Fields and Galois Theory

J.S. Milne

Version 4.22
March 30, 2011

A more recent version of these notes is available at www.jmilne.org/math/

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.

BibTeX information

```
@misc{milneFT,
  author={Milne, James S.},
  title={Fields and Galois Theory (v4.22)},
  year={2011},
  note={Available at www.jmilne.org/math/},
  pages={126}
}
```

v2.01 (August 21, 1996). First version on the web.
v2.02 (May 27, 1998). Fixed about 40 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; no change to numbering; 99 pages.
v4.00 (February 19, 2005). Minor corrections and improvements; added proofs to the section on infinite Galois theory; added material to the section on 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 problem with hyperlinks; 111 pages.
v4.22 (March 30, 2011). Minor changes; changed TEXstyle; 126 pages.

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

The photograph is of Sabre Peak, Moraine Creek, New Zealand.

Contents

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 $(a_i)_{i\in I}$, 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.

Dummit, D., and Foote, R.M., 1991, Abstract Algebra, Prentice Hall.
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, v3.11, 2011.
ANT Algebraic Number Theory, v3.02, 2009.

A reference monnnnn is to `http://mathoverflow.net/questions/nnnnn/`
PARI is an open source computer algebra system freely available from `http://pari.math.u-bordeaux.fr/`.

ACKNOWLEDGEMENTS

I thank the following for providing corrections and comments for earlier versions of the notes: Mike Albert, Maren Baumann, Leendert Bleijenga, Tommaso Centeleghe, Sergio Chouhy, Demetres Christofides, Antoine Chambert-Loir, Dustin Clausen, Keith Conrad, Hardy Falk, Jens Hansen, Albrecht Hess, Philip Horowitz, Trevor Jarvis, Henry Kim, Martin Klazar, Jasper Loy Jiabao, Dmitry Lyubshin, John McKay, Courtney Mewton, Shuichi Otsuka, Dmitri Panov, Alain Pichereau, David G. Radcliffe, Roberto La Scala, Prem L Sharma, Dror Speiser, Mathieu Vienney, Martin Ward (and class), Xiande YANG, and others.

CHAPTER 1

Basic Definitions and Results

Rings

A ***ring*** is a set R with two composition laws $+$ 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*** S of a ring R is a subset 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 with the properties

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

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:

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

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

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

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.

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 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 R is a commutative ring with no nontrivial 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*** $\alpha: F \to F'$ 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.

The characteristic of a field

One checks easily that the map

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

is a homomorphism of rings, and so its kernel is an ideal in $\mathbb{Z}$.

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

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

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 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

For more on the following, see Dummit and Foote 1991, Chapter 9. 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 defined by

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

For any ring R containing F as a subring and element r of R, there is a unique homomorphism $\alpha : F[X] \to R$ such that $\alpha(X) = r$ and $\alpha(a) = a$ for all $a \in F$.

1.6 ***Division algorithm***: given $f(X)$ and $g(X) \in F[X]$ 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 is a unique factorization domain.

1.7 From the division algorithm, it follows that an element a of F is a root of f (that is, $f(a) = 0$) if and only if $X - a$ 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 and $g \in F[X]$ have gcd $d(X)$. Euclid's algorithm constructs polynomials $a(X)$ and $b(X)$ such that

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

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 any 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 Euclidean division: typing `divrem(13,5)` in PARI returns $[2,3]$, meaning that $13=2\times5+3$, 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 Since $F[X]$ is an integral domain, we can form its field of fractions $F(X)$. Its elements are quotients f/g, f and g polynomials, $g\neq0$.

Factoring polynomials

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

PROPOSITION 1.11 *Suppose $r\in\mathbb{Q}$ is 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 let $r=c/d$, $c,d\in\mathbb{Z}$, $\gcd(c,d)=1$. 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 $\mathbb{Q}[X]$. 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 can remove all the prime factors of mn, and so obtain a factorization of f in $\mathbb{Z}[X]$. □

PROPOSITION 1.14 *If $f \in \mathbb{Z}[X]$ is monic, then any 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. □

REMARK 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 $\mathbb{C}$ — for an elementary proof of this, using nothing but the symmetric polynomials theorem (5.33), see Theorem 1.16 of my notes on algebraic geometry. 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:

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

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

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

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

$b_i, c_i \in \mathbb{Z}$, $r, s < m$. 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 with $\mathbb{Z}$ replaced by any unique factorization domain.

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. 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 $\bar{f} = \bar{g}\bar{h}$ 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). Such an E can be regarded as an F-vector space, and we write $[E\colon F]$ for the dimension, possibly infinite, of E as an F-vector space. This dimension is called the ***degree*** of E over F. We say that E is ***finite*** over F when it has finite degree over 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 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, R., Amer. Math. Monthly, **93** (1986), pp286–288, which proves that every nonprime integer $n \geq 1$ occurs as the degree of a polynomial in $\mathbb{Z}[X]$ 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) *Let $L \supset E \supset F$ (all fields and subfields). 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 of finite degree over F, then it is certainly of finite degree 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, 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 $a_{ij} = 0$.□

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 $X + (f(X))$. Then:

(a) The map

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

is a surjective homomorphism in which $f(X)$ maps to 0. Therefore, $f(x) = 0$.

(b) From the division algorithm, we know 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

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

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

(d) To multiply two elements expressed in the form (*), 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 $f(X)$ is irreducible. To find the inverse of an element $\alpha \in F[x]$, use (b) to write $\alpha = g(x)$ with $g(X)$ is 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 can conclude:

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

$$F[x] = F[X]/(f(X))$$

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

EXAMPLE 1.22 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 1.23 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

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

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 $F[X]$. We say that $F[\alpha]$ is a ***stem field***[4] for f if $f(\alpha) = 0$. Then

$$\alpha \leftrightarrow x : F[\alpha] \simeq F[x], \quad F[x] = F[X]/f(X).$$

Therefore, stem fields always exist, and each element of a stem field $F[\alpha]$ for f has a unique expression

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

i.e., $1, \alpha, \ldots, \alpha^{m-1}$ is a basis for $F[\alpha]$ over F. Arithmetic in $F[\alpha]$ can be performed using the same rules as in $F[x]$. If $F[\alpha']$ is a second stem field for f, then there is a unique F-isomorphism $F[\alpha] \to F[\alpha']$ sending α to α'.

The subring generated by a subset

An intersection of subrings of a ring is again a ring. 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 evidently the smallest subring of E containing 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 $F[S]$. When $S = \{\alpha_1, ..., \alpha_n\}$, we write $F[\alpha_1, ..., \alpha_n]$ for $F[S]$. For example, $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$.

LEMMA 1.24 *The ring $F[S]$ consists of the elements of E that can be expressed as finite sums of the form*

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

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

EXAMPLE 1.25 The ring $\mathbb{Q}[\pi]$, $\pi = 3.14159...$, consists of the complex 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 (*) will *not* be unique in general. This is so already in $\mathbb{R}[i]$.

LEMMA 1.26 *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 subrings (containing F) of an extension field E of F of finite degree.

[4] Following A. Albert, Modern Higher Algebra, 1937, who calls the splitting field of a polynomial its root field. More formally, a stem field for f is a pair (E, α) consisting of a field E containing F and a generator α such that $f(\alpha) = 0$.

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 evidently the smallest subfield of E containing 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, since this is a subfield of E containing F and S and contained in any other such field. When $S = \{\alpha_1, ..., \alpha_n\}$, we write $F(\alpha_1, ..., \alpha_n)$ for $F(S)$. Thus, $F[\alpha_1, \dots, \alpha_n]$ consists of all elements of E that can be expressed as polynomials in the α_i with coefficients in F, and $F(\alpha_1, \dots, \alpha_n)$ consists of all elements of E that can be expressed as the quotient of two such polynomials.

Lemma 1.26 shows that $F[S]$ is already a field if it is finite dimensional over F, in which case $F(S) = F[S]$.

EXAMPLE 1.27 The field $\mathbb{Q}(\pi)$, $\pi = 3.14\dots$ consists of the complex numbers that can be expressed as a quotient

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

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 F and F' is evidently 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 $F \cdot F'$. It can also be described as the subfield of E generated over F by F', or the subfield generated over F' by F:

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

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 $f \in F[X]$,

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

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

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 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 sets of conditions:

f is monic; $f(\alpha) = 0$ and divides every other polynomial g in $F[X]$ with $g(\alpha) = 0$.

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 1.23 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+1. 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 field extension E/F 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*** (or 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 *A field extension E/F is finite if and only if E is algebraic and finitely generated (as a field) 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

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

this process terminates.

$\Longleftarrow$: Let $E=F(\alpha_1,\dots,\alpha_n)$ with $\alpha_1,\alpha_2,\dots\alpha_n$ 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 any subring R of E containing F is a field.*

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

PROOF. (a) We observed above (p. 18), that if α is algebraic over F, then $F[\alpha]$ is a field. If $\alpha \in R$, then $F[\alpha] \subset R$, and so α has an inverse in R.

(b) Any $\alpha \in L$ is a root of some monic polynomial $f = X^m + a_{m-1}X^{m-1} + \cdots + a_0 \in E[X]$. Now each of the extensions $F[a_0,\dots,a_{m-1},\alpha] \supset F[a_0,\dots,a_{m-1}] \supset F$ is finite (1.20), and so $F[a_0,\dots,a_{m-1},\alpha]$ is finite (hence 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).[5]

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.)

2004: Euler's constant

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

has not yet been proven to be transcendental or even irrational.

2004: 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.*

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 $A(N)$ be 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. Count the elements of $A(10)$; then count the elements of $A(100)$; then count the elements of $A(1000)$, and so on.[6] □

[5] In 1873 Cantor proved the rational numbers countable.... He also showed that the algebraic numbers... were countable. However his attempts to decide whether the real numbers were countable proved harder. He had proved that the real numbers were not countable by December 1873 and published this in a paper in 1874 (`http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Cantor.html`).

[6] More precisely, 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. 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 $x_N = f(\Sigma_N)$. If α is rational,[8] $f(X) = X - \alpha$; otherwise, $f(X)$, 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 $x_N \neq 0$. Evidently, $x_N \in \mathbb{Q}$; in fact $(2^{N!})^d D x_N \in \mathbb{Z}$, and so

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

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 (*). □

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

[8]In fact α is not rational because its expansion to base 2 is not periodic.

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 $\sqrt{c}$.

PROOF. (SKETCH) 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., 1991, Algebra, Prentice Hall, 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*

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

PROOF. (a) Immediate from (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 $\cos 60^\circ = \frac{1}{2}$, to construct α, we have to solve $8x^3-6x-1=0$, which is irreducible (apply 1.11). □

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[9], so also is $\sqrt{\pi}$. □

[9]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.

We now consider another famous old problem, that of constructing a regular polygon. Note that $X^m - 1$ is not irreducible; in fact

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

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 $\mathbb{Q}$.*

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

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + a_2 X^2 + a_1 X + p,$$

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

$$\cos\tfrac{2\pi}{p} = (e^{\frac{2\pi i}{p}} + (e^{\frac{2\pi i}{p}})^{-1})/2.$$

But

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

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

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

shows that it is ≤ 2, and it is not 1 because $\mathbb{Q}[e^{\frac{2\pi i}{p}}]$ is not contained in $\mathbb{R}$. Hence

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

Thus, if the regular p-gon is constructible, then $(p-1)/2 = 2^k$ for some k (later (5.12), we shall see a converse), which implies $p = 2^{k+1} + 1$. But $2^r + 1$ can be a prime only if r is a power of 2, because otherwise r has an odd factor t and for t odd,

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

whence

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

Thus if the regular p-gon is constructible, then $p = 2^{2^k} + 1$ for some k. Fermat conjectured that all numbers of the form $2^{2^k} + 1$ are prime, and claimed to show that this is true for $k \leq 5$ — for this reason primes of this form are called ***Fermat primes.*** For $0 \leq k \leq 4$, the numbers $p = 3, 5, 17, 257, 65537$, are prime but Euler showed that $2^{32} + 1 = (641)(6700417)$, and we don't know of any more Fermat primes.

Gauss showed that[10]

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

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

[10] 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) $\Longrightarrow$ (b) $\Longrightarrow$ (c) $\Longrightarrow$ (a) are obvious.
(c) $\Longrightarrow$ (d). Let E be a finite extension of Ω. The minimum polynomial of any element α of E has degree 1, and so $\alpha \in \Omega$.
(d) $\Longrightarrow$ (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 said to be ***algebraically closed*** when it satisfies the equivalent statements of Proposition 1.42.

(b) A field Ω is said to be an ***algebraic closure*** of a subfield F when 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 1.21) that f has a root α in some finite extension Ω' of Ω. Set

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

and consider the fields

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

Each extension is algebraic and finitely generated, and hence finite (by 1.30). Therefore α lies in a finite extension of F, 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 (by 1.31) of finite degree over F (by 1.30). Thus, every element of $F[\alpha,\beta]$ is algebraic over F, including $\alpha\pm\beta$, α/β, $\alpha\beta$. □

The field constructed in the lemma 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 shall prove (using the axiom of choice) that every field has an algebraic closure.

Exercises

Exercises marked with an asterisk were required to be handed in.

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 any $a\in F$, 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 $(X-a)|f(X)$.
(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.

CHAPTER 2

Splitting Fields; Multiple Roots

Maps from simple extensions.

Let E and E' be fields containing F. An F-***homomorphism*** is a homomorphism

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

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

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

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. Note that if E and E' have the same finite degree over F, then every F-homomorphism is an F-isomorphism.

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*

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

(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 with coefficients in F. For any $\gamma \in \Omega$, there is a unique F-homomorphism $\varphi: F[\alpha] \to \Omega$ sending α to γ (see 1.5). This extends to the field of fractions $F(\alpha)$ of $F[\alpha]$ if and only if all nonzero elements of $F[\alpha]$ are sent to nonzero elements of Ω, which is so if and only if γ is transcendental.

(b) Let $f(X) = \sum a_i X^i$, and consider an F-homomorphism $\varphi: F[\alpha] \to \Omega$. On applying φ to the equation $\sum a_i \alpha^i = 0$, we obtain the equation $\sum a_i \varphi(\alpha)^i = 0$, 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 shall 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 of 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: if $f = \sum a_i X^i$ then $\varphi_0 f = \sum \varphi(a_i) X^i$. By an extension of φ_0 to $F(\alpha)$ we mean a homomorphism $\varphi: F(\alpha) \to \Omega$ such that $\varphi | F = \varphi_0$.

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 $E[X]$: $f(X) = \prod_{i=1}^{m}(X - \alpha_i)$ with $\alpha_i \in E$. If, in addition, E 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. Also, that if f has $\deg(f) - 1$ roots in E, then it splits in $E[X]$.

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 $\mathbb{C}$. Since the nonreal roots of f occur in conjugate pairs, either 1 or 3 of the α_i are real. 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 $[E_f : E] \leq n!$.□

REMARK 2.5 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 for $n > 1$ if $F = \mathbb{C}$ (see 5.6), nor for $n > 2$ if $F = \mathbb{F}_p$ (see 4.21) or $F = \mathbb{R}$. However, later (4.32) we shall see how to write down infinitely many polynomials of degree n in $\mathbb{Q}[X]$ whose splitting fields have 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) Suppose F is of characteristic p, and let $f = X^p - X - a \in F[X]$. If α is one root of f, then the remaining roots are $\alpha + 1, \ldots, \alpha + p - 1$, and so any field generated over F by α is a splitting field for f (and $F[\alpha] \simeq F[X]/(f)$ if f is irreducible).

(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 $f \in F[X]$. Let E be a field 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 each F-homomorphism $E \to \Omega$ is an isomorphism. In particular, any two splitting fields for f are F-isomorphic.*

PROOF. By f splitting in Ω, we mean that

$$f(X) = \prod_{i=1}^{\deg(f)} (X - \alpha_i), \quad \alpha_i \in \Omega,$$

in $\Omega[X]$. By f having distinct roots in Ω, we mean that $\alpha_i \neq \alpha_j$ if $i \neq j$.

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 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 assumption, $E = F[\alpha_1, \ldots, \alpha_m]$ with the α_i (some of the) roots of $f(X)$. The minimum polynomial of α_1 is an irreducible polynomial f_1 dividing f, and $\deg(f_1) = [F[\alpha_1] : F]$. 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 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 homomorphisms, $[E: F] \leq [\Omega: F]$. If E and Ω are both splitting fields for f, then (a) shows that there exist homomorphism $F \leftrightarrows E$, and so $[E: F] = [\Omega: F]$. Therefore, every F-homomorphism $E \to \Omega$ is an 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 f be the product of the minimum polynomials of the α_i. Let Ω be a splitting field for f regarded as an element of $L[X]$. The proposition shows that there is an F-homomorphism $E \to \Omega$, and the number of such homomorphisms is $\leq [E: F]$. 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. The corollary implies that there exists a finite extension Ω/L containing 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 is an F-isomorphism $E \to E'$, but there will in general be no *preferred* such isomorphism. Error and confusion can result if you simply identify the fields. 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

Let $f, g \in F[X]$. Even when f and g 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 $\Omega \supset F$. 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 $f \in F[X]$, and let

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

be a splitting of f in some extension field Ω of F. We say that α_i is a root of f of ***multiplicity*** m_i. If $m_i>1$, 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 (*) is independent of the extension field Ω in which f splits. 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 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 $X^p-a \overset{1.4}{=} (X-\alpha)^p$ in its splitting field. Thus an irreducible polynomial can have multiple roots.

Define the derivative $f'(X)$ of a polynomial $f(X)=\sum a_iX^i$ to be $\sum ia_iX^{i-1}$. 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 characteristic $p \neq 0$ and f is a polynomial in X^p;*
(d) *all the roots of f are multiple.*

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

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

Hence $f'(\alpha) = 0$, and so $\gcd(f, f') \neq 1$.

(b) $\implies$ (c). Since 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 the characteristic is $p \neq 0$ and f is a polynomial in X^p.

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

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

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

(d) $\implies$ (a). Obvious. □

DEFINITION 2.13 A polynomial $f \in F[X]$ is said to be ***separable over*** F if none of its irreducible factors has a multiple root (in a splitting field).[1]

The preceding discussion shows that $f \in F[X]$ will be separable unless

(a) the characteristic of F is $p \neq 0$, *and*
(b) at least one of the irreducible factors of f is a polynomial in X^p.

Note that, if $f \in F[X]$ is separable, then it remains separable over every field Ω containing F (condition (b) of 2.12 continues to hold — see 2.10).

DEFINITION 2.14 A field F is said to be ***perfect*** if all polynomials in $F[X]$ are separable (equivalently, all irreducible polynomials in $F[X]$ are separable).

PROPOSITION 2.15 *A field of characteristic zero is always perfect, and a field F of characteristic $p \neq 0$ is perfect if and only if every element of F is a pth power.*

PROOF. A field of characteristic zero is obviously perfect, and so we may suppose F to be of characteristic $p \neq 0$. If F contains an element a that is not a pth power, then $X^p - a \in F[X]$ is 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 $F[X]$,

$$\textstyle\sum a_i X^p = (\sum b_i X)^p \quad \text{if} \quad a_i = b_i^p,$$

and so is not irreducible. □

[1] This is the standard definition, although some authors, for example, Dummit and Foote 1991, 13.5, give a different definition.

EXAMPLE 2.16 (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.

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 any 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 gives a one-to-one correspondence between the subfields of the splitting field of a separable polynomial and the subgroups 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 (8.18) that by using the Axiom of Choice one can construct uncountably many more.

(b) Let $E = \mathbb{C}(X)$. Then $\mathrm{Aut}(E/\mathbb{C})$ consists of the maps[1] $X \mapsto \frac{aX+b}{cX+d}$, $ad-bc \neq 0$ (Jacobson 1964, IV, Theorem 7, p158), and so

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

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. This is not a coincidence: the field of meromorphic functions on the Riemann sphere $\mathbb{P}^1_{\mathbb{C}}$ is $\mathbb{C}(z) \simeq \mathbb{C}(X)$, and so there is certainly a map $\mathrm{Aut}(\mathbb{P}^1_{\mathbb{C}}) \to \mathrm{Aut}(\mathbb{C}(z)/\mathbb{C})$, which one can show to be 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 more X's, the group is unknown. (The group $\mathrm{Aut}(\mathbb{C}(X_1, \dots, X_n)/\mathbb{C})$ is the group of ***birational*** automorphisms of $\mathbb{P}^n_{\mathbb{C}}$. It is called the ***Cremona group.*** Its study is part of algebraic geometry.)

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

[1] By this I mean the map that sends a rational function $f(X)$ to $f(\frac{aX+b}{cX+d})$.

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

PROOF. Let $f = \prod f_i^{m_i}$, with the f_i irreducible and distinct. The splitting field of f is the same as the splitting field of $\prod f_i$. Hence we may assume f is a product of distinct separable irreducible polynomials, and so has $\deg f$ distinct roots in E. Now Proposition 2.7 shows that there are $[E:F]$ distinct F-homomorphisms $E \to E$. Because E has finite degree over F, they are automatically isomorphisms. □

EXAMPLE 3.3 (a) Consider a simple extension $E = F[\alpha]$, and let f be a polynomial with coefficients in F having α as a root. If f has no root in E other than α, then $\mathrm{Aut}(E/F) = 1$. For example, if $\sqrt[3]{2}$ denotes the real cube root of 2, then $\mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}) = 1$. Thus, in the proposition, it is essential that E be a *splitting* field.

(b) Let F be a field of characteristic $p \neq 0$, and let a be an element of F that is not a pth power. Then $f = X^p - a$ has only one root in a splitting field E, and so $\mathrm{Aut}(E/F) = 1$. Thus, in the proposition, it is essential 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 shall 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 $G = \{\sigma_1 = 1, \dots, \sigma_m\}$, and let $\alpha_1, \dots, \alpha_n$ be $n > m$ elements of E. We shall show that the α_i are linearly dependent over F. In the system of linear equations

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

there are m equations and $n > m$ unknowns, and hence there are nontrivial solutions in E — choose one $(c_1, \dots, c_n)$ having the fewest possible nonzero elements. After renumbering the α_i's, 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 $\sigma_1 = 1$) 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 and i, $k \neq 1 \neq i$. On applying σ_k to the equations

$$\begin{array}{c} \sigma_1(\alpha_1)c_1 + \cdots + \sigma_1(\alpha_n)c_n = 0 \\ \cdots \quad \cdots \\ \sigma_m(\alpha_1)c_1 + \cdots + \sigma_m(\alpha_n)c_n = 0 \end{array} \qquad (*)$$

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

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

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

COROLLARY 3.5 *For any finite group G of automorphisms of a field E, $G = \mathrm{Aut}(E/E^G)$.*

PROOF. We know that:

$[E:E^G] \leq (G:1)$ (by 3.4),

$G \subset \mathrm{Aut}(E/E^G)$ (obvious),

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

The inequalities

$$[E:E^G] \leq (G:1) \leq (\mathrm{Aut}(E/E^G):1) \leq [E:E^G]$$

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 said to be ***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 minimal polynomial is of the form $g(X^p)$, $g \in F[X]$.

For example, $E = \mathbb{F}_p(T)$ is an inseparable extension of $\mathbb{F}_p(T^p)$.

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 every irreducible polynomial $f \in F[X]$ having a root in E splits in E.

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

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

Therefore, E/F is normal and separable if and only if, for each $\alpha \in E$, the minimum polynomial of α has $[F[\alpha]:F]$ distinct roots in E.

EXAMPLE 3.8 (a) The field $\mathbb{Q}[\sqrt[3]{2}]$, where $\sqrt[3]{2}$ is the real cube root of 2, is separable but not normal over $\mathbb{Q}$ (X^3-2 doesn't split in $\mathbb{Q}[\alpha]$).

(b) The field $\mathbb{F}_p(T)$ is normal but not separable over $\mathbb{F}_p(T^p)$ — the minimum polynomial of T is the inseparable polynomial X^p-T^p.

DEFINITION 3.9 Let F be a field. A finite extension E of F is said to be ***Galois*** if F is the fixed field of the group of F-automorphisms of E. This group is then called the ***Galois group*** of E over F, and it is denoted $\mathrm{Gal}(E/F)$.

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) *$F = E^G$ for some finite group G of automorphisms of E.*
(c) *E is normal and separable, and of finite degree, over F.*
(d) *E is Galois over F.*

PROOF. (a) $\Longrightarrow$ (d). Let $G = \mathrm{Aut}(E/F)$, and let $F' = E^G \supset F$. Then E is also the splitting field of f regarded as a polynomial with coefficients in F', and f is still separable when it is regarded in this way. Hence Proposition 3.2 shows that

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

Since $\mathrm{Aut}(E/F') \overset{(3.5)}{=} G = \mathrm{Aut}(E/F)$, we conclude that $F = F'$, and so $F = E^G$.

(d) $\Longrightarrow$ (b). According to (2.8a) , $\mathrm{Gal}(E/F)$ is finite, and so this is obvious.

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

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

Any $\sigma \in G$ merely permutes the α_i. Since the a_i are symmetric polynomials in the α_i, we find that $\sigma a_i = a_i$ for all i, and so $g(X) \in F[X]$. It is monic, and $g(\alpha) = 0$, and so $f(X)|g(X)$ (see the definition of the minimum polynomial p. 17). But also $g(X)|f(X)$, because each α_i is a root of $f(X)$ (if $\alpha_i = \sigma\alpha$, then applying σ to the equation $f(\alpha) = 0$ gives $f(\alpha_i) = 0$). We conclude that $f(X) = g(X)$, and so $f(X)$ splits into distinct factors in E.

(c) $\Longrightarrow$ (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. Because E is normal over F, each f_i splits in E, and so E is the splitting field of $f = \prod f_i$. Because E is separable over F, f is separable. □

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

(b) Note that if $F = E^G$ for some finite group G, then, because E is the splitting field of a separable polynomial, Proposition 2.7 shows that $\mathrm{Gal}(E/F)$ has $[E:F]$ elements. Combined with Artin's theorem (3.4), this shows that $G = \mathrm{Gal}(E/F)$ and $(G:1) = [E:F]$.

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

PROOF. Let $E = F[\alpha_1, ..., \alpha_m]$. Let f_i be the minimum polynomial of α_i over F, and take E' to be the splitting field of $\prod f_i$ over F. □

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 drop the assumption that E is separable over F, 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 any finite extension generated by separable elements is separable. Therefore, the elements of a finite extension E of F that are separable over F form a subfield E_{sep} of E that is separable over F; write $[E:F]_{\text{sep}} = [E_{\text{sep}}:F]$ (***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 called a ***cyclic***, ***abelian,*** ..., ***solvable*** extension if it is Galois with 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 $M \mapsto \mathrm{Gal}(E/M)$ are inverse maps.

Let H be a subgroup of G. Then, as we observed in (3.11b), $\mathrm{Gal}(E/E^H) = H$.

Let M be an intermediate field. Then E is Galois over M by (3.13), which means that $E^{\mathrm{Gal}(E/M)} = M$.

(a) We have the obvious implications:

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

But $\mathrm{Gal}(E/E^{H_i}) = H_i$.

(b) As we observed in (3.11b), for any subgroup H of G, $[E\colon E^H] = (\mathrm{Gal}(E/E^H)\colon 1)$. This proves (b) in the case $H_2 = 1$, and the general case follows, using that

$$(H_1\colon 1) = (H_1\colon H_2)(H_2\colon 1) \quad \text{and} \quad [E\colon E^{H_1}] = [E\colon E^{H_2}][E^{H_2}\colon E^{H_1}].$$

(c) For $\tau \in G$ and $\alpha \in E$, $\tau\alpha = \alpha \iff \sigma\tau\sigma^{-1}(\sigma\alpha) = \sigma\alpha$. Therefore, $\mathrm{Gal}(E/\sigma M) = \sigma\,\mathrm{Gal}(E/M)\sigma^{-1}$, and so $\sigma\,\mathrm{Gal}(E/M)\sigma^{-1} \leftrightarrow \sigma M$.

(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

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

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, assume that M is normal over F, and write $M = F[\alpha_1, \ldots, \alpha_m]$. 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 $M_1, M_2, \ldots, M_r$ 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

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

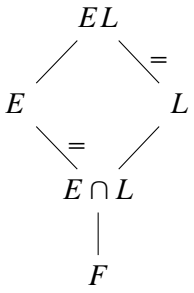
(b) Let H be a subgroup of G and let $M = E^H$. The largest normal subgroup contained in H is $N = \bigcap_{\sigma\in G} \sigma H\sigma^{-1}$ (see GT 4.10), and so E^N, which is the composite of the fields σM, is the smallest normal extension of F containing M. It is called the ***normal***, or ***Galois***,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

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

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. Any 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 1. Thus, $\sigma \mapsto \sigma|E$ is injective. If $\alpha \in E$ is fixed by all $\sigma \in \mathrm{Gal}(EL/L)$, then $\alpha \in L \cap E$. By the fundamental theorem, 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*

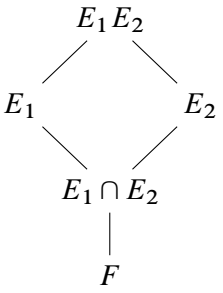
$$\sigma \mapsto (\sigma|E_1, \sigma|E_2) : \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

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 of separable polynomials $f_1, f_2 \in F[X]$. Now E_1E_2 is a splitting field for f_1f_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 prove that the image is the whole of H by counting.



From the fundamental theorem,

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

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). □

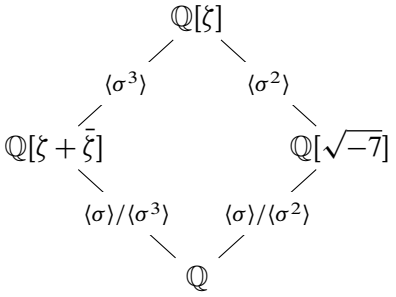
Examples

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). The subfield of $\mathbb{Q}[\zeta]$ corresponding to $\langle\sigma^3\rangle$ is $\mathbb{Q}[\zeta+\bar{\zeta}]$, and $\zeta + \bar{\zeta} = 2\cos\frac{2\pi}{7}$. Since $\langle\sigma^3\rangle$ 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[2] of $\zeta + \bar{\zeta}$ is

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

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

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

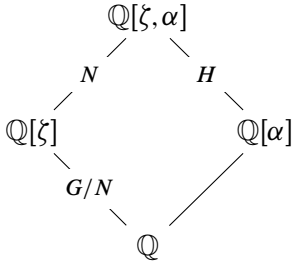
one obtains $1 + \zeta + \zeta^2 + \cdots + \zeta^6 = 0$.

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 $\mathbb{Q}[\sqrt{-7}]$.

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 $\mathbb{Q}[\zeta^i\alpha]$,

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

Constructible numbers revisited

Earlier, we showed (1.36) 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

$$\alpha \text{ constructible} \implies [\mathbb{Q}[\alpha]:\mathbb{Q}] = 2^s \text{ some } s. \tag{1}$$

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 (1) is false. We'll show below (4.9) that the Galois group of the splitting field E over $\mathbb{Q}$ of the polynomial $f(X) = X^4 - 4X + 2$ is S_4. If the four roots of $f(X)$ were constructible, then all the elements of E would be constructible (1.36a). Let H be a Sylow subgroup of S_4. Then E^H has odd degree over $\mathbb{Q}$, and so the elements of $E^H \smallsetminus \mathbb{Q}$ can't be constructible. [3]

[3] As Shuichi Otsuka has pointed out to me, 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.)

The Galois group of a polynomial

If the 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 $f = \prod_{i=1}^{n}(X-\alpha_i)$ 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 define permutations of $\{\alpha_1,\alpha_2,\dots,\alpha_n\}$, and as the α_i generated F_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 $\mathrm{Sym}(\{\alpha_1,\alpha_2,\dots,\alpha_n\}) \approx S_n$. In fact, G_f consists exactly of the permutations σ of $\{\alpha_1,\alpha_2,\dots,\alpha_n\}$ such that, for $P \in F[X_1,\dots,X_n]$,

$$P(\alpha_1,\dots,\alpha_n) = 0 \implies P(\sigma\alpha_1,\dots,\sigma\alpha_n) = 0.$$

This gives a description of G_f without mentioning fields or abstract groups (neither of which were available to Galois).

Note that this shows again that $(G_f\colon 1)$, hence $[F_f\colon F]$, 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. The equation $f = 0$ is solvable in radicals if and only if the Galois group of f is solvable.*

We shall prove this later (5.32). Also we shall exhibit polynomials $f(X) \in \mathbb{Q}[X]$ with Galois group S_n, which are therefore not solvable when $n \geq 5$ by GT 4.37.

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

(a) f may not be separable, and so not have a Galois group;
(b) $X^p - X - a = 0$ is not solvable by radicals even though it is separable with abelian Galois group (cf. Exercise 2-2).

If the definition of solvable is changed to allow extensions of the type in (b) in the chain, and f is required to be separable, then the theorem becomes true in characteristic p.

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 (*) [4] 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 $\alpha\beta$ 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.

[4] 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.

CHAPTER 4

Computing Galois Groups

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

When is $G_f \subset A_n$?

Consider a polynomial

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n$$

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., if f is separable with no multiple factors. Let G_f be the Galois group of f, and identify it with a subgroup of $\mathrm{Sym}(\{\alpha_1, \ldots, \alpha_n\})$ (as on p. 45). The choice of a numbering for the roots determines an isomorphism $\mathrm{Sym}(\{\alpha_1, \ldots, \alpha_n\}) \simeq S_n$, and the subgroup of $\mathrm{Sym}(\{\alpha_1, \ldots, \alpha_n\})$ corresponding to any normal subgroup of S_n is independent of the choice for $n \neq 6$ (because all automorphisms of S_n are inner when $n \neq 6$, cf. GT 3.4).

PROPOSITION 4.1 *Assume f is separable, and let $\sigma \in G_f$.*

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

PROOF. The first equation follows immediately from the definition of the signature of σ (see GT p. 65), and the second equation is obtained by squaring the first. □

COROLLARY 4.2 *Let $f(X) \in F[X]$ be of degree n and have only simple roots. Let F_f be a splitting field for f, so that $G_f = \mathrm{Gal}(F_f/F)$.*

(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 $G_f \stackrel{\text{def}}{=} \text{Gal}(F_f/F)$, and hence lies in F (by the fundamental theorem of Galois theory).

(b) Because f has simple roots, $\Delta(f) \neq 0$, and so the formula $\sigma\Delta(f) = \text{sign}(\sigma)\Delta(f)$ 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 discriminant of f can be expressed as a universal polynomial in the coefficients of f. For example:

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

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

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 2.39). 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.

Of course the converse is not true: when s is even, G_f is not necessarily contained in A_n.

When is G_f transitive?

PROPOSITION 4.4 *Let $f(X) \in F[X]$ have only simple roots. 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 $F_f = F[\alpha_1, \alpha_2, ...]$ with $\alpha_1 = \alpha$ and $\alpha_2, \alpha_3, \dots$ 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 $\iff$ 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 $a \in F \setminus F^3$. 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, $X^3 - 3X + 1 \in \mathbb{Q}[X]$ is irreducible (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 quartic polynomial without multiple roots. In order to determine G_f we shall 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

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

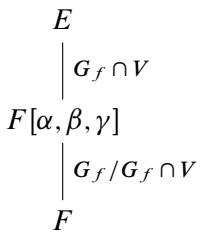
They are distinct because the α_i are distinct; for example,

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

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. Any permutation of the α_i (***a fortiori,*** any 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.

PROOF. (SKETCH) 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.

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 4.14 *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 4.15 *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 4.16 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

$$nf(X) = nX^p + a_1 X^{p-1} + \cdots + a_p,$$

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 quadratic factor, and so it certainly splits over $\mathbb{C}$ (high school algebra). Therefore, the proposition applies to f.[1]

EXAMPLE 4.17 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.

[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, p107, who credits the example to Brauer). The shorter argument in the text was suggested to me by Martin Ward.

Finite fields

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, the field of p elements. As we noted in §1, any other 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 $q-1$. Hence the nonzero elements of E are roots of $X^{q-1}-1$, and all elements of E (including 0) 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.

PROPOSITION 4.18 *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 the 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 4.19 *For each power $q = p^n$ there is a field $\mathbb{F}_q$ with q elements. It is the splitting field of $X^q - X$, and hence any two such fields 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 4.20 *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 4.21 *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 4.22 *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 4.23 *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 4.24 Since the $\mathbb{F}_{p^n}$'s 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 $\mathbb{F} = S/\sim$.

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 4.25 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 AMS, Feb. 2003, p. 198). For this reason finite fields are often called ***Galois fields*** and $\mathbb{F}_q$ is often denoted $GF(q)$.

Computing Galois groups over $\mathbb{Q}$

In the remainder of this chapter, I sketch 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 $\alpha_1, \alpha_2, \ldots$ of f in F_f:

$$G \subset \mathrm{Sym}\{\alpha_1, \alpha_2, \ldots\}.$$

The first result generalizes Proposition 4.4.

PROPOSITION 4.26 *Let $f(X)$ be a polynomial in $F[X]$ with only simple roots, 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 assume that f is monic. Let $\alpha_1,\dots,\alpha_m$, $m = \deg f$, 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 4.27 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

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

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

Now suppose F is finite, with p^n elements say. Then G_f is a cyclic group generated by the Frobenius automorphism $\sigma: x\mapsto x^p$. When we regard σ as a permutation of the roots of f, then distinct 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

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

LEMMA 4.28 *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, and let $\bar f$ be the image of f in $(R/P)[X]$. Assume that neither f nor $\bar f$ has a multiple root. Then the roots $\alpha_1,\dots,\alpha_m$ of f lie in some finite extension R' of R, and their reductions $\bar\alpha_i$ modulo PR' are the roots of $\bar f$. Moreover $G_{\bar f}\subset G_f$ when both are identified with subgroups of* $\mathrm{Sym}\{\alpha_1,\dots,\alpha_m\} = \mathrm{Sym}\{\bar\alpha_1,\dots,\bar\alpha_m\}$.

PROOF. Omitted — see van der Waerden, Modern Algebra, I, §61 (second edition) or ANT 3.41. □

On combining these results, we obtain the following theorem.

THEOREM 4.29 (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 $\bar f = \prod f_i$ 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 4.30 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. Hence G_f contains $(ik)(lmn)$ and (12345), and so also $((ik)(lmn))^3 = (ik)$. Therefore $G_f = S_5$ by (4.14).

LEMMA 4.31 *A transitive subgroup of $H \subset S_n$ containing a transposition and an $(n-1)$-cycle is equal to S_n.*

PROOF. After possibly renumbering, we may suppose 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 $(1n), (2n), \dots, (n-1\,n)$, and these elements obviously generate S_n. □

EXAMPLE 4.32 Select monic polynomials of degree n, f_1, f_2, f_3 with coefficients in $\mathbb{Z}$ such that:

(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 polys of odd degree) mod 5.

We also choose f_1, f_2, f_3 to have only simple roots. 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, $n \le 11$, 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 4.17) 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.

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 $n = \prod_{i=1}^{k} p_i^{r_i}$ is irreducible over $\mathbb{F}_q$ if and only if $\gcd(f(x), x^{q^{n/p_i}} - x) = 1$ for all i.

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?

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 shall 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 (4.18). 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. Let $\alpha_1 = \alpha, \dots, \alpha_s$ be the roots of f in some big field containing E, and let $\beta_1 = \beta, \beta_2, \dots, \beta_t$ be the roots of g. For $j \neq 1$, $\beta_j \neq \beta_1$, and so the the equation

$$\alpha_i + X\beta_j = \alpha_1 + X\beta_1,$$

has exactly one solution, namely, $X = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}$. 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 $\gamma = \alpha + c\beta$. Then 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 have computed the gcd in some field splitting fg, but we have seen (Proposition 2.10) that the gcd of two polynomials has coefficients in the same field as the coefficients of the polynomials. Hence $\beta \in F[\gamma]$, and this implies that $\alpha = \gamma - c\beta$ also lies in $F[\gamma]$. We have shown that $F[\alpha, \beta] = F[\gamma]$. □

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 E is Galois over F, then an element of this form will be a primitive element provided it is moved by every element of $\mathrm{Gal}(E/F)$ except 1. These remarks make it very easy to write down primitive elements.

Our hypotheses are minimal: if *two* of the αs 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 $M = M'$ — 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's, and consequently only finitely many possible M's. □

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 (see Dummit and Foote 1991, p508). 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 (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 any $c \in k$, 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]

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. Define $\mathbb{C}$ to be the splitting field of $X^2+1 \in \mathbb{R}[X]$, and let i be 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 $\mathbb{C}$.

The two facts we need to assume about $\mathbb{R}$ are:

- ◇ 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 in his thesis (University of Michigan 1977), 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 a difficult theorem 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 $f(X)(X^2 + 1)$ — we have to show that $E = \mathbb{C}$. Since $\mathbb{R}$ has characteristic zero, the polynomial is separable, and so E is Galois over $\mathbb{R}$. Let G be its Galois group, and let H be a Sylow 2-subgroup of G.

Let $M = E^H$. Then M is of odd degree over $\mathbb{R}$, and $M = \mathbb{R}[\alpha]$ some α (Theorem 5.1). The minimum polynomial of α over $\mathbb{R}$ has odd degree and so has a root in $\mathbb{R}$. It therefore has degree 1, and so $M = \mathbb{R}$ and $G = H$.

We now know 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 can therefore be obtained by extracting the square root of an element of $\mathbb{C}$ (see 3.24), but we have seen that all such elements already lie in $\mathbb{C}$. Hence $E^N = \mathbb{C}$, which is a contradiction. Thus $E = \mathbb{C}$. □

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 characteristic p not dividing n.

PROPOSITION 5.8 *Let F be a field of characteristic 0 or characteristic p not dividing n. 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. Any generator will have order n, and hence will be 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) 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, $\zeta = \zeta_0^m$,

$$\sigma\zeta = (\sigma\zeta_0)^m = \zeta_0^{im} = \zeta^i. \qquad \square$$

The map $\sigma \mapsto [i]\colon \mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ 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 saw in (1.41) that $[\mathbb{Q}[\zeta]\colon\mathbb{Q}] = p-1$, 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 $d \mid n$. The quotient of $X^n - 1$ by all these factors for $d < n$ 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 ask PARI by typing `polcyclo(n,X)`.

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 $[F[\zeta]\colon F] = \varphi(n)$;*
(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 is equal to it if and only if $[F[\zeta]\colon F] = \varphi(n)$, which is true if and only if the injection $\mathrm{Gal}(F[\zeta]/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is onto. $\square$

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

$$\zeta \text{ a root of } f(X) \implies \zeta^p \text{ a root of } f(X) \text{ for all primes } p \nmid n.$$

Write

$$\Phi_n(X) = f(X)g(X).$$

Proposition 1.14 shows that $f(X)$ and $g(X)$ lie in $\mathbb{Z}[X]$. Suppose 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 $h(X) \mapsto \bar{h}(X)$ for the map $\mathbb{Z}[X] \mapsto \mathbb{F}_p[X]$, and note that

$$\gcd_{\mathbb{Z}[X]}(f(X), g(X^p)) \neq 1 \implies \gcd_{\mathbb{F}_p[X]}(\bar{f}(X), \bar{g}(X^p)) \neq 1.$$

But $\bar{g}(X^p) = \bar{g}(X)^p$ (use the mod p binomial theorem and that $a^p = a$ for all $a \in \mathbb{F}_p$), and so $\bar{f}(X)$ and $\bar{g}(X)$ have a common factor. 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 and mysterious relations between what happens in characteristic 0 and in characteristic p. For example, let $f(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$. 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 $\bar{f} = 0$ in $\mathbb{F}_{p^n}$.

The Weil conjectures (Weil 1949; proved in part by Grothendieck in the 1960's 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 $\cos\frac{2\pi}{n}$ (or $\zeta = e^{2\pi i/n}$) 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. But (see GT 3.5)

$$\varphi(n) = \prod_{p|n}(p-1)p^{n(p)-1}, \quad n = \prod p^{n(p)},$$

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 $2^{2^k}+1$. It is known that these numbers are prime when $k = 0, 1, 2, 3, 4$, 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.

(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'S) *Let F be a field, and let G be a group (monoid will do). Then any finite set $\{\chi_1, \dots, \chi_m\}$ of 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. Induction on m. For $m = 1$, it's 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 now shows that $a_i' = 0$ for all $i \geq 2$. Since $\chi_2(g) - \chi_1(g) \neq 0$, we must have $a_2 = 0$, and the induction hypothesis shows that all the remaining a_i's are also zero. □

COROLLARY 5.15 *Let F_1 and F_2 be fields, and let $\sigma_1, ..., \sigma_m$ be distinct homomorphisms $F_1 \to F_2$. Then $\sigma_1, ..., \sigma_m$ are linearly independent over F_2.*

PROOF. Apply the theorem to $\chi_i = \sigma_i | F_1^\times$. □

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 over F, 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 $\sum_{i=1}^m c_i\sigma_i : E \to \Omega$ 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 with Galois group G. A ***normal basis*** for E is an F-basis of the form $\{\sigma\alpha \mid \sigma \in G\}$, i.e., an F-basis consisting of the conjugates of an element α of E.

THEOREM 5.18 (NORMAL BASIS THEOREM) *Every Galois extension has a normal basis.*

PROOF. Let E/F be a Galois extension with Galois group G. We give two proofs, the first of which assumes that F is infinite and the second that G is cyclic. Since every Galois extension of a finite field is cyclic (4.19), this covers all cases.[3]

Assume that F is infinite. This has the consequence that, if $f \in F[X_1,\dots,X_m]$ has the property that $f(a_1,\dots,a_m) = 0$ for all $a_1,\dots,a_m \in F$, then $f(X_1,\dots,X_m) = 0$. We prove this by induction on m. For $m = 1$ it follows from the fact that a nonzero polynomial in one symbol has only finitely many roots. For $m > 1$, write

$$f = \sum c_i(X_1,\dots,X_{m-1})X_m^i.$$

For any $m-1$-tuple, $a_1,\dots,a_{m-1}$,

$$f(a_1,\dots,a_{m-1},X_m)$$

is a polynomial in X_m having every element of F 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 zero.

Now number the elements of G as $\sigma_1,\dots,\sigma_m$ (with $\sigma_1 = 1$).

Let $f(X_1,\dots,X_m) \in F[X_1,\dots,X_m]$ 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

$$g(Y_1,\dots,Y_m) = f(\textstyle\sum_{i=1}^m Y_i\sigma_1\alpha_i, \sum_{i=1}^m Y_i\sigma_2\alpha_i,\dots).$$

The hypothesis on f implies that $g(a_1,\dots,a_m) = 0$ for all $a_i \in F$, and so $g = 0$. 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 shall show that $\{\sigma_i\alpha\}$ is a normal basis. For this, it suffices to show that $\sigma_i\alpha$ are linearly independent over F. Suppose

$$\sum\nolimits_{j=1}^m a_j\sigma_j\alpha = 0$$

[3]For two proofs that work equally well for finite and infinite fields, together with an outline of the history of the theorem, see Blessenohl, Dieter. On the normal basis theorem. Note Mat. 27 (2007), 5–10.

for some $a_j \in F$. On applying $\sigma_1, \dots, \sigma_m$ successively, we obtain a system of m-equations

$$\sum a_j \sigma_i \sigma_j \alpha = 0$$

in the m "unknowns" a_j. Because this system of equations is nonsingular, the a_j's are zero. This completes the proof of the lemma in the case that F is infinite.

Now assume that G is cyclic generated, say, by an element σ_0 of order n. Then $[E:F] = n$. 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 a $F[X]$-module, $\alpha, \sigma_0\alpha, \dots, \sigma_0\alpha^{n-1}$ is a F-basis for E. □

Hilbert's Theorem 90

Let G be a finite 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 to give a homomorphism $G \to \mathrm{Aut}(M)$ (automorphisms of M as an abelian group).

EXAMPLE 5.19 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 5.20 (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

$$x + \sigma x + \cdots + \sigma^{n-1} x = 0, \qquad (*)$$

Conversely, if $x \in M$ satisfies (*), 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

$$\{\text{crossed homs } f: G \to M\} \overset{f \leftrightarrow f(\sigma)}{\longleftrightarrow} \{x \in M \text{ satisfying (*)}\}.$$

(b) For any $x \in M$, 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. We leave it as an exercise to the reader to show that an exact sequence of G-modules

$$0 \to M' \to M \to M'' \to 0$$

gives rise to an exact sequence

$$0 \to M'^G \to M^G \to M''^G \to H^1(G, M') \to H^1(G, M) \to H^1(G, M'').$$

EXAMPLE 5.21 Let $\pi: \tilde{X} \to X$ 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 $H^1(X, \mathbb{Z}) \simeq H^1(\Gamma, \mathbb{Z}) = \text{Hom}(\Gamma, \mathbb{Z})$.

THEOREM 5.22 *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,

$$f(\sigma\tau) = f(\sigma) \cdot \sigma(f(\tau)), \quad \sigma, \tau \in G,$$

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

$$\beta \stackrel{\text{def}}{=} \sum_{\tau \in G} f(\tau)\tau\alpha \neq 0.$$

But then, for $\sigma \in G$,

$$\begin{aligned}\sigma\beta &= \sum_{\tau\in G} \sigma(f(\tau)) \cdot \sigma\tau(\alpha) \\ &= \sum_{\tau\in G} f(\sigma)^{-1}\ f(\sigma\tau)\cdot\sigma\tau(\alpha) \\ &= f(\sigma)^{-1}\ \sum_{\tau\in G} f(\sigma\tau)\sigma\tau(\alpha),\end{aligned}$$

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

$$\mathrm{Nm}\alpha = \prod_{\sigma\in G} \sigma\alpha.$$

For $\tau \in G$,

$$\tau(\mathrm{Nm}\alpha) = \prod_{\sigma\in G} \tau\sigma\alpha = \mathrm{Nm}\alpha,$$

and so $\mathrm{Nm}\alpha \in F$. The map

$$\alpha \mapsto \mathrm{Nm}\alpha\colon E^\times \to F^\times$$

is a obviously a homomorphism.

EXAMPLE 5.23 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 show that, for cyclic extensions, all elements with norm 1 are of this form.

COROLLARY 5.24 (HILBERT'S THEOREM 90) [4] *Let E be a finite cyclic extension of F with Galois group $\langle\sigma\rangle$; 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 5.20a) there is a crossed homomorphism $f\colon\langle\sigma\rangle \to E^\times$ with $f(\sigma) = \alpha$. Theorem 5.22 now shows that f is principal, which means that there is a β with $f(\sigma) = \beta/\sigma\beta$. □

[4] This 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 5.22 by E. Noether. Theorem 5.22, 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 the English translation (Springer 1998) written by F. Lemmermeyer and N. Schappacher.

Cyclic extensions

We are now able to classify the cyclic extensions of degree n of a field F in the case that F contains a primitive nth root of 1. 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.

Consider a field $E = F[\alpha]$ generated by an element α whose nth power is in F. Then α is a root of $X^n - a$, and the remaining roots are the elements $\zeta^i\alpha$, $1 \le i \le n-1$. Since these are all in E, E is a Galois extension of F, with Galois group G say. For any $\sigma \in G$, $\sigma\alpha$ 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

$$\sigma \mapsto \sigma\alpha/\alpha : G \to \mu_n$$

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 $\alpha^d \in F$. Thus the map is surjective if n is the smallest positive integer such that $\alpha^n \in F$. We have proved the first part of the following statement.

PROPOSITION 5.25 *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 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 second 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 $\alpha^n \in F$, and α^n is the smallest power of α that lies in F. According to the Normal Basis Theorem 5.18, there exists an element $\gamma \in E$ such that $\{\gamma, \sigma\gamma, \dots, \sigma^{n-1}\gamma\}$ is a basis for E as an F-vector space. Form the sum

$$\alpha = \sum \zeta^i \sigma^i \gamma.$$

Then $\alpha \neq 0$ because the $\sigma^i\gamma$ are linearly independent and the $\zeta^i \in F$, and $\sigma\alpha = \zeta^{-1}\alpha$. □

REMARK 5.26 (a) The polynomial $X^n - a$, $n \ge 2$, is irreducible in $F[X]$ under the following condition: a is not a pth power for any p dividing n, and, if $4|n$, then $a \notin -4F^4$. See Lang, Algebra, Addison-Wesley, 1965, VIII, §9, Theorem 16.

(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 extension of F which is cyclic of degree p is the splitting field of such a polynomial.

PROPOSITION 5.27 *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 containing a primitive nth root of 1, ζ. In particular, F either has characteristic 0 or characteristic p not dividing n.

The last two results 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 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

$$1 \to \mu_n \to E^\times \xrightarrow{x \mapsto x^n} E^{\times n} \to 1$$

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 5.28 *The map*

$$E \mapsto F^\times \cap E^{\times n}/F^{\times n}$$

defines a one-to-one correspondence between the finite abelian extensions of F of exponent n contained in some fixed algebraic closure Ω of F and the finite subgroups B of $F^\times/F^{\times n}$. 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 $[E:F] = (B:F^{\times n})$.

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,

$$[E:F] \geq [F[B(E)^{\frac{1}{n}}]:F] = (B(F[B(E)^{\frac{1}{n}}]):F^{\times n}) \geq (B(E):F^{\times n}).$$

If E/F is abelian of exponent n, then $[E:F] = (B(E):F^{\times n})$, 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

$$a \mapsto (\sigma \mapsto \frac{\sigma a^{\frac{1}{n}}}{a}): B(E)/F^{\times n} \to \mathrm{Hom}(G, \mu_n), \quad G = \mathrm{Gal}(E/F),$$

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 $\sigma a^{\frac{1}{n}}/a = 1$ 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 5.29 (a) The quadratic extensions of $\mathbb{R}$ are (certainly) in one-to-one correspondence with the subgroups of $\mathbb{R}^\times/\mathbb{R}^{\times 2} = \{\pm 1\}$.

(b) The finite abelian extensions of $\mathbb{Q}$ of exponent 2 are in one-to-one correspondence with the finite subgroups of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$, which is a direct sum of cyclic groups of order 2 indexed by the prime numbers plus ∞ (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).

REMARK 5.30 (KUMMER THEORY) Let E be an abelian extension of F of exponent n. Then

$$B(E) = \{a \in F^\times \mid a \text{ becomes an } n\text{th power in } E\}.$$

There is a perfect pairing

$$(a, \sigma) \mapsto \frac{\sigma a}{a}: \frac{B(E)}{F^{\times n}} \times \mathrm{Gal}(E/F) \to \mu_n.$$

In particular, $[E:F] = (B(E):F^{\times n})$. (Cf. Exercise 5 for the case $n = 2$.)

Proof of Galois's solvability theorem

LEMMA 5.31 *Let $f \in F[X]$ be separable, and let F' be an extension field of F. Then the Galois group of f as an element of $F'[X]$ is a subgroup of that of f as an element of $F[X]$.*

PROOF. Let E' be a splitting field for f over F', and let $\alpha_1, \ldots, \alpha_m$ be the roots of $f(X)$ in E'. Then $E = F[\alpha_1, ..., \alpha_m]$ is a splitting field of f over F. Any 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 5.32 *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 5.25 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 $\tilde{E}$ of F such that $f(X)$ splits in $\tilde{E}[X]$.

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.

Let G be the Galois group of Ω/F, and let $\tilde{E}$ be the Galois closure of $F_m[\zeta]$ in Ω. According to (3.17a), $\tilde{E}$ is the composite of the fields $\sigma F_m[\zeta]$, $\sigma \in G$, and so it is generated over F by the elements

$$\zeta, \alpha_1, \alpha_2, \ldots, \alpha_m, \sigma\alpha_1, \ldots, \sigma\alpha_m, \sigma'\alpha_1, \ldots.$$

We adjoin these elements to F one by one to get a sequence of fields

$$F \subset F[\zeta] \subset F[\zeta, \alpha_1] \subset \cdots \subset F' \subset F'' \subset \cdots \subset \tilde{E}$$

in which each field F'' is obtained from its predecessor F' by adjoining an rth root of an element of F' ($r = r_1, \ldots, r_m$, or n). According to (5.8) and (5.25), each of these extensions is abelian (and even cyclic after for the first), and so $\tilde{E}/F$ is a solvable extension. □

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 variables: for any particular values of a, b, c, the formula gives the roots of the particular equation. We shall 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 variables. We shall show that, when we regard f as a polynomial in X with coefficients in the field $F(t_1, \ldots, t_n)$, its Galois group is S_n. Then Theorem 5.32 proves the above remark (at least in characteristic zero).

SYMMETRIC POLYNOMIALS

Let R be a commutative ring (with 1). A polynomial $P(X_1, ..., X_n) \in R[X_1, \ldots, X_n]$ is said to be ***symmetric*** if it is unchanged when its variables are permuted, i.e., if

$$P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n), \quad \text{all } \sigma \in S_n.$$

For example

$$\begin{array}{lcll} p_1 & = & \sum_i X_i & = X_1 + X_2 + \cdots + X_n, \\ p_2 & = & \sum_{i<j} X_iX_j & = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_{n-1}X_n, \\ p_3 & = & \sum_{i<j<k} X_iX_jX_k, & = X_1X_2X_3 + \cdots \\ & \cdots & & \\ p_r & = & \sum_{i_1<\cdots<i_r} X_{i_1}...X_{i_r} & \\ & \cdots & & \\ p_n & = & X_1X_2\cdots X_n & \end{array}$$

are all symmetric because p_r is the sum of *all* monomials of degree r made up out of distinct X_i's. These particular polynomials are called the ***elementary symmetric polynomials***.

THEOREM 5.33 (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,

$$i_1 = j_1, \ldots, i_s = j_s, \text{ but } i_{s+1} > j_{s+1}.$$

For example,

$$X_1X_2^3X_3 > X_1X_2^2X_3 > X_1X_2X_3^2.$$

Let $X_1^{k_1}\cdots X_n^{k_n}$ be the highest monomial occurring in P with a coefficient $c \neq 0$. Because P is symmetric, it contains all monomials obtained from $X_1^{k_1}\cdots X_n^{k_n}$ by permuting the X's. Hence $k_1 \geq k_2 \geq \cdots \geq k_n$.

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

$$X_1^{d_1+d_2+\cdots+d_n}X_2^{d_2+\cdots+d_n}\cdots X_n^{d_n}. \tag{2}$$

Therefore the highest monomial of $P(X_1,\dots,X_n) - cp_1^{k_1-k_2}p_2^{k_2-k_3}\cdots p_n^{k_n}$ is strictly less than the highest monomial in $P(X_1,\dots,X_n)$. We can repeat this argument with the polynomial on the left, and after a finite number of steps, we will arrive at a representation of P as a polynomial in $p_1,\dots,p_n$. □

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:

$$f(X) = \textstyle\prod_{i=1}^n (X-\alpha_i),\ \alpha_i \in S.$$

Then

$$a_1 = -p_1(\alpha_1,\dots,\alpha_n),\quad a_2 = p_2(\alpha_1,\dots,\alpha_n),\quad \dots,\quad a_n = \pm p_n(\alpha_1,\dots,\alpha_n).$$

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.

SYMMETRIC FUNCTIONS

THEOREM 5.34 (SYMMETRIC FUNCTIONS THEOREM) *When S_n acts on $E = F(X_1,...,X_n)$ by permuting the X_i's, the field of invariants is $F(p_1,...,p_n)$.*

FIRST 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 $F[p_1,\dots,p_n]$ (5.33). Hence their quotient $f = Hf/H$ lies in $F(p_1,\dots,p_n)$. □

SECOND PROOF Clearly

$$F(p_1,\dots,p_n) \subset E^{S_n} \subset E.$$

On the one hand, $[E\colon F(p_1,\dots,p_n)] \le n!$ because E is the splitting field of $(T-X_1)\cdots(T-X_n)$ over $F(p_1,\dots,p_n)$; on the other, $[E\colon E^{S_n}] \ge n!$ by (2.8). □

COROLLARY 5.35 *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). □

As we noted in the second proof, $F(X_1,\dots,X_n)$ 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.

THE GENERAL POLYNOMIAL OF DEGREE n

THEOREM 5.36 *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 map

$$t_i \mapsto p_i : F[t_1, \ldots, t_n] \to F[p_1, \ldots, p_n]$$

is injective (i.e., the p_i are algebraically independent over F, see p. 99), then it will extend to an isomorphism

$$F(t_1, \ldots, t_n) \to F(p_1, \ldots, p_n)$$

sending $f(X)$ to

$$g(X) = X^n - p_1X^{n-1} + \cdots + (-1)^n p_n \in F(p_1, \ldots, p_n)[X].$$

Therefore the statement will follow from Corollary 5.35.

We now prove that the p_i are algebraically independent[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 (2), p. 74, 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 5.37 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?

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 variables 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, and Serre, J.-P., *Topics in Galois Theory*, 1992.

REMARK 5.38 Take $F = \mathbb{C}$, and consider the subset of $\mathbb{C}^{n+1}$ defined by the equation

$$X^n - T_1X^{n-1} + \cdots + (-1)^n T_n = 0.$$

[5]This can also 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).

It is a beautiful complex manifold S of dimension n. Consider the projection

$$\pi: S \to \mathbb{C}^n, \quad (x, t_1, \dots, t_n) \mapsto (t_1, \dots, t_n).$$

Its fibre over a point $(a_1, \dots, a_n)$ is the set of roots of the polynomial

$$X^n - a_1 X^{n-1} + \cdots + (-1)^n a_n.$$

The discriminant $D(f)$ of $f(X) = X^n - T_1 X^{n-1} + \cdots + (-1)^n T_n$ is a polynomial in $\mathbb{C}[T_1, \dots, T_n]$. 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 $\mathbb{C}^n \smallsetminus \Delta$.

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 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]

$$\mathrm{Tr}(\alpha) = \mathrm{Tr}(A),\ \det(\alpha) = \det(A),\ c_\alpha(X) = c_A(X)$$

where A is the matrix of α with respect to any basis of V. If β is a second endomorphism of V,

$$\begin{aligned} \mathrm{Tr}(\alpha + \beta) &= \mathrm{Tr}(\alpha) + \mathrm{Tr}(\beta); \\ \det(\alpha\beta) &= \det(\alpha)\det(\beta). \end{aligned}$$

[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.

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

$$\begin{array}{lcll} \mathrm{Tr}_{E/F}(\alpha) & = & \mathrm{Tr}(\alpha_L) & \text{(trace of } \alpha) \\ \mathrm{Nm}_{E/F}(\alpha) & = & \det(\alpha_L) & \text{(norm of } \alpha) \\ c_{\alpha,E/F}(X) & = & c_{\alpha_L}(X) & \text{(characteristic polynomial of } \alpha). \end{array}$$

Thus, $\mathrm{Tr}_{E/F}$ is a homomorphism $(E,+) \to (F,+)$, and $\mathrm{Nm}_{E/F}$ is a homomorphism $(E^\times,\cdot) \to (F^\times,\cdot)$.

EXAMPLE 5.39 (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

$$\mathrm{Tr}_{E/F}(a) = na,\ \mathrm{Nm}_{E/F}(a) = a^n,\ c_{a,E/F}(X) = (X-a)^n$$

where $n = [E\colon F]$.

Let $E = \mathbb{Q}[\alpha, i]$ be the splitting field of $X^8 - 2$. To compute the trace and norm of α in 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 5.40 *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, $A =_{\text{def}} (a_{ij})$ 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 5.41 *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

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

so that

$$\begin{aligned} a_1 &= -\textstyle\sum\alpha_i, \text{ and} \\ a_n &= (-1)^n \textstyle\prod\alpha_i. \end{aligned}$$

Then

$$c_\alpha(X) = (f(X))^m = X^{mn} + ma_1X^{mn-1} + \cdots + a_n^m,$$

so that

$$\begin{aligned} \mathrm{Tr}_{E/F}(\alpha) &= -ma_1 = m\textstyle\sum\alpha_i, \text{ and} \\ \mathrm{Nm}_{E/F}(\alpha) &= (-1)^{mn}a_n^m = (\textstyle\prod\alpha_i)^m. \end{aligned}$$

□

EXAMPLE 5.42 (a) Consider the extension $\mathbb{C} \supset \mathbb{R}$. If $\alpha \in \mathbb{C} \setminus \mathbb{R}$, 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 16). The minimum polynomial of α is $X^8 - 2$, and so

$$\begin{array}{rclcrcl} c_{\alpha,\mathbb{Q}[\alpha]/\mathbb{Q}}(X) &=& X^8-2, & & c_{\alpha,E/\mathbb{Q}}(X) &=& (X^8-2)^2 \\ \mathrm{Tr}_{\mathbb{Q}[\alpha]/\mathbb{Q}}\alpha &=& 0, & & \mathrm{Tr}_{E/\mathbb{Q}}\alpha &=& 0 \\ \mathrm{Nm}_{\mathbb{Q}[\alpha]/\mathbb{Q}}\alpha &=& -2, & & \mathrm{Nm}_{E/\mathbb{Q}}\alpha &=& 4 \end{array}$$

REMARK 5.43 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 5.41 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 5.44 *For finite extensions $E \supset M \supset F$, we have*

$$\begin{aligned} \mathrm{Tr}_{E/M} \circ \mathrm{Tr}_{M/F} &= \mathrm{Tr}_{E/F}, \\ \mathrm{Nm}_{E/M} \circ \mathrm{Nm}_{M/F} &= \mathrm{Nm}_{E/F}. \end{aligned}$$

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 5.45 *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*

$$\operatorname{disc} f(X) = (-1)^{m(m-1)/2} \operatorname{Nm}_{F[\alpha]/F} f'(\alpha)$$

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

$$\begin{aligned}
\operatorname{disc} f(X) &\stackrel{\text{def}}{=} \prod_{i<j}(\alpha_i-\alpha_j)^2 \\
&= (-1)^{m(m-1)/2} \cdot \prod_i \Big(\prod_{j\neq i}(\alpha_i-\alpha_j)\Big) \\
&= (-1)^{m(m-1)/2} \cdot \prod_i f'(\alpha_i) \\
&= (-1)^{m(m-1)/2} \operatorname{Nm}_{F[\alpha]/F}(f'(\alpha)) \qquad \text{(by 5.43).}
\end{aligned}$$

□

EXAMPLE 5.46 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

$$\begin{aligned}
f\left(\frac{-nb}{X+(n-1)a}\right) &= \frac{P(X)}{Q(X)} \\
P(X) &= (X+(n-1)a)^n - na(X+(n-1)a)^{n-1} + (-1)^n n^n b^{n-1} \\
Q(X) &= (X+(n-1)a)^n/b,
\end{aligned}$$

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 go 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 any 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 section, we prove that Zorn's lemma implies 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 (4.23), 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'S) *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.*

[1] There do exist naturally occurring fields, not contained in $\mathbb{C}$, that are uncountable. For example, for any field F there is a ring $F[[T]]$ of formal power series $\sum_{i \geq 0} a_i T^i$, $a_i \in F$, and its field of fractions is uncountable even if F is finite.

Zorn's lemma[2] is equivalent to the Axiom of Choice, and hence independent of the axioms of set theory.

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, 1959, Chap. 5 §4.)[3] 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 $x_j = a y_j$ for one $j \in I$ and $x_i = y_i$ for all $i \neq j$,

(Bourbaki, 1989, Chap. II, 3.9)[4]. 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, and 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).

[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 Choice (see Jech 1973). Zorn's contribution was to observe that it is more suited to algebraic applications like ours.

[3]Bourbaki, N., Éléments de mathématique. I: Les structures fondamentales de l'analyse. Fascicule XI. Livre II: Algèbre. Chapitre 4: Polynomes et fractions rationnelles. Chapitre 5: Corps commutatifs. Deuxième édition. Actualités Scientifiques et Industrielles, No. 1102 Hermann, Paris 1959 iv+222 pp. (2 inserts). MR 30 #4751

[4]Bourbaki, Nicolas. Algebra. I. Chapters 1–3. Translated from the French. Reprint of the 1974 edition. Elements of Mathematics. Springer-Verlag, Berlin, 1989. xxiv+709 pp.

Second proof of the existence of algebraic closures

(Jacobson 1964, p144.). After (4.23) we may assume F to be infinite. This implies that the cardinality of any field algebraic over F is the same as that of F (ibid. p143). 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 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. p144 for the details.)

Third proof of the existence of algebraic closures

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 $F[\dots,x_f,\dots] \to F'$ 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. It is also algebraic over F (because it is generated by the algebraic elements x_f), and so the next lemma shows that it is an algebraic closure of F.

LEMMA 6.5 *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 (and hence an algebraic closure of F).*

PROOF. 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 shall 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 $b \stackrel{\text{def}}{=} a^{p^m} \in F$ 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

$$(f(\beta))^{p^m} = \left(\sum_i a_i \beta^i\right)^{p^m} = \sum_i a_i^{p^m} \alpha^i = 0,$$

and so β is a root of f. □

NOTES In most expositions of the proof, which is credited to E. Artin, one lets $E_1 = \Omega$, $E_2 = (E_1)_1, \dots$, and shows that $\bigcup E_i$ is algebraically closed (see Dummit and Foote 1991, 13.4).[5]

(Non)uniqueness of algebraic closures

THEOREM 6.6 (*) *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., $E = F[\alpha_1, ..., \alpha_n, \dots]$. Then we can extend the inclusion map $F \to \Omega$ to $F[\alpha_1]$ (map α_1 to any root of its minimal 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 $(M, \varphi_M) \le (N, \varphi_N)$ 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 $M \ne E$. 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.

[5] I thank Keith Conrad for pointing out to me that E itself was known to be algebraically closed (Gilmer, Robert. A Note on the Algebraic Closure of a Field. Amer. Math. Monthly 75 (1968), no. 10, 1101–1102).

REMARK 6.7 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 any $E_1, E_2 \in \mathcal{E}$, 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 any 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 6.8 (a) A field Ω is said to be ***separably closed*** if every nonconstant separable polynomial in $\Omega[X]$ splits in Ω.

(b) A field Ω is said to be a ***separable closure*** of a subfield F if it is separable and algebraic over F and it is separably closed.

THEOREM 6.9 (*) *(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. □

CHAPTER 7

Infinite Galois Extensions

In this chapter, we make free use of Zorn's lemma.

Topological groups

DEFINITION 7.1 A set G together with a group structure and a topology is a ***topological group*** if the maps

$$(g,h) \mapsto gh: G \times G \to G,$$
$$g \mapsto g^{-1}: G \to G$$

are both continuous.

Let a be an element of a topological group G. Then $a_L: G \xrightarrow{g \mapsto ag} G$ 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 $a_R: g \mapsto ga$ and $g \mapsto g^{-1}$ are both homeomorphisms. In particular, for any subgroup H of G, the coset aH of H is open 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*[1]

(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 $N' \subset gNg^{-1}$;*

[1]For subsets S and S' of G, we set $SS' = \{ss' \mid s \in S, s' \in S'\}$, and $S^{-1} = \{s^{-1} \mid s \in S\}$.

(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 (and, in fact, 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. Clearly, Ω is Galois over F if and only if it is a union of finite Galois extensions.

PROPOSITION 7.3 *If Ω is Galois over F, then it is Galois over any 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 6.6 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. □

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 7.5 *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 $\bar{S} = \bigcup_{\sigma \in G} \sigma S$ is finite. Now $\sigma \bar{S} = \bar{S}$ for all $\sigma \in G$, and it follows that $G(\bar{S})$ is normal in G. Therefore, $\sigma G(\bar{S})\sigma^{-1} = G(\bar{S}) \subset G(S)$, 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.

PROPOSITION 7.6 *Let Ω be Galois over F. For any 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 any finite set S of generators of E over F, $\mathrm{Gal}(E/F) = G(S)$, which shows that the inverse image of $1_{\mathrm{Gal}(E/F)}$ is open in G. By homogeneity, the same is true for any element of $\mathrm{Gal}(E/F)$. □

PROPOSITION 7.7 *All Galois groups are compact and totally disconnected.*[2]

PROOF. Let $G = \mathrm{Gal}(\Omega/F)$. 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

$$G \to \mathrm{Sym}(S).$$

[2]Following Bourbaki, we require compact spaces to be Hausdorff. A topological space is ***totally disconnected*** if its connected components are the one-point sets.

Since every finite set is contained in a stable finite set, 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 $G(S_2) \to G(S_1)$. 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 7.8 *For any 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 7.6. □

ASIDE 7.9 There is a converse to the proposition: 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).

The fundamental theorem of infinite Galois theory

PROPOSITION 7.10 *Let Ω be Galois over F, with Galois group G.*

(a) *The field Ω is Galois over every subfield M containing F; moreover, $\mathrm{Gal}(\Omega/M)$ 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 follows from (7.8).

(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 $\sigma \in G \smallsetminus \bar{H}$. Then $\sigma G(S) \cap H = \emptyset$ for some finite subset S of Ω which we may assume to be stable under G. Now $\sigma G(S) \cap H = \emptyset$ implies $\sigma \notin HG(S)$, and so there exists an $\alpha \in F(S)$ that is fixed by H but moved by σ. This shows that $\sigma \notin \mathrm{Gal}(\Omega/\Omega^H)$, as required. □

THEOREM 7.11 *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 7.10).

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 7.10).

(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 7.10).

(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 7.12 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,

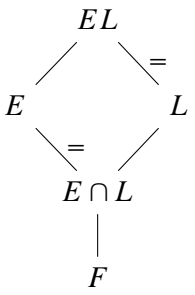
$$\mathrm{Gal}(\Omega/\textstyle\prod M_i) = \bigcap_{i\in I} H_i.$$

(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 7.13 *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. The proof that the map is an isomorphism of groups (neglecting the topology) is the same as in the finite case (3.18).

We next prove it 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 $G_1(S)$.

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 7.14 *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 7.15 Let Ω be an algebraic closure of a 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 $\langle\sigma\rangle$. 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 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 7.16 Let Ω be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$; then $\mathrm{Gal}(\Omega/\mathbb{Q})$ is one of the most basic, and intractable, objects in mathematics. It is expected that *every* finite group occurs as a quotient of it, and it certainly has S_n as a quotient group for every n (and every sporadic simple group, and every...) — cf. (5.37). We do understand $\mathrm{Gal}(F^{\mathrm{ab}}/F)$ where $F \subset \mathbb{C}$ is a finite extension of $\mathbb{Q}$ and F^{ab} is the union of all finite abelian extensions of F contained in $\mathbb{C}$. For example, $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \approx \hat{\mathbb{Z}}^\times$. (This is abelian class field theory — see my notes Class Field Theory.)

ASIDE 7.17 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 (7.10).

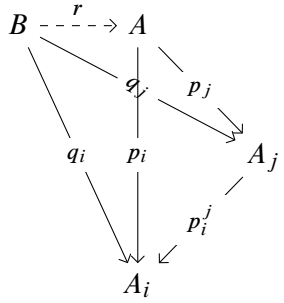
Galois groups as inverse limits

DEFINITION 7.18 A partial ordering $\leq$ on a set I is said to be ***directed***, and the pair $(I, \leq)$ is called a ***directed set***, if for all $i, j \in I$ there exists a $k \in I$ such that $i, j \leq k$.

DEFINITION 7.19 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 said to be 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 $\varprojlim(A_i, p_i^j)$, or just $\varprojlim A_i$.

EXAMPLE 7.20 Let $(G_i, p_i^j: G_j \to G_i)$ be an inverse system of groups. Let

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ all } i \le j\},$$

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 7.21 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

$$G = \{(g_i) \in \prod G_i \mid p_i^j(g_j) = g_i \text{ all } i \le j\},$$

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 7.22 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***[3].

If $(x_i) \notin G$, say $p_{i_0}^{j_0}(x_{j_0}) \ne x_{i_0}$, 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.[4]

EXAMPLE 7.23 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

[3] An inverse limit is also called a projective limit. Thus a profinite group is a projective limit of finite groups.

[4] More precisely, it is Exercise 3 of §7 of Chapter 3 of Bourbaki's General Topology.

$E \subset E'$ 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 (7.7).

Nonopen subgroups of finite index

We apply Zorn's lemma to construct a nonopen subgroup of finite index in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$.[5]

LEMMA 7.24 *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 7.25 *The group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}}/\mathbb{Q})$ has nonopen normal subgroups of index 2^n for all $n > 1$.*

PROOF. Let E be the subfield $\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}, \ldots]$ of $\mathbb{C}$. For each prime p,

$$\mathrm{Gal}(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}]/\mathbb{Q})$$

is a product of copies of $\mathbb{Z}/2\mathbb{Z}$ indexed by the set $\{\text{primes} \leq p\} \cup \{\infty\}$ (apply 5.30; see also 5.29b). Therefore,

$$\mathrm{Gal}(E/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}[\sqrt{-1}, \sqrt{2}, \ldots, \sqrt{p}]/\mathbb{Q})$$

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[6] 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. □

[5] 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.

[6] Better, let $(a_l) \in G$; then the sequence

$$(a_\infty, 0, 0, 0, \ldots), (a_\infty, a_2, 0, 0, \ldots), (a_\infty, a_2, a_3, 0, \ldots), \ldots$$

in H converges to (a_l).

ASIDE 7.26 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 7.27 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.)

ASIDE 7.28 It is necessary to assume the axiom of choice in order to have a sensible Galois theory of infinite extensions. For example, it is consistent with Zermelo-Fraenkel set theory that there be an algebraic closure L of the $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q})$ is trivial. See: Hodges, Wilfrid, Läuchli's algebraic closure of $\mathbb{Q}$. Math. Proc. Cambridge Philos. Soc. 79 (1976), no. 2, 289–297.

CHAPTER 8

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 8.1 (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 8.2 If $\alpha_1, ..., \alpha_n$ are algebraically independent over F, then

$$f(X_1, ..., X_n) \mapsto f(\alpha_1, ..., \alpha_n): F[X_1, ..., X_n] \to F[\alpha_1, ..., \alpha_n]$$

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 $F(\alpha_1, ..., \alpha_n)$ (5.36).

LEMMA 8.3 *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 8.4 When γ satisfies the equivalent conditions of Lemma 8.3, 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 8.5 (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 8.6 (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 8.7 (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 8.5) 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 8.7). If $k+1<m$, repeat the argument with A and B_1. Eventually we'll achieve $k=m$, and $m\leq n$. □

DEFINITION 8.8 A ***transcendence basis*** for Ω over F is an algebraically independent set A such that Ω is algebraic over $F(A)$.

LEMMA 8.9 *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 8.7 that Ω is algebraic over $F(A \smallsetminus \{\alpha\})$. □

THEOREM 8.10 *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, any minimal subset A' of A such that Ω is algebraic over $F(A')$ will be a transcendence basis. The second statement follows from Theorem 8.5. □

LEMMA 8.11 *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 8.12 *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 8.13 (*) *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 8.12 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 $F(X_1,\dots,X_n)$ has transcendence degree n over F.

EXAMPLE 8.14 Let $p_1,\dots,p_n$ be the elementary symmetric polynomials in $X_1,\dots,X_n$. The field $F(X_1,\dots,X_n)$ is algebraic over $F(p_1,\dots,p_n)$, and so $\{p_1,p_2,\dots,p_n\}$ contains a transcendence basis for $F(X_1,\dots,X_n)$. Because $F(X_1,\dots,X_n)$ has transcendence degree n, the p_i's must themselves be a transcendence basis.

EXAMPLE 8.15 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 8.16 *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 6.6). □

REMARK 8.17 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 8.18 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]

[1] A fairly elementary theorem of G. Mackey says that measurable homomorphisms of Lie groups are continuous (see David Witte Morris, Introduction to Arithmetic Groups, http://people.uleth.ca/~dave.morris/, Appendix I.C).

[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.

Lüroth's theorem

THEOREM 8.19 (LÜROTH'S THEOREM) *Any subfield E of $F(X)$ containing F but not equal to F is a pure transcendental extension of F.*

PROOF. Jacobson 1964, IV 4, p157. □

REMARK 8.20 This fails when there is more than one variable — see Zariski's example (footnote to Remark 5.5) and Swan's example (Remark 5.37). The best true statement is the following: 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).

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 8.21 *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 (8.10). 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 (8.9). 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, we may suppose that $\partial f/\partial X_{d+1}\neq 0$. Then $F(x_1,\dots,x_{d+1},x_{d+2})$ is algebraic over $F(x_1,\dots,x_d)$ and x_{d+1} is separable over $F(x_1,\dots,x_d)$, 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 8.22 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 8.23 (*) *Let Ω be a separably 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., $\Omega^G = F$.*

PROOF. Let $\alpha \in \Omega \smallsetminus F$. If α is transcendental over F, then it is part of a transcendence basis A for Ω over F (see 8.13). Choose an automorphism σ of A such that $\sigma(\alpha) \neq \alpha$. Then σ extends to an F-automorphism of $F(A)$, which extends to an F-automorphism of the separable closure Ω of $F(A)$ (see 6.9).

If α is algebraic over F, then by infinite Galois theory (7.8) there exists an F-automorphism σ of the separable closure of F in Ω such that $\sigma(\alpha) \neq \alpha$. As before, σ can be extended to an F-automorphism of Ω. □

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 8.24 *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

$$H \mapsto \Omega^H, \quad M \mapsto \mathrm{Aut}(\Omega/M) \tag{3}$$

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 (3):

$$\{\text{open compact subgroups of } G\} \overset{1:1}{\leftrightarrow} \{\text{fields } M \text{ such that } F \overset{\text{finitely generated}}{\subset} M \overset{\text{Galois}}{\subset} \Omega\}.$$

(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. □

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 $\sigma_i'\colon L\to\Omega$.

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 $2^{d!}$.

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 any 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 any prime p, find the Galois group over $\mathbb{Q}$ of the polynomial $X^5 - 5p^4X + p$.

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 $[L:K] = p^2$ and $[M:K] = q$;
(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 any 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. 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 so that $a^2 = \frac{4p}{3}$. Choose 3θ such that $\cos 3\theta = \frac{4q}{a^3}$. If $\beta = \cos\theta$ is a solution of the above equation, then $\alpha = a\beta$ will be a root of $X^3 - pX - q$.

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) Any 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 $F[X]$,

$$f(X) = (X^r + a_1X^{r-1} + \cdots + a_r)(X^{p-r} + \cdots), \quad 0 < r < p.$$

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 $F(X) = E[\alpha_1, \ldots, \alpha_n]$; 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.

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 $m_0 | p^n - 1$, $m = m_0 p^r$, 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 4.15).

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. Omitted.

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 $n \to \infty$.

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

$$1\longrightarrow \mathrm{Gal}(E_1E_2/F)\longrightarrow \mathrm{Gal}(E_1/F)\times\mathrm{Gal}(E_2/F)\longrightarrow \mathrm{Gal}(E_1\cap E_2/F)\longrightarrow 1.$$

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 $N: E^\times \to F^\times$ 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 (4.14). 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 any $\mathbb{R}$, 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 $\implies$ $[\Omega\colon E]$ 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 $\sigma\colon\Omega \to \Omega$ 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