conjugates of a. Also note that

$$X^n - a^n = (X-a)(X-\zeta a)\cdots(X-\zeta^{n-1}a) = (X-a)(X-\sigma(a))\cdots(X-\sigma^{n-1}(a)),$$

hence $a^n \in K$ since it is fixed by σ. Since $K(a) \leqslant E$, this shows that

$$n = [K(a):K] \leqslant [E:K] = n$$

and therefore

$$[K(a):K] = [E:K] = n,$$

whence $K(a) = E$. $\square$

6.5. Solvability and radical extensions

We begin by recalling some ideas about groups, see [**3, 5**] for further details.

6.26. Definition. A group G is *solvable*, *soluble* or *soluable* if there is a chain of subgroups (called a *subnormal series*)

$$\{1\} = G_\ell \leqslant G_{\ell-1} \leqslant \cdots \leqslant G_1 \leqslant G_0 = G$$

in which $G_{k+1} \triangleleft G_k$ and each *composition factor* G_k/G_{k+1} is abelian; we usually write

$$\{1\} = G_\ell \triangleleft G_{\ell-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G.$$

If each composition factor is a cyclic group of prime order the subnormal series is called a *composition series*. A group which is not solvable is called *insolvable*.

6.27. Remark. It is a standard result that we can always refine (*i.e.*, add extra terms) a subnormal series of a solvable group to obtain a composition series. The primes appearing as well as the number of times each occurs are all determined by $|G|$, only their order varying for different composition series.

6.28. Example. Let G be a finite abelian group. Then G is solvable.

6.29. Example. Let G be a finite p-group, where p is a prime. Then G is solvable.

In fact, for a finite p-group G, there is always a normal subgroup of a p-group with index p, so in this case we can assume each quotient G_k/G_{k+1} is cyclic of order p.

6.30. Proposition. *Let G be a group.*

(i) *If G is solvable then every subgroup $H \leqslant G$ and every quotient group G/N is solvable.*
(ii) *If $N \lhd G$ and G/N are solvable then so is G.*

In the opposite direction we can sometimes see that a group is insolvable. Recall that a group is *simple* if it has no non-trivial proper normal subgroups.

6.31. Proposition. *Let G be a finite group. Then G is insolvable if any of the following conditions holds:*

(i) *G contains a subgroup which is a non-abelian simple group.*
(ii) *G has a quotient group which is a non-abelian simple group.*
(iii) *G has a composition series in which one of the terms is a non-abelian simple group.*

6.32. Example. For $n \geqslant 5$, the alternating and symmetric groups A_n and S_n are insolvable.

Proof. This follows from the fact that if $n \geqslant 5$, A_n is a simple group and $\mathrm{A}_n \lhd \mathrm{S}_n$ with quotient group $\mathrm{S}_n/\mathrm{A}_n \cong \mathbb{Z}/2$. □

Now we explain how this relates to fields and their extensions. Let K be a field and L/K a finite extension. For simplicity, we assume also that $\operatorname{char} K = 0$.

6.33. Definition. L/K is a *radical extension* of K if it has the form $L = K(a_1, a_2, \ldots, a_n)$ with

$$a_k^{d_k} \in K(a_1, a_2, \ldots, a_{k-1})$$

for some $d_k \geqslant 1$. Thus every element of L is expressible in terms of iterated roots of elements of K.

We will need the following Lemma and its Corollary. According to [**4**], several text books make subtle errors or omissions related to this result, so beware when reading other sources!

6.34. Lemma. *Let L/K be a finite Galois extensions and let $L(u)/L$ be a radical extension. Let E/L be an extension where E is a splitting field for the polynomial* $\operatorname{minpoly}_{K,u}(X) \in L[X]$. *Then E/L is a radical Galois extension. In particular, if L/K is a radical Galois extension then so is E/K.*

Proof. Suppose that $u^d = a \in L$ with $a \neq 0$. Then $X^d - a$ has a d distinct roots in E, and if v is any other root then $(v/u)^d = 1$, so there are d distinct d-th roots of unity in E. Hence there is a primitive d-th root of unity $\zeta \in E$ and the subfield $L(\zeta, u) \leqslant E$ is normal over

L, so $L(\zeta,u)/L$ is a radical Galois extension. But $L(\zeta,u)/K$ need not be Galois. However, if $u=u_1,\dots,u_t\in E$ are the distinct roots of $\operatorname{minpoly}_{K,u}(X)$ in E, then

$$E=L(\zeta,u,u_1,\dots,u_t).$$

But this is clearly a radical extension of L.

If L/K is a radical Galois extension, say $L=K(a_1,\dots,a_n)$, then

$$E=L(a_1,\dots,a_n,\zeta,u,u_1,\dots,u_t),$$

which is a radical Galois extension of K. □

6.35. Corollary. *If L/K is a radical extension then it is contained in a radical Galois extension L'/K.*

Proof. Writing $L=K(a_1,a_2,\dots,a_n)$ as in Definition 6.33, this is proved by induction on n using Lemma 6.34. □

In the next definition, the word Galois is superfluous because of the preceding results.

6.36. Definition. If L is the splitting field of a polynomial $f(X)\in K[X]$, then $f(X)$ is *solvable by radicals* over K if L is contained in a radical (Galois) extension of K.

6.37. Definition. L/K is *solvable* if $L\leqslant L'$ where L'/K is a finite radical Galois extension of K.

6.38. Theorem. *Let E/K be a finite Galois extension. Then E/K is solvable if and only if the group* $\operatorname{Gal}(E/K)$ *is solvable.*

Proof. Suppose that $E\leqslant E'$ where E'/K is a finite radical Galois extension, so

$$E'=K(\zeta,u_1,\dots,u_m),$$

where $\zeta^d=1$, $u_1^{d_1}\in K(\zeta)$ and $u_r^{d_r}\in K(\zeta,u_1,\dots,u_{r-1})$ for $r=2,\dots,m$ with $d_1\cdots d_m\mid d$. If $G_r\lhd\operatorname{Gal}(E'/K)$ and

$$(E')^{G_r}=K(\zeta,u_1,\dots,u_r),$$

with

$$(E')^{G_0}=K(\zeta),$$

then

$$\{1\}=G_m\lhd G_{m-1}\lhd\cdots\lhd G_0\lhd\operatorname{Gal}(E'/K)$$

and

$$G_{r-1}/G_r\cong\operatorname{Gal}(K(\zeta,u_1,\dots,u_r)/K(\zeta,u_1,\dots,u_{r-1})),$$

which is abelian by Proposition 6.22. Hence $\operatorname{Gal}(E'/K)$ is solvable, and since $\operatorname{Gal}(E/K)$ is a quotient group of $\operatorname{Gal}(E'/K)$, is also solvable by Proposition 6.30.

Now suppose that $\operatorname{Gal}(E/K)$ is solvable and let $n=|\operatorname{Gal}(E/K)|$. Let E' be the splitting field of X^n-1 over E, so E' contains a primitive n-th root of unity ζ and therefore it contains a primitive d-th root of unity for every divisor d of n. Now $\operatorname{Gal}(E'/E)\lhd\operatorname{Gal}(E'/K)$ and by Theorem 6.7, $\operatorname{Gal}(E'/E)$ is abelian. Also, $\operatorname{Gal}(E'/K)/\operatorname{Gal}(E'/E)\cong\operatorname{Gal}(E/K)$ which is solvable, so $\operatorname{Gal}(E'/K)$ is solvable by Proposition 6.30. We will now show that E'/K is a radical extension.

Clearly $K(\zeta)/K$ is radical. Then $\mathrm{Gal}(E'/K(\zeta)) \lhd \mathrm{Gal}(E'/K)$ is solvable. Let

$$\{1\} = G_\ell \lhd G_{\ell-1} \lhd \cdots \lhd G_1 \lhd G_0 = \mathrm{Gal}(E'/K(\zeta))$$

be a composition series. The extension $(E')^{G_1}/K(\zeta)$ is radical by Proposition 6.25. Similarly, each extension $(E')^{G_{k+1}}/(E')^{G_k}$ is radical. Hence $E'/K(\zeta)$ is radical, as is E'/K. □

6.39. Example. The Galois group of the extension $\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}$ is solvable.

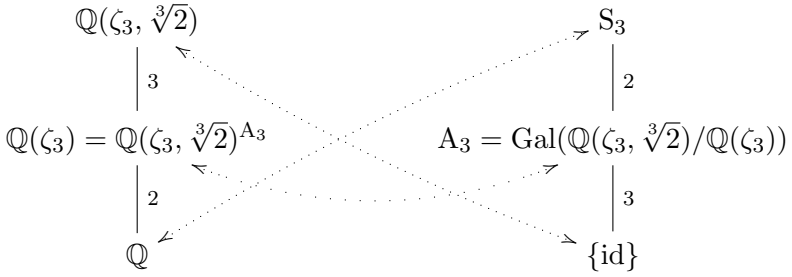
Proof. We have already studied this extension in Example 3.30 and 4.20. Clearly $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ is a radical extension of $\mathbb{Q}$ and

$$\mathbb{Q}(\zeta_3, \sqrt[3]{2}) = \mathbb{Q}(\zeta_3)(\sqrt[3]{2}).$$

We know that $\mathrm{Gal}(\mathbb{Q}(\zeta_3, \sqrt[3]{2})/\mathbb{Q}) \cong \mathrm{S}_3$, where we identify each element of the Galois group with a permutation of the three roots of $X^3 - 2$ in $\mathbb{Q}(\zeta_3, \sqrt[3]{2})$ which we list in the order

$$\sqrt[3]{2},\ \sqrt[3]{2}\,\zeta_3,\ \sqrt[3]{2}\,\zeta_3^2.$$

We have the following towers of subfields and subgroups related under the Galois Correspondence.



Here $\mathbb{Q}(\zeta_3)/\mathbb{Q}$ is itself a Galois extension and $\mathrm{A}_3 \lhd \mathrm{S}_3$. Notice that $\mathrm{A}_3 \cong \mathbb{Z}/3$ and $\mathrm{S}_3/\mathrm{A}_3 \cong \mathbb{Z}/2$, so we have the following composition series for S_3:

$$\{\mathrm{id}\} \lhd \mathrm{A}_3 \lhd \mathrm{S}_3.$$ □

It is also interesting to reverse the question and ask whether there are extensions which are *not* solvable. This was a famous problem pursued for several hundred years. To find examples, we first recall that the smallest non-abelian simple group is A_5 which has order 60. We should therefore expect to look for a polynomial of degree at least 5 to find a Galois group for a splitting field to be simple or occur as a composition factor of such a Galois group. Here is an explicit example over $\mathbb{Q}$.

6.40. Example. The splitting field of the polynomial $f(X) = X^5 - 35X^4 + 7 \in \mathbb{Q}[X]$ is not solvable.

Proof. Let $E \leqslant \mathbb{C}$ be the splitting field of $f(X)$ over $\mathbb{Q}$. Using the Eisenstein Test 1.38 with $p = 7$, we find that $f(X)$ is irreducible over $\mathbb{Q}$. By Theorem 4.8(iii), 5 divides the order of $\mathrm{Gal}(E/\mathbb{Q})$, so by Cauchy's Lemma this group contains an element of order 5.

Now observe that

$$f'(X) = 5X^4 - 140X^3 = 5X^3(X - 28), \quad f''(X) = 20X^4 - 420X^2 = 20X^2(X - 21).$$

There are two turning points, namely a maximum at $x = 0$ and a minimum at $x = 28$. Then

$$f(0) = 7 > 0 > f(28) = -4302585,$$

hence there are three real roots of $f(X)$ and two non-real complex ones. Then complex conjugation restricts to an element of order 2 in $\mathrm{Gal}(E/\mathbb{Q})$ which interchanges the non-real roots and fixes the others. If we list the roots of $f(X)$ as u_1, u_2, u_3, u_4, u_5 with u_1, u_2 being the non-real roots, then the transposition $(1\ 2) \in \mathrm{S}_5$ corresponds to this element. Furthermore, the only elements of S_5 of order 5 are 5-cycles; by taking an appropriate power we can assume that there is a 5-cycle of the form $(1\ 2\ 3\ 4\ 5)$ corresponding to an element of $\mathrm{Gal}(E/\mathbb{Q})$ which we can view as a subgroup of S_5. The next lemma shows that $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathrm{S}_5$.

6.41. Lemma. *Let $n \geqslant 1$. Suppose that $H \leqslant \mathrm{S}_n$ and H contains the elements $(1\ 2)$ and $(1\ 2\ \cdots\ n)$. Then $H = \mathrm{S}_n$.*

The proof is left as an exercise. This completes the verification of Example 6.40. □

It is worth remarking that the most extreme version of this occurs when we ask for a Galois group which is *simple*. There has been a great deal of research activity on this question in the past few decades, but apparently not all simple groups are known to occur as Galois groups of extensions of $\mathbb{Q}$ or other finite subextensions of $\mathbb{C}/\mathbb{Q}$. Here is an example whose Galois group is A_5; this is verified using Proposition 4.26.

6.42. Example. The Galois group of $f(X) = X^5 + 20X + 16$ over $\mathbb{Q}$ is $\mathrm{Gal}(\mathbb{Q}(f(X))/\mathbb{Q}) \cong \mathrm{A}_5$, hence it is not solvable.

6.6. Symmetric functions

Let k be a field. Consider the polynomial ring on n indeterminates $\Bbbk[X_1, \ldots, X_n]$ and its field of fractions $K = \Bbbk(X_1, \ldots, X_n)$. Each permutation $\sigma \in \mathrm{S}_n$ acts on $\Bbbk[X_1, \ldots, X_n]$ by

$$\sigma \cdot f(X_1, \ldots, X_n) = f^\sigma(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

Viewed as a function $\sigma\cdot\colon \Bbbk[X_1, \ldots, X_n] \longrightarrow \Bbbk[X_1, \ldots, X_n]$ is a ring isomorphism; this extends to a ring isomorphism $\sigma\cdot\colon \Bbbk(X_1, \ldots, X_n) \longrightarrow \Bbbk(X_1, \ldots, X_n)$. Varying σ we obtain actions of the group S_n on $\Bbbk[X_1, \ldots, X_n]$ and $\Bbbk(X_1, \ldots, X_n)$ by ring isomorphisms fixing $\Bbbk$ and in the latter case it is by field automorphisms fixing $\Bbbk$.

6.43. Definition. The field of *symmetric functions on n indeterminates* is

$$\mathrm{Sym}_n(\Bbbk) = \Bbbk(X_1, \ldots, X_n)^{\mathrm{S}_n} \leqslant \Bbbk(X_1, \ldots, X_n).$$

So if $f(X_1, \ldots, X_n) \in \Bbbk(X_1, \ldots, X_n)$, then

$$f(X_1, \ldots, X_n) \in \mathrm{Sym}_n(\Bbbk) \quad \Longleftrightarrow \quad \forall \sigma \in \mathrm{S}_n\ f(X_1, \ldots, X_n) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}).$$

6.44. Theorem. *The extension $\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk)$ is a finite Galois extension for which $\mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk)) \cong \mathrm{S}_n$.*

Proof. There are elements of $\Bbbk[X_1, \ldots, X_n] \subseteq \Bbbk(X_1, \ldots, X_n)$ called *elementary symmetric functions*,

$$e_k = \sum_{i_1 < i_2 < \cdots < i_k} X_{i_1} X_{i_2} \cdots X_{i_k},$$

where $1 \leqslant k \leqslant n$. It is easy to see that for every $\sigma \in \mathrm{S}_n$, $e_k^\sigma = e_k$, so $e_k \in \mathrm{Sym}_n(\Bbbk)$. Working in the ring $\Bbbk(X_1, \ldots, X_n)[Y]$ we have

$$f_n(Y) = Y^n - e_1 Y^{n-1} + \cdots + (-1)^{n-1} e_{n-1} Y + (-1)^n e_n = 0,$$

hence the roots of this polynomial are the X_i. So $\Bbbk(X_1, \ldots, X_n)$ is the splitting field of $f_n(Y)$ over $\mathrm{Sym}_n(\Bbbk)$. Now $\mathrm{S}_n \leqslant \mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk))$, hence

$$[\Bbbk(X_1, \ldots, X_n) : \mathrm{Sym}_n(\Bbbk)] = |\mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk))| \geqslant |\mathrm{S}_n| = n!.$$

But as every element of $\mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk))$ permutes the roots of $f_n(Y)$ and is determined by this permutation, we also have

$$n! \geqslant |\mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk))|.$$

Combining these inequalities we obtain $|\mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk))| = n!$ and therefore $\mathrm{Gal}(\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk)) = \mathrm{S}_n$. □

6.45. Remark. In fact, this proof shows that the extension $\Bbbk(X_1, \ldots, X_n)/\Bbbk(e_1, \ldots, e_n)$ is Galois of degree $n!$. Since $\Bbbk(e_1, \ldots, e_n) \leqslant \mathrm{Sym}_n(\Bbbk)$ we can also deduce that $\Bbbk(e_1, \ldots, e_n) = \mathrm{Sym}_n(\Bbbk)$. Hence every element of $\mathrm{Sym}_n(\Bbbk)$ is a rational function in the e_i. Analogous results are true for polynomials, *i.e.*,

$$\Bbbk[X_1, \ldots, X_n]^{\mathrm{S}_n} = \Bbbk[e_1, \ldots, e_n].$$

6.46. Corollary. *If $n \geqslant 5$, the extension $\Bbbk(X_1, \ldots, X_n)/\mathrm{Sym}_n(\Bbbk)$ is not solvable.*

Exercises on Chapter 6

6-1. Let $p > 0$ be a prime and G a group of order $|G| = p^n$ for some $n \geqslant 1$. Show by induction on n that there is a normal subgroup $N \triangleleft G$ with $|N| = p^{n-1}$. [*Hint: what do you know about the centre of G? Use this information to produce a quotient group of smaller order than G.*]

6-2. Let K be a field for which $\mathrm{char}\, K \neq 2$ and $n \geqslant 1$ be odd. If K contains a primitive n-th root of unity, show that then K contains a primitive $2n$-th root of unity.

6-3. Find all values of $n \geqslant 1$ for which $\varphi(n) \mid 4$. Using this, determine which roots of unity lie in the following fields:

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}\,i),\ \mathbb{Q}(\sqrt{3}\,i),\ \mathbb{Q}(\sqrt{5}\,i).$$

6-4. (a) Describe the elements of $(\mathbb{Z}/24)^\times$ explicitly and verify that this group is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$. Describe the effect of each element on $\mathbb{Q}(\zeta_{24})$ and $\mathbb{Q}(\cos(\pi/12))$ under the action described in Theorem 6.2.
(b) Determine the group $(\mathbb{Z}/20)^\times$ and describe the effect of each of its elements on $\mathbb{Q}(\zeta_{20})$ and $\mathbb{Q}(\cos(\pi/10))$ under the action described in Theorem 6.2.

6-5. Let $n \geqslant 1$.

(a) What can you say about $\sin(2\pi/n)$ and $\mathrm{Gal}(\mathbb{Q}(\sin(2\pi/n))/\mathbb{Q})$?
(b) Determine $\sin(\pi/12)$ and $\mathrm{Gal}(\mathbb{Q}(\sin(\pi/12))/\mathbb{Q})$.

6-6. In this question, work in the cyclotomic field $\mathbb{Q}(\zeta_5)$ where $\zeta_5 = e^{2\pi i/5}$.

(a) Describe the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ and its action on $\mathbb{Q}(\zeta_5)$.

(b) Determine the minimal polynomial of $\cos(2\pi/5)$ over $\mathbb{Q}$. Hence show that

$$\cos(2\pi/5) = \frac{-1+\sqrt{5}}{4}.$$

For which other angles θ is $\cos\theta$ a root of this minimal polynomial? What is the value of $\sin(2\pi/5)$?

(c) Find the tower of subfields of $\mathbb{Q}(\zeta_5)$ and express them as fixed fields of subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$.

6-7. In this question, let p be an odd prime and let $\zeta_p = e^{2\pi i/p} \in \mathbb{Q}(\zeta_p) \leqslant \mathbb{C}$.

(a) Consider the product

$$\xi = \prod_{r=1}^{(p-1)/2} (\zeta_p^r - \zeta_p^{-r}) \in \mathbb{Q}(\zeta_p).$$

Show that

$$\xi^2 = (-1)^{(p-1)/2} \prod_{r=1}^{p-1} (1-\zeta_p^r).$$

(b) Deduce that

$$\xi^2 = \begin{cases} p & \text{if } p \equiv 1 \pmod 4, \\ -p & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

(c) Conclude that

$$\xi = \begin{cases} \pm\sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ \pm\sqrt{p}\,i & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

and also $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ if $p \equiv 1 \pmod 4$ and $\sqrt{p}\,i \in \mathbb{Q}(\zeta_p)$ if $p \equiv 3 \pmod 4$.

6-8. Prove Lemma 6.41. [*Hint: show that every 2-cycle of the form* $(i\ i+1)$ *is in* H *by considering elements of the form* $(1\ 2\ \cdots\ n)^r(1\ 2)(1\ 2\ \cdots\ n)^{n-r}$.]

6-9. *This question is about an additive version of Hilbert's Theorem 90, see Theorem 6.18.* Let E/K be a Galois extension with cyclic Galois group $\mathrm{Gal}(E/K) = \langle\sigma\rangle$ of order n.

(a) Show that the function

$$T\colon E \longrightarrow E; \quad T(u) = u + \sigma(u) + \sigma^2(u) + \cdots + \sigma^{n-1}(u),$$

takes values in K and use this to define a K-linear mapping $\mathrm{Tr}_{E/K}\colon E \longrightarrow K$.

(b) If $v \in E$ has $\mathrm{Tr}_{E/K}(v) = 0$, show that there is a $w \in E$ such that $v = w - \sigma(w)$.

[*Hint: Show that there is an element* $t \in E$ *for which* $\mathrm{Tr}_{E/K}\, t \neq 0$*, then consider*

$$w = \frac{1}{(\mathrm{Tr}_{E/K}\, t)} \big(v\sigma(t) + (v+\sigma(v))\sigma^2(t) + \cdots + (v+\sigma(v)\sigma^2(t) + \cdots + \sigma^{n-2}(v))\sigma^{n-1}(t)\big)$$

and adapt the proof of Hilbert's Theorem 90 in Theorem 6.18, using $\mathrm{Tr}_{E/K}$ *in place of* $\mathrm{N}_{E/K}$.]

6-10. (a) For $n \geqslant 1$ and $1 \leqslant k \leqslant n$, the *$k$-th power sum* $s_k \in \Bbbk[X_1, \ldots, X_n]^{\mathrm{S}_n}$ is defined by

$$s_k = \sum_{1 \leqslant i \leqslant n} X_i^k.$$

Prove the formula

$$s_k = e_1 s_{k-1} - e_2 s_{k-2} + \cdots + (-1)^{k-1} e_{k-1} s_1 + (-1)^k k e_k.$$

(b) For $n \geqslant 1$ and $1 \leqslant k \leqslant n$, the *total symmetric function* is defined by

$$h_k = \sum_{j_1 \leqslant j_2 \leqslant \cdots \leqslant j_k} X_{j_1} X_{j_2} \cdots X_{j_k},$$

i.e., the sum of all the monomials in the X_i of degree k.

(i) For large values of n, express h_1, h_2, h_3 in terms of the elementary symmetric functions e_1, e_2, e_3.

(ii) Show that the power sum functions s_k of the previous question satisfy

$$s_k = -(h_1 s_{k-1} + h_2 s_{k-2} + \cdots + h_{k-1} s_1) + k h_k.$$

Bibliography

[1] E. Artin, Galois Theory, Dover Publications (1998); ISBN 0 486 62342 4.

[2] J-P. Escofier, Galois theory, Springer-Verlag, New York (2001); ISBN 0-387-98765-7. [*Highly recommended, especially for its historical notes*]

[3] J. B. Fraleigh, A First Course in Abstract Algebra, Addison Wesley (1999); ISBN 0 201 33596 4. [*Highly recommended*]

[4] T. W. Hungerford, A counterexample in Galois theory, American Mathematical Monthly **97** (1997), 54–57.

[5] S. Lang, Algebra, Addison Wesley (1993); ISBN 0 201 55540 9.

[6] R. Lidl & H. Niederreiter, Finite Fields, Cambridge University Press (1997); ISBN 0 521 39231 4.

[7] J. Rotman, Galois Theory, Springer-Verlag (1998); ISBN 0 387 98541 7.

[8] I. Stewart, Galois Theory, Chapman and Hall (1989); ISBN 0 412 34550-1. [*Very highly recommended.*]