FIELDS AND GALOIS THEORY

J.S. Milne

August 31, 2003*

Abstract

These notes, which are a revision of those handed out during a course taught to first-year graduate students, give a concise introduction to fields and Galois theory.

Please send comments and corrections to me at math@jmilne.org.

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

v3.01 (August 31, 2003). Fixed many minor errors; no change to numbering; 99 pages.

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 $*$.

Throughout the notes, p is a prime number: $p = 2, 3, 5, 7, 11, \dots$.

Let I and A be sets. A family of elements of A indexed by I, denoted $(a_i)_{i\in I}$, is a function $i \mapsto a_i \colon I \to A$.

$X \subset Y$ X is a subset of Y (not necessarily proper).

$X \stackrel{\text{df}}{=} Y$ X is defined to be Y, or equals Y by definition.

$X \approx Y$ X is isomorphic to Y.

$X \cong Y$ X and Y are canonically isomorphic (or there is a given or unique isomorphism).

References.

Artin, M., 1991, Algebra, Prentice Hall.

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.

Rotman, J.J., 1990, Galois Theory, Springer.

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

GT: Milne, J.S., Group Theory, v2.1, 2002.

ANT: Milne, J.S., Algebraic Number Theory, v2.1, 1998.

Prerequisites

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

Acknowledgements

I thank the following for providing corrections and comments for earlier versions of the notes: Demetres Christofides, Antoine Chambert-Loir, Hardy Falk, Jens Hansen, Albrecht Hess, Trevor Jarvis, Henry Kim, Martin Klazar, Dmitry Lyubshin, John McKay, Shuichi Otsuka, David G. Radcliffe, and others.

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 distributative 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. It is allowed that $1_R = 0$, but 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:

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

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.

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

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 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 is a b in F 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*** $\alpha\colon F \to F'$ is simply a homomorphism of rings. Such a homomorphism is always injective, because the 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

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

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

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

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 $n \mapsto n \cdot 1_F\colon \mathbb{Z} \to F$ 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 $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \ldots, \mathbb{Q}$ 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 $p|\binom{p}{r}$ for all r, $1 \le r \le p-1$. Therefore, when F has characteristic p,

$$(a+b)^p = a^p + b^p.$$

Hence $a \mapsto a^p$ is a homomorphism $F \to F$, called the ***Frobenius endomorphism*** of F. When F is finite, it is an isomorphism, called the ***Frobenius automorphism***.

Review of polynomial rings

For the following, see Dummit and Foote 1991, Chapter 9. Let F be a field.

1.5. We let $F[X]$ denote the polynomial ring in the indeterminate X with coefficients in F. Thus, $F[X]$ is a commutative ring containing F as a subring whose elements can be written uniquely in the form

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

For a ring R containing F as a subring and an element r of R, there is a unique homomorphism $\alpha\colon F[X] \to R$ 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 $\deg(r) < \deg(g)$ 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 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 $\deg(f) \ge \deg(g)$ 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},..., 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 $< \deg(f)$.

Maple knows Euclid's algorithm — to learn its syntax, type "?gcdex;".

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, $g \neq 0$.

Factoring polynomials

The following results help in deciding whether a polynomial is irreducible, and, when it is not, 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, $g_1 =_{\text{df}} mg$ and $h_1 =_{\text{df}} nh$ 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 $mg, nf \in \mathbb{Z}[X]$. 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 $\mathbb{Z}[X]$. The algebraic integers form a subring of $\mathbb{C}$ — for an elementary proof of this, using nothing but the symmetric polynomials theorem (5.30), see ANT, Theorem 2.2. Now let $\alpha_1, \dots, \alpha_m$ be the roots of f in $\mathbb{C}$. By definition, they are algebraic integers. 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 $\mathbb{Z}$, because Proposition 1.11 shows that any algebraic integer in $\mathbb{Q}$ is in $\mathbb{Z}$.

PROPOSITION 1.16 (EISENSTEIN'S CRITERION). *Let*

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

suppose that there is a prime p such that:

- *p does not divide a_m,*
- *p divides $a_{m-1}, \dots, a_0$,*
- *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 $b_0, b_1, \dots, b_r$, which contradicts the fact 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

$$f(X) = X^m + a_1X^{m-1} + \cdots + a_m, \quad a_i \in \mathbb{Z}.$$

From the fundamental theorem of algebra (see 5.6), 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 Maple) have to do only a finite amount of checking.

Thus, we need not concern ourselves with the problem of factoring polynomials in $\mathbb{Q}[X]$ or $\mathbb{F}_p[X]$, since Maple knows how to do it. For example

`>factor(6*X^2+18*X-24);` will find the factors of $6X^2 + 18X - 24$, and

`>Factor(X^2+3*X+3) mod 7;` will find the factors of $X^2 + 3X + 3$ modulo 7, i.e., in $\mathbb{F}_7[X]$.

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

[2]In an earlier version of these notes, I said that I didn't know an elementary proof of this, but several correspondents sent me such proofs, the simplest of which is the following. It uses 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 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

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 in an obvious fashion as an F-vector space. We write $[E : F]$ for the dimension, possibly infinite, of E as an F-vector space, and call $[E : F]$ the ***degree*** of E over F. We often 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 $\mathbb{Q}$ — because $\mathbb{Q}$ is countable, every finite-dimensional $\mathbb{Q}$-vector space is also countable, but a famous argument of Cantor shows that $\mathbb{R}$ is not countable. More explicitly, there are specific real numbers α, for example, π, whose powers $1, \alpha, \alpha^2, \ldots$ are linearly independent over $\mathbb{Q}$ (see the subsection on transcendental numbers p15).

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

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

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. *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*

$$[L : F] = [L : E][E : F].$$

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-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,

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

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

The general study of such polynomials requires nonelementary methods. See, for example, the paper Brandl, Rolf, Integer polynomials that are reducible modulo all primes, Amer. Math. Monthly, **93** (1986), pp286–288,
which proves that every nonprime integer $n \ge 1$ occurs as the degree of a polynomial in $\mathbb{Z}[X]$ that is irreducible over $\mathbb{Z}$ but reducible modulo all primes.

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 $\alpha \in F[x]$, write α in the form (*), i.e., set $\alpha = g(x)$ where $g(X)$ 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 (courtesy of Maple) gives

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

Hence

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

and we have found the inverse of β.

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 written 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 $x \mapsto \alpha x\colon R \to R$ 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.

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 $f(\alpha) = 0$;

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:

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

Moreover, each element of $F[\alpha]$ has a unique expression

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}, \qquad a_i \in F,$$

where $m = \deg(f)$. In other words, $1, \alpha, \dots, \alpha^{m-1}$ is a basis for $F[\alpha]$ over F. Hence $[F(\alpha) : F] = m$. Since $F[x] \cong F[\alpha]$, arithmetic in $F[\alpha]$ can be performed using the same rules as in $F[x]$.

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. Maple knows how to compute in $\mathbb{Q}[\alpha]$. For example,

`factor(X^4+4);` returns the factorization

$$(X^2 - 2X + 2)(X^2 + 2X + 2).$$

Now type: `alias(c=RootOf(X^2+2*X+2));`. Then

`factor(X^4+4,c);` returns the factorization

$$(X + c)(X - 2 - c)(X + 2 + c)(X - c),$$

i.e., Maple has factored $X^4 + 4$ in $\mathbb{Q}[c]$ where c has minimum polynomial $X^2 + 2X + 2$.

A field extension E/F is said to be ***algebraic***, or 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

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

this process terminates.

$\Longleftarrow$: Let $E = F(\alpha_1, ..., \alpha_n)$ 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, 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, 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 almost all numbers are transcendental (but it is usually very difficult to prove that any particular number is transcendental).[3]

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.)

1994: Euler's constant

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

[3]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`).

has not yet been proven to be transcendental.

1994: The numbers $e+\pi$ and $e-\pi$ are surely transcendental, but 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.[4] □

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. [5]Suppose not, and let

$$f(X)=X^d+a_1X^{d-1}+\cdots+a_d,\quad a_i\in\mathbb{Q},$$

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,[6] $f(X)=X-\alpha$; 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 $(2^{N!})^dDx_N\in\mathbb{Z}$, and so

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

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

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

[4]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.

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

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

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 (*). □

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 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:

> A line in the F-plane is a line through two points in the F-plane. Such a line is given by an equation:
>
> $$ax + by + c = 0, \quad a, b, c \in F.$$
>
> A circle in the F-plane is a circle with centre an F-point and radius an element of F. Such a circle is given by an equation:
>
> $$(x - a)^2 + (y - b)^2 = c^2, \quad a, b, c \in F.$$

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

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 Rotman 1990, Appendix 3.) □

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 field of the form*

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

PROOF. (a) Immediate from (a) of Lemma 1.35.

(b) From (a) we know that the set of constructible numbers is a field containing $\mathbb{Q}$, and it follows from (a) and Lemma 1.35 that every number in $\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_r}]$ is constructible. Conversely, it follows from Lemma 1.34 that every constructible number is in a field of the form $\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_r}]$. □

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 $[\mathbb{Q}[\sqrt{a_1}, \dots, \sqrt{a_r}] : \mathbb{Q}]$ 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 a 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. 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[7], so also is $\sqrt{\pi}$. □

[7]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. Set $f(X) = X^{p-1} + \cdots + 1$, so that

$$f(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \cdots + a_2X^2 + a_1X + p,$$

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. □

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

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

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

Algebraically closed fields

We say that a polynomial ***splits*** in $F[X]$ 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 $\alpha \in F$.
(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 $f \in \Omega[X]$. 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 all its roots lie in Ω. In particular, $\alpha \in \Omega$. □

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

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

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 (§6) we shall show that the axiom of choice implies that every field has an algebraic closure.

Exercises 1–4

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

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 $a, b, c \in \mathbb{Q}$.

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

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.

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

2 Splitting fields; multiple roots

Maps from simple extensions.

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

$$\varphi\colon E \to E'$$

such that $\varphi(a) = a$ for all $a \in F$. Thus an F-homorphism 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 $\varphi\colon F(\alpha) \to \Omega$, $\varphi(\alpha)$ is transcendental over F, and the map $\varphi \mapsto \varphi(\alpha)$ defines a one-to-one correspondence*

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

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

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

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 indeterminate α with coefficients in F. For any $\gamma \in \Omega$, there is a unique F-homomorphism $\varphi\colon F[\alpha] \to \Omega$ 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 $\varphi\colon F[\alpha] \to \Omega$. 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 $X + f(X) \mapsto \alpha\colon F[X]/(f(X)) \to F[\alpha]$, it 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 $\varphi_0\colon F \to \Omega$ 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*

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

(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*

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

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 $\varphi\colon F(\alpha) \to \Omega$ 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 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.

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

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

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

$$[E_f\colon F] \leq (\deg f)!.$$

PROOF. Let g_1 be an irreducible factor of $f(X)$, and let

$$F_1 = F[X]/(g_1(X)) = F[\alpha_1], \quad \alpha_1 = X + (g_1).$$

Then α_1 is a root of $f(X)$ in F_1, and we define $f_1(X)$ to be the quotient $f(X)/(X - \alpha_1)$ (in $F_1[X]$). The same construction applied to $f_1 \in F_1[X]$ gives us a field $F_2 = F_1[\alpha_2]$ with α_2 a root of f_1 (and hence also of f). By continuing in this fashion, we obtain a splitting field E_f.

Let $n = \deg f$. Then $[F_1 : F] = \deg g_1 \leq n$, $[F_2 : F_1] \leq n - 1, \dots$, and so $[E_f\colon E] \leq n!$. □

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 4.18) or $F = \mathbb{R}$. However, later (4.28) we shall see how to write down large numbers of polynomials (in fact infinitely many) 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 remainder are $\zeta^2, \zeta^3, \dots, \zeta^{p-1}$, 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 remainder are $\alpha + 1, ..., \alpha + p - 1$, and so any field generated over F by α is a splitting field for f (and $F[\alpha] \cong F[X]/(f)$).

(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 n^{th} 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 p^{th} roots of 1.

PROPOSITION 2.7. *Let $f \in F[X]$. Assume that $E \supset F$ is generated by roots of f, and let $\Omega \supset F$ be a field in which f splits.*

(a) *There exists at least one F-homomorphism $\varphi\colon E \to \Omega$.*
(b) *The number of F-homomorphisms $E \to \Omega$ is $\le [E : F]$, and equals $[E : F]$ if f has $\deg(f)$ distinct roots in Ω.*
(c) *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 having $\deg(f)$ distinct roots in Ω, we mean that

$$f(X) = \textstyle\prod_{i=1}^{\deg(f)}(X - \alpha_i), \quad \alpha_i \in \Omega, \quad \alpha_i \ne \alpha_j \text{ if } i \ne j.$$

If f has this property, then so also does any factor of f in $\Omega[X]$.

By assumption, $E = F[\alpha_1, ..., \alpha_m]$ with the α_i roots of $f(X)$. The minimum polynomial of α_1 is an irreducible polynomial f_1 dividing f. As f (hence f_1) splits in Ω, Proposition 2.1 shows that there exists an F-homomorphism $\varphi_1\colon F[\alpha_1] \to \Omega$, and the number of φ_1's is $\le \deg(f_1) = [F[\alpha_1] : F]$, with equality holding when f_1 has distinct roots in Ω.

The minimum polynomial of α_2 over $F[\alpha_1]$ is an irreducible factor f_2 of f in $F[\alpha_1][X]$. According to Proposition 2.2, each φ_1 extends to a homomorphism $\varphi_2\colon F[\alpha_1, \alpha_2] \to \Omega$, and the number of extensions is $\le \deg(f_2) = [F[\alpha_1, \alpha_2] : F[\alpha_1]]$, with equality holding when f_2 has $\deg(f_2)$ distinct roots in Ω.

On combining these statements we conclude that there exists an F-homomorphism $\varphi\colon F[\alpha_1, \alpha_2] \to \Omega$, and that the number of such homomorphisms is $\le [F[\alpha_1, \alpha_2] : F]$, with equality holding when f has $\deg(f)$ distinct roots in Ω.

After repeating the argument several times, we obtain (a) and (b).

Any homomorphism $E \to \Omega$ is injective, and so, if there exists such a homomorphism, $[E : F] \le [\Omega : F]$. Now (a) shows that if E and Ω are both splitting fields for f, then $[E\colon F] = [\Omega\colon F]$, and so any 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 $[E\colon F]$.*

(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 $\leq [E : F]$. Since every F-homomorphism $E \to L$ can be regarded as an F-homomorphism $E \to \Omega$, this proves both (a) and (b). □

REMARK 2.9. 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 is a finite extension Ω/L containing an isomorphic copy of every E_i.

Warning! If E and E' are both splitting fields of $f \in F[X]$, 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.

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 write $\gcd(f, g)$, 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 (2.7c).

We say that f ***has a multiple root*** when at least 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 has contains an element a that is not a p^{th}-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 $f(X) = \sum a_i X^i$ to be $\sum i a_i X^{i-1}$. 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 $\deg(f') < \deg(f)$,

$$\gcd(f, f') \neq 1 \implies f' = 0 \implies f \text{ is a polynomial in } X^p.$$

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

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

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***[8] ***over*** F if none of its irreducible factors has a multiple root (in a splitting field).

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

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

(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).

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 $F = F^p$, i.e., every element of F is a p^{th} power.*

PROOF. We may suppose F is of characteristic $p \neq 0$. If F contains an element a that is not a p^{th} power, then $X^p - a \in F[X]$ is not separable (see 2.11). Conversely, if $F = F^p$, then every polynomial in X^p with coefficients in F is a p^{th} power in $F[X]$ — $\sum a_i X^p = (\sum b_i X)^p$ if $a_i = b_i^p$ — and so it is not irreducible. □

EXAMPLE 2.16. (a) A finite field F is perfect, because the Frobenius endomorphism $a \mapsto a^p \colon F \to F$ 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 p^{th} power.

Exercises 5–10

5*. 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 $\varphi \colon E \to E'$ 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.

6*. (a) Let F be a field of characteristic p. Show that if $X^p - X - a$ is reducible in $F[X]$, then it splits in $F[X]$.
(b) For any prime p, show that $X^p - X - 1$ is irreducible in $\mathbb{Q}[X]$.

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

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

9. 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 $g(X)$.

10*. 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.

3 The fundamental theorem of Galois theory

In this section, 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[9] $X \mapsto \frac{aX+b}{cX+d}$, $ad - bc \neq 0$ (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 $\mathbb{C}(z) \cong \mathbb{C}(X)$, 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.

PROPOSITION 3.2. *If E is a splitting field of a monic 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 monic 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 monic 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 $\mathrm{Aut}(E/F) = 1$.

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

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 p^{th} 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 write

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

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.

PROPOSITION 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 a nontrivial solution $(c_1, \dots, c_n)$ with 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

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

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

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

is also a solution to the system of equations (*). On subtracting it from the first, we obtain a solution $(0, \dots, c_i - \sigma_k(c_i), \dots)$, which is nonzero (look at the i^{th} 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:
- $[E : E^G] \le (G : 1)$ (by 3.4),
- $G \subset \mathrm{Aut}(E/E^G)$ (obvious),
- $(\mathrm{Aut}(E/E^G) : 1) \le [E : E^G]$ (by 2.8a).

The inequalities

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

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 $E[X]$.

Thus, 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

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

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) $\implies$ (b,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

$$[E : F'] = \#\,\mathrm{Aut}(E/F')$$

$$[E : F] = \#\,\mathrm{Aut}(E/F).$$

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

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

(b) $\implies$ (c). By Proposition 3.4, we know that $[E : F] \leq (G : 1)$; in particular, it is finite. Let $\alpha \in E$ and let f be the minimum polynomial of α; we have to 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 p14). 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) $\implies$ (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. 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) $\implies$ (c) of the above theorem we showed that the minimum polynomial of α is $\prod(X - \alpha_i)$.

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 $f \in F[X]$; 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. Let E be a finite extension of F. An element $\alpha \in E$ is said to be ***separable*** over F if its minimum polynomial over F is separable. The elements of E separable over F form a subfield E' of E that is separable over F; write $[E:F]_{\text{sep}} = [E':F]$ (***separable degree*** of E over F). If Ω is an algebraically closed field containing F, then 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,

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

For proofs, see Jacobson 1964, I 10.

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 $G = \mathrm{Gal}(E/F)$. The maps $H \mapsto E^H$ and $M \mapsto \mathrm{Gal}(E/M)$ are inverse bijections between the set of subgroups of G and the set of intermediate fields between E and F:*

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

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., $E^{\sigma H \sigma^{-1}} = \sigma(E^H)$; $\mathrm{Gal}(E/\sigma M) = \sigma\,\mathrm{Gal}(E/M)\sigma^{-1}$.*
(d) *H is normal in $G \iff E^H$ is normal (hence Galois) over F, in which case*

$$\mathrm{Gal}(E^H/F) = G/H.$$

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 E is Galois over E^H by (3.13), which means that $\mathrm{Gal}(E/E^H) = H$.

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) The field E is Galois over E^{H_1}, hence the splitting field of a separable polynomial (3.10), and so (3.2) shows that $[E : E^{H_1}] = \mathrm{Gal}(E/E^{H_1})$. This proves (b) in the case $H_2 = 1$, and the general case follows, using that

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

(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, and let $M = E^H$. Because $\sigma H\sigma^{-1} = H$ for all $\sigma \in G$, we must have $\sigma M = M$ for all $\sigma \in G$, i.e., the action of G on E stabilizes M. We therefore have a homomorphism

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

whose kernel is H. Let G' be the image. Then $F = M^{G'}$, and so M is Galois over F (by Theorem 3.10). Thus, $F = M^{\mathrm{Gal}(M/F)}$, and the first part of the theorem applied to the M/F implies that $\mathrm{Gal}(M/F) = G'$.

Conversely, assume that M is normal over F, and write $M = F[\alpha_1, ..., \alpha_m]$. 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 $M_1, M_2, \dots, M_r$ be intermediate fields, and let H_i be the subgroup corresponding to M_i (i.e., $H_i = \mathrm{Gal}(E/M_i)$). Then (by definition) $M_1M_2\cdots M_r$ is the smallest field containing all M_i; hence it must correspond to the largest subgroup contained in all H_i, which is $\bigcap H_i$. Therefore

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

(b) Let H be a subgroup of G and let $M = E^H$. The largest normal subgroup contained in H is $N = \cap_{\sigma\in G}\sigma H\sigma^{-1}$ (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*

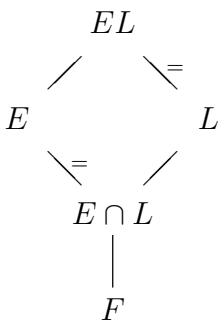
$$\sigma \mapsto \sigma|E \colon \mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/E\cap L)$$

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

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



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*

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

PROOF. According to 1.20,

$$[EL\colon F] = [EL\colon L][L\colon F],$$

but

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

□

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*

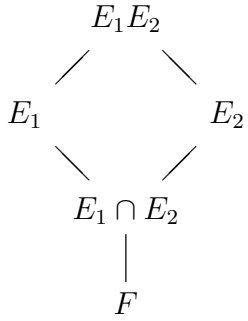
$$\sigma \mapsto (\sigma|E_1, \sigma|E_2) : \mathrm{Gal}(E_1E_2/F) \to \mathrm{Gal}(E_1/F) \times \mathrm{Gal}(E_2/F)$$

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,

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

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

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

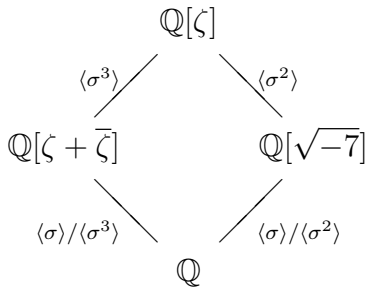
which equals $[E_1E_2\colon F]$ by (3.19). □

Examples

EXAMPLE 3.21. We analyse the extension $\mathbb{Q}[\zeta]/\mathbb{Q}$, where ζ is a primitive 7^{th} 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 $\sigma \in G$, $\sigma\zeta = \zeta^i$, 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 $\sigma^3\zeta = \zeta^6 = \overline{\zeta}$ (complex conjugate of ζ). The subfield of $\mathbb{Q}[\zeta]$ corresponding to $\langle\sigma^3\rangle$ is $\mathbb{Q}[\zeta + \overline{\zeta}]$, and $\zeta + \overline{\zeta} = 2\cos\frac{2\pi}{7}$. Since $\langle\sigma^3\rangle$ is a normal subgroup of $\langle\sigma\rangle$, $\mathbb{Q}[\zeta + \overline{\zeta}]$ is Galois over $\mathbb{Q}$, with Galois group $\langle\sigma\rangle/\langle\sigma^3\rangle$. The conjugates of $\alpha_1 =_{\text{df}} \zeta + \overline{\zeta}$ 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[10] of $\zeta + \overline{\zeta}$ is

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

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

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

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

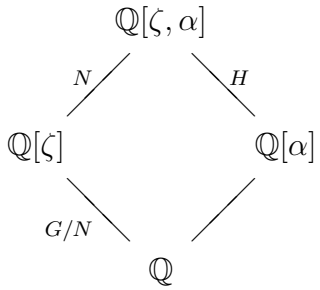
EXAMPLE 3.22. We compute the Galois group of a splitting field E of $X^5 - 2 \in \mathbb{Q}[X]$.

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

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

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

Recall from Exercise 7 that $E = \mathbb{Q}[\zeta, \alpha]$ where ζ is a primitive 5^{th} 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 5^{th} root of 2. We have the picture at right. The degrees



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

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 corresponding to $\mathbb{Q}[\zeta]$ 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, $H \cong G/N \cong (\mathbb{Z}/5\mathbb{Z})^\times$, 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 number α is constructible if and only if it is contained in a field $\mathbb{Q}[\sqrt{a_1}] \cdots [\sqrt{a_r}]$. In particular

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

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

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

PROOF. Suppose $\alpha \in E$ where E is Galois over $\mathbb{Q}$ of degree 2^r, and let $G = \mathrm{Gal}(E/\mathbb{Q})$. From a theorem on the structure of p-groups (GT 6.7), we know there will be 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.

But the next lemma shows that every quadratic extension is obtained by extracting a square root, and we know (1.35) that square roots can be constructed using only a ruler and compass. 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 $G \cong (\mathbb{Z}/p\mathbb{Z})^\times$, which has order $p - 1 = 2^k$. □

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 $\cos \frac{2\pi}{65537}$.

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 elements of $\mathrm{Gal}(F_f/F)$ map roots of f to roots of f, i.e., they map the set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ into itself. Being automorphisms, they define permutations of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. As $F_f = F[\alpha_1, ..., \alpha_n]$, an element of $\mathrm{Gal}(F_f/F)$ is uniquely determined by its action on $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Thus G_f can be identified with a subset of $\mathrm{Sym}(\{\alpha_1, \alpha_2, \ldots, \alpha_n\}) \approx S_n$. In fact, G_f consists of the permutations σ of $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ such that, for $P \in F[X_1, \ldots, X_n]$,

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

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

Note that this shows that $(G_f : 1)$, 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 m^{th} 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 3.26 (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 (5.29). 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 4.29.

REMARK 3.27. 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.
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 11–13

11*. 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.]

12*.[11] Let p be an odd prime, and let ζ be a primitive p^{th} 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 $p \equiv 3 \mod 4$.

13*. 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.

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

4 Computing Galois groups.

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

When is $G_f \subset A_n$?

Consider a polynomial

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

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

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

The ***discriminant*** of f is defined to be $D(f)$. Note that $D(f)$ is nonzero if and only if f has only simple roots, i.e., if f is separable with no multiple factors. Let G_f be the Galois group of f, and identify it with a subgroup of $\mathrm{Sym}(\{\alpha_1, \dots, \alpha_n\})$ (as on p38). The choice of a numbering for the roots determines an isomorphism $\mathrm{Sym}(\{\alpha_1, \dots, \alpha_n\}) \cong S_n$, and the subgroup of $\mathrm{Sym}(\{\alpha_1, \dots, \alpha_n\})$ corresponding to any normal subgroup of S_n is independent of the choice.

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 §4), 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 $G_f =_{df} \mathrm{Gal}(F_f/F)$, 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 $\sigma\Delta(f) = \mathrm{sign}(\sigma)\Delta(f)$ shows that an element of G_f fixes $\Delta(f)$ if and only if it lies in A_n. Thus, under the Galois correspondence,

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

Hence,

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

□

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, Maple knows them: the syntax is "`discrim(f,X);`" where f is a polynomial in the variable X.

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 there is an obvious F-isomorphism $F[\alpha] \to F[\beta]$, namely,

$$F[\alpha] \cong F[X]/(f(X)) \cong F[\beta], \qquad \alpha \leftrightarrow X \leftrightarrow \beta.$$

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 $\alpha \mapsto \beta\colon F[\alpha] \to F_f$ 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 ≤ 3

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 4.28). 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 $\alpha, \beta,$ 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:

$$\begin{array}{c} E \\ \Big| {\scriptstyle G_f\cap V} \\ F[\alpha,\beta,\gamma] \\ \Big| {\scriptstyle G_f/G_f\cap V} \\ F \end{array}$$

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 $f(X) = X^4 + 4X^2 + 2 \in \mathbb{Q}[X]$. 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 4.10. 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 4.11. 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), Maple knows how to factor polynomials with coefficients in $\mathbb{Q}[\alpha]$.

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 4.12. *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 may suppose $\sigma = (1\, 2\, j_3 \ldots j_p)$, and after renumbering again, we may suppose $\sigma = (1\, 2\, 3 \ldots p)$. Then we'll have (12), $(2\, 3)$, $(3\, 4)$, $(4\, 5), \ldots$ in the group generated by σ and τ, and these elements generate S_p. □

PROPOSITION 4.13. *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 $G_f \subset S_p$ 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 4.14. Let $p \geq 5$ be a prime number. Choose a positive even integer m and even integers

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

Let $f(X) = g(X) - 2$, where

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

When we write $f(X) = X^p + a_1 X^{p-1} + \cdots + a_p$, then all a_i are even, and $a_p = -(m \prod n_i) - 2$ is not divisible by 4. Hence Eisenstein's criterion implies that $f(X)$ is irreducible.

The polynomial $g(X)$ certainly has exactly two nonreal roots. Its graph crosses the x-axis exactly $p - 2$ times, and its maxima and minima all have absolute value > 2 (because its values at odd integers have absolute value > 2). Hence the graph of $f(X) = g(X) - 2$ also crosses the x-axis exactly $p - 2$ times, and the proposition applies to f.

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 $X^{q-1}-1$, 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 4.15. *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 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 $a^q - a = 0$ and $b^q - b = 0$, 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 4.16. *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 3.9). □

COROLLARY 4.17. *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 4.18. *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 4.19. *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 4.20. *The field $\mathbb{F}_p$ has an algebraic closure $\mathbb{F}$.*

PROOF. Choose a sequence of integers $1 = n_1 < n_2 < n_3 < \dots$ such that $n_i|n_{i+1}$ for all i, for example, $2 < 2 \times 3 < 2 \times 3 \times 5 < \dots$. Define the fields $\mathbb{F}_{p^{n_i}}$ inductively as follows: $\mathbb{F}_{p^{n_1}} = \mathbb{F}_p$; $\mathbb{F}_{p^{n_{i+1}}}$ is the splitting field of $X^{p^{n_{i+1}}} - X$ over $\mathbb{F}_{p^{n_i}}$. Then, $\mathbb{F}_{p^{n_1}} \subset \mathbb{F}_{p^{n_2}} \subset \mathbb{F}_{p^{n_3}} \subset \cdots$, and we define $\mathbb{F} = \cup \mathbb{F}_{p^{n_i}}$. As a union 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 4.21. 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 $\mathbb{F} = S/\sim$.

Maple factors polynomials modulo p very quickly. The syntax is "`Factor(f(X)) mod p;`". Thus, for example, to obtain a list of all monic polynomials of degree $1, 2,$ or 4 over $\mathbb{F}_5$, ask Maple to factor $X^{625} - X$.

Finite fields were sometimes called[12] ***Galois fields,*** and $\mathbb{F}_q$ used to be denoted $GF(q)$ (it still is in Maple). Maple contains a "Galois field package" to do computations in finite fields. For example, it can find a primitive element for $\mathbb{F}_q$ (i.e., a generator for $\mathbb{F}_q^\times$). To start it, type: `readlib(GF):`.

Computing Galois groups over $\mathbb{Q}$

In the remainder of this section, I sketch a practical method for computing Galois groups over $\mathbb{Q}$ and similar fields. Recall that for a monic separable polynomial $f \in F[X]$, F_f

[12] From a letter to the Notices of the AMS, February 2003 (Pálfy): "full credit should be given to [Galois] for constructing finite fields in general. In one of the few papers published during his short lifetime, entitled "Sur la théorie des nombres", which appeared in the Bulletin des Sciences Mathématiques in June 1830, Galois — at that time not even nineteen years old — defined finite fields of arbitrary prime power order and established their basic properties, e.g. the existence of a primitive element. So it is fully justified when finite fields are called Galois fields and customarily denoted by $GF(q)$."

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

PROOF. Let $\alpha_1, \ldots, \alpha_m$, $m = \deg f$, be the roots of $f(X)$ in F_f. The monic factors of $f(X)$ in $F_f[X]$ correspond to subsets S of $\{\alpha_1, \ldots, \alpha_m\}$,

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

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 $\{\alpha_1, \ldots, \alpha_m\}$ stable under G_f, but these subsets S are precisely the orbits of G_f in $\{\alpha_1, \ldots, \alpha_m\}$. □

REMARK 4.23. Note that the proof shows the following: let $\{\alpha_1, \ldots, \alpha_m\} = \bigcup O_i$ be the decomposition of $\{\alpha_1, \ldots, \alpha_m\}$ into a disjoint union of orbits for the group G_f; then

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

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 $\sigma\colon x \mapsto x^p$. 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 4.22). Hence, if the degrees of the distinct irreducible factors of f are $m_1, m_2, \ldots, m_r$, then σ has a cycle decomposition of type

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

LEMMA 4.24. *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 $\overline{f}$ be the image of f in $(R/P)[X]$. Assume that neither f nor $\overline{f}$ has a multiple root. Then the roots $\alpha_1, \ldots, \alpha_m$ of f lie in some finite extension R' of R, and their reductions $\overline{\alpha}_i$ modulo PR' are the roots of $\overline{f}$. Moreover $G_{\overline{f}} \subset G_f$ when both are identified with subgroups of* $\mathrm{Sym}\{\alpha_1, \ldots, \alpha_m\} = \mathrm{Sym}\{\overline{\alpha}_1, \ldots, \overline{\alpha}_m\}$.

PROOF. Omitted — see van der Waerden, Modern Algebra, I, §61 (second edition) or ANT 3.43. □

On combining these results, we obtain the following theorem.

THEOREM 4.25 (DEDEKIND). *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree m, and let p be a prime such that $f \mod p$ has simple roots (equivalently, $D(f)$ is not divisible by p). Suppose that $\overline{f} = \prod f_i$ with f_i irreducible of degree m_i in $\mathbb{F}_p[X]$. Then G_f contains an element whose cycle decomposition is of type*

$$m = m_1 + \cdots + m_r = m.$$

EXAMPLE 4.26. 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 (4.12).

LEMMA 4.27. *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 $1 \leq i \leq n-1$. 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 4.28. 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) $f_2 = (\text{degree } 1)(\text{irreducible of degree } n-1) \mod 3$;
(c) $f_3 = (\text{irreducible of degree } 2)(\text{product of } 1 \text{ or } 2 \text{ irreducible polys of odd degree}) \bmod 5$.

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, $n \leq 11$, and gives the cycle types of their elements and the orbit lengths of the subgroup acting on the r-sets of

roots. With few exceptions, these invariants are sufficient to determine the subgroup up to isomorphism.

Maple V can compute Galois groups for polynomials of degree ≤ 7 over $\mathbb{Q}$. To learn the syntax, type "`?galois;`".

See also, Soicher and McKay, *Computing Galois groups over the rationals*, J. Number Theory, 20 (1985) 273–281.

Exercises 14–20

14*. Find the splitting field of $X^m - 1 \in \mathbb{F}_p[X]$.

15*. Find the Galois group of $X^4 - 2X^3 - 8X - 3$ over $\mathbb{Q}$.

16*. Find the degree of the splitting field of $X^8 - 2$ over $\mathbb{Q}$.

17*. Give an example of a field extension E/F of degree 4 such that there does not exist a field M with $F \subset M \subset E$, $[M : F] = 2$.

18. List all irreducible polynomials of degree 3 over $\mathbb{F}_7$ in 10 seconds or less (there are 112).

19. "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 "galois" command in Maple?

20*. 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.

Additional exercise: 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.

5 Applications of Galois theory

In this section, 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 13) 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.

We say 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 $E = F[\alpha_1,...,\alpha_r]$ be a finite extension of F, and assume that $\alpha_2,...,\alpha_r$ 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 (4.15). Hence we may assume F to be infinite. It suffices to prove the statement for $r = 2$. 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 $F[\gamma][X]$, 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. Assume F to be 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 α's are not separable, then the extension need not be simple. Before giving an example to demonstrate, 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 $[k(X,Y) : F] = p^2$. Hence there are infinitely many distinct intermediate fields.[13]

Fundamental Theorem of Algebra

We finally prove the misnamed[14] 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".)

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 $\sqrt{\alpha} = c+di$.

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.

[13] 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.

[14] 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.

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 have 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 4.15). 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*** n^{th} 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 n^{th} root of 1 in E.*

(b) *If ζ is a primitive n^{th} 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 n^{th} roots of 1. The n^{th} 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 n^{th} 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 n^{th} root of 1, then the remaining primitive n^{th} 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 n^{th} 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 n^{th} 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 $[\mathbb{Q}[\zeta] : \mathbb{Q}] = p - 1$, 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 $d|n$. The quotient of $X^n - 1$ by all these factors for $d < n$ is called the n^{th} ***cyclotomic polynomial*** Φ_n. Thus

$$\Phi_n = \prod (X - \zeta) \qquad \text{(product over the primitive } n^{\text{th}} \text{ roots of } 1).$$

It has degree $\varphi(n)$, the order of $(\mathbb{Z}/n\mathbb{Z})^\times$. Since every n^{th} root of 1 is a primitive d^{th} root of 1 for exactly one d dividing n, we see that

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

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 Maple by typing:

```
with(numtheory);
cyclotomic(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 $\mathbb{Z}$ (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 n^{th} root of 1 in some extension field. The following are equivalent:*

(a) *the n^{th} cyclotomic polynomial Φ_n is irreducible;*
(b) *the degree $[F[\zeta] : F] = \varphi(n)$;*
(c) *the homomorphism*

$$\mathrm{Gal}(F[\zeta]/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$$

is an isomorphism.

PROOF. Because ζ is a root of Φ_n, the minimum polynomial of ζ divides Φ_n. It is equal to it if and only if $[F[\zeta] : F] = \varphi(n)$, which is true if and only if the injection $\mathrm{Gal}(F[\zeta]/F) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ is onto. □

THEOREM 5.10. *The n^{th} 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 n^{th} roots of 1, and we have to show they include ***all*** primitive n^{th} 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 $h(X) \mapsto \overline{h}(X)$ for the map $\mathbb{Z}[X] \mapsto \mathbb{F}_p[X]$, and note that

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

But $\overline{g}(X^p) = \overline{g}(X)^p$ (use the $\mod p$ binomial theorem and that $a^p = a$ for all $a \in \mathbb{F}_p$), and so $\overline{f}(X)$ and $\overline{g}(X)$ 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 have ***only*** been 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 $\overline{f} = 0$ 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 3.10)

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

and this is a power of 2 if and only if n has the required form. □

REMARK 5.13. The final section of Gauss's, *Disquisitiones Arithmeticae* (1801) is titled "Equations defining sections of a Circle". In it Gauss proves that the n^{th} 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[15]. 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.

Independence of characters

THEOREM 5.14 (DEDEKIND'S THM ON THE INDEPENDENCE OF CHARACTERS). *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 $\sum_{i=1}^m c_i\sigma_i \colon E \to \Omega$ 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. □

[15] "Whenever $n-1$ involves prime factors other than 2, we are always led to equations of higher degree....WE CAN SHOW WITH ALL RIGOR THAT THESE HIGHER-DEGREE EQUATIONS CANNOT BE AVOIDED IN ANY WAY NOR CAN THEY BE REDUCED TO LOWER-DEGREE EQUATIONS. The limits of the present work exclude this demonstration here, but we issue this warning lest anyone attempt to achieve geometric constructions for sections other than the ones suggested by our theory (e.g. sections into 7, 9, 11, 13, 19, etc. parts) and so spend his time uselessly." Ibid. §365.

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 (4.16), this covers all cases.

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 variable 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, $\det(A) = f(X_1, \dots, X_m)$. Clearly, $f(1, 0, \dots, 0)$ 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, f is not identically zero, and so there exists an $\alpha \in E^\times$ such that $f(\sigma_1\alpha, \dots, \sigma_m\alpha)$ $(= \det(\sigma_i\sigma_j\alpha))$ 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

$$\textstyle\sum_{j=1}^m a_j\sigma_j\alpha = 0$$

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

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

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 $\mathrm{id}, \sigma_0, \dots, \sigma_0^{n-1}$ 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 $f\colon G \to M$ 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 $f\colon G \to M$ be a crossed homomorphism. For any $\sigma \in G$,

$$\begin{aligned} f(\sigma^2) &= f(\sigma) + \sigma f(\sigma), \\ f(\sigma^3) &= f(\sigma \cdot \sigma^2) = f(\sigma) + \sigma f(\sigma) + \sigma^2 f(\sigma) \\ &\dots = \dots \\ f(\sigma^n) &= f(\sigma) + \sigma f(\sigma) + \cdots + \sigma^{n-1} f(\sigma). \end{aligned}$$

Thus, if G is a cyclic group of order n generated by σ, then a crossed homomorphism $f\colon G \to M$ is determined by its value, x say, on σ, and x satisfies the equation

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

Conversely, if $x \in M$ satisfies (*), then the formulas $f(\sigma^i) = x + \sigma x + \cdots + \sigma^{i-1}x$ define a crossed homomorphism $f\colon G \to M$. Thus, for a finite group $G = \langle\sigma\rangle$, there is a one-to-one correspondence

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

(b) For any $x \in M$, we obtain a crossed homomorphism by putting

$$f(\sigma) = \sigma x - x, \qquad \text{all } \sigma \in G.$$

Such a crossed homomorphism 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.

EXAMPLE 5.21. Let $\pi\colon \tilde{X} \to X$ 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 $H^1(X, \mathcal{M}) \cong H^1(\Gamma, M)$. For example, when $M = \mathbb{Z}$ with the trivial action of Γ, this becomes the isomorphism $H^1(X, \mathbb{Z}) \cong H^1(\Gamma, \mathbb{Z}) = \mathrm{Hom}(\Gamma, \mathbb{Z})$.

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

$$\textstyle\sum_{\tau\in G} f(\tau)\tau\colon E \to E$$

is not the zero map, i.e., there exists an $\alpha \in E$ such that

$$\beta \overset{\text{df}}{=} \textstyle\sum_{\tau\in G} f(\tau)\tau\alpha \neq 0.$$

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

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

which equals $f(\sigma)^{-1}\beta$ because, as τ runs over G, so also does $\sigma\tau$. Therefore, $f(\sigma) = \frac{\beta}{\sigma(\beta)}$ and we can take $\beta = \gamma^{-1}$. □

Let E be a Galois extension of F with Galois group G. We define the ***norm*** of an element $\alpha \in E$ to be

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

For $\tau \in G$,

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

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

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

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 if α is of the form $\frac{\beta}{\tau\beta}$, then $\operatorname{Nm}(\alpha) = 1$. Our next result show that, for cyclic extensions, all elements with norm 1 are of this form.

COROLLARY 5.24 (HILBERT'S THEOREM 90). [16]*Let E be a finite cyclic extension of F with Galois group $\langle\sigma\rangle$; if $\operatorname{Nm}_{E/F}\alpha = 1$, then $\alpha = \beta/\sigma\beta$ for some $\beta \in E$.*

PROOF. Let $m = [E : F]$. The condition on α is that $\alpha\cdot\sigma\alpha\cdots\sigma^{m-1}\alpha = 1$, and so (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 $f(\sigma) = \beta/\sigma\beta$. □

Cyclic extensions.

We are now able to classify the cyclic extensions of degree n of a field F in the case that F contains n n^{th} roots of 1.

THEOREM 5.25. *Let F be a field containing a primitive n^{th} root of 1.*

(a) *The Galois group of $X^n - a$ is cyclic of order dividing n.*
(b) *Conversely, if E is cyclic of degree n over F, then there is an element $\beta \in E$ such that $E = F[\beta]$ and $\beta^n \in F$; hence E is the splitting field of $X^n - \beta^n$.*

[16]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.

PROOF. (a) If α is one root of $X^n - a$, then the other roots are the elements of the form $\zeta\alpha$ with ζ an n^{th} root of 1. Hence the splitting field of $X^n - a$ is $F[\alpha]$. The map $\sigma \mapsto \frac{\sigma\alpha}{\alpha}$ is an injective homomorphism from $\mathrm{Gal}(F[\alpha]/F)$ into the cyclic group $\langle\zeta\rangle$.

(b) Let ζ be a primitive n^{th} root of 1 in F, and let σ generate $\mathrm{Gal}(E/F)$. Then $\mathrm{Nm}\,\zeta = \zeta^n = 1$, and so, according to Hilbert's Theorem 90, there is an element $\beta \in E$ such that $\sigma\beta = \zeta\beta$. Then $\sigma^i\beta = \zeta^i\beta$, and so only the identity element of $\mathrm{Gal}(E/F)$ fixes β — we conclude by the fundamental theorem of Galois theory that $E = F[\beta]$. On the other hand $\sigma\beta^n = \zeta^n\beta^n = \beta^n$, and so $\beta^n \in F$. □

REMARK 5.26. (a) Assume F contains a primitive n^{th} root of 1. Then, two cyclic extension $F[a^{\frac{1}{n}}]$ and $F[b^{\frac{1}{n}}]$ of F are isomorphic if and only if a and b generate the same subgroup of $F^\times/F^{\times n}$.

(b) The polynomial $X^n - a$, $n \geq 2$, is irreducible in $F[X]$ under the following condition: a is not a p^{th} 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.

(c) If F has characteristic p (hence has no p^{th} 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.

REMARK 5.27 (KUMMER THEORY). Theorem 5.25 and Remark 5.26a classify the cyclic extensions of F order n in the case that F contains a primitive n^{th} root of 1. Under the same assumption on F, it is possible to extend this to a classification of the Galois extensions of F with abelian Galois group of exponent n (i.e., with Galois group a quotient of $(\mathbb{Z}/n\mathbb{Z})^r$ for some r).

Let E be such an extension of F, and let

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

Then $S(E)$ is a subgroup of $F^\times$ containing $F^{\times n}$, and the map $E \mapsto S(E)$ defines a one-to-one correspondence between the abelian extensions of E of exponent n and the groups $S(E)$,

$$F^\times \supset S(E) \supset F^{\times n},$$

such that $(S(E) : F^{\times n}) < \infty$. The field E is recovered from $S(E)$ as the splitting field of $\prod(X^n - a)$ (product over a set of representatives for $S(E)/F^{\times n}$). Moreover, there is a perfect pairing

$$(a, \sigma) \mapsto \frac{\sigma a}{a} \colon \frac{S(E)}{F^{\times n}} \times \mathrm{Gal}(E/F) \to \mu_n \text{ (group of } n^{th} \text{ roots of } 1).$$

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

Proof of Galois's solvability theorem

LEMMA 5.28. *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 $\alpha_1, \dots, \alpha_m$ be the roots of $f(X)$ in E'. Then $E = F[\alpha_1, ..., \alpha_m]$ is a splitting field of f over F. 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 5.29. *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 n^{th} 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 5.25b 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 n^{th} root ζ of 1. For example, choose a primitive element γ for F_m/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

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

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

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

in which each field F'' is obtained from its predecessor F' by adjoining an r^{th} root of an element of F' ($r = r_1, \dots, r_m$, or n). According to (5.8) and (5.25a), each of these extensions is cyclic, 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 5.29 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

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

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 5.30 (SYMMETRIC POLYNOMIALS THEOREM). *Every symmetric polynomial $P(X_1, ..., X_n)$ in $R[X_1, ..., X_n]$ is equal to a polynomial in the elementary symmetric polynomials with coefficients in R, i.e., $P \in R[p_1, ..., p_n]$.*

PROOF. We define an ordering on the monomials in the X_i by requiring that

$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} > X_1^{j_1}X_2^{j_2}\cdots X_n^{j_n}$$

if either

$$i_1 + i_2 + \cdots + i_n > j_1 + j_2 + \cdots + j_n$$

or equality holds and, for some s,

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

For example,

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

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

$$X_1^{d_1+d_2+\cdots+d_n}X_2^{d_2+\cdots+d_n}\cdots X_n^{d_n}. \tag{1}$$

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 5.31 (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 $F(p_1,...,p_n)$.*

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 $F[p_1,\dots,p_n]$ (5.30). Hence their quotient $f = Hf/H$ lies in $F(p_1,\dots,p_n)$. □

COROLLARY 5.32. *The field $F(X_1,...,X_n)$ is Galois over $F(p_1,...,p_n)$ with Galois group S_n (acting by permuting the X_i).*

PROOF. We have shown that $F(p_1,\dots,p_n) = F(X_1,\dots,X_n)^{S_n}$, and so this follows from (3.10). □

The general polynomial of degree n

THEOREM 5.33. *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

$$t_i \mapsto p_i \colon F[t_1, \dots, t_n] \to F[p_1, \dots, p_n]$$

is injective (i.e., the p_i are algebraically independent over F, see p77), then it will extend to an isomorphism

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

sending $f(X)$ to

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

But $g(X) = \prod(X - X_i)$ in $F(X_1, \dots, X_n)[X]$, and so $F(X_1, \dots, X_n)$ is the splitting field of $g(X)$ over $F(p_1, \dots, p_n)$. Corollary 5.32 then shows that g has Galois group S_n, which must also be the Galois group of f.

Let $P(t_1, \dots, t_n)$ be such that $P(p_1, \dots, p_n) = 0$. Equation 1, 64, shows that if $m_1(t_1, \dots, t_n)$ and $m_2(t_1, \dots, t_n)$ are distinct monomials, then $m_1(p_1, \dots, p_n)$ and $m_2(p_1, \dots, p_n)$ have distinct highest monomials. Therefore, cancellation can't occur, and so $P(t_1, \dots, t_n)$ must be the zero polynomial. □

REMARK 5.34. 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 variables), then it occurs infinitely often as a Galois group over $\mathbb{Q}$. For the proof, realize E as the splitting field of a polynomial $f(X) \in k[t_1, \dots, t_n][X]$ 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 $F(X_1, \dots, X_n)^G \approx F(t_1, ..., t_n)$ (for variables t_i). Unfortunately, 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 5.35. Take $F = \mathbb{C}$, and consider the subset of $\mathbb{C}^{n+1}$ defined by the equation

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

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

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

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

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

The discriminant $D(f)$ of $f(X) = X^n - T_1X^{n-1} + \cdots + (-1)^n T_n$ is a polynomial in $\mathbb{C}[T_1, \dots, T_n]$. 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 $A = (a_{ij})$

$$\begin{array}{rcll} \operatorname{Tr}(A) & = & \sum_i a_{ii} & \text{(trace of } A\text{)} \\ \det(A) & = & \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}, & \text{(determinant of } A\text{)} \\ c_A(X) & = & \det(XI_n - A) & \text{(characteristic polynomial of } A\text{).} \end{array}$$

Moreover,

$$c_A(X) = X^n - \operatorname{Tr}(A)X^{n-1} + \cdots + (-1)^n \det(A).$$

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[17]

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

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

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

[17]The coefficients of the characteristic polynomial

$$c_\alpha(X) = X^n + c_1X^{n-1} + \cdots + c_n,$$

of α have the following description

$$c_i = (-1)^i \operatorname{Tr}(\alpha | \Lambda^i V)$$

— 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

$$\alpha_L\colon E \to E, \quad x \mapsto \alpha x,$$

and we define

$$\mathrm{Tr}_{E/F}(\alpha) = \mathrm{Tr}(\alpha_L),\ \mathrm{Nm}_{E/F}(\alpha) = \det(\alpha_L),\ c_{\alpha,E/F}(X) = c_{\alpha_L}(X).$$

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 5.36. (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 $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, 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 $n = [E:F]$.

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 5.37. *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 $\beta_1, ..., \beta_n$ be a basis for $F[\alpha]$ over F, and let $\gamma_1, ..., \gamma_m$ 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, $A =_{\text{df}} (a_{ij})$ 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 5.38. *Suppose that the roots of the minimum polynomial of α are $\alpha_1, \dots, \alpha_n$ (in some splitting field containing E), and that $[E : F[\alpha]] = m$. 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 5.39. (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

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

REMARK 5.40. 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 5.38 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 $[E : F[\alpha]]$ times (because each F-homomorphism $F[\alpha] \to \Omega$ has $[E : F[\alpha]]$ 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 5.41. *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 5.42. *Let $f(X) \in F[X]$ factor as $f(X) = \prod_{i=1}^{m}(X - \alpha_i)$ in some splitting field, and let $\alpha = \alpha_1$. Then, with $f' = \frac{df}{dX}$ (formal derivative), we have*

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

PROOF. Compute that

$$\begin{aligned}
\operatorname{disc} f(X) &\overset{\text{df}}{=} \textstyle\prod_{i<j}(\alpha_i - \alpha_j)^2 \\
&= (-1)^{m(m-1)/2} \cdot \textstyle\prod_i(\prod_{j\neq i}(\alpha_i - \alpha_j)) \\
&= (-1)^{m(m-1)/2} \cdot \textstyle\prod_i f'(\alpha_i) \\
&= (-1)^{m(m-1)/2} \operatorname{Nm}_{F[\alpha]/F}(f'(\alpha)) \qquad \text{(by 5.40).}
\end{aligned}$$

□

EXAMPLE 5.43. 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

$$\gamma \overset{\text{df}}{=} f'(\alpha) = n\alpha^{n-1} + a, \quad f(\alpha) = 0.$$

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 Maple V 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 21–23

21*. 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}.

22*. 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 $\mathbb{Q}[i]/\mathbb{Q}$.)

23*. Prove that a finite extension of $\mathbb{Q}$ can contain only finitely many roots of 1.

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 (4.20), 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[18] 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.*

Zorn's Lemma[19] 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).

[18] 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.

[19] 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.

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.)[20] 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 $\otimes_F A_i$ to be the quotient of the F-vector space with basis ΠA_i by the subspace generated by elements of the form:

$(x_i) + (y_i) - (z_i)$ with $x_j + y_j = z_j$ for one $j \in I$ and $x_i = y_i = z_i$ for all $i \neq j$;

$(x_i) - a(y_i)$ with $x_j = ay_j$ for one $j \in I$ and $x_i = y_i$ for all $i \neq j$.

It can be made into a commutative F-algebra in an obvious fashion (Bourbaki, 1989, Chap. 3, 3.9)[21], and there are canonical homomorphisms $A_i \to \otimes_F A_i$ of F-algebras.

For each polynomial $f \in F[X]$, choose a splitting field E_f, and let $\Omega = (\otimes_F E_f)/M$ where M is a maximal ideal in $\otimes_F E_f$ (whose existence is ensured by Zorn's lemma). Note that $F \subset \otimes_F E_f$ and $M \cap F = 0$. Then Ω has no ideals other than (0) and Ω, and hence is a field (see 1.2). The composite of the F-homomorphism $E_f \to \otimes_F E_f \to \Omega$, 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 (1.44).

Second proof of the existence of algebraic closures

(Jacobson 1964, p144.). After (4.20) 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

(E. Artin, see Dummit and Foote 1991, 13.4). Consider the polynomial ring $F[\ldots, x_f, \ldots]$ in a family of variables x_f indexed by the nonconstant monic polynomials $f \in F[X]$. If 1

[20] 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

[21] 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.

lies in the ideal I in $F[\dots, x_f, \dots]$ 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 F' be an extension of F containing a root α_i of f_i, $i = 1, \dots, n$. Under the F-homomorphism $F[\dots, x_f, \dots] \to F'$,

$$\begin{cases} x_{f_i} \mapsto \alpha_i \\ x_f \mapsto 0, \quad f \notin \{f_1, \dots, f_n\} \end{cases}$$

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. Let $E_1 = F[\dots, x_f, \dots]/M$. Then E_1 is a field containing (a copy of) F in which every nonconstant polynomial in $F[X]$ has at least one root. Repeat the process starting with E_1 instead of F to obtain a field E_2. Continue in this way to obtain a sequence of fields

$$F = E_0 \subset E_1 \subset E_2 \subset \cdots,$$

and let $E = \bigcup E_i$. Then E is algebraically closed, because the coefficients of any nonconstant polynomial $g \in E[X]$ lie in E_i for some i, and then g has a root in E_{i+1}. Therefore, the algebraic closure of F in E is an algebraic closure of F (1.46).[22]

(Non)uniqueness of algebraic closures

THEOREM 6.5 (*). *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 $\varphi' \colon M' \to \Omega$ 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 $\alpha \in \varphi(E)$. □

[22] In fact, E is algebraic over F. To see this, note that E_1 is generated by algebraic elements over F, and so is algebraic over F (apply 1.45). Similarly, E_2 is algebraic over E_1 and therefore also over F (see 1.31b). Continuing in this way, we find that every element of every E_i is algebraic over F.

The above proof is a typical application of Zorn's lemma: once we know how to do something in a finite (or countable) situation, Zorn's lemma allows us to do it in general.

REMARK 6.6. 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 $\Omega \to \Omega'$.

7 Infinite Galois extensions

Recall (3.10) 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. Equivalently, a field $\Omega \supset F$ is Galois over F if it is a union of subfields E finite and Galois over F.

For a Galois extension Ω/F, we let $\mathrm{Gal}(\Omega/F) = \mathrm{Aut}(\Omega/F)$. Consider the map

$$\sigma \mapsto (\sigma|E)\colon\ \mathrm{Gal}(\Omega/F) \to \prod \mathrm{Gal}(E/F)$$

(product over the finite Galois extensions E of F contained in Ω). This map is injective, because Ω is a union of finite Galois extensions. We give each finite group $\mathrm{Gal}(E/F)$ the discrete topology and $\prod \mathrm{Gal}(E/F)$ the product topology, and we give $\mathrm{Gal}(\Omega/F)$ the subspace topology. Thus the subgroups $\mathrm{Gal}(\Omega/E)$, $[E : F] < \infty$, form a fundamental system of neighbourhoods of 1 in $\mathrm{Gal}(\Omega/F)$.

By the Tychonoff theorem, $\prod \mathrm{Gal}(E/F)$ is compact, and it is easy to see that the image of $\mathrm{Gal}(\Omega/F)$ is closed — hence it is compact and Hausdorff.

THEOREM 7.1. *Let Ω be Galois over F with Galois group G. The maps*

$$H \mapsto \Omega^H, \quad M \mapsto \mathrm{Gal}(\Omega/M)$$

*define a one-to-one correspondence between the **closed** subgroups of G and the intermediate fields M. A field M is of finite degree over F if and only if $\mathrm{Gal}(\Omega/M)$ is open in $\mathrm{Gal}(\Omega/F)$.*

PROOF. Omit—it is not difficult given the finite case. See for example, E. Artin, Algebraic Numbers and Algebraic Functions, p103. □

REMARK 7.2. The remaining assertions in the Fundamental Theorem of Galois Theory carry over to the infinite case provided that one requires the subgroups to be closed.

EXAMPLE 7.3. 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 $a_i \equiv 0 \mod n$. 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 $\alpha \mapsto \sigma^\alpha \colon \hat{\mathbb{Z}} \to \mathrm{Gal}(\Omega/\mathbb{F}_p)$ 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 7.4. 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...). 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.*)

8 Transcendental extensions

In this section we consider fields $\Omega \supset F$ with Ω much bigger than F. For example, we could have $\mathbb{C} \supset \mathbb{Q}$.

Elements $\alpha_1, ..., \alpha_n$ of Ω give rise to an F-homomorphism

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

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

$$a_{i_1,\dots,i_n} \in F, \quad \sum a_{i_1,\dots,i_n}\alpha_1^{i_1}...\alpha_n^{i_n} = 0 \implies a_{i_1,\dots,i_n} = 0 \text{ all } i_1, ..., i_n.$$

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

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

is an injection, and hence an isomorphism. This isomorphism then extends to the fields of fractions,

$$X_i \mapsto \alpha_i\colon F(X_1, ..., X_n) \to F(\alpha_1, ..., \alpha_n)$$

In this case, $F(\alpha_1, ..., \alpha_n)$ is called a ***pure transcendental extension*** of F. The polynomial

$$f(X) = X^n - \alpha_1 X^{n-1} + \dots (-1)^n \alpha_n$$

has Galois group S_n over $F(\alpha_1, ..., \alpha_n)$ (5.33).

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 $\gamma^n + \beta_1\gamma^{n-1} + \dots + \beta_n = 0$;*
(c) *there exist $\beta_0, \beta_1, \dots, \beta_n \in F[A]$, not all 0, such that $\beta_0\gamma^n + \beta_1\gamma^{n-1} + \dots + \beta_n = 0$;*
(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 $F[X_1,\dots,X_m]$,

$$f(X_1,\dots,X_m,Y)=\sum f_i(X_1,\dots,X_m)Y^{n-i}.$$

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 section 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
$A\subset$ span(B)	A algebraically dependent on B
basis	transcendence basis
dimension	transcendence degree

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 $m\le n$.

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

$$B_1 \stackrel{\text{df}}{=} B \cup \{\alpha_{k+1}\} \smallsetminus \{\beta_j\}.$$

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 $\alpha \in S$ that is algebraically dependent on $S \smallsetminus \{\alpha\}$. 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 $F(A)$. □

THEOREM 8.13 (*). *Every field Ω containing F has a transcendence basis over F.*

PROOF. Let S be the set of algebraically independent subsets of Ω. We can partially order it by inclusion. Let T be a totally ordered subset, and let $B = \cup\{A \mid A \in T\}$. 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, which, according to Proposition 8.12, is a transcendence basis for Ω over F. □

It is possible to show that any two (possibly infinite) transcendence bases for Ω over F have the same cardinality. The cardinality of a transcendence basis for Ω over F is called the ***transcendence degree*** of Ω over F. For example, the pure transcendental extension $F(X_1, \ldots, X_n)$ has transcendence degree n over F.

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

EXAMPLE 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 $\varphi\colon A \to A'$, which φ extends uniquely to an F-isomorphism $\varphi\colon F[A] \to F[A']$, 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 6.5). □

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 31 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 (or, so I've been told), and it is known that the Zorn's Lemma (equivalently, the Axiom of Choice) is required to construct nonmeasurable functions.

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 5.34). 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).

A Review exercises

24. 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?

25. 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 $\mathbb{Q}$?

26. Prove that the two fields $\mathbb{Q}[\sqrt{7}]$ and $\mathbb{Q}[\sqrt{11}]$ are not isomorphic.

27.
(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.

28. 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.

29. Prove as directly as you can that if ζ is a primitive p^{th} root of 1, p prime, then the Galois group of $\mathbb{Q}[\zeta]$ over $\mathbb{Q}$ is cyclic of order $p - 1$.

30. 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.

31.
(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.

32. Let F be a field with 16 elements. How many roots in F does each of the following polynomials have? $X^3 - 1$; $X^4 - 1$; $X^{15} - 1$; $X^{17} - 1$.

33. Find the degree of a splitting field of the polynomial $(X^3 - 5)(X^3 - 7)$ over $\mathbb{Q}$.

34. Find the Galois group of the polynomial $X^6 - 5$ over each of the fields $\mathbb{Q}$ and $\mathbb{R}$.

35. 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.

36. 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 $n!$.

37. Find a primitive element for the field $\mathbb{Q}[\sqrt{3}, \sqrt{7}]$ over $\mathbb{Q}$, i.e., an element such that $\mathbb{Q}[\sqrt{3}, \sqrt{7}] = \mathbb{Q}[\alpha]$.

38. 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.)?

39. Let F be a finite field of characteristic $\neq 2$. Prove that $X^2 = -1$ has a solution in F if and only if $\#F \equiv 1 \mod 4$.

40. 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 $E = \mathbb{Q}[\alpha]$.)

41. 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.

42. Let ζ be a primitive 12^{th} root of 1 over $\mathbb{Q}$. How many fields are there strictly between $\mathbb{Q}[\zeta^3]$ and $\mathbb{Q}[\zeta]$.

43. For the polynomial $X^3 - 3$, find explicitly its splitting field over $\mathbb{Q}$ and elements that generate its Galois group.

44. 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 $i = \sqrt{-1}$.

45. Let E be an extension field of F, and let Ω be an algebraic closure of E. Let $\sigma_1, \ldots, \sigma_n$ be distinct F-isomorphisms $E \to \Omega$.

(a) Show that $\sigma_1, \ldots, \sigma_n$ are linearly dependent over Ω.
(b) Show that $[E : F] \geq m$.
(c) Let F have characteristic $p > 0$, and let L be a subfield of Ω containing E and such that $a^p \in E$ for all $a \in L$. Show that each σ_i has a unique extension to a homomorphism $\sigma_i' : L \to \Omega$.

46. Identify the Galois group of the splitting field K of $X^4 - 3$ over $\mathbb{Q}$. Determine the number of quadratic subfields.

47. 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.)

48. Prove or disprove by counterexample.

(a) If L/K is an extension of fields of degree 2, then there is an automorphism σ of L such that K is the fixed field of σ.
(b) The same as (a) except that L is also given to be finite.

49. 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 $[F : K] = 100$.

50. 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.

51. 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, $0 \leq i \leq n-1$, $[F_{i+1} : F_i] = 3$.

52. 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 $[F : \mathbb{Q}]$?

53. 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 $2^{d!}$.

54. 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) $(X^2 + 3)(X^5 - 1)$.

55. 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.)

56. Find the group of $\mathbb{Q}$-automorphisms of the field $k = \mathbb{Q}[\sqrt{-3}, \sqrt{-2}]$.

57. 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.

58. 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 $[K : F] = 2$.

59. 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 p^{th} power. Show that there exists an automorphism α of K such that $\theta\alpha^2 = 1$ if and only if n is odd.

60. Describe the splitting field and Galois group, over $\mathbb{Q}$, of the polynomial $X^5 - 9$.

61. 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) $K_1 K_2 = E$.

62. 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.

63. 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: $X^{80} - 1$, $X^{81} - 1$, $X^{88} - 1$.

64. Describe the Galois group of the polynomial $X^6 - 7$ over $\mathbb{Q}$.

65. 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 $F \supset L \supset K$.

66. Find the splitting field and Galois group of the polynomial $X^3 - 5$ over the field $\mathbb{Q}[\sqrt{2}]$.

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

68. 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.

69. 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 $\rho\colon \mathbb{Q}[\alpha] \to \mathbb{C}$. 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 $\rho\colon \mathbb{Q}[\alpha] \to \mathbb{C}$.

70. 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.

71. 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 $\mathbb{C}$.]

72. 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 $\mathbb{Q}[X]$.

73. 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 $E = \mathbb{Q}[\gamma]$.

74. 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 $\sigma(x) = x^{-1}$.

75. 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 $\#F$.

76. Let L/K be an algebraic extension of fields. Prove that L is algebraically closed if every polynomial over K factors completely over L.

77. 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.

78. 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.

79. 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.

80. Let ζ be a primitive 7^{th} 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 $\mathbb{Q}$.

81. Find the degree over $\mathbb{Q}$ of the Galois closure K of $\mathbb{Q}[2^{\frac{1}{4}}]$ and determine the isomorphism class of $\mathrm{Gal}(K/\mathbb{Q})$.

82. 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 $K = \mathbb{Q}[\gamma]$.

B Solutions to Exercises

These solutions fall somewhere between hints and complete solutions. Students were expected to write out complete solutions.

1. Similar to Example 1.28.

2. Verify that 3 is not a square in $\mathbb{Q}[\sqrt{2}]$, and so $[\mathbb{Q}[\sqrt{2},\sqrt{3}]:\mathbb{Q}]=4$.

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).

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.

5. (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 i^{th} 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 $\{\pm1\}$, 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 $E=F[X]/(X^2-a)$, $a\notin\mathbb{F}_p^2$.

6. (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. 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) The polynomial X^p-X-1 has no root in $\mathbb{F}_2$ (check 0 and 1), and therefore (a) implies X^p-X-1 is irreducible in $\mathbb{F}_2[X]$, and also in $\mathbb{Z}[X]$ (see 1.18).

7. Let α be the real 5^{th} 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 5^{th} 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 $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 5$.

8. 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.)

9. 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 $g(X) = \prod (X - \alpha_i)$.

10. 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 $\alpha_i^{p^e} = a_i$.

11. 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 $E =_{df} F(X) \cap F(X^2 - X)$. But $\alpha\tau X = 1 + X$, and so $(\sigma\tau)^m(X) = m + X$. Thus $\mathrm{Aut}(F(X)/E)$ is infinite, which implies that $[F(X) : E]$ is infinite (otherwise $F(X) = E[\alpha_1, \dots, \alpha_n]$; an E-automorphism of $F(X)$ is determined by its values on the α_i, and its value on α_i is a root of the minimum polynomial of α_i). If E contains a polynomial $f(X)$ of degree $m > 0$, then $[F(X) : E] \leq [F(X) : F(f(X))] = m$ — contradiction.

12. 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 $\mathbb{Q}[\sqrt{-p}]$.

13. (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.

14. The splitting field is the smallest field containing all m^{th} roots of 1. Hence it is $\mathbb{F}_{p^n}$ where n is the smallest positive integer such that $m_0|p^n-1$, $m=m_0p^r$.

15. 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 1.4??), 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 4.13??).

16. 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 8^{th} root of 2. As usual for polynomials of this type, the splitting field is $\mathbb{Q}[\alpha,\zeta]$ where ζ is any primitive 8^{th} 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 $[\mathbb{Q}[\alpha,i]:\mathbb{Q}]=2$. Therefore the degree is $2\times 8=16$.

17. 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 (see 4.23). We can take $E=L^{S_3}$.

18. Type: "Factor$(X^{343} - X)$ mod 7;" and discard the 7 factors of degree 1.

19. 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 $\mathrm{PGL}_2(\mathbb{F}_5)$.

20. $\Longleftarrow$: 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.

21. 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.]

22. 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.

23. The degree $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$, ζ_n a primitive n^{th} root of 1, and $\varphi(n) \to \infty$ as $n \to \infty$.

24. (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 $X^{p^m} - X = 0$.

25. 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 $-27a^2 = -3(3a)^2$.]

26. 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 $7\mathbb{Q}^{\times 2}$.

27. (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 $X^2 + X + 2$.

28. 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.

29. Use Eisenstein to show that $X^{p-1} + \cdots + 1$ is irreducible, etc. Done in class.

30. 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).

31. (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 $\mathbb{C}$.

32. 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.

33. 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.

34. 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 6^{th} 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.

35. Let the coefficients of f be $a_1, \ldots, a_n$ — 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 $F[X]$.

36. If f is separable, $[E\colon F] = (G_f\colon 1)$, which is a subgroup of S_n. Etc..

37. $\sqrt{3} + \sqrt{7}$ will do.

38. 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).

39. The multiplicative group of F is cyclic of order $q - 1$. Hence it contains an element of order 4 if and only if $4|q - 1$.

40. Take $\alpha = \sqrt{2} + \sqrt{5} + \sqrt{7}$.

41. 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.

42. We have $\mathbb{Q}[\zeta] = \mathbb{Q}[i, \zeta']$ where ζ' is a primitive cube root of 1 and $\pm i = \zeta^3$ etc..

43. The splitting field is $\mathbb{Q}[\zeta, \sqrt[3]{3}]$, and the Galois group is S_3.

44. Use that

$$(\zeta + \zeta^4)(1 + \zeta^2) = \zeta + \zeta^4 + \zeta^3 + \zeta$$

45. (a) is Dedekind's theorem. (b) is Artin's lemma 3.4b. (c) is O.K. because $X^p - a^p$ has a unique root in Ω.

46. 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..

47. From Hilbert's theorem 90, we know that the kernel of the map $N\colon E^\times \to F^\times$ consists of elements of the form $\frac{\sigma\alpha}{\alpha}$. The map $E^\times \to E^\times$, $\alpha \mapsto \frac{\sigma\alpha}{\alpha}$, has kernel $F^\times$. Therefore the kernel of N has order $\frac{q^m-1}{q-1}$, and hence its image has order $q - 1$. There is a similar proof for the trace — I don't know how the examiners expected you to prove it.

48. (a) is false—could be inseparable. (b) is true—couldn't be inseparable.

49. 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.

50. 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.

51. Theorem on p-groups plus the Fundamental Theorem of Galois Theory.

52. It was proved in class that S_p is generated by an element of order p and a transposition (4.12). There is only one F, and it is quadratic over $\mathbb{Q}$.

53. 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 $a \mapsto a^{-1}$.]

54. 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 $C_2 \times C_4$.

55. Let $a_1, \ldots, a_5$ 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..

56. $C_2 \times C_2$.

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

58. (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.

59. 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.

60. It has order 20, generators (12345) and (2354).

61. 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 ....

62. See Exercise 14.

63. The group $F^\times$ is cyclic of order 80; hence 80, 1, 8.

64. 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.

65. Example 5.5.

66. Omit.

67. 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.

68. Its roots are primitive 8^{th} roots of 1. It splits completely in $\mathbb{F}_{25}$. (a) $(X^2+2)(X^2+3)$.

69. $\rho(\alpha)\overline{\rho(\alpha)} = q^2$, 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 $\mathbb{C}$.

70. 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.

71. (a) $C_2 \times C_2$ and S_3. (b) No. (c). 1

72. Omit.

73. Omit.

74. $1024 = 2^{10}$. 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 $2^{11}/2^{10} = 2$.

75. Pretty standard. False; true.

76. Omit.

77. Similar to a previous problem.

78. Omit.

79. This is really a group theory problem disguised as a field theory problem.

80. (a) Prove it's irreducible by apply Eisenstein to $f(X+1)$. (b) See example worked out in class.

81. Its D_4, with generators (1234) and (12).

82. Omit.

C 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 $b = \frac{2cd}{c^2-pd^2}$.

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 $2^8 - 1 = 255 = 3 \times 5 \times 17$.

Solutions

1. (a) Let σ be an automorphism of a field E. If $\sigma^4 = 1$ and

$$\sigma(\alpha) + \sigma^3(\alpha) = \alpha + \sigma^2(\alpha) \qquad \text{all } \alpha \in E,$$

show that $\sigma^2 = 1$.

If $\sigma^2 \neq 1$, then $1, \sigma, \sigma^2, \sigma^3$ are distinct automorphisms of E, and hence are linearly independent (Dedekind 5.14) — contradiction. [If $\sigma^2 = 1$, then the condition becomes $2\sigma = 2$, so either $\sigma = 1$ or the characteristic is 2 (or both).]

(b) Let p be a prime number and let a, b be rational numbers such that $a^2 + pb^2 = 1$. Show that there exist rational numbers c, d such that $a = \frac{c^2+pd^2}{c^2-pd^2}$ and $b = \frac{2cd}{c^2-pd^2}$.

Apply Hilbert's Theorem 90 to $\mathbb{Q}[\sqrt{p}]$ (or $\mathbb{Q}[\sqrt{-p}]$, depending how you wish to correct the sign).

2. Let $f(X)$ be an irreducible polynomial of degree 4 in $\mathbb{Q}[X]$, and let $g(X)$ be the resolvent cubic of f. What is the relation between the Galois group of f and that of g? Find the Galois group of f if

(a) $g(X) = X^3 - 3X + 1$;

(b) $g(X) = X^3 + 3X + 1$.

We have $G_g = G_f/G_f \cap V$, where $V = \{1, (12)(34), \ldots\}$. The two cubic polynomials are irreducible, because their only possible roots are ± 1. From their discriminants, one finds that the first has Galois group A_3 and the second S_3. Because $f(X)$ is irreducible, $4|(G_f : 1)$ and it follows that $G_f = A_4$ and S_4 in the two cases.

3. (a) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{F}_2[X]$ have, and what are their degrees?

Its roots are the nonzero elements of $\mathbb{F}_{2^8}$, which has subfields $\mathbb{F}_{2^4} \supset \mathbb{F}_{2^2} \supset \mathbb{F}_2$. There are $256 - 16$ elements not in $\mathbb{F}_{16}$, and their minimum polynomials all have degree 8. Hence there are 30 factors of degree 8, 3 of degree 4, and 1 each of degrees 2 and 1.

(b) How many monic irreducible factors does $X^{255} - 1 \in \mathbb{Q}[X]$ have, and what are their degrees?

Obviously, $X^{255} - 1 = \prod_{d|255} \Phi_d = \Phi_1\Phi_3\Phi_5\Phi_{15} \cdots \Phi_{255}$, and we showed in class that the Φ_d are irreducible. They have degrees $1, 2, 4, 8, 16, 32, 64, 128$.

4. Let E be the splitting field of $(X^5 - 3)(X^5 - 7) \in \mathbb{Q}[X]$. What is the degree of E over $\mathbb{Q}$? How many proper subfields of E are there that are not contained in the splitting fields of both $X^5 - 3$ and $X^5 - 7$?

The splitting field of $X^5 - 3$ is $\mathbb{Q}[\zeta, \alpha]$, which has degree 5 over $\mathbb{Q}[\zeta]$ and 20 over $\mathbb{Q}$. The Galois group of $X^5 - 7$ over $\mathbb{Q}[\zeta, \alpha]$ is (by ...) a subgroup of a cyclic group of order 5, and hence has order 1 or 5. Since 7 is not a 5th power in $\mathbb{Q}[\zeta, \alpha]$, it must be 5. Thus $[E : \mathbb{Q}] = 100$, and

$$G = \mathrm{Gal}(E/\mathbb{Q}) = (C_5 \times C_5) \rtimes C_4.$$

We want the nontrivial subgroups of G not containing $C_5 \times C_5$. The subgroups of order 5 of $C_5 \times C_5$ are lines in $(\mathbb{F}_5)^2$, and hence $C_5 \times C_5$ has $6 + 1 = 7$ proper subgroups. All are normal in G. Each subgroup of $C_5 \times C_5$ is of the form $H \cap (C_5 \times C_5)$ for exactly

3 subgroups H of G corresponding to the three possible images in $G/(C_5 \times C_5) = C_4$. Hence we have 21 subgroups of G not containing $C_5 \times C_5$, and 20 nontrivial ones. Typical fields: $\mathbb{Q}[\alpha]$, $\mathbb{Q}[\alpha, \cos\frac{2\pi}{5}]$, $\mathbb{Q}[\alpha, \zeta]$.
[You may assume that 7 is not a 5th power in the splitting field of $X^5 - 3$.]

5. Consider an extension $\Omega \supset F$ of fields. Define $\alpha \in \Omega$ to be *F-constructible* if it is contained in a field of the form

$$F[\sqrt{a_1}, \dots, \sqrt{a_n}], \qquad a_i \in F[\sqrt{a_1}, \dots, \sqrt{a_{i-1}}].$$

Assume Ω is a finite Galois extension of F and construct a field E, $F \subset E \subset \Omega$, such that every $a \in \Omega$ is E-constructible and E is minimal with this property.

Suppose E has the required property. From the primitive element theorem, we know $\Omega = E[a]$ for some a. Now a E-constructible $\implies$ $[\Omega : E]$ is a power of 2. Take $E = \Omega^H$, where H is the Sylow 2-subgroup of $\mathrm{Gal}(\Omega/F)$.

6. Let Ω be an extension field of a field F. Show that every F-homomorphism $\Omega \to \Omega$ is an isomorphism provided:
(a) Ω is algebraically closed, and
(b) Ω has finite transcendence degree over F.

Can either of the conditions (i) or (ii) be dropped? (Either prove, or give a counterexample.)

Let A be a transcendence basis for Ω/F. Because $\sigma\colon \Omega \to \Omega$ 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