Math 806
Notes on Galois Theory

Mark Reeder *

April 12, 2012

Contents

*Thanks to Beth Romano for careful reading and corrections

1 Basic ring theory

A **ring** is a set R together with two functions $+, \cdot : G \times G \to G$, satisfying the following three axioms:

R1 $(R, +)$ is an abelian group with zero element 0_R.

R2 $(R, \cdot)$ is associative with unit element 1_R satisfying $r \cdot 1_R = 1_R \cdot r = r$ for all $r \in R$.

G3 The distributive law holds: $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ and $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ for all $a, b, c \in R$.

We usually write $ab = a \cdot b$, $0 = 0_R$ and $1 = 1_R$. There is no assumption that $1_R \neq 0_R$. But if $1_R = 0_R$ then $R = \{0_R\}$.

A **unit** in R is an element $u \in R$ having a multiplicative inverse: $u \cdot u^{-1} = u^{-1} \cdot u = 1_R$. The set $R^\times$ of units in R forms a group under $\cdot$.

A **subring** is a subset $S \subset R$ containing $0_R, 1_R$ and closed under both operations $+, \cdot$, such that $(S, +)$ is a subgroup of $(R, +)$.

A **ring homomorphism** $f : R \to R'$ is a function from one ring R to another ring R' such that $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$ and $f(1_R) = 1_{R'}$. The image $f(R)$ is a subring of R'. Every ring R admits the **canonical homomorphism**

$$\epsilon : \mathbb{Z} \longrightarrow R,$$

such that $\epsilon(n) = n1_R$, which is the sum of 1_R with itself n-times.

If R, S are two rings then the **direct product** $R \times S$ has a ring structure with operations $(r, s)+(r', s') = (r + r', s + s')$ and $(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$. The zero element is $0_{R\times S} = (0_R, 0_S)$ and the unit element is $1_{R\times S} = (1_R, 1_S)$. The projection maps from $R \times S$ to R and S are ring homomorphisms.

A ring R is **commutative** if $ab = ba$ for all $a, b \in R$. All of our rings will be commutative unless otherwise noted.

A commutative ring R is an **integral domain** if the cancellation law holds: If $ab = ac$ then $b = c$ for all $a, b, c, \in R$.

An **ideal** in the commutative ring R is a subset $I \subset R$ that is closed under addition from within and multiplication from outside, that is, $a + b \in I$ for all $a, b \in I$, and $ra \in I$ for all $r \in R$ and $a \in I$. The sets $\{0\}$ and R are ideals. The latter is sometimes called the **unit ideal** because an ideal $I = R$ precisely when I contains a unit of R. The kernel $\ker f = \{r \in R : \ f(r) = 0_{R'}\}$ of a ring homomorphism $f : R \to R'$ is an ideal.

If I, J are two ideals in R then the intersection $I \cap J$, the sum $I + J = \{a + b : \ a \in I, \ b \in J\}$ and product IJ consisting of all finite sums $\sum_i a_i b_i$ with $a_i \in I$ and $b_i \in J$ are ideals in R such that

$$IJ \subset I \cap J \subset I + J.$$

The ideal $I + J$ is the smallest ideal containing both I and J and is called the **ideal generated by** I **and** J. If $I + J = R$ then $IJ = I \cap J$.

An ideal I is **principal** if $I = Ra = \{ra : \ r \in R\}$ for some $a \in I$. We often write $(a) = Ra$. More generally, the **ideal generated by** elements $a_1, \ldots, a_n$ of R is the ideal

$$(a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n = \{\sum_{i=1}^{n} r_i a_i : \ r_i \in R \, \forall i\}.$$

If R is an integral domain and a, b are two nonzero elements of R then $(a) = (b)$ if and only if $b = ua$ for some unit $u \in R^\times$. If $R = \mathbb{Z}$, then every ideal is principal; we have $I = (n)$ where $\pm n$ are the elements of I with smallest positive absolute value.

For any ideal $I \subset R$ we can form the **quotient ring**

$$R/I = \{r + I : \ r \in R\}$$

whose elements are cosets $r + I$; we have $r + I = r' + I$ exactly when $r - r' \in I$. The ring operations on R/I are given by $(r+I)+(r'+I) = (r+r')+I$ and $(r+I)(r'+I) = rr'+I$. The zero element is $0_{R/I} = 0 + I$, and the unit element is $1_{R/I} = 1 + I$. The operations are well-defined precisely because I is an ideal. Any ring homomorphism $f : R \to R'$ with $I \subset \ker f$ induces a quotient homomorphism $\bar{f} : R/I \to R$ such that $\bar{f}(r)+I = f(r)$. If $I = \ker f$ then $\bar{f}$ induces an isomorphism $\bar{f} : R/I \xrightarrow{\sim} f(R)$. The ideals in R/I are of the form $J/I = \{j + I : \ j \in J\}$ where J is an ideal of R containing I.

A **field** is a commutative ring F such that $F^\times := F - \{0\}$ is a group under the operation $\cdot$. In particular, $F^\times$ is nonempty, so $1_F \neq 0_F$. A **subfield** $F' \subset F$ is a subring which is also a field.

Lemma 1.1 *A commutative ring $R \neq \{0\}$ is a field if and only if R has no ideals other than $\{0\}$ and R.*

Proof: If R is a field then every nonzero ideal $I \subset R$ contains a unit, hence $I = R$. Conversely, assume $\{0\}$ and R are the only ideals in R. Let $a \in R$ be any nonzero element. Then the principal ideal (a) is nonzero, so must be R. Hence $1 \in (a)$. This means there is $b \in R$ such that $1 = ba$. Hence a is a unit. ■

A **field homomorphism** is a ring homomorphism $f : F \to F'$ between two fields F, F'. Since $f(1_F) = 1_{F'} \neq 0_{F'}$ we cannot have $\ker f = F$. From Lemma 1.1 we have

Corollary 1.2 *Every field homomorphism is injective.*

There are two kinds of fields. Let F be a field and consider the canonical homomorphism $\epsilon : \mathbb{Z} \to F$, sending $n \mapsto n \cdot 1_R$, is an ideal in $\mathbb{Z}$. If $\ker \epsilon = \{0\}$ then ϵ extends to a field homomorphism $\epsilon : \mathbb{Q} \longrightarrow F$, sending r/s (in lowest terms) to $(r \cdot 1_F)(s \cdot 1_F)^{-1} \in F$. Thus we have a canonical embedding $\mathbb{Q} \hookrightarrow F$. In this case we say F has **characteristic zero**. If $\ker \epsilon \neq 0$ then $\ker \epsilon = n\mathbb{Z}$ for some integer $n > 0$. If $n = km$ for positive integers $k, m < n$, then $\mathrm{im}(\epsilon) = \mathbb{Z}/n\mathbb{Z}$ is a subring of F hence is an integral domain, so $n = p$ is prime. Thus, we have a canonical embedding $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F$. In this case, we say F has **characteristic** p. In such a field we have $p \cdot 1_F = 0_F$.

Let A be a commutative ring. An **A-algebra** is a ring R together with a homomorphism $\epsilon : A \to R$ whose image is contained in the center of R. If $A = F$ is a field, then we may regard R as an F-vector space via $a \cdot r = \epsilon(a)r$ for $a \in F$ and $r \in R$. In this case we say that R is a **finite-dimensional F-algebra** if $\dim_F R < \infty$.

Proposition 1.3 *1. A finite integral domain is a field.*

2. *If E is a field and F is a finite subring of E then F is a field.*
3. *If F is a field and R is a finite dimensional F-algebra which is also an integral domain, then R is a field.*

Proof: Suppose F is a finite integral domain. Then for any nonzero $a \in F$, the map $L_a : F \to F$ given by $L_a(b) = ab$ is injective, by the definition of integral domain. Since F is finite, L_a is also surjective, so there is $b \in F$ such that $L_a(b) = 1$. This proves item 1, of which item 2 is a special case, since a subring of a field is an integral domain. Finally if R is a finite dimensional F-algebra we again take any nonzero element $r \in R$ and consider the map $L_r : R \to R$ given by $L_r(s) = rs$. Since the map $\epsilon : F \to R$ giving the F-algebra structure on R maps F into the center of R, it follows that the map L_r is F-linear. Again L_r is injective, hence surjective since $\dim_F R < \infty$, so r is a unit in R ■

An ideal P in a commutative ring R is **prime** if R/P is an integral domain. Equivalently, $R - P$ is closed under multiplication. That is, if $a, b \in R$ and $ab \in P$ then $a \in P$ or $b \in P$.

An ideal M in a commutative ring R is **maximal** if R/M is a field. Equivalently, if I is any ideal such that $M \subset I \subset R$ then either $I = R$ or $I = M$.

A maximal ideal is prime, but not conversely in general, see below.

An integral domain R is a **principal ideal domain** (PID) if every ideal in R is principal. If R is a PID then every prime ideal is maximal.

1.1 Some applications of Zorn's lemma

An **ordering** on a set X is a relation $x \leq y$ between some pairs of elements $x, y \in X$ such that

- $x \leq x$,

- $x \leq y$ and $y \leq z \Rightarrow x \leq z$,
- $x \leq y$ and $y \leq x \Rightarrow x = y$.

A subset $T \subset X$ is **totally ordered** if for all $x, y \in T$ we have either $x \leq y$ or $y \leq x$. An **upper bound** of a subset $S \subset X$ is an element $b \in X$ such that $x \leq b$ for all $x \in S$.

Zorn's Lemma asserts that if every non-empty totally ordered subset of X has an upper bound then there exists $m \in X$ such that if $x \in X$ and $x \geq m$ then $x = m$. Such an element m, which need not be unique, is called a **maximal element** of X. Zorn's lemma is equivalent to the axiom of choice, hence has no naive proof.

Applications of Zorn's lemma include:

1. Every vector space has a basis.
2. The arbitrary product of compact sets is compact (Thychonoff's theorem).
3. Every field has an algebraic closure.
4. Every ideal in a commutative ring is contained in a maximal ideal.
5. The intersection of all prime ideals in a commutative ring R is the set of nilpotent elements in R.

We use Zorn's lemma to prove the last two items here.

Item 3: Let R be a commutative ring and let I be an ideal of R. We apply Zorn to the set X of ideals of R containing I, ordered by inclusion. If T is a totally ordered subset of X, then $b(T) := \bigcup_{J \in T} J$ is again an ideal in X Indeed, the only non-obvious point is closure under addition, but if $x \in J$ and $x' \in J'$ with both $J, J' \in T$, then $x + x'$ is in the greater of J, J' hence is in T. Therefore T has the upper bound $b(T)$. Let M be a maximal element of X. Then $I \subset M$ and if J is any ideal containing M then $J \in X$ so $J = M$, so M is a maximal ideal of R containing I.

Item 4: An element $a \in R$ is **nilpotent** if $a^n = 0$ for some integer $n \geq 1$. By induction on n, one sees that a nilpotent element is contained in every prime ideal. Suppose now that $a \in R$ is contained in every prime ideal of R but $a^n \neq 0$ for every integer $n \geq 1$. Let $S = \{1, a, a^2, \dots\}$ and let X be the set of ideals $I \subset R$ such that $I \cap S = \varnothing$. If T is a totally ordered subset of X then as above $b(T) = \bigcup_{J \in T} J$ is an ideal in R and $M(T) \cap S = \varnothing$. By Zorn, there exists a maximal element $M \in X$. We show that M is prime. Suppose not. Then there exist $x, y \in R$ and $xy \in M$, but $x \notin M$ and $y \notin M$. By maximality of M, the ideals (x, M) and (y, M) meet S. Hence there are $u, v \in M$ and $a, b, c, d \in R$ such that $ax + bu \in S$ and $cy + dv \in S$. The product

$$(ax + bu)(cy + dv) = acxy + bcuy + adxv + bduv$$

is again in S since S is closed under multiplication, but is is also in M since $xy, u, v, uv \in M$. This contradicts M being in X. Therefore M is prime, so $a \in M$, another contradiction. Hence $a^n = 0$ for some integer n so a is nilpotent.

1.2 Polynomial Rings

A **polynomial** over a commutative ring R is a finite formal sum $f = c_0 + c_1 x + \cdots + c_n x^n$, where all coefficients $c_i \in R$ and $n \geq 0$ is and integer. The polynomials over R form a ring $R[x]$ under the usual addition and multiplication of polynomials. The **degree** $\deg(f)$ of a nonzero polynomial $f \in R[x]$ is the largest n such that $c_n \neq 0$. We say f is **monic** if $c_n = 1$, where $n = \deg(f)$. We identify R with the polynomials in $R[x]$ of degree zero. The units in $R[x]$ are the units in R.

If R is an integral domain then for any two polynomials $f, g \in R[x]$ we have

$$\deg(fg) = \deg(f) + \deg(g).$$

It follows that $R[x]$ is also an integral domain. However, if R is a PID then $R[x]$ need not be a PID. For example, if $R = \mathbb{Z}$ and p is a prime, then $\mathbb{Z}[x]$ has the ideal (p, x) which is not principal, as well as the prime ideal (p) which is not maximal.

A polynomial $f \in R[x]$ is **reducible** $f = gh$ for some polynomials $g, h \in R[x]$ having $\deg(g), \deg(h)$ both strictly less than $\deg(f)$. We call such a factorization $f = gh$ a **nontrivial factorization**. A polynomial $f \in R[x]$ is **irreducible** if f has no nontrivial factorization in $F[x]$.

Let F be a field. Then the polynomial ring $F[x]$ is a PID; if $I \subset F[x]$ is a nonzero ideal then $I = (f)$ where f is a polynomial in I of minimal degree. For example if $I = (f, g)$ is generated by two polynomials $f, g \in F[x]$ then $(f, g) = (h)$, where $h = \gcd(f, g)$ is the greatest common divisor of f, g. Note that $\gcd(f, g)$ is only defined up to a nonzero constant factor. One can compute $\gcd(f, g)$ using the Euclidean Algorithm for polynomials.

Let $f \in F[x]$ be a nonzero polynomial with $\deg(f) = n > 0$. Let $\alpha = x + (f) \in F[x]$. Using the division algorithm one can write every element $\beta \in F[x]/(f)$ uniquely in the form

$$\beta = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \tag{1}$$

with all $c_i \in F$. In other words, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of the F-vector space $F[x]/(f)$, and

$$\dim_F F[x]/(f) = n = \deg(f).$$

The product of two elements in the form (1) can be reduced to another of the same form using the rule $f(\alpha) = 0$.

Since $F[x]$ is a PID, the following are equivalent for a polynomial $f \in F[x]$:

1. the ideal (f) is maximal (that is, $F[x]/(f)$ is a field);
2. the ideal (f) is prime (that is, $F[x]/(f)$ is an integral domain);
3. if $f = gh$ for $g, h \in F[x]$ then one of g or h is constant.
4. f is irreducible in $F[x]$.

It is important to specify F here since if $E \supset F$ is a larger field then f could be irreducible in $F[x]$ but reducible in $E[x]$.

A general polynomial $f \in F[x]$ has a unique factorization in the form

$$f = cf_1 f_2 \cdots f_k,$$

where $c \in F$ and each f_i is monic and irreducible in $F[x]$. We say that f **splits** in $F[x]$ if each f_i has $\deg(f_i) = 1$. In this factorization it is possible to have $f_i = f_j$ for $i \neq j$. However, let f' be the formal derivative of f. If $\gcd(f, f') = 1$ then all of the f_i are distinct.

Proposition 1.4 *Let F be a field and let $f \in F[x]$ have degree $\deg(f) > 0$. Then there exists a field $E \supset F$ and an element $\alpha \in E$ such that $f(\alpha) = 0$. And there exists a field $K \supset E$ such that f splits in $K[x]$.*

Proof: Let f_1 be an irreducible factor of f in $F[x]$ and let $E = F[x]/(f_1)$. Then E is a field containing the element $\alpha = x + (f_1)$ and we have $f(\alpha) = f + (f_1) = 0 + (f_1)$ since $f \in (f_1)$. We view F as a subfield of E via the embedding $F \hookrightarrow E$ sending $c \mapsto +(f_1) \in E$, for any $c \in F$. This proves the first assertion.

In $E[x]$ we have $f = (x - \alpha)g$, for some $g \in E[x]$. If $\deg g = 0$, then f splits in $E[x]$. If $\deg(g) > 0$ we repeat the above process with f replaced by g, to construct a field $L \supset E$ and an element $\beta \in L$ such that $g(\beta) = 0$. Then $g = (x - \beta)h$ and $f = (x - \alpha)(x - \beta)h$ in $L[x]$. Continuing, we construct a tower of at most $\deg(f)$ fields $F \subset E \subset L \subset \cdots \subset K$ such that f splits in $K[x]$. ■

The ring $F[x]/(f)$ may also be described as follows.

Proposition 1.5 *Let F be a field and let $f \in F[x]$ be a nonzero polynomial with factorization $f = cf_1^{m_1} \cdots f_\ell^{m_\ell}$, where $c \in F^\times$, each $f_j \in F[x]$ is monic irreducible, $f_j \neq f_k$ if $j \neq k$ and the m_j are positive integers. Then the ring $F[x]/(f)$ is isomorphic to a direct product of rings*

$$F[x]/(f) \simeq \prod_{j=1}^{\ell} F[x]/(f_j^{m_j}),$$

via the isomorphism sending $g + (f) \in F[x]/(f)$ to $(g + (f_1^{m_1}), g + (f_2^{m_2}), \ldots, g + (f_\ell^{m_\ell}))$.

Proof: This is an application of the Chinese Remainder Theorem, which asserts that if R is a commutative ring and $I_1, \ldots, I_\ell$ are ideals in R with intersection $\cap_j I_j = I$ such that $I_j + I_k = R$ for all pairs of indices $j \neq k$ then we have a ring isomorphism

$$R/I \xrightarrow{\sim} \prod_j R/I_j, \tag{2}$$

sending $r + I \mapsto (r + I_1, \ldots, r + I_p)$. See [Lang] for a proof of (2). To apply this result to $R = F[x]$, we first have to check that the ideals $I_j = (f_j^{m_j})$ satisfy $I_j + I_k = F[x]$ for $i \neq j$. Since f_j, f_k

are distinct monic irreducible polynomials, the ideals (f_j) and (f_k) are distinct maximal ideals of $F[x]$ hence $(f_j, f_k) = F[x]$. Let $I_j + I_k = (h)$. If $\deg(h) > 0$ there exists a field $E \supset F$ and $\alpha \in E$ such that $h(\alpha) = 0$. Since $f_j^{m_j}, f_k^{m_k} \in (h)$, this implies that $f_j(\alpha) = f_k(\alpha) = 0$, contradicting $(f_i, f_k) = F[x]$. Hence $\deg(h) = 0$, so $I_j + I_k = F[x]$ as required.

Finally, since $I_j + I_k = F[x]$ we have $I_j I_k = I_j \cap I_k$, so that

$$(f) = (f_1^{m_1} \cdots f_\ell^{m_\ell}) = \prod_{j=1}^{\ell} I_j = \bigcap_{j=1}^{\ell} I_j,$$

and Prop. 1.5 indeed follows from (2). ■

1.3 Polynomials over $\mathbb{Q}$

Here are four useful results on the irreducibility of polynomials in $\mathbb{Q}[x]$. By clearing denominators, it suffices to consider only polynomials in $\mathbb{Z}[x]$, that is, polynomials with integral coefficients.

Proposition 1.6 (rational root test) *Suppose $f = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}[x]$ has a rational root $r = a/b$ with a, b relatively prime integers. Then $a \mid c_0$ and $b \mid c_n$. In particular if $f \in \mathbb{Z}[x]$ is monic then all rational roots of f are integers dividing $f(0)$.*

Proof: Clearing denominators in the equation $f(r) = 0$, we have

$$c_0 b^n + c_1 b^{n-1} a + \cdots + c_{n-1} b a^{n-1} + c_n a^n = 0,$$

so $a \mid c_0 b^n$ and $b \mid c_n a^n$. Since $\gcd(a, b) = 1$ we must have $a \mid c_0$ and $b \mid c_n$. ■

The next three results will use **reduction modulo a prime**. Let p be a prime in $\mathbb{Z}$, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field. Let $c \mapsto \bar{c}$ denote the canonical projection $\mathbb{Z} \to \mathbb{F}_p$. For each $f = \sum c_i x_i \in \mathbb{Z}[x]$, let $\bar{f} = \sum \bar{c}_i x^i \in \mathbb{F}_p[x]$. The mapping $f \mapsto \bar{f}$ is a surjective ring homomorphism $\mathbb{Z}[x] \to \mathbb{F}_p[x]$, whose kernel is the ideal $p\mathbb{Z}[x]$ consisting of the integral polynomials all of whose coefficients are divisible by p.

Proposition 1.7 (Gauss' lemma) *If $f \in \mathbb{Z}[x]$ has a nontrivial factorization in $\mathbb{Q}[x]$ then f has a nontrivial factorization in $\mathbb{Z}[x]$.*

Proof: Suppose $f = gh \in \mathbb{Q}[x]$ with $\deg(g), \deg(h)$ both strictly less than $\deg(f)$. There exist positive integers m, n such that $g_1 := mg$ and $h_1 := nh$ belong to $\mathbb{Z}[x]$ and have the same degrees as g, h, repectively. We have $N_1 f = g_1 h_1$, where $N_1 = mn$. If $N_1 = 1$ then f has a nontrivial factorization in $\mathbb{Z}[x]$ as claimed. If $N_1 > 1$ there exists a prime $p \mid N_1$. Let $\bar{f}, \bar{g}_1, \bar{h}_1 \in \mathbb{F}_p[x]$ be the polynomials obtained from g_1, h_1 by reduction modulo p. We have

$$\bar{g}_1 \bar{h}_1 = \overline{g_1 h_1} = \overline{N_1 f} = \bar{N}_1 \bar{f} = 0,$$

since $p \mid N_1$. Since $\mathbb{F}_p[x]$ is an integral domain, one of $\bar{g}_1$ or $\bar{h}_1$ must be zero. Say $\bar{g}_1 = 0$. This means p divides every coefficient of g_1, so that $g_2 := p^{-1}g_1 \in \mathbb{Z}[x]$. Let $N_2 = N_1/p$, and set $h_2 = h_1$. We now have $N_2 f = g_2 h_2$, where $g_2, h_2 \in \mathbb{Z}[x]$ have the same degrees as g, h. Repeating this we get $N_2 > N_3 > \dots$ until eventually $N_k = 1$ for some k, and $f = g_k h_k$ is a nontrivial factorization of f in $\mathbb{Z}[x]$. ■

Proposition 1.8 *Let $f = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}[x]$ have degree n and let p be a prime not dividing c_n. Suppose $\bar{f}$ is irreducible in $\mathbb{F}_p[x]$. Then f is irreducible in $\mathbb{Q}[x]$.*

Proof: If f is reducible in $\mathbb{Q}[x]$ then f has a nontrivial factorization $f = gh$ in $\mathbb{Z}[x]$, by Gauss' Lemma. Since p does not divide the leading coefficient of f, it cannot divide either leading coefficient of g or h. Now $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{F}_p[x]$, and $\deg(\bar{g}) = \deg(g), \deg(\bar{h}) = \deg(h)$, so this is a nontrivial factorization of $\bar{f}$, contradicting the hypothesis. ■

Proposition 1.9 (Eisenstein's criterion) *Let $f = c_0 + c_1 x + \cdots + c_n x^n \in \mathbb{Z}[x]$. Suppose there exists a prime p such that $p^2 \nmid c_0,\ p \mid c_0, \dots, c_{n-1},\ p \nmid c_n$. Then f is irreducible in $\mathbb{Q}[x]$.*

Proof: If f is reducible in $\mathbb{Q}[x]$ then there exists a nontrivial factorization $f = gh$ in $\mathbb{Z}[x]$. By the last two assumptions, we have $\bar{g}\bar{h} = \bar{c}_n x^n \neq 0$ in $\mathbb{F}_p[x]$. By unique factorization $\mathbb{F}_p[x]$ there are integers a, b and $0 < k < n$ such that $\bar{g} = \bar{a}x^k$, $\bar{h} = \bar{b}x^{n-k}$. It follows that p divides both $g(0)$ and $h(0)$. Hence p^2 divides $g(0)h(0) = f(0) = c_0$, contradicting the first assumption. ■

Example: We illustrate some of the above ideas with the the **cyclotomic polynomial**

$$\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1} = \frac{x^p - 1}{x - 1}, \tag{3}$$

where p is a prime number. Since

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p-1} \binom{p}{k} x^{p-1}$$

and $p \mid \binom{p}{k}$ for $0 < k < p$, it follows from Eisenstein's criterion that $\Phi_p(x)$ is irreducible in $\mathbb{Q}[x]$. The roots of Φ_p in $\mathbb{C}$ are $\zeta, \zeta^2, \dots, \zeta^{p-1}$, where $\zeta = e^{2\pi i/p}$. Evaluating polynomials in $\mathbb{Q}[x]$ at $x = \zeta$ gives a homomorphism $\mathbb{Q}[x] \to \mathbb{C}$ with image $\mathbb{Q}(\zeta) = \{c_0 + c_1\zeta + \cdots + c_{p-1}\zeta^{p-1} :\ c_i \in \mathbb{Q}\}$ and this induces an isomorphism

$$\mathbb{Q}[x]/(\Phi_p) \xrightarrow{\zeta} \mathbb{Q}(\zeta).$$

Since $x^p - 1 = (x-1)\Phi_p(x)$, we also have, from Prop. **??**,

$$\mathbb{Q}[x]/(x^p - 1) \simeq \mathbb{Q}[x]/(x-1) \times \mathbb{Q}[x]/(\Phi_p) \simeq \mathbb{Q} \times \mathbb{Q}(\zeta),$$

where $\mathbb{Q}[x]/(x-1) \simeq \mathbb{Q}$ via evaluation at $x = 1$.

2 Finite fields

Let $f \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. We have seen that it is useful to consider the polynomial $\bar{f} \in \mathbb{F}_p[x]$ obtained by reduction modulo p. Galois observed that such polynomials may not have roots in $\mathbb{F}_p$, just as polynomials in $\mathbb{Q}[x]$ may not have roots in $\mathbb{Q}$, but may instead have roots in some larger field. This led him to develop the theory of finite fields. Placing himself in the essential case where f is irreducible, the eighteen year old Galois writes

> Dans ce cas, la congruence n'admettra donc aucune racine entieère, ne même aucune racine incommensurable de degré inférieur. Il faut donc regarder les racines de cette congruence comme des espèces de symboles imaginaires, puisqu'elles ne satisfont pas aux questions des nombres entiérs, symboles dont l'emploi, dans le calcul, sera souvent aussi utile que celui de l'imaginaire $\sqrt{-1}$ dans l'analyse ordinaire.
>
> C'est la classification de ces imaginaires, et leur réduction au plus petit nombre possible, qui va nous occuper. [1]

Galois goes on to develop almost the entire theory of finite fields in six pages. Because he is starting with an irreducible $f(x) \in \mathbb{Z}[x]$, Galois seems not to be concerned with the existence of such polynomials. That is where we begin, before merging with Galois' path.

Proposition 2.1 *Let F be a field of finite cardinality $|F|$. Then there exists a prime p, an integer n, and an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n such that $|F| = p^n$ and*

$$F \simeq \mathbb{F}_p[x]/(f).$$

Proof: Since F is finite, the canonical homomorphism $\epsilon : \mathbb{Z} \to F$ must have nonzero kernel of the form $p\mathbb{Z}$ for some prime p. Hence ϵ induces a canonical embedding $\mathbb{F}_p \hookrightarrow F$. We may thus regard F as a vector space over $\mathbb{F}_p$. The dimension $\dim_{\mathbb{F}_p} F$ must be finite since F is finite, so $|F| = p^n$, where $n = \dim_{\mathbb{F}_p} F$.

Recall that the multiplicative group $F^\times$ is cyclic. Choose a generator $\gamma \in F$ of $F^\times$. Evaluating polynomials at $x = \gamma$ gives a homomorphism $\varphi_\gamma : \mathbb{F}_p[x] \to F$ which is surjective since $\varphi_\gamma(x) = \gamma$. The kernel of φ_γ is a maximal ideal of $\mathbb{F}_p[x]$, which must be of the form (f), for some irreducible polynomial $f \in \mathbb{F}_p[x]$, so φ_γ induces an isomorphism $\mathbb{F}_p[x]/(f) \simeq F$. ■

Our next aim is to prove that for any prime power p^n there exists a field F with $|F| = p^n$. We find F by reverse engineering, by examining the properties of such a hypothetical field. Since $F^\times$ is a group of order $|F^\times| = p^n - 1$, every nonzero element $\beta \in F$ satisfies $\beta^{p^n-1} = 1$. Hence every $\beta \in F$ (including $\beta = 0$) satisfies $\beta^{p^n} = \beta$. In other words, F must be a field consisting of the roots of the polynomial

[1] In this case, the congruence $[f(x) \equiv 0 \mod p]$ will admit no integer root, nor even a non-integral root of lower degree. One must therefore regard the roots of this congruence as kinds of imaginary symbols, because they do not satisfy questions of ordinary integers, symbols whose use, in calculation, will often be just as useful as that of the imaginary $\sqrt{-1}$ in ordinary analysis.

It is the classification of these imaginaries, and their reduction to the smallest possible number, which will concern us.

$f = x^{p^n} - x$. And these roots are distinct, since $f' = -1$ has no roots, much less any root in common with f. Such fields are almost constructed by Prop. 1.4, except the field E in that result could have more elements than just the roots of $x^{p^n} - x$. A small adjustment will fix this problem, and allow us to prove:

Proposition 2.2 *For all primes p and integers $n \geq 1$ there exists a field of cardinality p^n.*

Proof: Let $f = x^{p^n} - x$ and let E be a field containing $\mathbb{F}_p$ in which f splits. Let $\phi : E \to E$ be the Frobenius endomorphism, given by $\phi(\beta) = \beta^p$. Then the n-fold composition ϕ^n is the endomorphism of E given by $\phi^n(\beta) = \beta^{p^n}$. Its fixed points $F := E^{\phi^n} = \{\beta \in E : \ \beta^{p^n} = \beta\}$ are a finite subring of E and are hence a subfield of E, consisting precisely of the p^n distinct roots of f. ■

The larger field E used in the construction of Prop. 2.2 is not unique; but the field F is unique up to isomorphism, as we will soon show. First we need the factorization of $x^{p^n} - x$ in $\mathbb{F}_p[x]$.

Let $\mathrm{Irr}(p, d)$ be the set of irreducible monic polynomials in $\mathbb{F}_p[x]$ of degree d.

Proposition 2.3 *In $\mathbb{F}_p[x]$ we have the factorization*

$$x^{p^n} - x = \prod_{\substack{d|n \\ f \in \mathrm{Irr}(p,d)}} f.$$

Proof: For any $f \in \mathrm{Irr}(p, n)$ the field $F = \mathbb{F}_p[x]/(f)$ has cardinality $|F| = p^n$ and contains the root $\alpha = x + (f)$ of f. Since f is irreducible, we have $(f) = \{g \in \mathbb{F}_p[x] : \ g(\alpha) = 0\}$. As before, the polynomial $x^{p^n} - x$ splits in $F[x]$:

$$x^{p^n} - x = \prod_{\beta \in F} (x - \beta).$$

Since $\alpha \in F$ we have $\alpha^{p^n} - \alpha = 0$, so $x^{p^n} - x \in (f)$, which means that $f \mid x^{p^n} - x$. This shows that every polynomial in $\mathrm{Irr}(p, n)$ divides $x^{p^n} - x$.

Suppose a, b are positive integers with $a \mid b$; write $b = ac$. In $\mathbb{Z}[x]$ have

$$x^b - 1 = (x^a)^c - 1 = (x^a - 1)(x^{a(c-1)} + x^{a(c-2)} + \cdots + x^{2a} + x^a + 1),$$

so $x^a - 1 \mid x^b - 1$. This is also true in $\mathbb{Z}$ if x is replaced by any integer. If $d \mid n$ we therefore have $p^d - 1 \mid p^n - 1$. But now taking $a = p^d - 1$ and $b = p^n - 1$ we get $x^{p^d-1} - 1 \mid x^{p^n-1} - 1$. Multiplying by x we have

$$x^{p^d} - x \mid x^{p^n} - x.$$

We have already shown that every $f \in \mathrm{Irr}(n, d)$ divides $x^{p^d} - x$. Hence every $f \in \mathrm{Irr}(n, d)$ also divides $x^{p^n} - x$.

It remains to show there are no other divisors of $x^{p^n} - x$. Suppose $g \in \mathrm{Irr}(p, e)$ for some e and $g \mid x^{p^n} - x$. Let F be any field of cardinality $|F| = p^n$. We know that $x^{p^n} - x$ splits in F, so g has a

root $\beta \in F$. Evaluation at β gives a ring homomorphism $\mathbb{F}_p[x] \xrightarrow{\beta} F$ with kernel (g). This induces an embedding of the field $L = \mathbb{F}_p[x]/(g)$ into F. Hence we may regard F as a vector space over L. Let $r = \dim_L F$ be the dimension of F. Since $\deg g = e$ we have $|L| = p^e$, so that

$$p^n = |F| = |L|^r = (p^e)^r,$$

and $n = er$ so $e \mid n$. This completes the proof of Prop. 2.3. ■

Now we can prove uniqueness of finite fields.

Proposition 2.4 *Any two finite fields of the same cardinality are isomorphic as fields.*

Let F and F' be two finite fields with $|F| = |F'|$. As before there exist $f, g \in \mathrm{Irr}(p, n)$ such that

$$F \simeq \mathbb{F}_p[x]/(f) \qquad \text{and} \qquad F' \simeq \mathbb{F}_p[x]/(g).$$

In $F[x]$ we factor

$$x^{p^n} - x = \prod_{\beta \in F} (x - \beta).$$

By Prop. 2.3 we have $g \mid x^{p^n} - x$. Hence g has a root $\beta \in F$, and evaluation at β gives an embedding $F' \simeq \mathbb{F}_p[x]/(g) \hookrightarrow F$. Since $|F| = |F'|$ this embedding is an isomorphism. ■

For every prime power p^n we write $\mathbb{F}_{p^n}$ for a field of cardinality $\mathbb{F}_{p^n} = p^n$. Beware that $\mathbb{F}_{p^n}$ is only defined up to isomorphism but has many incarnations. For example, suppose n is prime. Then Prop. 2.3 shows that

$$\frac{x^{p^n} - x}{x^p - x} = \prod_{f \in \mathrm{Irr}(p,n)} f.$$

Comparing degrees on both sides, we find that the number of irreducible polynomials in $\mathbb{F}_p[x]$ of prime degree n is

$$|\mathrm{Irr}(p, n)| = \frac{p^n - p}{n}.$$

Galois considered the case $p = 7, n = 3$, where there are $|\mathrm{Irr}(7, 3)| = 122$ different polynomials $f \in \mathbb{F}_7[x]$ such that $\mathbb{F}_7[x]/(f) \simeq \mathbb{F}_{7^3}$. One of them is $x^3 - 2$. Galois denotes a root of this by i, so we have the incarnation

$$F = \mathbb{F}_7[x]/(x^3 - 2) = \{a + bi + ci^2 : \ a, b, c \in \mathbb{F}_7\},$$

with multiplication rule $i^3 = 2$. In this field i has order 9; its powers $1, i, i^2$ give a basis of F, but Galois asks for a generator of the multiplicative group $F^\times$. Factoring $7^3 - 1 = 2 \cdot 9 \cdot 19$, he notes that

$$F^\times \simeq C_2 \times C_9 \times C_{19},$$

and it suffices to find generators of each factor. The first two factors are generated by -1 and i. The remaining factor is generated by an element of order 19. Optimistically writing this element as $a + bi$, Galois computes (using the rule $i^3 = 2$) that $i - 1$ has order 19. Hence the element

$$\alpha := -1 \cdot i \cdot (i - 1) = i - i^2$$

generates $F^\times$ and has equation $\alpha^3 - \alpha + 2 = 0$. Hence the field

$$E = \mathbb{F}_p[x]/(x^3 - x + 2)$$

is a different incarnation of $\mathbb{F}_{7^3}$ for which the element $\alpha = x + (x^3 - x + 2)$ generates $E^\times$.

Finally, the subfields of finite fields are easily described.

Proposition 2.5 *The subfields of $\mathbb{F}_{p^n}$ are in bijection with the divisors of n. Namely, the divisor $d \mid n$ corresponds to the subfield $\{\beta \in \mathbb{F}_{p^n} : \ \beta^{p^d} = \beta\} \simeq \mathbb{F}_{p^d}$.*

Proof: Assuming $d \mid n$, the proof of Prop. 2.2 shows that $\{\beta \in \mathbb{F}_{p^n} : \ \beta^{p^d} = \beta\}$ is the unique subfield of $\mathbb{F}_{p^n}$ isomorphic to $\mathbb{F}_{p^d}$. Conversely, if F is a subfield of $\mathbb{F}_{p^n}$, let β be a generator of $F^\times$. Being an element of $\mathbb{F}_{p^n}$, β is a root of $x^{p^n} - x$. By Prop. 2.3, there exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree $d \mid n$ such that $f(\beta) = 0$. This gives an embedding $\mathbb{F}_{p^d} \simeq \mathbb{F}_p[x]/(f) \hookrightarrow \mathbb{F}_{p^n}$. ■

The Frobenius automorphism $\phi \in \mathrm{Aut}(\mathbb{F}_{p^n})$ given by $\phi(\beta) = \beta^p$ has order n. Thus the cyclic group C_n acts on $\mathbb{F}_{p^n}$ by field automorphisms. The divisors $d \mid n$ parametrize the subgroups $\langle \phi^d \rangle \simeq C_{n/d}$ of C_n. And the subfield of $\mathbb{F}_{p^n}$ of elements fixed by $\langle \phi^d \rangle$ is the unique subfield having p^d elements. Thus, Prop. 2.5 can be rephrased as follows.

Proposition 2.6 *There is a bijection between the subgroups of C_n and the subfields of $\mathbb{F}_{p^n}$, whereby the subgroup $D \leq C_n$ corresponds to the subfield consisting of elements in $\mathbb{F}_{p^n}$ fixed by D.*

Note that the bijection in Prop. 2.6 is inclusion-reversing, so that the lattice of subgroups of C_n is reciprocal to the lattice of subfields of $\mathbb{F}_{p^n}$. This is a simple case of the main theorem of Galois theory.

3 Extensions of rings and fields

The main objects of study in Number Theory is the field of **algebraic numbers**

$$\bar{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \ f(\alpha) = 0 \text{ for some } f \in \mathbb{Z}[x]\}$$

and the ring of **algebraic integers**

$$\bar{\mathbb{Z}} := \{\alpha \in \mathbb{C} : \ f(\alpha) = 0 \text{ for some monic } f \in \mathbb{Z}[x]\}.$$

Clearly $\bar{\mathbb{Z}} \subset \bar{\mathbb{Q}}$. The rational root test shows that $\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. However, it is not obvious that $\bar{\mathbb{Q}}$ is a field or that $\bar{\mathbb{Z}}$ is a ring. We will show that they are, and that $\bar{\mathbb{Q}}$ is the quotient field of $\bar{\mathbb{Z}}$. First we develop some useful ideas about polynomials.

3.1 Symmetric polynomials

Let R be an integral domain with quotient field F. Let $f(x) = c_0 + c_1 x + \cdots c_n x^n \in R[x]$ be a polynomial of degree n, with roots $\alpha_1, \ldots, \alpha_n$ in some field $E \supset F$. In $E[x]$ we have two expressions for $f(x)$:

$$c_n \prod_{i=1}^{n} (x - \alpha_i) = f(x) = \sum_{k=0}^{n} c_k x^k.$$

In these expressions, the coefficients c_i are known, and the roots α_i are usually mysterious. Let us therefore regard the α_i as variables, and rename them t_i. The coefficients c_k will become functions of the t_i. Dropping c_n, we consider the two expressions for the **general polynomial of degree** n:

$$\prod_{i=1}^{n} (x - t_i) = \sum_{k=0}^{n} (-1)^k s_k x^{n-k}. \tag{4}$$

This is an equation in the ring $R[t_1, \ldots, t_n][x]$ of polynomials in x; the coefficients s_k are themselves polynomials in $t_1, \ldots, t_n$. Expanding the left side of (4), we find these coefficients to be

$$\begin{aligned}
s_0 &= 1 \\
s_1 &= \sum_{1 \le i \le n} t_i \\
s_2 &= \sum_{1 \le i < j \le n} t_i t_j \\
&\vdots \\
s_k &= \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} t_{i_1} \cdots t_{i_k} \\
&\vdots \\
s_n &= t_1 \cdots t_n.
\end{aligned} \tag{5}$$

The functions $s_k \in R[t_1, \ldots, t_n]$ are the **elementary symmetric polynomials**.

The symmetric group S_n acts on the ring $R[t_1, \ldots, t_n]$ by

$$(\sigma \cdot f)(t_1, \ldots, t_n) = f(t_{\sigma 1}, \ldots, t_{\sigma n}),$$

where $\sigma \in S_n$ and $f \in R[t_1, \ldots, t_n]$. The S_n-invariant polynomials form the subring

$$R[t_1, \ldots, t_n]^{S_n} = \{ f \in R[t_1, \ldots, t_n] : \ \sigma \cdot f = f \}.$$

of **symmetric polynomials**. Each s_k belongs to $R[t_1, \ldots, t_n]^{S_n}$ and these symmetric polynomials are "elementary" in the sense that every symmetric polynomial is a polynomial in $s_1, \ldots, s_n$. More precisely, we have the

Theorem 3.1 (Symmetric Polynomial Theorem) *The map*

$$R[t_1, \ldots, t_n] \longrightarrow R[t_1, \ldots, t_n]^{S_n}$$

sending $f(t_1, \ldots, t_n) \mapsto f(s_1, \ldots, s_n)$ *is a ring isomorphism.*

Proof: The map is clearly a ring homomorphism. To prove that it is bijective, it is convenient to use multi-index notation for polynomials. Let M be the set of n-tuples $(m_1, m_2, \ldots, m_n)$ of integers $m_i \geq 0$. For $\mu = (m_1, m_2, \ldots, m_n) \in M$, let $|\mu| = m_1 + m_2 + \cdots + m_n$. We define a total ordering on M by declaring $\mu' \leq \mu$ if either $|\mu'| < |\mu|$ or there is $1 \leq k < n$ such that

$$m'_1 = m_1, \quad m'_2 = m_2, \quad \cdots, m'_k = m_k, \quad \text{but} \quad m'_{k+1} < m_{k+1}. \tag{6}$$

We need two properties of this ordering. First, adding componentwise we have

$$\mu' \leq \mu \text{ and } \nu' \leq \nu \quad \Rightarrow \quad \mu' + \nu' \leq \mu + \nu. \tag{7}$$

Second, if $\mu = (m_1, \ldots, m_n)$ with $m_1 \geq m_2 \geq \cdots \geq m_n$ and μ' is obtained from μ by a nontrivial permutation of the coordinates m_i, then $\mu' < \mu$.

Now each element $f \in R[t_1, \ldots, t_n]$ can be written as $\sum_{\mu \in M} c_\mu t^\mu$, where $t^\mu = t_1^{m_1} \ldots t_n^{m_n}$ and all but finitely many c_μ are zero. Let $\mu(f)$ be the maximal $\mu \in M$ such that $c_\mu \neq 0$. From (7) it follows that

$$\mu(fg) = \mu(f) + \mu(g).$$

Now $\mu(s_k) = (1, 1, \ldots, 1, 0, \ldots, 0)$, with k 1's. It follows that for integers $d_k \geq 0$ we have

$$\mu(s_1^{d_1} s_2^{d_2} \cdots s_n^{d_n}) = (d_1 + d_2 + \cdots + d_n, d_2 + d_3 + \cdots + d_n, \ldots, d_n). \tag{8}$$

We now show that the map in Prop. 3.1 is surjective. Let $f = \sum_{\mu \in M} c_\mu t^\mu \in R[t_1, \ldots, t_n]^{S_n}$ and let $\mu(f) = (m_1, \ldots, m_n)$. Since f is symmetric, all μ' obtained by nontrivial permutations of the m_i also have $c_{\mu'} \neq 0$. Since $\mu(f)$ is maximal, we must have $m_1 \geq m_2 \geq \cdots \geq m_n$. For $1 \leq i < n$ let $d_i = m_i - m_{i+1}$, and let $d_n = m_n$. Then $d_k + \cdots + d_n = m_k$ so

$$\mu(s_1^{d_1} s_2^{d_2} \cdots s_n^{d_n}) = \mu(f).$$

Hence letting

$$f' = f - c_{\mu(f)} s_1^{d_1} s_2^{d_2} \cdots s_n^{d_n},$$

we have $\mu(f') < \mu(f)$. Repeating this process with f' and continuing, we eventually express f as a polynomial in $s_1, \ldots, s_n$. Hence the map in Prop. 3.1 is surjective.

Now for injectivity. A polynomial $f = \sum_{\lambda \in M} c_\lambda t^\lambda \in R[t_1, \ldots, t_n]$ is mapped to $f(s) = \sum_{\lambda \in M} c_\lambda s^\lambda$, and we have seen above that $\mu(s^\lambda) = (\ell_1 + \cdots + \ell_n, \ell_2 + \cdots + \ell_n, \ldots, \ell_n)$. Equation (8) shows that if $\lambda' \neq \lambda$ then $\mu(s^\lambda) \neq \mu(s^{\lambda'})$. Hence $\mu(f(s)) = \max\{\mu(s^\lambda) : \ c_\lambda \neq 0\}$. This shows that if $f \neq 0$ then $f(s) \neq 0$. Hence the map in Prop. 3.1 is injective. ■

Example 1: For each $k \geq 0$ the polynomial

$$p_k = t_1^k + t_2^k + \cdots + t_n^k$$

is symmetric. We have

$$p_1 = s_1, \quad p_2 = s_1^2 - 2s_2, \quad p_3 = s_1^3 - 3s_1 s_2 + 3s_3.$$

In general, p_k can be expressed in terms of the elementary symmetric polynomials via the recursive formula ("Newton's identities")

$$ks_k + \sum_{i=1}^{k} (-1)^k s_{k-i} p_i = 0.$$

Example 2: The polynomial

$$d = \prod_{1 \le i < j \le n} (t_i - t_j)$$

is not quite symmetric. We have $\sigma \cdot d = \mathrm{sgn}(\sigma) d$, so d is invariant under the alternating group A_n but not the full symmetric group S_n. However the square

$$D = \prod_{1 \le i < j \le n} (t_i - t_j)^2$$

is symmetric. This D is the **discriminant** polynomial. Its expression in terms of elementary symmetric polynomials is complicated even for small n:

$$\begin{aligned}
n = 2: \quad & D = s_1^2 - 4s_2 \\
n = 3: \quad & D = s_1^2 s_2^2 - 27 s_3^2 - 4 s_2^3 - 4 s_1^3 s_3 + 18 s_1 s_2 s_3 \\
n = 4: \quad & D = s_1^2 s_2^2 s_3^2 + 256 s_4^3 - 27 s_3^4 - 27 s_1^4 s_4^2 + 144 s_1^2 s_2 s_4^2 - 128 s_2^2 s_4^2 + 4 s_1^2 s_2^3 s_4 + 16 s_2^4 s_4 \\
& \quad - 192 s_1 s_3 s_4^2 + 18 s_1^3 s_2 s_3 s_4 - 80 s_1 s_2^2 s_3 s_4 - 6 s_1^2 s_3^2 s_4 + 144 s_2 s_3^2 s_4 - 4 s_2^3 s_3^2 - 4 s_1^3 s_3^3 \\
& \quad + 18 s_1 s_2 s_3^3.
\end{aligned} \tag{9}$$

In general the degree of D is $n(n-1)$ and $\mu(D) = 2(n-1, n-2, \ldots, 1) = \mu(s_1^2 s_2^2 \cdots s_n^2)$ so $s_1^2 s_2^2 \cdots s_n^2$ appears with coefficient $= 1$ in D. Does s_n^{n-1} always appear with coefficient $\pm n^n$? For $n = 5$ this coefficient is $+5^5$. Does s_{n-1}^n always appear with coefficient $\pm(n-1)^{n-1}$? For $n = 5$ this coefficient is $+256$.

3.2 Integral ring extensions

Let R be an integral domain and let S be a subring of R. An element $\alpha \in R$ is **integral over** S if there exists a monic polynomial $f \in S[x]$ such that $f(\alpha) = 0$. Let

$$R_S = \{\alpha \in R : \ \alpha \text{ is integral over } S\}.$$

Every $s \in S$ is the root of the monic polynomial $x - s \in S[x]$, so $S \subset R_S$, so we have

$$S \subset R_S \subset R.$$

Proposition 3.2 *R_S is a subring of R.*

Proof: Let $\alpha, \beta \in R_S$ be roots of monic polynomials $f, g \in S[x]$. Let $h = fg \in S[x]$ and let E be a field containing S in which h splits. By specializing $t_i \mapsto \gamma_i$ in the general polynomial (4), we have

$$h = \prod_{i=1}^{n}(x - \gamma_i) = \sum_{k=0}^{n}(-1)^k s_k(\gamma_1, \ldots, \gamma_n)x^{n-k}.$$

Since $h \in S[x]$, each coefficient $s_k(\gamma_1, \ldots, \gamma_n)$ belongs to S. By the symmetric polynomial theorem, we have $f(\gamma_1, \ldots, \gamma_n) \in S$ for each symmetric polynomial $f \in S[t_1, \ldots, t_n]$. Now the coefficients of

$$H_\times = \prod_{1 \le i < j \le n}(x - \gamma_i\gamma_j) \qquad \text{and} \qquad H_+ = \prod_{1 \le i < j \le n}(x - \gamma_i - \gamma_j)$$

are symmetric polynomials evaluated at $(\gamma_1, \ldots, \gamma_n)$, hence these coefficients lie in S, and $H_\times, H_+$ are monic polynomials in $S[x]$. Since $\alpha\beta \in \{\gamma_i\gamma_j\}$ and $\alpha + \beta \in \{\gamma_i + \gamma_j\}$ we have $H_\times(\alpha\beta) = 0$ and $H_+(\alpha + \beta) = 0$, so $\alpha\beta$ and $\alpha + \beta$ are integral over S. ■

Integral extensions of $\mathbb{Z}$ have a property in common with PID's, namely:

Proposition 3.3 *Let R be an integral domain in which every element is integral over $\mathbb{Z}$. Then every nonzero prime ideal in R is maximal.*

Proof: Let P be a prime ideal in R. Choose a nonzero element $\beta \in P$. Then β satisfies an equation $\beta^n + c_1\beta^{n-1} + \cdots + c_n = 0$, with all $c_i \in \mathbb{Z}$. Factoring out powers of β, and remembering that R is an integral domain, we may assume that $c_n \neq 0$. Then $c_n \in R\beta \subset P$. This shows that $P \cap \mathbb{Z} \neq \{0\}$. Since it is clear that $P \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, we have $P \cap \mathbb{Z} = p\mathbb{Z}$ for some prime number p. Now $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow R/P$, via the canonical homomorphism $\epsilon : \mathbb{Z} \to R$. Hence R/P is an $\mathbb{F}_p$-algebra.

Let $\alpha \in R$ have nonzero image $\bar{\alpha} \in R/P$. Since R is integral over $\mathbb{Z}$ we have R/P algebraic over $\mathbb{F}_p$. Hence the homomorphism $\mathbb{F}_p[x] \to R/P$ given by evaluation at α has kernel generated by an irreducible polynomial $f \in \mathbb{F}_p[x]$. As $\mathbb{F}_p[x]/(f)$ is a field, it follows that $\bar{\alpha}$ is contained in a subfield of R/P and is therefore invertible in R/P. Hence R/P is a field, so P is maximal. ■

Not every integral extension of $\mathbb{Z}$ is a PID. For example, the ring $\mathbb{Z}[\sqrt{-6}]$ is integral over $\mathbb{Z}$. Indeed, every $\alpha \in \mathbb{Z}[\sqrt{-6}]$ is a root of the polynomial $x^2 - (\alpha + \bar{\alpha})x + \alpha\bar{\alpha}$, where $\bar{\alpha}$ is the complex conjugate of α. However, the ideal $P = (2, \sqrt{-6})$ in $\mathbb{Z}[\sqrt{-6}]$ is not principal. For if $P = (2m + n\sqrt{-6})$ with $m, n \in \mathbb{Z}$, then there would exist $\alpha, \beta \in \mathbb{Z}[\sqrt{-6}]$ such that

$$2 = \alpha \cdot (2m + n\sqrt{-6}), \quad \sqrt{-6} = \beta \cdot (2m + n\sqrt{-6}),$$

so

$$4 = \alpha\bar{\alpha}(4m^2 + 6n^2), \quad 6 = \beta\bar{\beta} \cdot (4m^2 + 6n^2),$$

and $4m^2 + 6n^2$ would divide $2 = 6 - 4$, impossible. However, P is maximal by Prop. 3.3. Indeed, P is the kernel of the ring homomorphism $R \to \mathbb{F}_2$ sending $a + b\sqrt{-6} \mapsto a \mod 2$.

3.3 Prime ideals in $\mathbb{Z}[x]$: elementary classification

In $\mathbb{Z}[x]$ we have only a partial division algorithm.

Proposition 3.4 *If f and g are polynomials in $\mathbb{Z}[x]$ and f is monic, then there exist $q, r \in \mathbb{Z}[x]$ with $\deg(r) < \deg(f)$ such that $g = qr + r$.*

Proof: The proof for polynomials over a field works just as well here, since we do not have to divide by the leading coefficient of f. ■

The condition that f be monic is necessary. For example, there are no polynomials $q, r \in \mathbb{Z}[x]$ with $\deg(r) < \deg(2x)$ such that $x^2 = 2x \cdot q + r$. This complicates the picture of ideals in $\mathbb{Z}[x]$. For example, not every ideal in $\mathbb{Z}[x]$ is principal.

A polynomial $f \in \mathbb{Z}[x]$ is **primitive** if $\gcd(f) = 1$. Every $f \in \mathbb{Z}[x]$ can be written as $f = cf_1$ where $c = \gcd(f)$ and $f_1 \in \mathbb{Z}[x]$ is primitive.

Lemma 3.5 *The product of two primitive polynomials is primitive. More generally, for $f, g \in \mathbb{Z}[x]$ we have $\gcd(fg) = \gcd(f) \cdot \gcd(g)$.*

Proof: If f and g are primitive but p is a prime dividing $\gcd(fg)$. Then $\overline{fg} = \bar{f}\bar{g} = 0 \in \mathbb{F}_p[x]$, so either $\bar{f} = 0$ or $\bar{g} = 0$, so p divides $\gcd(f)$ or $\gcd(g)$, a contradiction.

In general, let $f = af_1$ and $g = bg_1$, where $a = \gcd(f)$, $b = \gcd(g)$ and f_1, g_1 are primitive. Then $\gcd(fg) = \gcd(af_1 \cdot bg_1) = ab \gcd(f_1 g_1) = ab$, by the first case. ■

Lemma 3.6 *If $f \in \mathbb{Q}[x]$ is a monic polynomial then there is $d \in \mathbb{Z}$ such that $f_1 := df \in \mathbb{Z}[x]$ and is primitive; we have $f\mathbb{Q}[x] \cap \mathbb{Z}[x] = f_1\mathbb{Z}[x]$*

Proof: Write

$$f = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + \cdots + \frac{a_{n-1}}{b_{n-1}}x^{n-1} + x^n$$

with all $a_i, b_i \in \mathbb{Z}$ and $\gcd(a_i, b_i) = 1$. Let d be the least common multiple of the b_i's. Then $df \in \mathbb{Z}[x]$ has leading term dx^n. Let p be a prime dividing d and write $d = mp^r$, where $p \nmid m$. Then $r > 0$ is the maximal power of p dividing any b_i. Choose i such that $p^r \mid b_i$. Then $p \nmid (d/b_i)$. And $p \nmid a_i$ because $\gcd(a_i, b_i) = 1$ Hence p does not divide the coefficient da_i/b_i of df, so df is primitive.

It is clear that the polynomial $f_1 := df$ belongs to $f\mathbb{Q}[x] \cap \mathbb{Z}[x]$, so that $f_1\mathbb{Z}[x] \subset f\mathbb{Q}[x] \cap \mathbb{Z}[x]$. Conversely, suppose $g \in f\mathbb{Q}[x] \cap \mathbb{Z}[x]$. Let $g = fh$, with $h \in \mathbb{Q}[x]$. Choose $c \in \mathbb{Z}$ such that $ch \in \mathbb{Z}[x]$. Then $cdg = f_1 \cdot ch$, so $cd \cdot \gcd(g) = \gcd(ch)$. But since $c \mid \gcd(ch)$ we have $h \in \mathbb{Z}[x]$ to begin with, and $d \cdot \gcd(g) = \gcd(h)$, so we even have $h \in d\mathbb{Z}[x]$. Write $h = dh_1$ with $h_1 \in \mathbb{Z}[x]$. Then $g = fh = f \cdot dh_1 = f_1 h_1 \in f_1\mathbb{Z}[x]$. ■

Theorem 3.7 *Every polynomial $f \in \mathbb{Z}[x]$ factors as $f = cf_1 \cdots f_n$, where $c = \gcd(f) \in \mathbb{Z}$ and f_i in $\mathbb{Z}[x]$ are primitive nonconstant and irreducible in $\mathbb{Z}[x]$. This factorization is unique up to sign and the order of the factors.*

Proof: We may assume that f is primitive. If $f = gh$ for nonconstant $g, h \in \mathbb{Z}[x]$ then $1 = \gcd(f) = \gcd(g)\gcd(h)$ by Lemma 3.5, so g, h are primitive. Repeating this, we obtain a factorization of f into a product of primitive irreducible nonconstant polynomials. Suppose $f_1 \cdots f_k = f = g_1 \cdots g_\ell$ are two factorizations of f into primitive nonconstant irreducible polynomials in $\mathbb{Z}[x]$. By Gauss' Lemma, each of the polynomials f_i and g_i are irreducible in $\mathbb{Q}[x]$. By unique factorization in $\mathbb{Q}[x]$ we have $k = \ell$ and after re-indexing there are rational numbers a_i/b_i such that $f_i = (a_i/b_i)g_i$ for all i. Since f_i and g_i are both primitive we have

$$b_i = \gcd(b_i f_i) = \gcd(a_i g_i) = a_i$$

so $f_i = g_i$ up to sign. ■

We now classify the prime ideals in $\mathbb{Z}[x]$. We note first that $P \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$, hence either $P \cap \mathbb{Z} = \{0\}$ or $P \cap \mathbb{Z} = p\mathbb{Z}$ for a unique prime $p \in \mathbb{Z}$.

Theorem 3.8 *The nonzero prime ideals in $\mathbb{Z}[x]$ are classified as follows.*

1. *If $P \cap \mathbb{Z} = \{0\}$ then $P = f\mathbb{Z}[x]$, where f is the unique (up to sign) primitive polynomial in P of minimal degree.*
2. *If $P \cap \mathbb{Z} = p\mathbb{Z}$ and P contains no primitive polynomial, then $P = p\mathbb{Z}[x]$.*
3. *If $P \cap \mathbb{Z} = p\mathbb{Z}$ and P contains a primitive polynomial then $P = p\mathbb{Z}[x] + f\mathbb{Z}[x]$ where $f \in \mathbb{Z}[x]$ is primitive with irreducible reduction $\bar{f} \in \mathbb{F}_p[x]$. The ideal $(\bar{f})$ in $\mathbb{F}_p[x]$ depends only on P.*

Proof:

Assume that $P \cap \mathbb{Z} = p\mathbb{Z}$ and P contains no primitive polynomial. Let $f \in P$ and write $f = cf_1$ with $c = \gcd(f)$ and f_1 primitive. Since $f_1 \notin P$, we must have $c \in P \cap \mathbb{Z}$. Hence $p \mid c$ so $f \in p\mathbb{Z}[x]$ as claimed.

For the rest of the proof we assume that P contains a primitive polynomial and let m be the minimal degree of a primitive polynomial in P. If $f \in P$ is primitive with $\deg f = m$ then Theorem 3.7 implies that f is irreducible in $\mathbb{Z}[x]$.

Suppose that $P \neq f\mathbb{Z}[x]$. Let $n \geq 0$ be the minimal degree of a polynomial in $P - f\mathbb{Z}[x]$ and choose $g \in P - f\mathbb{Z}[x]$ of this minimal degree n. Suppose g factors as $g = hk$ in $\mathbb{Z}[x]$. Neither h nor k can belong to $f\mathbb{Z}[x]$. If, say, $h \in P$ then by minimality $\deg(h) = \deg(g)$ and k is constant. By Gauss' Lemma, f and g are irreducible in $\mathbb{Q}[x]$ so there exist $a(x), b(x) \in \mathbb{Q}[x]$ such that $af + bg = 1$. Clearing denominators in the coefficients of a, b we find $d \in \mathbb{Z}$ such that $da, db \in \mathbb{Z}[x]$ and $daf + dbg = d \in P$.

If $P \cap \mathbb{Z} = \{0\}$ this is a contradiction, so $P = f\mathbb{Z}[x]$ as claimed, and any other primitive polynomial $h \in P$ of degree m is divisible by f in $\mathbb{Z}[x]$, so $h = \pm f$.

If $P \cap \mathbb{Z} = p\mathbb{Z}$ then $p \mid d$ and the ideal $(p, f) = p\mathbb{Z}[x] + f\mathbb{Z}[x]$ is contained in P. Let $\bar{f} \in \mathbb{F}_p[x]$ be the reduction of f modulo p. Since f is primitive, we have $\bar{f} \neq 0$. Suppose $\bar{f}$ is reducible in $\mathbb{F}_p[x]$. Then there are polynomials $h, k, r \in \mathbb{Z}[x]$ such that $f = hk + pr$, both h and k are nonconstant, and

$\deg(h) + \deg(k) = \deg(\bar{f}) \leq \deg(f)$. Since $p \in P$ we have $hk \in P$. By minimality of m, either h or k is constant, a contradiction. Therefore $\bar{f}$ is irreducible in $\mathbb{F}_p$. It follows that

$$\mathbb{Z}[x]/(p, f) \simeq \mathbb{F}_p/(\bar{f})$$

is a field, so (p, f) is a maximal ideal in $\mathbb{Z}[x]$ and we have $(p, f) = P$, as claimed.

Finally, suppose $(p, f) = P = (p, g)$ where $f, g \in \mathbb{Z}[x]$ are primitive with irreducible reductions $\bar{f}, \bar{g} \in \mathbb{F}_p[x]$. There are $h, k \in \mathbb{Z}[x]$ such that $f = ph + gk$, so $\bar{f} = \bar{g}\bar{k} \in (\bar{g})$. Likewise $\bar{g} \in (\bar{f})$, so that $(\bar{f}) = (\bar{g})$. This completes the proof of Thm. 3.8. ■

From Prop. 3.3 we know that prime ideals in integral extensions of $\mathbb{Z}$ are maximal. We can now sharpen this as follows.

Corollary 3.9 *Let R be an integral domain and let α in R be integral over $\mathbb{Z}$ with minimal monic irreducible polynomial $f \in \mathbb{Z}[x]$. Then every nonzero prime ideal P of R is maximal and has the form $P = (p, g(\alpha))$, where $p \in \mathbb{Z}$ is prime and $g \in \mathbb{Z}[x]$ is monic such that $\bar{g}$ is an irreducible factor $\bar{f}$ in $\mathbb{F}_p[x]$ and we have*

$$\mathbb{Z}[\alpha]/P \simeq \mathbb{F}_p[x]/\bar{g}\mathbb{F}_p[x] \simeq \mathbb{F}_{p^d},$$

where $d = \deg g$.

Proof: Let $f \in \mathbb{Z}[x]$ be the monic irreducible polynomial of α. Then $\mathbb{Z}[x]/f\mathbb{Z}[x] \simeq \mathbb{Z}[\alpha]$ via evaluation at α, so the prime ideals of $\mathbb{Z}[\alpha]$ correspond to the prime ideals of $\mathbb{Z}[x]$ containing f. From the classification of prime ideals in $\mathbb{Z}[x]$, we see these primes consist of $f\mathbb{Z}[x]$ itself and the primes (p, g), where $\bar{g}$ is irreducible modulo p and $f = gh + pk$ for some $h, k \in \mathbb{Z}[x]$. This last is equivalent to having $\bar{f} = \bar{g}\bar{h}$ in $\mathbb{F}_p[x]$. In other words, $\bar{g}$ must be an irreducible factor of $\bar{f}$ in $\mathbb{F}_p[x]$. When this holds, we have isomorphisms

$$\mathbb{Z}[\alpha]/(p, g(\alpha)) \xleftarrow{\sim} \mathbb{Z}[x]/(p, g) \xrightarrow{\sim} \mathbb{F}_p[x]/\bar{g}\mathbb{F}_p[x],$$

induced by evaluation at α and reduction modulo p, respectively. Since $\bar{g}$ is irreducible of degree d, the ring $\mathbb{F}_p[x]/\bar{g}\mathbb{F}_p[x]$ is a field of cardinality p^d. ■

3.4 The spectrum of a commutative ring

Let R be a commutative ring. Define $\mathrm{Spec}(R)$ to be the set of prime ideals of R. There is a topology on $\mathrm{Spec}(R)$ for which the closed sets are those of the form

$$V(I) = \{P \in \mathrm{Spec}(R) : \ I \subset P\},$$

where I is an ideal in R. One checks that

- $V(\{0\}) = R$ and $V(R) = \varnothing$;
- $V(I) \cup V(J) = V(IJ)$ for any two ideals I, J in R;

- $\bigcap_j V(I_j) = V\left(\sum_j I_j\right)$ for any family of ideals $\{I_j\}$ in R,

so that the sets $V(I)$ are indeed the closed sets of a topology on $\mathrm{Spec}(R)$. The open sets are then the complements $U(I) = \{P \in \mathrm{Spec}(R) : I \not\subset P\}$.

In this topology points in $\mathrm{Spec}(R)$ are not generally closed. If $P \in \mathrm{Spec}(R)$ and $V(I)$ contains P, then $V(P) \subset V(I)$. It follows that the closure of $\{P\}$ is $V(P)$. We have $\{P\} = V(P)$ exactly when P is maximal. Hence, the closed points in $\mathrm{Spec}(R)$ are the maximal ideals of R. At the other extreme, if R is an integral domain then $\{0\} \in \mathrm{Spec}(R)$, and

$$\overline{\{\ \{0\}\ \}} = V(\{0\}) = R.$$

That is, the point $\{0\}$ is dense in $\mathrm{Spec}(R)$. We set $\xi_R = \{0\}$ and call this the **generic point** in $\mathrm{Spec}(R)$.

The correspondence theorem for ideals gives a bijection

$$\mathrm{Spec}(R/I) \xrightarrow{\sim} V(I)$$

which is a homeomorphism because it sends any closed set $V((I+J)/I) \subset \mathrm{Spec}(R/I)$ to the closed set $V(I) \cap V(J) \subset V(I)$.

More generally, any ring homomorphism $\varphi : R \to R'$ gives a function

$$\varphi^* : \mathrm{Spec}(R') \longrightarrow \mathrm{Spec}(R) \quad Q \mapsto \varphi^{-1}(Q).$$

One checks that $(\varphi^*)^{-1}(V(I)) = V(I')$, where I' is the ideal of R' generated by $\varphi(I)$. It follows that φ^* is continuous.

For any ideal $J \subset R'$, one checks that

$$\varphi^*(V(J)) = \mathrm{im}\,\varphi^* \cap V(\varphi^{-1}(J)).$$

If we give $\mathrm{im}\,\varphi^*$ the subspace topology from $\mathrm{Spec}(R)$ then $\varphi^* : \mathrm{Spec}(R') \to \mathrm{im}\,\varphi^*$ is a closed map.

If R is a subring of R' and $\varphi : R \hookrightarrow R'$ is the inclusion then $\varphi^*(Q) = Q \cap R$, for any $Q \in \mathrm{Spec}(R')$.

If R' is an integral domain then $\ker\varphi$ is a prime ideal in R and φ^* sends the generic point $\xi_{R'} \in \mathrm{Spec}(R')$ to $\ker\varphi \in \mathrm{Spec}(R)$.

3.4.1 $\mathrm{Spec}(\mathbb{Z}[x])$

We illustrate all of this with the evident ring homomorphisms

$$\begin{array}{ccccc} \mathbb{Q}[x] & \longleftarrow & \mathbb{Z}[x] & \longrightarrow & \mathbb{F}_p[x]\ , \\ & & \uparrow & & \\ & & \mathbb{Z} & & \end{array}$$

which give continuous maps

$$\begin{array}{ccccc} \mathrm{Spec}(\mathbb{Q}[x]) & \xrightarrow{\eta} & \mathrm{Spec}(\mathbb{Z}[x]) & \xleftarrow{\pi} & \mathrm{Spec}(\mathbb{F}_p[x]) \\ & & \downarrow{\scriptstyle \varepsilon} & & \\ & & \mathrm{Spec}(\mathbb{Z}) & & \end{array}.$$

We have

$$\begin{array}{lcccl} \mathrm{Spec}(\mathbb{Z}) & = & \{\xi_{\mathbb{Z}}\} & \cup & \{p\mathbb{Z} : \ p \ \text{prime}\} \\ \mathrm{Spec}(\mathbb{Q}[x]) & = & \{\xi_{\mathbb{Q}[x]}\} & \cup & \{f\mathbb{Q}[x] : \ f \in \mathbb{Q}[x] \ \text{ irreducible}\} \\ \mathrm{Spec}(\mathbb{F}_p[x]) & = & \{\xi_{\mathbb{F}_p[x]}\} & \cup & \{f\mathbb{F}_p[x] : \ f \in \mathbb{Q}[x] \ \text{ irreducible}\}. \end{array}$$

From Theorem 3.8, the points $P \in \mathrm{Spec}(\mathbb{Z}[t])$ are of three types:

i) $P = f\mathbb{Z}[x]$, where $f \in \mathbb{Z}[x]$ is primitive and irreducible.

ii) $P = p\mathbb{Z}[x]$, where p is a prime in $\mathbb{Z}$.

iii) $P = p\mathbb{Z}[x] + f\mathbb{Z}[x]$ where $p \in \mathbb{Z}$ is prime and $f \in \mathbb{Z}[x]$ is primitive with $\bar{f} \in \mathbb{F}_p$ irreducible.

This classification fits in neatly with the partition of $\mathrm{Spec}(\mathbb{Z}[x])$ into fibers of ε:

The primes of type i) are the points in the generic fiber $\varepsilon^{-1}(\xi_{\mathbb{Z}})$.

The primes in types ii) are dense in the closed fiber $\varepsilon^{-1}(p\mathbb{Z})$.

The primes of type iii) are the closed points in $\varepsilon^{-1}(p\mathbb{Z})$.

Moreover, η and π give homeomorphisms onto the fibers (with the subspace topology)

$$\mathrm{Spec}(\mathbb{Q}[x]) \xrightarrow[\eta]{\sim} \varepsilon^{-1}(\xi_{\mathbb{Z}}) \quad \subset \quad \mathrm{Spec}(\mathbb{Z}[x]) \quad \supset \quad \varepsilon^{-1}(p\mathbb{Z}) \xleftarrow[\pi]{\sim} \mathrm{Spec}(\mathbb{F}_p[x]).$$

Explicitly, we have

$$\eta(f\mathbb{Q}[x]) = f_1\mathbb{Z}[x],$$

where f_1 is the unique primitive irreducible polynomial in $f\mathbb{Q}[x] \cap \mathbb{Z}[x]$ (cf. Lemma 3.6) and $\pi(\bar{f}\mathbb{F}_p[x]) = p\mathbb{Z}[x] + f\mathbb{Z}[x]$ (cf. part 3 of Theorem 3.8).

We also have the following "transverse" partition of $\mathrm{Spec}(\mathbb{Z}[x])$. Let $f \in \mathbb{Z}[x]$ be primitive and irreducible. Then the closure of the point $f\mathbb{Z}[x]$ is

$$\overline{\{f\mathbb{Z}[x]\}} = V(f\mathbb{Z}[x]) = \{f\mathbb{Z}[x]\} \cup \{(p, g) : \ \bar{g} \text{ is an irreducible factor of} \bar{f} \in \mathbb{F}_p[x]\},$$

and is homeomorphic to $\mathrm{Spec}(\mathbb{Z}[\alpha])$, where α is an element in a number field with minimal integral (not necessarily monic) polynomial f. Thus, the points in $\overline{\{f\mathbb{Z}[x]\}} \cap \varepsilon^{-1}(p\mathbb{Z})$ correspond to the irreducible factors of f modulo p, and also the the primes in $\mathbb{Z}[\alpha]$ which contain p.

3.5 Algebraic field extensions

If a field F is a subfield of a field E, we say that E/F is a field extension. Let E/F be a field extension. We say that $\alpha \in E$ is **algebraic** over F if there exists a nonzero polynomial $f \in F[x]$ such

that $f(\alpha) = 0$. [2] Equivalently, α is algebraic over F if the map $\varphi_\alpha : F[x] \to E$ has nonzero kernel. In this case $\ker \varphi_\alpha = (f_\alpha)$, where f_α is the unique monic polynomial in $\ker \varphi_\alpha$ of lowest degree, and φ induces an isomorphism

$$\varphi_\alpha : F[x]/(f_\alpha) \xrightarrow{\sim} F(\alpha),$$

where $F(\alpha) = \operatorname{im} \varphi_\alpha$ is the subfield of E generated by F and α. We have

$$F(\alpha) = \{c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} : \ c_i \in F\},$$

where $n = \deg f_\alpha$. The polynomial f_α is the **minimal polynomial of** α. A field extension E/F itself an **algebraic extension** if every element of E is algebraic over F.

Corollary 3.10 *Given a field extension E/F, the set $L = \{\alpha \in E : \ \alpha$ is algebraic over $F\}$ is a subfield of E containing F.*

Proof: That L is a subring of E follows from Prop. 3.2. If α is a nonzero element of L with minimal polynomial $f_\alpha \in F[x]$ of degree n, then α^{-1} is a root of the polynomial $g(x) = x^n f_\alpha(1/x) \in F[x]$, so $\alpha^{-1} \in L$. Therefore L is a field. ■

Remark: If K/E and E/F are two algebraic field extensions, then K/F is also algebraic. We defer the proof of this to the next section (see Cor. 3.15).

The typical situation in which integrality and algebraicity are related is as follows. Let S be an integral domain with quotient field F and let E/F be a field extension. The **integral closure** of S in E is the subring $R \subset E$ consisting of elements of E which are integral over S.

Proposition 3.11 *If $\alpha \in E$ is algebraic over F then there exists $s \in S$ such that $s\alpha \in R$.*

Proof: Let $f_\alpha = \sum c_k x^k$ be the minimal polynomial of α over F, with $n = \deg f_\alpha$. There exists $s \in S$ such that $rc_k \in S$ for all k, and $s\alpha$ is a root of the monic polynomial $s^n f_\alpha(x/s) \in S[x]$. ■

Corollary 3.12 *Let S be an integral domain with quotient field F, let E/F be an algebraic extension and let R be the integral closure of S in E. Then E is the quotient field of R.*

3.5.1 The ring of algebraic integers and the field of algebraic numbers

The **field of algebraic numbers** is the field $\overline{\mathbb{Q}}$ consisting of complex numbers which are algebraic over $\mathbb{Q}$. That is, $\overline{\mathbb{Q}}$ consists of those complex numbers α which are roots of polynomials in $\mathbb{Q}[x]$.

The **ring of algebraic integers** is the ring $\overline{\mathbb{Z}}$ consisting of complex numbers which are integral over $\mathbb{Z}$. That is, $\overline{\mathbb{Z}}$ consists of those complex numbers α which are roots of monic polynomials in $\mathbb{Z}[x]$.

[2] If this holds, we could arrange f to be monic, so α is integral over the subring F of E. We use the word "algebraic" instead of "integral" in the context fields to emphasize that we are only interested in the property that the powers of α satisfy an algebraic relation.

From Cor. 3.12 it follows that $\overline{\mathbb{Q}}$ is the quotient field of $\overline{\mathbb{Z}}$.

The rational root test shows that $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

The ring $\overline{\mathbb{Z}}$ and its quotient field $\overline{\mathbb{Q}}$ are the main objects of study in number theory.

3.6 Field extensions of finite degree

A field extension E/F is **finite** if E has finite dimension as an F-vector space. In this case we write

$$[E : F] = \dim_F E.$$

Proposition 3.13 *IF L/E and E/F are finite extensions of fields then L/F is finite and we have*

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

Proof: Let $\{\alpha_1, \ldots, \alpha_n\}$ be an F-basis of E and let $\{\beta_1, \ldots, \beta_m\}$ be an E-basis of L. One checks that $\{\alpha_i\beta_j : \ 1 \leq i \leq n, \ 1 \leq j \leq m\}$ is an F-basis of L. ■

A pair of extensions $L/E, E/F$ is called a **tower** of fields. Towers often appear by adjoining elements, as follows. Suppose K/F is a field extension and $\alpha \in K$. The field $F(\alpha)$ is the intersection of all subfields of K containing α. More generally, given $\alpha_1, \ldots, \alpha_n \in K$, the field $F(\alpha_1, \ldots, \alpha_n)$ is the intersection of all subfields of K containing $\{\alpha_1, \ldots, \alpha_n\}$. We have $F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ and the field $F(\alpha_1, \ldots, \alpha_n)$ can be obtained from F adjoining one element at a time, forming a tower:

$$F \subset F(\alpha_1) \subset F(\alpha_1, \alpha_2) \subset \cdots F(\alpha_1, \cdots, \alpha_n) \subset K.$$

A field $F(\alpha_1, \cdots, \alpha_n)$ obtained in this way is **finitely generated over** F.

Proposition 3.14 *A finite field extension E/F is algebraic. If E/F is algebraic and E is finitely generated over F then E/F is finite.*

Proof: Let E/F be a finite extension and let $\alpha \in E$. Then the set of powers $\{\alpha^i\}$ must be linearly dependent over F. A dependence relation is of the form $c_0 + c_1\alpha + \cdots + c_n x^n = 0$, with all $c_k \in F$. Thus α is a root of the polynomial $c_0 + c_1 x + \cdots + c_n x^n$, so α is algebraic over F. Since $\alpha \in E$ was arbitrary, we have E/F algebraic.

Now suppose $E = F(\alpha)$ is an algebraic extension of F generated by a single element α with minimal polynomial $f_\alpha \in F[x]$. Then $F[x]/(f_\alpha) \simeq E$ via evaluation at α, and $[E : F] = \deg f_\alpha < \infty$, so E/F is finite. Finally suppose $E = F(\alpha_1, \ldots, \alpha_n)$ is finitely generated and algebraic over F. Let $F_0 = F$ and for $1 \leq i \leq n$ let $F_i = F(\alpha_1, \ldots, \alpha_i) = F_{i-1}(\alpha_i)$. By what we just proved for a single generator, $[F_i : F_{i-1}] < \infty$ for each $1 \leq i \leq n$. From Prop. 3.13 we have $[F_i : F] = [F_i : F_{i-1}][F_{i-1} : F_{i-2}] \cdots [F_1 : F] < \infty$. In particular $[E : F] < \infty$. ■

Now we can prove that algebraicity is preserved under towers.

Corollary 3.15 *If L/E and E/F are algebraic then L/F is algebraic.*

Proof: Let $\alpha \in L$. Since L/E is algebraic, there is $f = \sum_{k=0}^{n} c_k x^k \in E[x]$ such that $f(\alpha) = 0$. Each coefficient c_k lies in E and E/F is algebraic so each c_k is algebraic over F. That is, each c_k lies in the algebraic closure $\overline{F}_E$ of F in E. Since $\overline{F}_E$ is a field (Cor. 3.10), the finitely generated field $K = F(c_0, \ldots, c_n) \subset \overline{F}_E$ is is algebraic over F. Hence K/F is finite by Prop. 3.13. And $f \in K[x]$, so α is algebraic over K so $K(\alpha)/K$ is finite, again by Prop. 3.13. So $K(\alpha)/F$ is finite, hence algebraic over F, so α is algebraic over F. Since $\alpha \in L$ was arbitrary, the extension L/F is algebraic. ■

3.6.1 Some abelian numbers

An **abelian number** is an element of $\mathbb{Q}(e^{2\pi i/n})$ for some integer $n \geq 1$. [3]

Both complex numbers $e^{\pm 2\pi i/n}$ are roots of $x^n - 1$, hence lie in $\overline{\mathbb{Z}}$. Since $\overline{\mathbb{Z}}$ is closed under addition, it follows that $2\cos(2\pi/n) = e^{2\pi i/n} + e^{-2\pi i/n}$ is an algebraic integer. The factor of 2 is necessary. For example, $\alpha = \cos(2\pi/12) = \sqrt{3}/2$ satisfies $4\alpha^2 - 3 = 0$, but no monic polynomial over $\mathbb{Z}$. For $1 \leq n \leq 12$ we list the monic polynomials in $\mathbb{Z}[x]$ of minimal degree having $e^{2\pi i/n}$ and $2\cos(2\pi/n)$ as roots:

n	$e^{2\pi i/n}$	$2\cos(2\pi/n)$
1	$x - 1$	$x - 2$
2	$x + 1$	$x + 2$
3	$x^2 + x + 1$	$x + 1$
4	$x^2 + 1$	x
5	$x^4 + x^3 + x^2 + x + 1$	$x^2 + x - 1$
6	$x^2 - x + 1$	$x - 1$
7	$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	$x^3 + x^2 - 2x - 1$
8	$x^4 + 1$	$x^2 - 2$
9	$x^6 + x^3 + 1$	$x^3 - 3x + 1$
10	$x^5 - x^4 + x^3 - x^2 + x - 1$	$x^2 - x - 1$
11	$x^{10} + x^9 + \cdots + x + 1$	$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$
12	$x^4 - x^2 + 1$	$x^2 - 3$

(10)

For a general prime $p > 2$, the minimal polynomial $\Psi_p(x)$ of $2\cos(2\pi/p)$ is found as follows. Write $p = 2n + 1$, so that

$$z^{-n}\Phi_p(z) = z^n + z^{n-1} + \cdots + z^{1-n} + z^{-n} = \Psi(z + z^{-1}),$$

where $\Psi \in \mathbb{Z}[x]$ is a monic polynomial of degree n, which we will compute in a moment. Since n is the degree of the minimal polynomial of $2\cos(2\pi/p)$ and

$$\Psi(2\cos(2\pi/p)) = \Psi(e^{2\pi i/p} + e^{-2\pi i/p}) = e^{-2n\pi i/p}\Phi_p(e^{2\pi i/p}) = 0,$$

it follows that $\Psi = \Psi_p$ is the minimal polynomial of $2\cos(2\pi/p)$. To determine Ψ_p, let

$$f_n(z) = z^n + z^{n-2} + \cdots + z^{2-n} + z^{-n}.$$

[3] The term "abelian" will make more sense when we see the Kronecker-Weber theorem.

Then we have the Clebsch-Gordon rule [4]

$$f_1 \cdot f_n = f_{n-1} + f_n. \tag{11}$$

Using equation (11) one verifies by induction that

$$\begin{aligned} f_{2k}(z) &= (-1)^k \sum_{i=0}^{k} (-1)^i \binom{k+i}{k-i} (z+z^{-1})^{2i} = g_{2k}(z+z^{-1}) \\ f_{2k+1}(z) &= (-1)^k \sum_{i=0}^{k} (-1)^i \binom{k+i+1}{k-i} (z+z^{-1})^{2i+1} = g_{2k+1}(z+z^{-1}), \end{aligned} \tag{12}$$

where

$$\begin{aligned} g_{2k}(x) &= (-1)^k \sum_{i=0}^{k} (-1)^i \binom{k+i}{k-i} x^{2i} \\ g_{2k+1}(x) &= (-1)^k \sum_{i=0}^{k} (-1)^i \binom{k+i+1}{k-i} x^{2i+1}. \end{aligned} \tag{13}$$

Since $\Psi_p(z+z^{-1}) = f_n(z) + f_{n-1}(z) = g_n(z+z^{-1}) + g_{n-1}(z+z^{-1})$, it follows that the minimal polynomial of $2\cos(2\pi/p)$ is given by

$$\Psi_p(x) = g_n(x) + g_{n-1}(x), \tag{14}$$

where the polynomials g_n, g_{n-1} are given by (13). Since these two polynomials have opposite parity, there is no cancellation between their terms.

3.6.2 Constructible numbers

The geometric constructions in Euclid's *Elements* can be explained in terms of finite and algebraic extensions of $\mathbb{Q}$. The allowed constructions are of two types:

1. Given distinct points $\alpha, \beta \in \mathbb{C}$ we can draw the line through α and β.
2. Given $\alpha \in \mathbb{C}$ and a real number $r > 0$ we can draw the circle with center α and radius r.

A number $\alpha \in \mathbb{C}$ is **constructible** if, starting with $0, 1$ we can obtain α by a sequence of constructions of types 1 and 2 and taking intersections. Let

$$K = \{\alpha \in \mathbb{C} : \ \alpha \text{ is constructible}\}.$$

[4] $f_n(z)$ is the trace of a matrix in $\mathrm{SL}_2(\mathbb{C})$ with eigenvalues z, z^{-1} acting on the space Sym^n of symmetric polynomials of degree n on $\mathbb{C}^2$, and the Clebsch-Gordon rule gives the tensor product decomposition of representations

$$\mathrm{Sym}^1 \otimes \mathrm{Sym}^n = \mathrm{Sym}^{n-1} \oplus \mathrm{Sym}^{n+1}.$$

Many of the geometric constructions in the *Elements* can be expressed in algebraic language as follows.

Theorem 3.16 *The set K is a subfield of $\mathbb{C}$, algebraic over $\mathbb{Q}$ and closed under taking square-roots.*

Proof: Intersections of lines and circles are found by solving a linear or quadratic equation with coefficients already constructed. Hence a complex number α is constructible exactly when there is tower of extensions

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$$

with each $[F_i : F_{i-1}] = 2$, and $\alpha \in F_n$. Each $\alpha \in K$ lies in a finite extension of $\mathbb{Q}$, hence is algebraic over $\mathbb{Q}$. And the square-roots of a given complex number can constructed using operations 1 and 2. Hence $\alpha \in K$ implies (both values of) $\sqrt{\alpha}$ are in K. ■

The constructible numbers are precisely those which can be expressed in terms of nested square-roots. For example Prop. I.1 in the *Elements* constructs $e^{2\pi i/6} = (-1 + \sqrt{-3})/2$, whose minimal polynomial is $x^2 - x + 1$, by drawing the line through $0, 1$, then drawing the circles of radius 1 centered at $0, 1$. Elsewhere in the *Elements* Euclid proves that the root of unity $e^{2\pi i/n}$ is constructible for

$$n = 2, 3, 4, 5, 6, 8, 10, 12, 15 \tag{15}$$

and that $e^{2\pi i/n}$ constructible implies $e^{\pi i/n}$ constructible. This shows that $2\cos(2\pi/n)$ is also constructible for these n. Constructing $e^{2\pi i/n}$ or $2\cos(2\pi/n)$ is equivalent to constructing a regular polygon with n sides. Naturally, the Greeks and those who came after were tantalized by the gaps in Euclid's list (15).

The Three Problems of Antiquity are really questions about K.

1. To square the circle. [Is $\pi \in K$?]
2. To duplicate the cube. [Is $\sqrt[3]{2} \in K$?]
3. To trisect a given angle. [For example, is $\cos(2\pi/9) \in K$?]

As the Greeks suspected, the answers to the three questions are No, No and No. We address the second and third No's here. [5]

Let $\alpha \in K$ and let $\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$ be a tower of quadratic extensions with $\alpha \in F_n$. Then $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset F_n$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ divides $[F_n : \mathbb{Q}] = 2^n$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is the degree of the minimal polynomial $f_\alpha \in \mathbb{Q}[x]$ of α over $\mathbb{Q}$, this proves

Proposition 3.17 *If $\alpha \in K$ then $\deg f_\alpha$ is a power of 2.*

[5] The No for problem 1 is the transcendence of π (that is, π is not algebraic over $\mathbb{Q}$). This was proved in 1882 by Lindenmann. Proofs abound on the web, using facts about algebraic numbers and symmetric polynomials that we have proved, and some basic analysis.

For $\alpha = \sqrt[3]{2}$ we have $f_\alpha = x^3 - 2$, so $\sqrt[3]{2} \notin K$.

For $\alpha = \cos(2\pi/9)$ we have $f_\alpha = x^3 - 3x + 1$ (see the list (10)) so $\cos(2\pi/9) \notin K$.

This explains the absence of $n = 9$ in the list (10). The other missing numbers are primes or twice a prime. For $n = p$ a prime, the minimal polynomial of $e^{2\pi i/p}$ is the cyclotomic polynomial $\Phi_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ (see (3)). Hence $e^{2\pi i/p}$ can only be constructible if $p - 1$ is a power of 2, which forces $p = 2^{2^m} + 1$ to be a Fermat prime. The known Fermat primes are

$$3 = 2 + 1, \quad 5 = 2^2 + 1, \quad 17 = 2^4 + 1, \quad 257 = 2^8 + 1, \quad 65537 = 2^{16} + 1.$$

These are the only known primes for which $e^{2\pi i/p}$ could be constructible. In fact each of these roots of unity is constructible. For an expression of $e^{2\pi i/17}$ in terms of nested square roots, see [Hardy-Wright, p.60]. The issue here is that the converse of Prop. 3.17 is false: there are algebraic integers $\alpha \in \overline{\mathbb{Z}}$ for which $\deg f_\alpha$ a power of 2 yet α is not constructible. The precise criterion for constructibility requires more information about f_α than just its degree. This extra information comes from Galois theory.

3.7 Splitting fields

Let F be a field and let $f \in F[x]$. Recall from Prop. 1.4 that there exists a field $L \supset F$ such that f splits into product of linear factors in $L[x]$. The field L is not unique; indeed, a smaller field may suffice to split f. We seek minimal fields in which f splits.

We say that E is a **splitting field for** f **over** F if

1. f is a product of linear factors in E, and
2. E is generated by the roots of f in E.

Example 1: We constructed $\mathbb{F}_{p^n}$ as the splitting field of $f = x^{p^n} - x$ over $\mathbb{F}_p$.

Example 2: Let $F = \mathbb{Q}$ and let $f = x^3 - 2$. The roots of f in $\mathbb{C}$ are $\alpha, \zeta\alpha, \zeta^2\alpha$, where $\zeta = e^{2\pi i/3}$ and α is the real cube-root of 2. A splitting field is constructed via the tower

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \zeta).$$

Since $f_\alpha = x^3 - 2$, we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Since ζ is not real, its minimal polynomial $x^2 + x + 1$ over $\mathbb{Q}$ remains irreducible over $\mathbb{Q}(\alpha)$ and therefore $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] = 2$. Hence the splitting field $\mathbb{Q}(\alpha, \zeta)$ has degree $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}] = 2 \cdot 3 = 6$ over $\mathbb{Q}$.

Example 3: Let $F = \mathbb{Q}$ and let $f = x^3 + x^2 - 2x - 1$. This is the minimal polynomial of $\alpha = 2\cos(2\pi/7)$ and the other roots of f are $\beta = 2\cos(4\pi/7)$ and $\gamma = 2\cos(6\pi/7)$. The trigonometric identities

$$\cos 2\theta = 2\cos\theta - 1, \qquad \cos 3\theta = 4\cos^3\theta - 3\cos\theta.$$

show that β, γ are rational polynomial expressions in α. Hence $\mathbb{Q}(\alpha)$ is the splitting field of f and its degree is $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$.

It turns out that the splitting field of a cubic polynomial $f = x^3 + ax^2 + bx + c \in F[x]$ has degree either 3 or 6 over F, and this can be detected (without knowing anything about the roots of f) by whether the discriminant (see (9))

$$D(f) = a^2b^2 - 27c^2 - 4b^3 - 4a^3c + 18abc \tag{16}$$

is a square in $F^\times$. In Example 2, we have $D(f) = -27 \cdot 4$ a non-square in $\mathbb{Q}^\times$, while in Example 3, we have $D(f) = 49 \in \mathbb{Q}^{\times 2}$.

Splitting fields always exist. For if we choose any field L in which f splits, say

$$f = c\prod_{i=1}^{n}(x - \alpha_i) \in L[x],$$

the field $E = F(\alpha_1, \ldots, \alpha_n)$ is a splitting field for f over F. [6]

Any splitting field is has finite degree over F, since it is obtained by adjoining finitely many roots.

However, splitting fields are not unique. For example, take $F = \mathbb{Q}$ and $f = x^2 - 2 \in \mathbb{Q}[x]$. The polynomial $\mathbb{Q}$ splits in $\mathbb{R}$ and also in the p-adic field $\mathbb{Q}_p$ for when $2 \in \mathbb{F}_p^{\times 2}$, which occurs exactly when $16 \mid (p^2 - 1)$. We have infinitely many splitting fields $E = \mathbb{Q}(\alpha)$, where α is a root of $x^2 - 2$ in $\mathbb{R}$ or $\mathbb{Q}_p$ for such p. Each of these fields consist of completely different elements (real or p-adic numbers) but they are both isomorphic to $\mathbb{Q}[x]/(x^2 - 2)$, hence $E \simeq E'$ as fields. So the best we can hope for is that splitting fields are unique up to isomorphism. This is true.

Proposition 3.18 *Let F be a field, let $f \in F[x]$ and let E, E' be two splitting fields of f over F. Then there is a field isomorphism $\varphi : E \xrightarrow{\sim} E'$ such that $\varphi(a) = a$ for all $a \in F$.*

The assertion of Prop. 3.18 may be visualized in the commutative diagram, where the vertical arrows are the inclusion maps.

$$\begin{array}{ccc} E & \xrightarrow[\varphi]{\sim} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow[\mathrm{id}]{} & F \end{array} \tag{17}$$

An isomorphism φ as in the diagram (17) is called an **isomorphism over** F.

Prop. 3.18 will follow from a more flexible result whose proof is more amenable to induction: We replace the lower line in (17) by a fixed isomorphism of fields $\psi : F \to F'$. This extends to an isomorphism of polynomial rings $\psi : F[x] \to F'[x]$ given by $\psi(\sum c_k x^k) = \sum \psi(c_k)x^k$. It will be convenient to write $g' = \psi(g)$ for $g \in F[x]$.

Theorem 3.19 (The Extension Theorem) *Fix a field isomorphism $\psi : F \xrightarrow{\sim} F'$ as above. Let $f \in F[x]$, with $f' = \psi(f) \in F'[x]$ and suppose E, E' are splitting fields of f, f' over F, F', respectively.*

[6] $F(\alpha_1, \ldots, \alpha_n)$ is the intersection of all subfields of L containing F and $\{\alpha_1, \ldots, \alpha_n\}$. Inductively, we have $F(\alpha_1, \ldots, \alpha_n) = F(\alpha_1, \ldots, \alpha_{n-1}(\alpha_n)$.

There exists a field isomorphism $\varphi : E \xrightarrow{\sim} E'$ extending ψ, that is, so that we have a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow[\varphi]{\sim} & E' \\ \uparrow & & \uparrow \\ F & \xrightarrow[\psi]{\sim} & F' \end{array} \tag{18}$$

Proof: We use induction on $[E : F]$, which is finite. If $[E : F] = 1$ there is nothing to prove. Otherwise, there is a root α of f in E such that $\alpha \notin F$. Let $g \in F[x]$ be the minimal polynomial of α. Then g' is irreducible in $F'[x]$. And $g \mid f$ in $F[x]$, so $g' \mid f'$ in $F'[x]$. Since f' splits in E', there is a root $\alpha' \in E'$ of g'. And g' is the minimal polynomial of α' in $F'[x]$. Hence we have field isomorphisms

$$F(\alpha) \xleftarrow[\alpha]{\sim} F[x]/(g) \xrightarrow[\psi]{\sim} F'[x]/(g') \xrightarrow[\alpha']{\sim} F'(\alpha')$$

which give an isomorphism $\psi_1 : F(\alpha) \xrightarrow{\sim} F'(\alpha')$ extending ψ. Since $[E : F(\alpha)] < [E : F]$, the isomorphism ψ_1 extends, by induction, to an isomorphism $\varphi : E \xrightarrow{\sim} E'$. Clearly φ also extends ψ. ■

Corollary 3.20 *Let $f \in F[x]$ and let L/F be a field extension such that f splits in $L[x]$ as*

$$f = c\prod_{i=1}^{k}(x - \alpha_i)^{m_i},$$

where the α_i are the distinct roots of f in L and the m_i are positive integers. Then the set $\{m_i\}$, with multiplicities, is independent of L.

Proof: Let L'/F be another extension splitting f, so that $f = c\prod_{j=1}^{\ell}(x - \alpha'_j)^{m'_i}$ in $L'[x]$. Let $E = F(\alpha_1, \ldots, \alpha_k)$ and $E' = F(\alpha'_1, \ldots, \alpha'_\ell)$ be the splitting fields of f over F in L and L' respectively. By Prop. 3.18, there is an isomorphism $\varphi : E \xrightarrow{\sim} E'$ over F. The induced map $\varphi : E[x] \to E'[x]$ is the identity on $F[x]$, so in $E'[x]$ we have

$$c\prod_{i=1}^{k}(x - \varphi(\alpha_i))^{m_i} = \varphi(f) = f = c\prod_{j=1}^{\ell}(x - \alpha'_j)^{m'_i}.$$

By unique factorization in $E'[x]$ we have

$$\{\varphi(\alpha_i)\} = \{\alpha'_j\}, \quad \text{and} \quad \{m_i\} = \{m'_j\}$$

as sets-with-multiplicities. ■

It therefore makes sense to say that a polynomial $f \in F[x]$ has a **multiple root** if f has a repeated factor (some $m_i > 1$) in a splitting field of f over F. Otherwise (if all $m_i = 1$) we say f has **distinct roots**. Having multiple or distinct roots is a quality independent of the choice of splitting field containing the roots.

Example: Suppose F has characteristic p and let $f = x^p - a \in F[x]$ where $a \in F$. Let E/F be an extension in which f splits and let α, β be two roots of f in E. Then $\alpha^p = a = \beta^p$, so α/β is a root of $x^p - 1 = (x-1)^p$, meaning that $\alpha = \beta$. Hence $f = (x-\alpha)^p$ in $E[x]$, so f has a multiple root. Assume now that a is not the p^{th} power of any element in F. I claim that f is irreducible in $F[x]$. For if $g \in F[x]$ is a nonconstant monic factor of f then g also divides f in $E[x]$ so $g = (x-\alpha)^k$ for some $1 \leq k \leq p$. The coefficient of x^{k-1} in g is $-k\alpha$, which must belong to F, since $g \in F[x]$. But $\alpha \notin F$, since $a \notin F^p$. Hence $k = p$ and $g = f$. Therefore f is an irreducible polynomial having a multiple root.

Proposition 3.21 *Let F be a field. For a nonconstant irreducible polynomal $f \in F[x]$, the following are equivalent.*

1. *f has a multiple root.*
2. *The formal derivative $\dot{f}$ is the zero polynomial.* [7]
3. *The field F has characteristic $p > 0$ and $f \in F[x^p]$.*

Proof: $(1 \Rightarrow 2)$: Let E be a splitting field for f. If f has a multiple root then f has a root $\alpha \in E$ such that $f(x) = (x-\alpha)^m g(x)$ in $E[x]$, with $m > 2$. Then $\dot{f}(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m \dot{g}(x)$ so $\dot{f}(\alpha) = 0$. Since f is irreducible in $F[x]$ it follows that $f \mid \dot{f}$. If $\dot{f} \neq 0$ then $\deg \dot{f} < \deg f$ would be a contradiction, so $\dot{f} = 0$ in $F[x]$.

$(2 \Rightarrow 3)$: Suppose $\dot{f} = 0$ in $F[x]$. If $f = \sum_{k=0}^{n} c_k x^k$, then $\dot{f} = \sum_{k=1}^{n} k c_k x^{k-1} = 0$. Hence $kc_k = 0$ for all $1 \leq k \leq n$, so if x^k appears in f we must have $k = 0 \in F$. This forces F to have characteristic $p > 0$ and $p \mid k$ whenever $c_k \neq 0$, meaning that $f \in F[x^p]$.

$(3 \Rightarrow 1)$: Suppose $f \in F[x^p]$, so that $f(x) = g(x^p)$ for some $g \in F[x]$. Let E be a splitting field of g over F. In $E[x]$ we have $g = c\prod(x-\alpha_i)^{m_i}$. Enlarging E if necessary, we may assume that $x^p - \alpha_i$ splits in E for each i. The previous example shows that there exist β_i in E such that $x^p - \alpha_i = (x-\beta_i)^p$. We have

$$f = c\prod(x^p - \alpha_i)^{m_i} = c\prod(x-\beta_i)^{pm_i}.$$

Since each $pm_i > 1$, the polynomial f has a multiple root. ■

A polynomial $f \in F[x]$ is **separable** if each irreducible factor of f in $F[x]$ has distinct roots. A product of separable polynomials is separable.

An algebraic extension E/F is **separable** if every polynomial $f \in F[x]$ having a root in E is separable over F. Equivalently, E/F is separable if for every $\alpha \in E$ the minimal polynomial of α over F has distinct roots. An algebraic extension E/F is **inseparable** if it is not separable.

If F has characteristic zero then every algebraic extension E/F is separable.

F is a finite field of characteristic p then every algebraic extension E/F is separable. For the Frobenius map $\phi : F \to F$ sending $\phi(a) = a^p$ is injective (since $a^p - 1 = (a-1)^p$) hence surjective since F

[7] If $f = \sum_{k=0}^{n} c_k x^k$ then $\dot{f} = \sum_{k=1}^{n} k c_k x^{k-1}$.

is finite. It follows that $F[x^p] = F[x]^p$. Hence $F[x^p]$ contains no nonconstant irreducible polynomials over F, so every irreducible polynomial $f \in F[x]$ is separable.

A field F can have inseparable extensions only if F is infinite of characteristic p. For example, let $F = \mathbb{F}_p(T)$ be the field of rational functions over $\mathbb{F}_p$ in the variable T. Then the polynomial $x^p - T \in F[x]$ is not separable over F (see the example prior to Prop. 3.21), and its splitting field $E = \mathbb{F}_p(T^{1/p})$ is an inseparable extension of F.

3.8 Automorphisms and Galois Extensions

3.8.1 Field automorphisms

For any field extension E/F, let

$$\mathrm{Aut}(E/F) = \{\sigma \in \mathrm{Aut}(E) : \ \sigma(a) = a \text{ for all } a \in F\}$$

denote the group of automorphisms of E which are the identity on F. An element $\sigma \in \mathrm{Aut}(E/F)$ makes the following diagram (cf. (17)) commute:

$$\begin{array}{ccc} E & \xrightarrow{\ \sigma\ } & E \\ \uparrow & & \uparrow \\ F & \xrightarrow[\ \mathrm{id}\ ]{} & F. \end{array} \tag{19}$$

If F is the prime field (either $\mathbb{Q}$ or $\mathbb{F}_p$ according as the characteristic is 0 or $p > 0$, then every automorphism of E is trivial on F, so in this case $F = \mathrm{Aut}(E)$ is the full automorphism group of E.

Each $\sigma \in \mathrm{Aut}(E/F)$ extends to an automorphism of the polynomial ring $E[x]$ by acting on the coefficients: $\sigma(\sum c_k x^k) := \sum \sigma(c_k) x^k$. If $f \in F[x]$, then $\sigma(f) = f$. Hence if $\alpha \in E$ is a root of f, then $\sigma(\alpha)$ is also a root of f. Thus, $\mathrm{Aut}(E/F)$ permutes the roots of every polynomial $f \in F[x]$.

3.8.2 Automorphisms of finite extensions

If E/F is a finite extension, then the automorphism group $\mathrm{Aut}(E/F)$ is finite. More precisely, we have:

Proposition 3.22 *If E/F is a finite extension of degree n, then $\mathrm{Aut}(E/F)$ is isomorphic to a subgroup of S_n.*

Proof: Assume E/F is finite and let $G = \mathrm{Aut}(E/F)$. Then we have $E = F(\alpha_1, \ldots, \alpha_n)$ for some elements $\alpha_i \in E$. Let $f_i \in F[x]$ be the minimal polynomial of α_i and let n_i be the number of roots of f_i in E. These roots are permuted by G which acts faithfully on $\{\alpha_1, \ldots, \alpha_n\}$, since the α_i generate E over F. This gives an injective homomorphism $G \hookrightarrow S_n$. ■

Beware that $\mathrm{Aut}(E/F)$ can be trivial even when $E \supsetneq F$. For example, let $F = \mathbb{Q}$ and let $E = \mathbb{Q}(\alpha)$ where α is the real root of $x^3 - 2$. The other roots of $x^3 - 2$ are not real and they do not lie in E. Hence any element of $\mathrm{Aut}(E)$ must fix α and hence is trivial since α generates E. The problem is that $\mathbb{Q}(\alpha)$ is too small to display the symmetry of the three roots of $x^3 - 2$.

3.8.3 Galois extensions

A finite extension E/F is **Galois** if E is the splitting field of a separable polynomial $f \in F[x]$. If K is any intermediate field, $F \subset K \subset E$, then E is also the splitting field of f over K, so the extension E/K is Galois. When E/F is Galois the group $\mathrm{Aut}(E/F)$ is called the **Galois group** of E/F.

Proposition 3.23 *If E/F is a Galois extension then* $|\mathrm{Aut}(E/F)| = [E : F]$.

Proof: We use induction on the degree $[E : F]$. Let $f \in F[x]$ be a separable polynomial for which E is the splitting field over F. Let f_1 be an irreducible factor of f. Then f_1 has distinct roots, since f is separable. Let $\alpha_1, \ldots, \alpha_s$ be these distinct roots of f_1, where $s = \deg f_1$. These roots generate the splitting field $F_1 = F(\alpha_1, \ldots, \alpha_s)$ of f_1 in E. For each $1 \le i \le s$, the isomorphisms

$$F(\alpha_1) \xleftarrow[\alpha_1]{\sim} F[x]/(f_1) \xrightarrow[\alpha_i]{\sim} F(\alpha_i)$$

give an isomorphism $F(\alpha_1) \xrightarrow{\sim} F(\alpha_i)$ which extends, by Prop. 3.19, to an automorphism $\varphi_i \in \mathrm{Aut}(F_1/F)$ sending $\alpha_1 \mapsto \alpha_i$. Hence $\mathrm{Aut}(F_1/F)$ is transitive on the roots of f_1. The stabilizer of α_1 is $\mathrm{Aut}(F_1/F(\alpha_1))$, which by induction has order

$$|\mathrm{Aut}(F_1/F(\alpha_1))| = [F_1 : F(\alpha_1)]$$

and has index $s = \deg f_1 = [F(\alpha_1) : F]$ in $\mathrm{Aut}(F_1/F)$. Therefore we have

$$|\mathrm{Aut}(F_1/F)| = |\mathrm{Aut}(F_1/F(\alpha_1))| \cdot [F(\alpha_1) : F] = [F_1 : F(\alpha_1)] \cdot [F(\alpha_1) : F] = [F_1 : F].$$

If $F_1 = E$, we are done. Assume $F_1 \neq E$. Since $\mathrm{Aut}(E/F)$ permutes the roots of f_1, and these roots generate F_1, each automorphism in $\mathrm{Aut}(E/F)$ restricts to an automorphism of $\mathrm{Aut}(F_1/F)$, giving a homomorphism $r : \mathrm{Aut}(E/F) \to \mathrm{Aut}(F_1/F)$. Since E is also the splitting field of f over F_1, it follows from Prop. 3.19 that r is surjective. And $\ker r = \mathrm{Aut}(E/F_1)$ by definition. Thus we have an exact sequence

$$1 \longrightarrow \mathrm{Aut}(E/F_1) \longrightarrow \mathrm{Aut}(E/F) \xrightarrow{r} \mathrm{Aut}(F_1/F) \longrightarrow 1.$$

Again by induction we have $|\mathrm{Aut}(E/F_1)| = [E : F_1]$. And we have shown above that $|\mathrm{Aut}(F_1/F)| = [F_1 : F]$. Therefore

$$|\mathrm{Aut}(E/F)| = |\mathrm{Aut}(E/F_1)| \cdot |\mathrm{Aut}(F_1/F)| = [E : F_1] \cdot [F_1 : F] = [E : F],$$

as was to be shown. ■

If G is any subgroup of $\mathrm{Aut}(E)$, the **fixed field of** G is the subfield E^G of elements in E fixed by every element of G:

$$E^G = \{\alpha \in E : \ \sigma(\alpha) = \alpha \text{ for all } \sigma \in G\}.$$

Lemma 3.24 *Let E be a field and let G be a finite subgroup of* $\mathrm{Aut}(E)$. *Then* $[E : E^G] \leq |G|$.

Proof: We show that any set of more than $|G|$ elements in E is linearly dependent over E^G. Let $\{\alpha_1, \ldots, \alpha_n\} \subset E$, with $n > |G|$. Let $V \subset E^n$ be the set of simultaneous solutions of the linear equations

$$\mathrm{eq}(\sigma): \quad \sigma(\alpha_1)x_1 + \sigma(\alpha_2)x_2 + \cdots + \sigma(\alpha_n)x_n = 0,$$

one equation for each $\sigma \in G$. If $v = (v_1, \ldots, v_n) \in V$ then $\tau(v) := (\tau(v_1), \ldots, \tau(v_n))$ is a solution of $\mathrm{eq}(\tau\sigma)$ for all $\sigma \in G$, which is the same set of equations permuted, so $\tau(v) \in V$ for any $\tau \in G$.

Since there are fewer equations $\mathrm{eq}(\sigma)$ than variables x_i, the solution space V is nonzero. For each $v = (v_1, \ldots, v_n) \in V$ let $m(v)$ be the number of nonzero entries v_i and let

$$m = \min\{m(v) : \ 0 \neq v \in V\} > 0.$$

Choose a solution v with $m(v) = v$, and let v_i be a nonzero entry of v. Then $u = v_i^{-1}v$ is another solution in V with m nonzero entries, and now $u_i = 1$.

For any $\tau \in G$ the solution $\tau(u)$ has nonzero entries in the same places as u, and $\tau(u_i) = 1 = u_i$. So $m(\tau(u) - u) < m$, so $\tau(u) - u = 0$. Therefore $\tau(u) = u$ for every $\tau \in G$, so each entry u_j of u lies in E^G. Considering $\mathrm{eq}(\sigma)$ for $\sigma = e$, we have

$$\alpha_1 u_1 + \cdots + \alpha_n u_n = 0.$$

Thus, the α_i are indeed linearly independent over E^G. ■

Proposition 3.25 *Let E be a field and let G be a finite subgroup of* $\mathrm{Aut}(E)$. *Then E/E^G is Galois, with Galois group* $\mathrm{Aut}(E/E^G) = G$, *and* $[E : E^G] = |G|$.

Proof: Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a G-orbit in E. The polynomial $g = \prod(x - \alpha_i)$ is fixed by G, hence it belongs to $E^G[x]$ and $g(\alpha_1) = 0$. Hence α_1 is algebraic over E^G. Let $f \in E^G[x]$ be the minimal polynomial of α_1. Then f is also fixed by G, so each α_i is also a root of f and $g \mid f$. Since f is irreducible in $E^G[x]$ we have $f = g = \prod(x - \alpha_i)$.

By Lemma 3.24, the extension E/E^G is finite, so $E = E^G(\beta_1, \ldots, \beta_s)$ for some elements $\beta_i \in E$. By the second claim, the minimal polynomial $f_i \in E^G[x]$ of β_i splits into distinct linear factors in $E[x]$. Hence E is the splitting field of the separable polynomial $f = \prod f_i \in E^G[x]$, so E/E^G is Galois.

By definition we have $G \leq \mathrm{Aut}(E/E^G)$. And Prop. 3.23 and Lemma 3.24 imply that

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

It follows that $G = \mathrm{Aut}(E/E^G)$.

The equality $[E : E^G] = |G|$ now follows from Prop. 3.23. ■

Theorem 3.26 *Let E/F be a finite extension of fields, and let $G = \mathrm{Aut}(E/F)$. Then the following are equivalent.*

1. *E/F is Galois;*
2. *$F = E^G$;*
3. *$[E : F] = |G|$.*

Proof: First note that G is finite, by Prop. 3.22, so Prop. 3.25 applies, and we have

$$E/E^G \text{ is Galois}, \quad G = \mathrm{Aut}(E/E^G) \quad \text{and} \quad [E : E^G] = |G|.$$

This shows that $3 \Leftrightarrow 2 \Rightarrow 1$. And $1 \Rightarrow 3$ is Prop. 3.23. ■

Remark: It is not true that if L/E and E/F are Galois then L/F is Galois. Consider the tower [8]

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}).$$

From the proofs of Props. 3.23 and 3.25 we can extract additional corollaries.

Corollary 3.27 *Let E/F be a Galois extension with Galois group $G = \mathrm{Aut}(E/F)$, and let $f \in E[x]$.*

1. *We have $f \in F[x]$ if and only if $\sigma(f) = f$ for all $\sigma \in G$.*
2. *If $f \in F[x]$ and f has root in E then f splits in $E[x]$.*
3. *If $f \in F[x]$ and f has root in E then f is irreducible in $F[x]$ iff G is transitive on the roots of f.*

3.8.4 The Galois correspondence

Let E/F be a Galois extension with Galois group $G = \mathrm{Aut}(E/F)$. The Main Theorem of Galois Theory asserts that subgroups H of G and the intermediate fields M lying between F and E are in bijection. A more precise statement of the theorem is as follows.

Theorem 3.28 (The Galois Correspondence) *There are mutually inverse bijections*

$$\{\textit{subgroups } H \leq G\} \quad \longleftrightarrow \quad \{\textit{intermediate fields } F \subset M \subset E\}$$

sending $H \mapsto E^H$, and sending $M \mapsto \mathrm{Aut}(E/M)$. These bijections have the following properties.

1. *If H and J are subgroups of G then $H \leq J$ if and only if $E^J \subset E^H$.*
2. *If $H \leq J \leq G$ we have $[J : H] = [E^H : E^J]$.*
3. *If $g \in G$ then $E^{gHg^{-1}} = g(E^H)$ and if $M = E^H$ we have $\mathrm{Aut}(E/g(M)) = g\,\mathrm{Aut}(E/M)g^{-1}$.*

[8] Thanks to Andrew Phillips for providing this example.

4. *The following are equivalent:*

   i) The subgroup H is normal in G;

   ii) the extension E^H/F is Galois;

   iii) G preserves E^H.

   When i)-iii) hold, we have an isomorphism $G/H \simeq \mathrm{Aut}(E^H/F)$, via restriction.

Proof: By Prop. 3.23, the group G is finite of order $|G| = [E : F]$. Hence every subgroup $H \leq G$ is finite, so Prop. 3.25 shows that $\mathrm{Aut}(E/E^H) = H$. Conversely if M is an intermediate field then E/M is Galois. Let $H = \mathrm{Aut}(E/M)$. Theorem 3.26 shows that $M = E^H$. Hence the correspondences $H \mapsto E^H$ and $M \mapsto \mathrm{Aut}(E/M)$ are mutually inverse bijections.

Let H and J be subgroups of G. If $H \leq J$ then clearly $E^J \subset E^H$. Conversely, if $E^J \subset E^H$ then H acts trivially on E^J so $H \leq \mathrm{Aut}(E/E^J) = J$.

When $H \leq J$ and $E^J \subset E^H$, we have

$$[J : H] = \frac{|J|}{|H|} = \frac{|\mathrm{Aut}(E/E^J)|}{|\mathrm{Aut}(E/E^H)|} = \frac{[E : E^J]}{[E : E^H]} = \frac{[E : E^H] \cdot [E^H : E^J]}{[E : E^H]}.$$

In a G-action, the fixed-point sets of conjugate subgroups $H, gHg^{-1} \leq G$ are conjugate by g. This shows that $E^{gHg^{-1}} = g(E^H)$. Then we have

$$\mathrm{Aut}(E/g(E^H)) = \mathrm{Aut}(E/E^{gHg^{-1}}) = gHg^{-1} = g\,\mathrm{Aut}(E/E^H)g^{-1}.$$

If H is normal in G then $g(E^H) = E^{gHg^{-1}} = E^H$, so G preserves E^H. If G preserves E^H we have a restriction map $r : G \to \mathrm{Aut}(E^H)$ whose kernel is the subgroup fixing E^H. This subgroup is H, so $H = \ker r$ is normal in G. And G/H is a finite subgroup of $\mathrm{Aut}(E^H/F)$ with fixed-field F, so E^H/F is Galois. And if E^H/F is Galois then E^H is the splitting field of a separable polynomial $f \in F[x]$. Letting $\alpha_1, \ldots, \alpha_s$ be the roots of f in E^H, we have $E^H = F(\alpha_1, \ldots, \alpha_s)$. The group G fixes f, hence permutes the roots $\{\alpha_i\}$, so G preserves E^H. This proves item 4. ■

3.9 The Galois group of a polynomial

Let F be a field, let $f \in F[x]$ be a separable polynomial, and let E be a splitting field of f, so that we have the Galois group $\mathrm{Aut}(E/F)$. If E' is another splitting field of f then we have an isomorphism $E \simeq E'$ over F (see Prop. 3.18), which induces an isomorphism of Galois groups $\mathrm{Aut}(E/F) \simeq \mathrm{Aut}(E'/F)$. The isomorphism class of the group

$$G_f := \mathrm{Aut}(E/F)$$

is therefore independent of E; the group G_f is the **Galois group of f over F**.

Note that G_f is a more refined object than $\mathrm{Aut}(E/F)$. The latter group depends only on the extension E/F, and E could be the splitting field of many different polynomials. [9] But with G_f we single out a particular polynomial $f \in F[x]$, hence a particular set of orbits of $\mathrm{Aut}(E/F)$ in E, and a particular realization of $\mathrm{Aut}(E/F)$ as a group of permutations.

Suppose f has degree n, and let X be the set of roots of f in E. The group G_f permutes the roots in X, giving a homomorphism $G_f \to S_X \simeq S_n$, which is injective since E is generated by X. Thus G_f is isomorphic to a subgroup of S_n, where $n = \deg f$.

Assume now that f is irreducible in $F[x]$. This occurs exactly when G_f is transitive on X. Let $\alpha \in X$ and let $H_\alpha \leq G_f$ be the stabilizer of α in G_f. Then $E^{H_\alpha} = F(\alpha)$, so H_α and $F(\alpha)$ are related by the Galois correspondence. Note that $[G_f : H] = [E : F(\alpha)] = n$, as it should be.

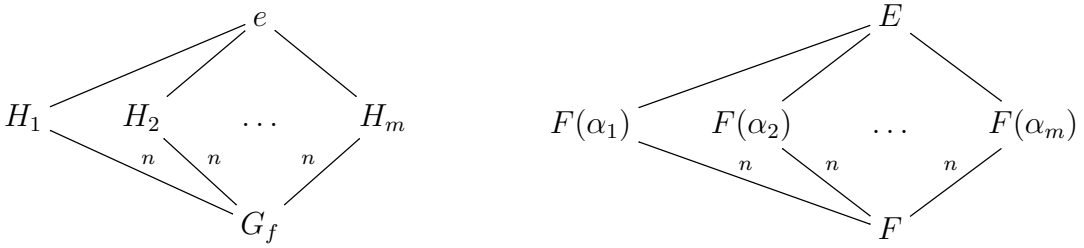
Since G_f is transitive on X, the subgroups H_α are conjugate to each other in G_f and the subfields $F(\alpha)$ are permuted transitively by G_f. However, some of these subgroups and subfields could coincide. This means we have an equivalence relation on X, via the rule:

$$\alpha \sim \beta \quad \Leftrightarrow \quad F(\alpha) = F(\beta).$$

Let

$$X = \prod_{i=1}^{m} X_i$$

be the partition of X into equivalence classes X_i, which we call **blocks**. Two roots $\alpha, \beta \in X$ are in the same block X_i exactly when α is a polynomial expression in β and vice-versa. If we now choose one root $\alpha_i \in X_i$ for each $1 \leq i \leq m$, and let H_i be the stabilizer of α_i in G, we have distinct subgroups $H_1, \ldots, H_m$ and distinct subfields $F(\alpha_1), \ldots, F(\alpha_m)$, related by the following partial picture of the Galois correspondence:



These are partial pictures of the Galois correspondence that appear for any irreducible $f \in F[x]$. The missing part of these pictures depends on the structure of G_f.

[9] For example, if $\alpha = \sqrt[3]{2}$ and $\zeta = \exp(2\pi i/3)$, then $E = \mathbb{Q}(\alpha, \zeta)$ is the splitting field of $f_1 = x^3 - 2$, so G_{f_1} is naturally a subgroup of S_3, permuting the three roots $\alpha, \alpha\zeta, \alpha\zeta^2$ of f_1. But also $\mathbb{Q}(\alpha, \zeta) = \mathbb{Q}(\alpha + \zeta)$, so E is also the splitting field of $f_2 = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9$, which is the minimal polynomial of $\alpha + \zeta$ over $\mathbb{Q}$. Now G_{f_2} is naturally a subgroup of S_6, permuting the six roots of f_2, which are $\alpha\zeta^i + \zeta^j$ for $i = 0, 1, 2$ and $j = 1, 2$.

3.9.1 Imprimitive group actions and Galois groups

In the above pictures, the extensions $F(\alpha_i)/F$ will be Galois (equivalently $H_i \lhd G_f$) exactly when $m = 1$. However, even if $F(\alpha_i)/F$ is not Galois, the automorphism group $\mathrm{Aut}(F(\alpha_i)/F)$ need not be trivial. This group is is independent of i, since the subgroups H_i and subfields $F(\alpha_i)$ are all G_f-conjugate, and is therefore canonically attached to G_f.

To determine $\mathrm{Aut}(F(\alpha_i)/F)$ we first consider blocks in the setting of general group actions. Let G be a finite group acting transitively on a set X and suppose there exists a partition

$$X = \coprod_{i=1}^{m} X_i$$

into disjoint subsets X_i permuted by G. Let k be the common cardinality $|X_i| = k$. The G-action on X is called **imprimitive** if there exists such a partition with $k > 1$.

Various subgroups are associated to a partition $X = \coprod X_i$, as follows.

$$J_i = \{g \in G : \ gX_i = X_i\}, \qquad H_i = \{g \in G : \ gx = x \quad \forall x \in X_i\}.$$

Then J_i acts transitively on X_i and H_i acts trivially on X_i, so we have an injective homomorphisim $J_i/H_i \hookrightarrow S_{X_i}$. Let Z_i be the centralizer of J_i/H_i in S_{X_i}. The groups J_i, H_i, Z_i are permuted by G.

Lemma 3.29 *The following conditions are equivalent:*

1. *The H_i are distinct;*
2. *J_i is the full normalizer of H_i in G;*
3. *X_i is the full fixed-point set of H_i in X.*

Proof: This is a straightforward exercise. ■

Assume the conditions of Lemma 3.29 hold. The centralizer $Z = C_{S_X}(G)$ preserves each X_i, and commutes there with J_i/H_i, so $Z \subset \prod Z_i$. Let $z_i \in Z_i$ be such that $z = (z_1, \ldots, z_m) \in Z$. We will show that all z_i are determined by z_1. Choose $g \in G$ such that $gX_1 = X_i$. Pick $x_1 \in X_1$ and let $x_i = gx_1 \in X_i$. Then

$$z_i g \cdot x_1 = zg \cdot x_1 = gz \cdot x_1 = gz_1 \cdot x_1,$$

so $z_i = gz_1g^{-1}$. The element $z_i = gz_1g^{-1} \in Z_i$ depends only on i and not on the choice of g. Hence for any $z_1 \in Z_1$ we can *define* $z_i = gz_1g^{-1}$ for any $g \in G$ sending $gX_1 = X_i$ and we have

$$Z = \{(z_1, \ldots, z_m) : \ z_1 \in Z_1\} \simeq Z_1.$$

We return to return to the setting of Galois groups. Let $f \in F[x]$ be irreducible and separable, with splitting field E and Galois group $G_f = \mathrm{Aut}(E/F)$. Recall we have partitioned the set X of roots of

f into equivalence classes $X = \coprod X_i$, via the relation $\alpha \sim \beta \Leftrightarrow F(\alpha) = F(\beta)$. Choose one root α_i in each block X_i. The field $F_i = F(\alpha_i)$ depends only on i and not on the choice of α_i. The objects in the abstract theory of blocks become

$$J_i = \{g \in G : \ gF_i = F_i\}, \qquad H_i = \mathrm{Aut}(E/F_i), \qquad J_i/H_i = \mathrm{Aut}(F_i/F).$$

Proposition 3.30 *For all $1 \leq i \leq m$ we have $\mathrm{Aut}(F_i/F) \simeq C_{S_X}(G_f)$, the centralizer of G_f in S_X.*

Proof: From the Galois correspondence we have $F_i = E^{H_i}$. The F_i are distinct, so the subgroups H_i are distinct. Hence the conditions of Lemma 3.29 hold, and we have $C_{S_X}(G) \simeq Z_1$.

But more is true: An automorphism $\sigma \in \mathrm{Aut}(F_i/F)$ is completely determined by its effect on α_i. And $\mathrm{Aut}(F_i/F)$ acts transitively on X_i by the extension theorem. Hence $J_i/H_i \simeq \mathrm{Aut}(F_i/F)$ acts freely and transitively on X_i, so the action of J_i/H_i on X_i is isomorphic to the left regular representation of J_i/H_i. For any group, the centralizer of the left regular representation is the right regular representation. Hence Z_i is the image of the right regular representation of J_i/H_i, so $Z_i \simeq J_i/H_i$. We conclude that $C_{S_X}(G) \simeq \mathrm{Aut}(F_i/F)$ for all $1 \leq i \leq m$. ■

3.9.2 The Primitive Element Theorem

We have seen, in the example $\mathbb{Q}(1^{1/3}, 2^{1/3}) = \mathbb{Q}(1^{1/3} + 2^{1/3})$ that a field given by two generators may be generated by a single element. We saw this also with finite fields, whose multiplicative groups are cyclic. Galois used this result heavily (see next section) so we will prove it now.

Theorem 3.31 (Primitive Element Theorem) *Let E/F be a finite separable extension. Then there exists $\gamma \in E$ such that $E = F(\gamma)$.*

Proof: (From Milne [FG].) Since we know the result when F is finite, assume F is infinite. We may also assume by induction that $E = F(\alpha, \beta)$. We will find an element $c \in F$ such that $E = F(\alpha + c\beta)$. Let f, g be the minimal polynomials of α, β over F. Since E/F is separable, these have distinct roots, $\alpha = \alpha_1, \ldots, \alpha_s$ and $\beta = \beta_1, \ldots, \beta_t$ in some field $L \supset E$. Since F is infinite, there exists $c \in F$ such that

$$c \neq \frac{\alpha_i - \alpha}{\beta - \beta_j}$$

for all $j \neq 1$. We set $\gamma = \alpha + c\beta$, and claim that $F(\alpha, \beta) = F(\gamma)$. The polynomials $g(x)$ and $f(\gamma - cx)$ have coefficients in $F(\gamma)$. Our choice of c ensures that they have only one root in common, namely β. Hence the ideal they generate in $F(\gamma)[x]$ is generated by a polynomial h with coefficients in $F(\gamma)$ having β as its unique root. Hence h splits in $F(\gamma)[x]$ and $\beta \in F(\gamma)$. And then $\alpha = \gamma - c\beta \in F(\gamma)$ as well, so $F(\alpha, \beta) = F(\gamma)$. ■

Example: Let $E \subset \mathbb{C}$ be the splitting field over $\mathbb{Q}$ of $x^3 - 2$. We know that $E = \mathbb{Q}(\alpha, \zeta)$, where α is the real root of $x^3 - 2$ and $\zeta = e^{2\pi i/3}$. I claim that

$$E = \mathbb{Q}(\alpha + \zeta).$$

This follows from the proof above, once we check that none of

$$\alpha - \alpha, \qquad \alpha\zeta - \alpha, \qquad \alpha\zeta^2 - \alpha$$

are equal to $\zeta - \zeta^2$. The minimal polynomial of $\alpha + \zeta$ is

$$f = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9,$$

whose discriminant is $-2^4 \cdot 3^{17}$.

3.9.3 Galois' view of Galois groups

Speaking from the grave, Galois introduced mankind to Galois groups with the following statement. [10]

> *THÉORÈME. - Soit une équation donnée, dont a,b,c,... sont les m racines. Il y aura toujours un groupe de permutations des lettres a,b,c,... qui jouira de la propriété suivante:*
>
> 1^o *Que toute fonction des racines, invariable par les substitutions de ce groupe, soit rationnellement connue;*
>
> 2^o *Réciproquement, que toute fonction des racines, déterminable rationnellement, soit invariable par les substitutions.*

Here is a literal translation:

> *THEOREM.- Let an equation be given, where $a, b, c, \ldots$ are the m roots. There will always be a group of permutations of the letters $a, b, c, \ldots$ which will enjoy the following property:*
>
> 1. *That any function of the roots, invariant by the substitutions of this group, be rationally known;*
> 2. *Conversely, that any function of the roots, rationally determinable, be invariant by the substitutions.*

In a footnote, Galois clarifies that by "invariant by the substitutions" he means the values of a function at the roots are invariant, not just the function itself. And "rationally known" means the values are expressible in terms of the coefficients of the given equation, along with some "adjoined quantities" (I'm not sure what Galois means by the latter).

Here is a mathematical translation. We are given an equation $f(x) = 0$, where $f \in F[x]$ is a polynomial, and $\alpha_1, \ldots, \alpha_m$ are the m roots of this equation in some splitting field E. Let $R = F[x_1, \ldots, x_m]$ be the ring of polynomials in variables $x_1, \ldots, x_m$. For $r \in R$, write $r(\alpha) = r(\alpha_1, \ldots, \alpha_m)$ for the value of r at the roots, so that $E = \{r(\alpha) : \ r \in R\}$. These values $r(\alpha)$ are Galois' "functions of

[10] "Mémoire sur les conditions de résolubilité des équations par radicaux", published in 1846. Galois died in 1832. Note that he uses the future tense.

the roots", and to be "rationally known" means that $r(\alpha) \in F$. Recall the group S_m acts on R by $(\sigma, r) \mapsto {}^{\sigma}r$, where

$$ {}^{\sigma}r(x_1, \ldots, x_m) = r(x_{\sigma 1}, \ldots, x_{\sigma m}). $$

With this notation, Galois' theorem becomes

Theorem 3.32 *There is a subgroup $G \leq S_m$ characterized by the following property:*

$$ [{}^{\sigma}r(\alpha) = r(\alpha) \text{ for all } \sigma \in G] \Leftrightarrow r(\alpha) \in F. \tag{20} $$

Let us first verify that our Galois group $G_f = \mathrm{Aut}(E/F)$, viewed as subgroup of S_m via its action on the roots $\{\alpha_i\}$, is the same as Galois' Galois group G.

If $\sigma \in G_f$ then for all $r \in R$ we have $\sigma(r(\alpha)) = r(\sigma(\alpha)) = {}^{\sigma}r(\alpha)$. Since $E^{G_f} = F$, we have $r(\alpha) \in F$ iff ${}^{\sigma}r(\alpha) = r(\alpha)$ for all $\sigma \in G_f$. Hence the elements of G_f satisfy the property (20), so we have $G_f \leq G$.

For the other containment, let $I_\alpha = \{r \in R : \ r(\alpha) = 0\}$ be the kernel of the ring homomorphism $R \to E$, sending $r \mapsto r(\alpha)$. This gives an isomorphism $R/I_\alpha \simeq E$. Suppose now that $\sigma \in G$. For all $r \in I_\alpha$ we have $r(\alpha) = 0 \in F$, so ${}^{\sigma}r(\alpha) = r(\alpha) = 0$. Thus, G preserves I_α and we get a homomorphism $G \to \mathrm{Aut}(R/I_\alpha) \simeq \mathrm{Aut}(E)$. Since S_m acts trivially on $F \subset R$, the image of this homomorphism lies in $\mathrm{Aut}(E/F) = G_f$. Finally the homomorphism is injective because G acts faithfully on the roots $\{\alpha_i\}$. Thus we have an injection $G \hookrightarrow G_f$, so $G = G_f$. ■

We now give Galois' proof of his theorem, using the language of Thm. 3.32, and filling in the details.

The first step is to construct the permutation group G. Let E be a field containing the roots $\alpha_1, \ldots, \alpha_m$ of f. By the Primitive Element Theorem 3.31, [11] there exists γ in E such that $E = F(\gamma)$. Hence there are polynomials $h_1, \ldots, h_m \in F[x]$ such that

$$ \alpha_i = h_i(\gamma), \qquad 1 \leq i \leq m. $$

Let $g \in F[x]$ be the minimal polynomial of γ over F and let $\gamma = \gamma_1, \ldots, \gamma_n$ be the roots of g, where $n = \deg g = [E : F]$. Galois proves [12] that for any i, j the value $h_i(\gamma_j)$ is also a root of f. To see this, note that for any i we have $f(h_i(\gamma)) = f(\alpha_i) = 0$, so the polynomial $f \circ h_i$ is divisible by the minimal polynomial g of γ, so $f(h_i(\gamma_j)) = 0$ for all j. It follows that for each i, j we have

$$ h_i(\gamma_j) = \sigma_j \alpha_i \tag{21} $$

for some permutation σ_j of $\{\alpha_1, \ldots, \alpha_m\}$. The group G is then

$$ G = \{\sigma_j : \ 1 \leq j \leq n\}. $$

[11] In Lemme II of [op. cit.] Galois states the Primitive Element Theorem without proof but he is careful to assume f is separable, and he remarks that we may take γ to be an F-linear combination of the α_i's, as we see from the proof of Thm. 3.31.

[12] See Lemme IV of op. cit.

We now prove that if $\sigma_j \in G$ and $r \in F[x_1, \ldots, x_m]$ satisfies ${}^{\sigma_j} r(\alpha) = r(\alpha)$, then $r(\alpha) \in F$. Let $r_h \in F[x]$ be the polynomial $r_h(x) = r(h_1(x), h_2(x), \ldots, h_m(x))$. Then $r_h(\gamma) = r(\alpha)$ and the equations (21) become

$$r_h(\gamma_j) = r_h(\gamma), \qquad 1 \leq j \leq n.$$

These equations imply that $r(\alpha) \in F$. To see this, note that the polynomial

$$(x - r(\alpha))^n = \prod_{j=1}^{n} (x - r_h(\gamma_j)) \tag{22}$$

has coefficients given in terms of the elementary symmetric polynomials: $s_k(r_h(\gamma_1), \ldots, r_h(\gamma_n))$. But the polynomials $s_k(r_h(x_1), \ldots, r_h(x_n))$ are themselves symmetric, hence they lie in $F[s_1, \ldots, s_n]$, by the Symmetric Polynomial Theorem. And the values $s_k(\gamma_1, \ldots, \gamma_n)$ are the coefficients of $g(x)$, hence they lie in F, so $s_k(r_h(\gamma_1), \ldots, r_h(\gamma_n)) \in F$ for each k. Now differentiating $(x - r(\alpha))^n$, we get $r(\alpha) \in F$, as claimed.

Conversely, if $r(\alpha) \in F$, then the polynomial $r_h - r(\alpha)$ belongs to $F[x]$. Since $r_h(\gamma) = r(\alpha)$, it follows that $r_h - r(\alpha)$ is divisible by the minimal polynomial g of γ. Hence each γ_j is a root of $r_h - r(\alpha)$, so for each j we have ${}^{\sigma}_{j} r(\alpha) = r_h(\gamma_j) = r(\alpha)$. ■

4 Computing Galois groups of polynomials

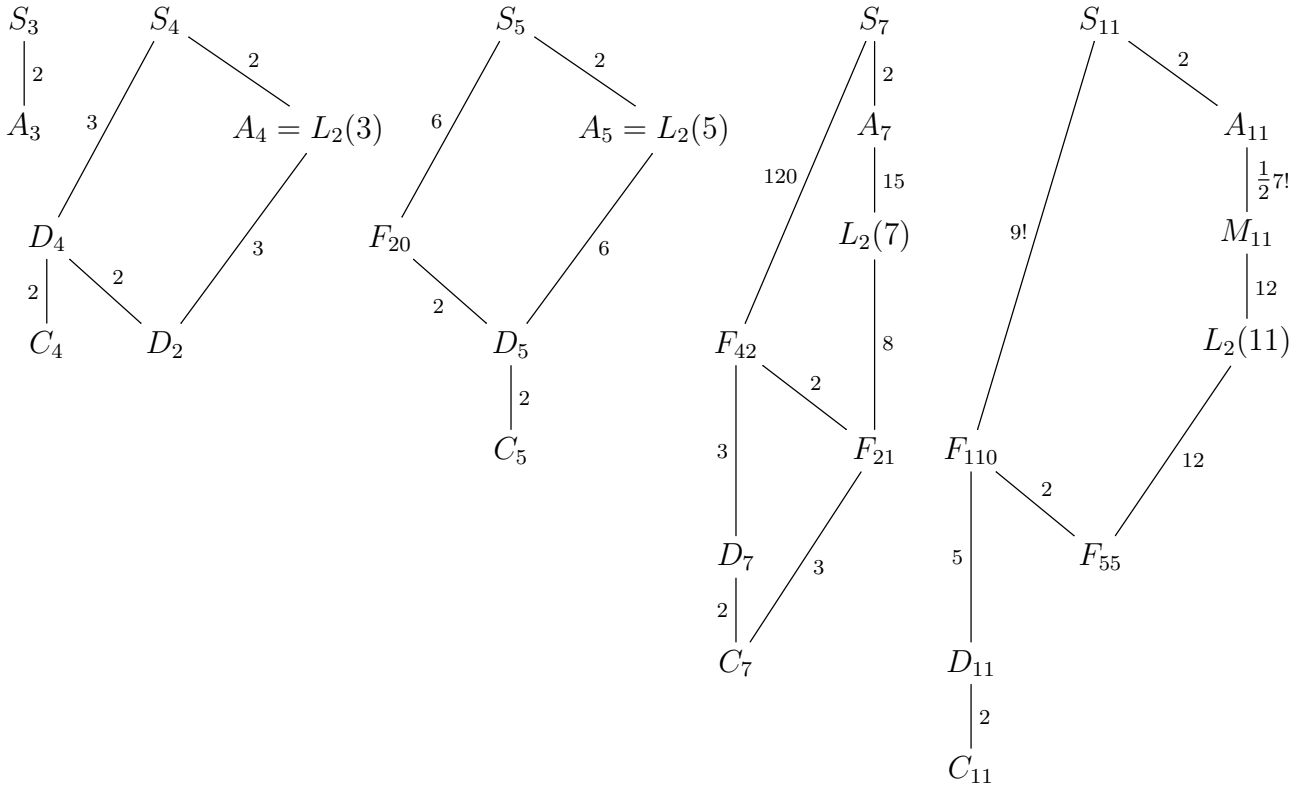
Let F be a field, and let $f \in F[x]$ be a separable irreducible polynomial of degree n, with splitting field $E = F(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n$ are the roots of F in E. What can we say about the Galois group G_f? [13]

4.1 Transitive subgroups

Since f is irreducible, G_f is a transitive subgroup of S_n, via its permutations of the roots α_i. The lattices of transitive subgroups of S_n for some small values of n are as follows. [14]

[13] For tables of number fields of small degree, see http://hobbes.la.asu.edu/courses/low-grd/

[14] For more group tables, see http://math.asu.edu/ jj/Groups/.

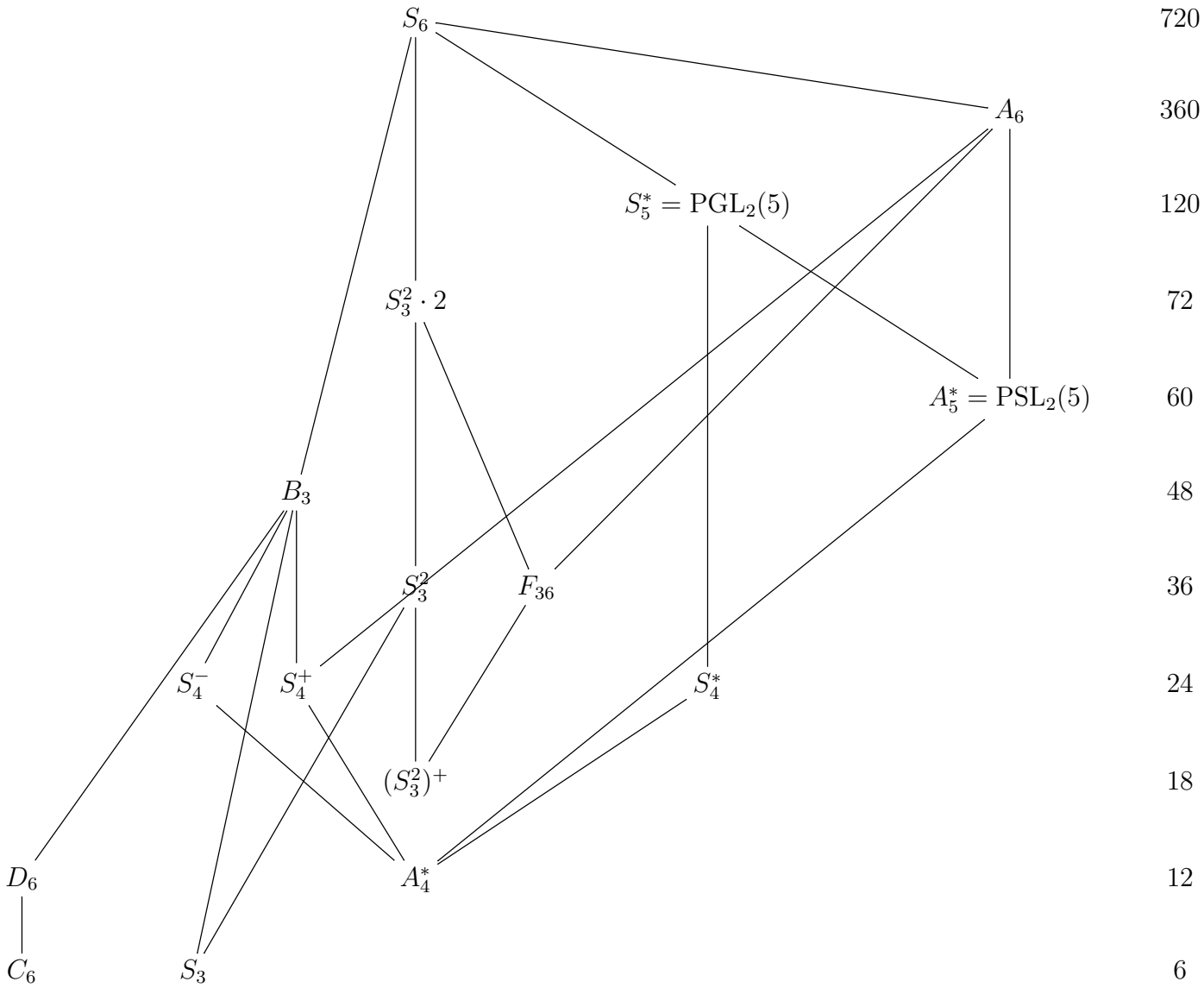


Here the groups S_n, A_n, D_n, C_n are as usual the symmetric, alternating, dihedral (of order $2n$) and cyclic groups. The other groups are as follows.

$L_2(p) = \mathrm{PSL}_2(p)$ acting via its exceptional permutation representation of degree p. These were discovered by Galois, who noted they only exist for $p = 3, 5, 7, 11$.

$F_{p(p-1)} = \mathbb{F}_p \rtimes \mathbb{F}_p^\times$ is the $ax + b$ group over $\mathbb{F}_p$, which has subgroups $F_{ph} = \mathbb{F}_p \rtimes H$, for each divisor $h \mid (p-1)$, where $H \leq \mathbb{F}_p^\times$ is the unique subgroup of order h.

M_{11} is the Mathieu group of order $8 \cdot 9 \cdot 10 \cdot 11 = 7920$, the smallest simple sporadic group.



4.2 Invariant Theory and Resolvents

Let F be a field, and recall that the symmetric group S_n acts on the ring $R = F[t_1, \ldots, t_n]$ by ${}^\sigma r(t_1, \ldots, t_n) = r(t_{\sigma 1}, \ldots, t_{\sigma n})$, and that the symmetric polynomials $R^{S_n} = \{r \in R : {}^\sigma r = r\}$

$$R^{S_n} = F[s_1, \ldots, s_n],$$

where $s_k(t_1, \ldots, t_n) = \sum t_{i_1} \ldots t_{i_k}$, summed over all $1 \leq i_1 < \cdots < i_k \leq n$, is the elementary symmetric polynomial of degree k.

4.2.1 The discriminant

From now on we assume that $\mathrm{char}(F) \neq 2$. The polynomial $d \in R = F[t_1, \ldots, t_n]$ given by

$$d = \prod_{i<j} t_i - t_j,$$

has square equal to the discriminant polynomial

$$D = d^2 \in R^{S_n}.$$

For all $\sigma \in S_n$ we have

$$^{\sigma}d = \mathrm{sgn}(\sigma) \cdot d,$$

so $d \in R^{A_n}$ is invariant under the alternating group A_n.

Let $f \in F[x]$ be a polynomial of degree n, with distinct roots $\alpha_1, \ldots, \alpha_n$. Then

$$f = \sum_{k=0}^{n} (-1)^k s_k(\alpha) x^{n-k},$$

so the values $s_k(\alpha)$ lie in F. Since $D \in R^{S_n}$ is a polynomial in the s_k's, its value $D(\alpha)$ is that same polynomial evaluated at the coefficients of f, which are known. We write this value as

$$D_f = D(\alpha) = d(\alpha)^2 = \prod_{i<j} (\alpha_i - \alpha_j)^2 \in F.$$

Since f has distinct roots, we have $D_f \neq 0$.

The Galois group of G_f is a subgroup of S_n via its permutations of the roots, so we can ask when $G_f \leq A_n$. The answer is as follows.

Proposition 4.1 *We have $G_f \leq A_n$ if and only if $D_f \in F^{\times 2}$ is a nonzero square in F.*

Proof: If $G_f \leq A_n$ then d is invariant under G_f so we have $\sigma(d(\alpha)) = {}^{\sigma}d(\alpha) = d(\alpha)$ for all $\sigma \in G_f$. Hence $d(\alpha) \in F^{\times}$ so $D_f = d(\alpha)^2 \in F^{\times 2}$. Conversely, if $D_f \in F^{\times 2}$ then reversing the previous argument shows that $d(\alpha) = {}^{\sigma}d(\alpha) = \mathrm{sgn}(\sigma) \cdot d(\alpha)$ for all $\sigma \in G_f$. Since $d(\alpha) \neq 0$, this implies $G_f \leq A_n$. ■

The explicit formula for D_f in terms of the coefficients of f is complicated, as we have seen in section 3.1. You can call it up in Mathematica by the command `Discriminant[`$poly, x$`]`. One can simplify the formulas for D_f (at least if the characteristic of k does not divide n) by replacing $f(x) = x^n + ax^{n-1} + \ldots$ by $f(x - a/n) = x^n + 0x^{n-1} + \ldots$, which does not change G_f. Thus, we have the formulas

$$\begin{array}{ll}
f = x^3 + bx + c: & D_f = -4b^3 - 27c^2 \\
f = x^4 + bx^2 + cx + d: & D_f = -4b^3c^2 - 27c^4 + 16b^4d + 144bc^2d - 128b^2d^2 + 256d^3 \\
f = x^5 + bx^3 + e: & D_f = 2^2 3^3 b^5 e^2 + 5^5 e^4 \\
f = x^5 + cx^2 + e: & D_f = 2^2 3^3 c^5 e + 5^5 e^4 \\
f = x^5 + dx + e: & D_f = 4^4 d^5 + 5^5 e^4
\end{array}$$

It can be shown that $f = x^n + rx + s$ has discriminant

$$D_f = a_n s^{n-1} + a_{n-1} r^n, \qquad a_n = (-1)^{n(n-1)/2} n^n.$$

Invariant theory is the study of polynomials invariant under an action of a group G on a polynomial ring $R = F[t_1, \ldots, t_n]$. These invariants form a subring

$$R^G := \{r \in R : {}^g r = r\} \subset R.$$

For example, we have seen that when $G = S_n$ acts on R by ${}^\sigma r(t_1, \ldots, t_n) = r(t_{\sigma 1}, \ldots, t_{\sigma n})$, the invariants Now let $G = G_f$ be the Galois group of our polynomial f, viewed as a subgroup of S_n by permuting the roots $\alpha_1, \ldots, \alpha_n$ of f in a splitting field E. For $r \in R$, we abbreviate

$$r(\alpha) = r(\alpha_1, \ldots, \alpha_n) \in E.$$

One can use Invariant theory to move down the lattice of transitive subgroups as follows. Suppose that we have subgroups $H \leq J \subset S_n$ and that $G_f \subset J$. [15] We want to decide if G_f is contained in some conjugate of H. For subgroups B, C of a group A, let us write $B \leq_A C$ if there exists $a \in A$ such that $B \leq C^a$. So we want to decide if $G_f \leq_J H$.

Let $r \in R$ be a polynomial whose stabilizer in J is H:

$$H = \{\sigma \in J : {}^\sigma r = r\}.$$

The data $\{J, H, r\}$ combine to give a **resolvent** polynomial:

$$\mathrm{Res}_{J/H}(t, x) = \prod_{\sigma \in J/H} (x - {}^\sigma r) \in R^J[x].$$

Note that $\mathrm{Res}_{J/H}(t, x)$ is a polynomial in x whose coefficients in R are polynomials in $t_1, \ldots, t_n$. It makes sense to take the product over the cosets J/H because H fixes r, and since J permutes the cosets, the coefficients of $\mathrm{Res}_{J/H}(t, x)$ in fact lie in R^J, as claimed.

If we now specialize $t \mapsto \alpha$, we get a polynomial

$$\mathrm{Res}_{J/H}(\alpha, x) = \prod_{\sigma \in J/H} (x - {}^\sigma r(\alpha)) \in F[x].$$

At first glance it may seem only that $\mathrm{Res}_{J/H} \in E[x]$. However, if $c(t) \in R^J$ is some coefficient of $\mathrm{Res}_{J/H}(t, x)$, then since $G_f \leq J$ we have $\tau(c(\alpha)) = {}^\tau c(\alpha) = c(\alpha)$ for all $\tau \in G_f$, so in fact $c(\alpha) \in F$ and $\mathrm{Res}_{J/H}(\alpha, x)$ lies in $F[x]$ as claimed.

The polynomial $\mathrm{Res}_{J/H}(\alpha, x)$ contains the following information about G_f.

Proposition 4.2 *If $G_f \leq_J H$ then $\mathrm{Res}_{J/H}(\alpha, x)$ has a root in F. And if $\mathrm{Res}_{J/H}(\alpha, x)$ has a* simple *root in F, then $G_f \leq_J H$.*

[15] For example, we could have $J = S_n$, or perhaps $J < S_n$ and by previous work we have found that $G_f \leq J$.

Proof: Suppose $G_f \leq \sigma H \sigma^{-1}$ for some $\sigma \in J$. We know that ${}^{\sigma}r(\alpha)$ is a root of $\mathrm{Res}_{J/H}(\alpha, x)$, and for all $\tau \in G_f$ we have

$$\tau({}^{\sigma}r(\alpha)) = {}^{\tau\sigma}r(\alpha) = {}^{\sigma\cdot\sigma^{-1}\tau\sigma}r(\alpha) == {}^{\sigma}r(\alpha),$$

since $\sigma^{-1}\tau\sigma \in H$ fixes r.

Conversely, if $\mathrm{Res}_{J/H}(\alpha, x)$ has a simple root in F, then this root is ${}^{\sigma}r(\alpha)$ for some $\sigma \in J$. Now for all $\tau \in G_f$ we have

$${}^{\sigma}r(\alpha) = \tau({}^{\sigma}r(\alpha)) = {}^{\tau\sigma}r(\alpha).$$

Since the root is simple, we must have ${}^{\sigma}r = {}^{\tau\sigma}r$, so $\sigma^{-1}\tau\sigma$ fixes r. Since $\tau \in G_f$ was arbitrary, this means $\sigma^{-1}G_f\sigma \leq H$, or $G_f \leq \sigma H \sigma^{-1}$, as claimed. ■

4.2.2 Cubic Polynomials

Recall our assumption that $\mathrm{char}(F) \neq 2$ Let $f = x^3 + ax^2 + bx + c$ be an irreducible cubic polynomial over F with distinct roots α, β, γ generating a splitting field E. The discriminant

$$D_f = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2 \in F^{\times}.$$

If $D_f \in F^{\times 2}$ then $G_f = A_3$ has no proper subgroups. Hence there are no proper intermediate fields, we have $F(\alpha) = F(\beta) = F(\gamma)$. This means that each root is a polynomial expression in the others.

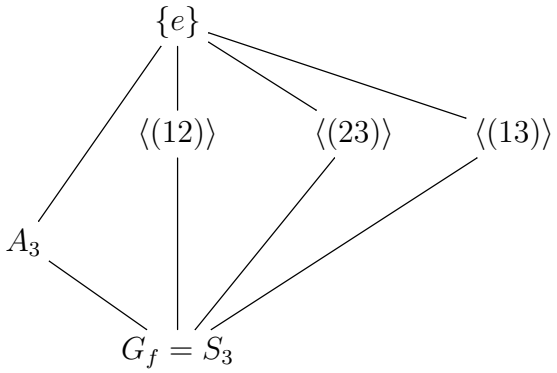
Example 1: Let $F = \mathbb{Q}$. The polynomial $f = x^3 + x^2 - 2x - 1 \in \mathbb{Q}[x]$ has $D_f = 49$ and roots

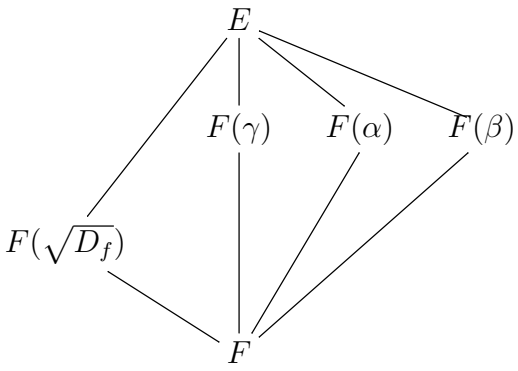
$$\alpha = 2\cos(2\pi/7), \quad 2\cos(4\pi/7), \quad 2\cos(6\pi/7),$$

satisfying the relations $\beta = \alpha^2 - 2,\ \gamma = -\alpha^2 - \alpha + 1$.

Example 2: [16] The polynomial $f(x) = x^3 - tx^2 + (t-3)x + 1 \in \mathbb{Q}(t)[x]$ has discriminant $D_f = (t^2 - 3t + 9)^2$, hence has Galois group A_3 over $\mathbb{Q}(t)$. Specializing t to any value in $\mathbb{Q}$ such that $t^2 - 3t + 9 \neq 0$, we get a cubic in $\mathbb{Q}[x]$ with Galois group A_3 over $\mathbb{Q}$.

If $f \in F[x]$ has $D_f \in F^{\times} - F^{\times 2}$ then $G_f = S_3$ and the correspondence between subgroups and intermediate fields is given by





[16] Serre, "Topics in Galois Theory", p. 1

4.2.3 Quartic Polynomials

Let $f = x^4 + ax^3 + bx^2 + cx + d$ be an irreducible separable quartic polynomial over F with roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. The polynomials

$$\begin{aligned} A &= t_1t_3 + t_2t_4 \\ B &= t_1t_2 + t_3t_4 \\ C &= t_1t_4 + t_2t_3 \end{aligned} \tag{23}$$

Form an S_4-orbit in R; the stabilizer of any one of A, B, C is a D_4, while the stabilizer of all three is K_4. One checks that

$$(A-B)(B-C)(A-C) = \prod_{1 \le i < j \le 4} (t_i - t_j). \tag{24}$$

Letting

$$J = C_{S_4}((1\ 3)(2\ 4)) = Stab_{S_4}(A) \simeq D_4,$$

we get the generic resolvent

$$\mathrm{Res}_{S_4/D_4}(t, x) = (x-A)(x-B)(x-C) = x^3 - s_2x^2 + (s_3s_1 - 4s4)x + (4s_4s_2 - s_4s_1^2 - s_3^2).$$

This specializes to the **cubic resolvent**

$$g = \mathrm{Res}_{S_4/J}(\alpha, x) = x^3 - bx^2 + (ac - 4d)x + (4bd - a^2d - c^2),$$

whose roots are

$$\begin{aligned} \alpha &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \beta &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \gamma &= \alpha_1\alpha_4 + \alpha_2\alpha_3. \end{aligned} \tag{25}$$

Under this same specialization, equation (24) becomes the equality of discriminants

$$D_g = D_f. \tag{26}$$

In particular, since f has distinct roots, so does g. Let $L = F(\alpha, \beta, \gamma)$ be the splitting field of g in E. Then L is Galois over F so $L = E^H$ for some normal subgroup $H \triangleleft G_f$, and there is an exact sequence

$$1 \longrightarrow \underset{\mathrm{Aut}(E/L)}{H} \longrightarrow \underset{\mathrm{Aut}(G_f/F)}{G_f} \longrightarrow \underset{\mathrm{Aut}(L/F)}{G_f/H} \longrightarrow 1. \tag{27}$$

Since K_4 fixes the polynomials A, B, C, it fixes their specializations α, β, γ, so we have $K_4 \le H$.

We again assume $\mathrm{char}(F) \neq 2$.

Case 1: $D_f \notin F^{\times 2}$ and g has no root in F. Then G_f is not contained in A_4 or D_4, so we must have $G_f = S_4$. The exact sequence (27) becomes

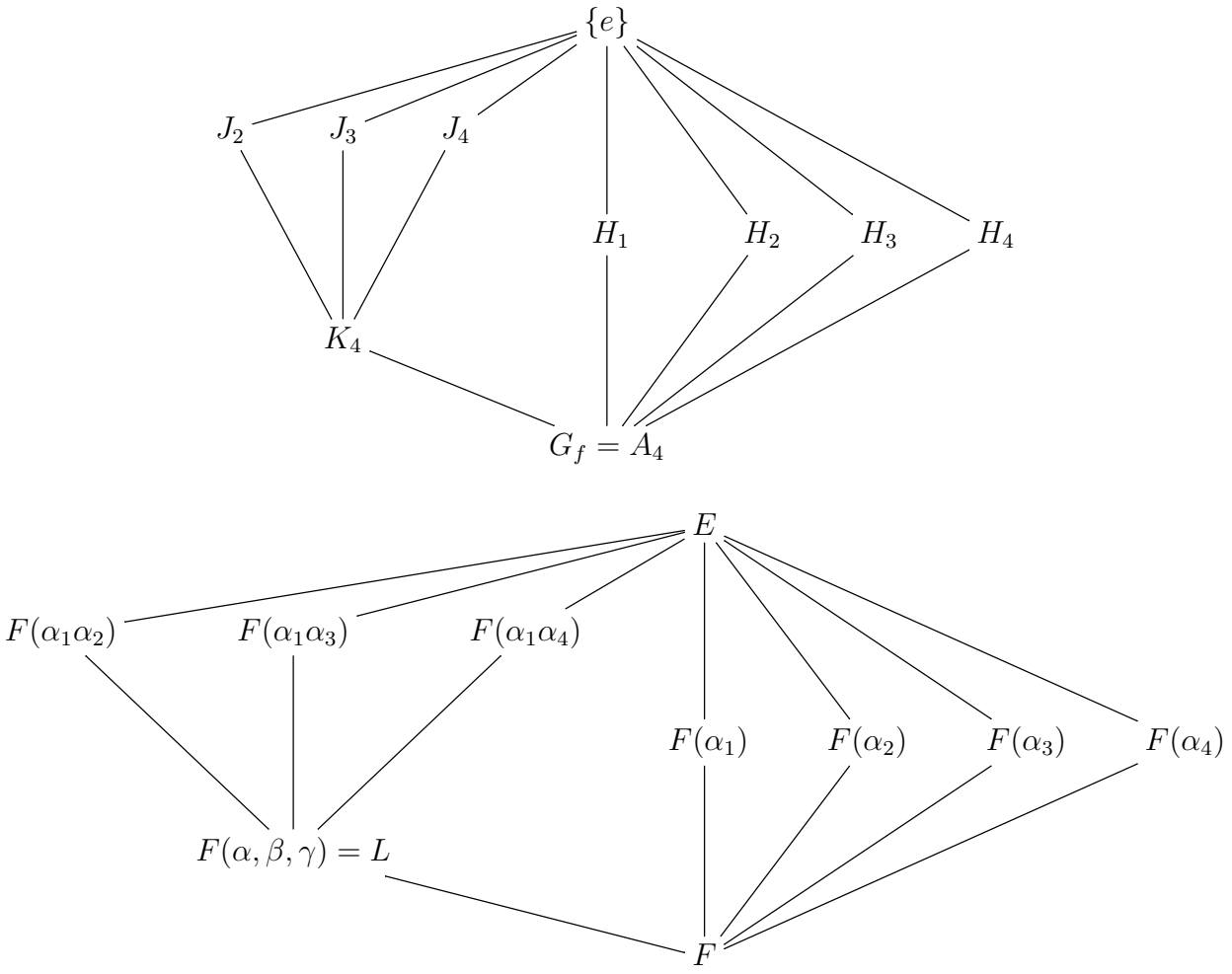
$$1 \longrightarrow K_4 \longrightarrow S_4 \longrightarrow S_3 \longrightarrow 1.$$

Since most polynomials do not have rational roots, almost all quartics f have $G_f = S_4$.

Case 2: $D_f \in F^{\times 2}$ and g has no root in F. Then G_f is contained in A_4 but not in D_4, so we must have $G_f = A_4$. Since $D_g = D_f \in F^{\times 2}$, the extension L/F has degree three with Galois group A_3. The exact sequence (27) becomes

$$1 \longrightarrow K_4 \longrightarrow A_4 \longrightarrow A_3 \longrightarrow 1.$$

Let $H_i \simeq C_3$ be the stabilizer of α_i in G_f, and let $J_i = \langle (1\ i)(jk) \rangle$ be the stabilizer of the root $\alpha_1\alpha_i$ of the irreducible quadratic equation $x^2 - (\alpha_1\alpha_i + \alpha_j\alpha_k)x + d$ over L. The correspondence between subgroups and intermediate fields is given by



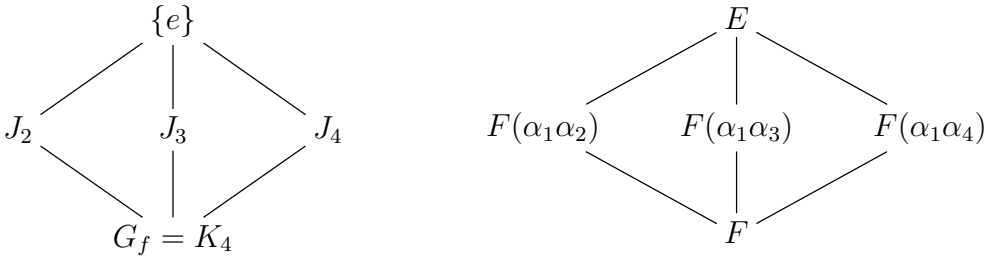
Examples of quartics $f \in \mathbb{Q}[x]$ with $G_f = A_4$ include:

quartic f	discriminant D_f	resolvent cubic g
$x^4 + 8x + 12$	$2^{12} \cdot 3^4$	$x^3 - 48x - 64$
$x^4 + 9x^2 + 13x + 30$	$3^6 \cdot 7^2 \cdot 13^2$	$x^3 - 9x^2 - 120x + 911$
$x^4 + 18x^2 - 4x + 82$	$2^8 \cdot 109^2$	$x^3 - 18x^2 - 328x + 5888$

Case 3: $D_f \in F^{\times 2}$ and g has a root in F. Then $G_f \leq A_4 \cap D_4 = K_4$ acts trivially on $\{\alpha, \beta, \gamma\}$ so g splits over F. The exact sequence (27) becomes

$$1 \longrightarrow K_4 \longrightarrow K_4 \longrightarrow 1 \longrightarrow 1.$$

Since $[E : F] = 4$, each root α_i generates E over F. Since $\alpha = \alpha_1\alpha_3 + \alpha_2\alpha_4 \in F$ the polynomial $x^2 - \alpha x + d$ lies in $F[x]$ and has roots $\alpha_1\alpha_3,\ \alpha_2\alpha_4$ in E. Similarly for β and γ. Hence for $i = 2, 3, 4$ we have subfields $F(\alpha_1\alpha_i) \subset E$ quadratic over F. The correspondence between subgroups and intermediate fields is given by



Examples of quartics $f \in \mathbb{Q}[x]$ with $G_f = K_4$ include:

quartic f	discriminant D_f	resolvent cubic g
$x^4 + 1$	4^4	$x(x^2 - 4)$
$x^4 + x^2 + 1$	$2^4 \cdot 3^2$	$(x - 1)(x^2 - 4)$
$x^4 - 10x^2 + 1$	$2^{14} \cdot 3^2$	$(x + 10)(x^2 - 4)$.

These are the minimal polynomials of $e^{\pi i/4},\ e^{\pi i/6},\ \sqrt{2} + \sqrt{3}$, respectively.

Case 3: If $D_f \notin F^{\times 2}$ and g has a root in F then either $G_f = D_4$ or $G_f = C_4$.

The next proposition addresses this ambiguity.

Proposition 4.3 *Assume that $D_f \notin F^{\times 2}$ and the cubic resolvent g has a root $\alpha \in F$. Then*

1. *$G_f \simeq C_4$ if and only if f is reducible over the subfield $M = F(\sqrt{D_f})$.*
2. *α is the unique root of g in F.*
3. *$G_f \simeq C_4$ if and only if $\alpha^2 - 4d$ and $a^2 + 4(\alpha - b)$ are both squares in M.* [17]

Proof: We have $g = (x - \alpha)h(x)$, where $h(x) \in F[x]$. Let β, γ be the roots of h. Then $h(x) = x^2 - (\beta + \gamma)x + \gamma\beta$, so $\beta + \gamma$ and $\beta\gamma$ lie in F. Since

$$D_f = D_g = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 = h(\alpha)^2(\beta - \gamma)^2 \notin F^{\times 2},$$

we cannot have $\beta - \gamma \in F$, so α is the unique root of g in F. From this we also see that $\beta, \gamma \in M$, so M is the splitting field of g over F.

[17] L.C. Kappe, B. Warren, Amer. Math. Monthly 1989

Under the Galois correspondence, we have $M = E^{G\cap A_4} \lhd G$, and $G \cap A_4 = \mathrm{Aut}(E/M)$ Since $G \leq D_4$ we have

$$G \cap A_4 = G \cap K_4 = \begin{cases} K_4 & \text{if } G \simeq D_4 \\ \langle \tau^2 \rangle & \text{if } G = \langle \tau \rangle \simeq C_4. \end{cases}$$

Now f is irreducible in $M[x]$ iff $G \cap A_4 = \mathrm{Aut}(E/M)$ is transitive on the roots of f, which happens exactly when $G \simeq D_4$. Otherwise, if f is reducible in $M[x]$ then $G \cap A_4$ cannot be transitive on the roots of f, which happens exactly when $G \simeq C_4$.

The last assertion is equivalent to the polynomial

$$h(x) = (x^2 - \alpha x + d)(x^2 + ax + b - \alpha) \tag{28}$$

splitting in M. We may number the roots of f as $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ of f so that $\alpha = \alpha_1\alpha_3 + \alpha_2\alpha_4$. In this labelling $G \leq C_{S_4}((1\,3)(2\,4)) \simeq D_4$. The two factors of h have roots $\alpha_1\alpha_3,\ \alpha_2\alpha_4$ and $\alpha_1+\alpha_3,\ \alpha_2+\alpha_4$, respectively, so h splits in E.

If $G \simeq C_4$ then E/F contains only one quadratic subfield, namely M. Hence every quadratic polynomial splitting in E must split in M, so h splits in M.

Conversely, suppose h splits in M. Then $\alpha_1\alpha_3,\ \alpha_2\alpha_4,\ \alpha_1 + \alpha_3,\ \alpha_2 + \alpha_4 \in M$, so the polynomial

$$k(x) := (x^2 - (\alpha_1 + \alpha_3)x + \alpha_1\alpha_3 = (x - \alpha_1)(x - \alpha_3) \in M[x].$$

Let L be the splitting field of k over M. Then $\alpha_1, \alpha_3 \in L$ and also $\alpha, \beta, \gamma \in M \subset L$, since g splits in M. Hence $\alpha_2 + \alpha_4 = -a - (\alpha_1 + \alpha_3) \in L$.

One checks that $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_4)$ is invariant under $C_{S_4}((1\,3)(1\,4))$, hence under G, so it lies in $F^\times$. From $D_f = D_g$ we get

$$(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4) \in F^\times \cdot (\beta - \gamma).$$

Since $\alpha_1, \alpha_3, \beta, \gamma \in L$ it follows that $\alpha_2 - \alpha_4 \in L$.

We have now shown that $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in L$, so $L = E$. Since $\deg k = 2$, this shows that $[E : M] \leq 2$, so $[E : F] \leq 4$ and $G = \langle (1\,2\,3\,4) \rangle \simeq C_4$. ■

One can also approach this using resolvents. Let $J = C_{S_4}((1\,3)(1\,4))$ and let $H \leq J$ be the subgroup

$$H = \langle (1\,2\,3\,4) \rangle = Stab_J(t_1t_2^2 + t_2t_3^2 + t_3t_4^2 + t_4t_1^2) \simeq C_4.$$

The D_4/C_4-resolvent is

$$\mathrm{Res}_{D_4/C_4}(t, x) = [x - (t_1t_2^2 + t_2t_3^2 + t_3t_4^2 + t_4t_1^2)][x - (t_1^2t_2 + t_2^2t_3 + t_3^2t_4 + t_4^2t_1] \in R^J[x],$$

which specializes to the **quadratic resolvent** [18]

$$\begin{aligned} q(x) =& x^2 - (2c - ab + a\alpha)x + \tfrac{1}{2}\left(a^2d - 4bd + 2b^3 + 2a^3c - 10abc + 11c^2\right) \\ &+ \left(ac - 2a^2b + 2b^2 + 4d\right)\alpha + \left(2a^2 - b\right)\alpha^2 - 3\alpha^3, \end{aligned} \tag{29}$$

whose roots are

$$\begin{aligned} \eta &= \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_4^2 + \alpha_4\alpha_1^2 \\ \xi &= \alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_4 + \alpha_4^2\alpha_1. \end{aligned} \tag{30}$$

and whose discriminant $D_q = (\eta - \xi)^2$ is given rationally by

$$D_q = a^2b^2 - 4b^3 + 2a^2b\alpha - 4b^2\alpha - 3a^2\alpha^2 + 2b\alpha^2 + 6\alpha^3 - 4a^3c + 16abc + 2a\alpha c - 18c^2 - 2a^2d + 8bd - 8\alpha d.$$

Assume $D_q \neq 0$. Then we have $G \leq C_4$ iff $D_q \in F^{\times 2}$, by Prop. 4.2. Unfortunately, D_q is often zero, meaning that the quadratic resolvent has one root of multiplicity two, so Prop. 4.2 does not apply in these cases. However, when $D_q \neq 0$ its square-class gives independent confirmation of the decision of whether $G_f \leq C_4$.

Examples of quartics $f \in \mathbb{Q}[x]$ with $G_f = D_4$ include:

quartic f	discriminant D_f	resolvent cubic g	D_q
$x^4 + 4x + 2$	2^{11}	$(x-4)(x^2-8)$	0
$x^4 + d$ $(d \neq \square)$	$4^4 \cdot d^3$	$x(x^2 - 4d)$	0
$x^4 + ax^3 + (b-2)x^2 + ax + 1$	$(a^2 - 4b + 16)^2(b^2 - 4a^2)$	$(x-2)(x^2 + (4-b)x + a^2 - 2b + 4)$	D_f

In the last line we assume $b^2 - 4a^2 \neq \square$.

Examples of quartics $f \in \mathbb{Q}[x]$ with $G_f = C_4$ include:

quartic f	discriminant D_f	resolvent cubic g	D_q
$x^4 + x^3 + x^2 + x + 1$	5^3	$(x-2)(x^2 + x - 1)$	5^2
$x^4 + x^3 + 2x^2 - 4x + 3$	$3^2 \cdot 13^3$	$(x-5)(x^2 + 3x - 1)$	13^2
$x^4 + x^3 - 6x^2 - x + 1$	$2^2 \cdot 17^3$	$(x+2)(x^2 - 4x - 12)$	$2^2 \cdot 17^2$
$x^4 + x^3 + 4x^2 + 20x + 23$	$7^2 \cdot 29^3$	$(x+2)(x^2 - 4x - 12)$	$2^2 \cdot 29^2$
$x^4 - 2ax^2 + a^2 - b^2d$ $(a^2 - b^2d = \square \cdot d \neq \square)$	$4^4 \cdot b^4d^2(a^2 - b^2d)$	$x(x^2 - 4d)$	0

The first four examples are the quartic subfields of $\mathbb{Q}(e^{2\pi i/p})$ for $p = 5, 13, 17, 29$ (see section 1.7). In the last example, $f = x^4 - 2ax^2 + a^2 - b^2d$ has splitting field $E = \mathbb{Q}(\sqrt{a + b\sqrt{d}})$. The polynomial in (28) is $(x^2 + 2ax + a^2 - b^2d) \cdot x^2$, which splits over $\mathbb{Q}(\sqrt{d})$, giving $G_f = C_4$.

[18] To compute this specialization, we have to express the two coefficients of $\mathrm{Res}_{D_4/C_4}(t, x)$ in terms of the J-invariant polynomial $T := t_1t_3 + t_2t_4$ and symmetric polynomials. The hardest coefficient is the constant term $\mathrm{Res}_{D_4/C_4}(t, 0)$. Since it has degree six, we set

$$(t_1t_2^2 + t_2t_3^2 + t_3t_4^2 + t_4t_1^2)(t_1^2t_2 + t_2^2t_3 + t_3^2t_4 + t_4^2t_1) = S_6 + S_4T + S_2T^2 + S_0T,$$

where S_k are unknown symmetric polynomials of degree k. One can use the `SymmetricReduction` command in Mathematica to find S_4, S_2, S_0 such that $T - (S_4T + S_2T^2 + S_0T)$ is symmetric, which gives S_6.

4.2.4 Constructible numbers revisited

Recall the field K of constructible numbers, from section 3.6.2. These are the numbers in $\alpha \in \mathbb{C}$ such that $\mathbb{Q}(\alpha)$ is at the top of a tower of fields

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n = \mathbb{Q}(\alpha) \tag{31}$$

such that $[F_i : F_{i-1}] = 2$ for each $1 \leq i \leq n$. As we have seen in Prop. 3.17, this implies that the minimal polynomial f_α of every element $\alpha \in K$ over $\mathbb{Q}$ has degree a power of 2. We can now see why this degree condition is not sufficient to guarantee that $\alpha \in K$.

For suppose such a tower (31) exists. Since quadratic extensions are always Galois, and Galois extensions are preserved under towers (see Prop. **??**), having $\alpha \in K$ forces $\mathbb{Q}(\alpha)$ to be Galois over $\mathbb{Q}$, and the Galois group $\mathrm{Aut}(\mathbb{Q}(\alpha))$ must be a 2-group. But if we take any irreducible quartic polynomial $f \in \mathbb{Q}[x]$ with $G_f = A_4$, then the subfields $\mathbb{Q}(\alpha_i)$ generated by the roots of f are quartic non-Galois extensions of $\mathbb{Q}$. Hence the numbers α_i are not constructible. Note that the quartic fields $\mathbb{Q}(\alpha_i)$ have no quadratic subfields, corresponding to A_4 having no subgroups of index two. Thus, the failure of the converse of Prop. 3.17 corresponds to the failure of the converse to Lagrange's theorem.

However, if $\mathbb{Q}(\alpha)/\mathbb{Q}$ is *Galois* of degree 2^n over $\mathbb{Q}$, then the Galois group $G = \mathrm{Aut}(\mathbb{Q}(\alpha))$ has order 2^n and from group theory we know there is a chain of subgroups

$$\{e\} = G_n < G_{n-1} < \cdots < G_0 = G,$$

with $|G_i| = 2^{n-i}$ for each i. The Galois correspondence then gives a tower of fields as in (31), where F_i is the fixed-field of G_i in $F_n = \mathbb{Q}(\alpha)$. Thus we have proved:

Theorem 4.4 *3.17 A number $\alpha \in \mathbb{C}$ is constructible if and only if $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$ with degree a power of 2.*

5 Galois groups and prime ideals

Let $f \in \mathbb{Z}[x]$ be a monic polynomial with Galois group G_f over $\mathbb{Q}$. For each prime p in $\mathbb{Z}$ we can reduce the coefficients of f modulo p and get a polynomial $\bar{f} \in \mathbb{F}_p[x]$. Thus we have another Galois group $G_{\bar{f}}$, this time over $\mathbb{F}_p$. The permutation group $G_{\bar{f}}$ is completely determined by the factorization of $\bar{f}$ in $\mathbb{F}_p[x]$, hence can be calculated explicitly for any given prime p. The remarkable fact is that $G_{\bar{f}}$ is a subquotient of G_f, and is even a subgroup of G_f for all but finitely many primes p. The origin of this fact is the relation between primes in $\mathbb{Z}$ and prime ideals in the ring of integers in the splitting field of f over $\mathbb{Q}$.

5.1 The ring of integers in a number field

A **number field** is a field $E \supset \mathbb{Q}$ for which E is a finite dimensional $\mathbb{Q}$-vector space. The **ring of integers** in E is the subring R of elements in E which are integral over $\mathbb{Z}$. We have seen that R is a ring. In this section we consider the structure of the additive group of R.

An abelian group A is **free of rank** n if $A \simeq \mathbb{Z}^n$. Equivalently there exists a subset $\{\alpha_1, \ldots, \alpha_n\} \subset A$, called a **basis**, which generates A and is linearly independent over $\mathbb{Z}$. We have $A \simeq \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ and every element of A can be written uniquely as a $\mathbb{Z}$-linear combination of elements of the basis $\{\alpha_1, \ldots, \alpha_n\}$. Note that for any prime p we have $A/pA \simeq (\mathbb{Z}/p\mathbb{Z})^n$, so the rank n depends only on A and not on the choice of basis.

Lemma 5.1 *Let B be a free abelian group of rank $n \geq 1$ and let A be a subgroup of B. Then A is free abelian of rank $\leq n$.*

Proof: Let $\{\beta_1, \ldots, \beta_n\}$ be a basis of B. For $1 \leq r \leq n$ we set

$$B_r = \bigoplus_{i=1}^{r} \mathbb{Z}\beta_i, \qquad A_r = A \cap B_r,$$

so that $A_n = A$. We prove by induction on r that A_r has rank $\leq r$ for all r.

At the first step, $A_1 = A \cap \mathbb{Z}\beta_1$ is a subgroup of $\mathbb{Z}\beta_1 \simeq \mathbb{Z}$, so there is $a \in \mathbb{Z}$ such that $A_1 = \mathbb{Z}a\beta_1$ is zero if $a = 0$ and is free of rank $1 \leq n$ if $a \neq 0$.

Assume that A_{r-1} is free of rank $s \leq r-1$, and let $\{\alpha_1, \ldots, \alpha_s\}$ be a basis of A_{r-1}. Let $\pi : B_r \to \mathbb{Z}\beta_r$ be the map sending

$$b_1\beta_1 + \cdots + b_r\beta_r \mapsto b_r\beta_r.$$

Then $\pi(A_r)$ is a subgroup of $\mathbb{Z}\beta_r \simeq \mathbb{Z}$. Let $\alpha \in A_r$ be any element such that $\pi(\alpha)$ generates $\pi(A_r)$. It is easy to check that $\{\alpha_1, \ldots, \alpha_s, \alpha\}$ spans A_r. If $\pi(\alpha) = 0$ then $\{\alpha_1, \ldots, \alpha_s\}$ is also a basis of A_r and we're done. Assume $\pi(\alpha) \neq 0$ and suppose $c_1\alpha_1 + \cdots + c_s\alpha_s + c\alpha = 0$, with all $c_i, c \in \mathbb{Z}$. Then $c\alpha \in A_{r-1} \subset \ker \pi$, so $c\pi(\alpha) = 0$, forcing $c = 0$. Now the remaining $c_i = 0$ by linear indpendence of $\{\alpha_1, \ldots, \alpha_s, \alpha\}$. Hence $\{\alpha_1, \ldots, \alpha_s, \alpha\}$ is a basis of A_r and the proof is complete. ■

Lemma 5.2 *Let $A \leq B$ be free abelian groups of rank n and let C be an intermediate group: $A \leq C \leq B$. Then C is free abelian of rank n.*

Proof: Applying Lemma 5.1 to the containment $C \leq B$ we have C free of rank $m \leq n$. From the containment $A \leq C$ we have A free of rank $\leq m$. But since A has rank n we must have $m = n$. ■

Proposition 5.3 *Let E be a number field, of degree n over $\mathbb{Q}$. Then the ring of integers R of E is a free abelian group of rank n.*

We first assume that $E/\mathbb{Q}$ is Galois. From Prop. 3.12 we have $\mathbb{Q}R = E$. It follows that E has a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ contained in R. Note that $\{\alpha_1, \ldots, \alpha_n\}$ need not be a $\mathbb{Z}$-basis of R. Let A be the subgroup of R generated by $\{\alpha_1, \ldots, \alpha_n\}$. Since linear independence over $\mathbb{Q}$ implies linear indendence over $\mathbb{Z}$, the set $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of A, so A is free of rank n. We will find $r \in \mathbb{Q}$ such that $R \subset rA$. Since rA is also free of rank n, the Proposition will then follow from Lemma 5.2.

The group $G = \mathrm{Aut}(E)$ has order n; list its elements as $G = \{\sigma_1, \ldots, \sigma_n\}$, and set $\alpha_{ij} = \sigma_j(\alpha_i)$, obtaining an $n \times n$ matrix $[\alpha_{ij}]$. If we apply some $\sigma \in G$ to each entry α_{ij} the columns of the matrix are permuted, so the determinant $\delta := \det[\alpha_{ij}]$ will change by at most a sign $\pm$. Hence the number $D := \delta^2$ is invariant under G and we have $D \in R \cap \mathbb{Q} = \mathbb{Z}$.

Let $\beta \in R$ and write $\beta = c_0^{-1}(c_1\alpha_1 + \cdots + c_n\alpha_n)$, with $c_i \in \mathbb{Z}$. Then

$$\sigma_j(\beta) = \sum_{i=1}^{n} \frac{c_i}{c_0}\alpha_{ij},$$

so we have

$$[\alpha_{ij}] \begin{pmatrix} c_1/c_0 \\ \vdots \\ c_n/c_0 \end{pmatrix} = \begin{pmatrix} \sigma_1(\beta) \\ \vdots \\ \sigma_n(\beta) \end{pmatrix}.$$

From the formula for the inverse of a matrix, it follows that $\delta \cdot [\alpha_{ij}]^{-1}$ has entries in R, so that $\delta \cdot (c_i/c_0) \in R$ for each i, and then $D \cdot (c_i/c_0) \in R \cap \mathbb{Q} = \mathbb{Z}$, so that $D \cdot \beta \in A$ and $\beta \in D^{-1} \cdot A$. Therefore $R \subset D^{-1} \cdot A$ and the proposition is proved when $E/\mathbb{Q}$ is Galois.

Now let $E/\mathbb{Q}$ be an arbitrary finite extension. Choose a Galois extension $L/\mathbb{Q}$ containing E and let S be the ring of integers of L. By what we just proved, S is free of rank $[L : \mathbb{Q}]$. Now $R = S \cap E$, so R is free of some rank $m \leq [L : \mathbb{Q}]$, by Lemma 5.1. Since a $\mathbb{Z}$-basis of R is a $\mathbb{Q}$-basis of E, we must have $m = n$, so R is free of rank n, as claimed. ■.

Remark: The number D appearing in the proof is **discriminant of** $E/\mathbb{Q}$, usually denoted $D_{E/\mathbb{Q}}$:

$$D_{E/\mathbb{Q}} = \det[\alpha_{ij}]^2. \tag{32}$$

It is related to discriminants of polynomials as follows. If $E = \mathbb{Q}(\alpha)$ where $\alpha \in R$ has monic minimal polynomial $f \in \mathbb{Z}[x]$ then

$$D_f = [R : \mathbb{Z}[\alpha]]^2 \cdot D_{E/\mathbb{Q}}.$$

Proposition 5.4 *Let E be a number field, of degree n over $\mathbb{Q}$, let R be the ring of integers in E, let p be a prime in $\mathbb{Z}$ and let P be a prime ideal of R containing p. Then R/P is a finite field of cardinality dividing p^n.*

Proof: From Prop. 3.3, we have that P is a maximal ideal in R, so R/P is a field. Let $n = [E : \mathbb{Q}]$. From Lemma 5.3, we have $R \simeq \mathbb{Z}^n$, as abelian groups. Hence $R/pR \simeq (\mathbb{Z}/p\mathbb{Z})^n$. Since $p \in P$, we have a surjective map $R/pR \to R/P$, and the proposition follows. ■

For each prime p in $\mathbb{Z}$, the subset

$$\mathrm{Spec}(R/pR) = \{P \in \mathrm{Spec}(R) : \ p \in P\} = \{P \in \mathrm{Spec}(R) : \ P \cap \mathbb{Z} = p\mathbb{Z}\}$$

is the set of prime ideals in R containing p. In more geometric terms, $\mathrm{Spec}(R/pR)$ is the fiber over $p\mathbb{Z}$ of the map $\mathrm{Spec}(R) \to \mathrm{Spec}(\mathbb{Z})$ induced by the canonical homomorphism $\epsilon : \mathbb{Z} \to R$.

Remark: Assume [19] that $R = \mathbb{Z}[\alpha]$ is generated by a single element α with minimal monic polynomial $f \in \mathbb{Z}[x]$. Then $\mathrm{Spec}(R) = \mathrm{Spec}(\mathbb{Z}[x]/f\mathbb{Z}[x])$ is the closure of the point $f\mathbb{Z}[x]$ in $\mathrm{Spec}(\mathbb{Z}[x])$ and $\mathrm{Spec}(\mathbb{F}_p[x]) = \mathrm{Spec}(\mathbb{Z}[x]/p\mathbb{Z}[x])$ is the fiber of $\mathrm{Spec}(\mathbb{Z}[x])$ over $p\mathbb{Z} \in \mathrm{Spec}(\mathbb{Z})$. Then $\mathrm{Spec}(R/pR)$ is the intersection of these two sub-schemes of $\mathrm{Spec}(\mathbb{Z}[x])$:

$$\mathrm{Spec}(R/pR) = \mathrm{Spec}(\mathbb{Z}[x]/f\mathbb{Z}[x]) \cap \mathrm{Spec}(\mathbb{Z}[x]/p\mathbb{Z}[x]).$$

Now

$$R/pR \simeq \mathbb{F}_p[x]/(\bar{f}) \simeq \prod_{i=1}^{\ell} \mathbb{F}_p[x]/(\bar{f}_i^{e_i}),$$

where $\bar{f} = \bar{f}_1^{e_1} \cdots \bar{f}_\ell^{e_\ell}$ and the $\bar{f}_i$ are distinct and irreducible in $\mathbb{F}_p[x]$. Each factor is a local ring with maximal ideal $P_i = (p, \bar{f}_i)$ and we have $\mathrm{Spec}(R/pR) = \{(p, f_i) : \ i = 1, \ldots, \ell\}$.

5.2 Decomposition and inertia groups

Now let $E/\mathbb{Q}$ be a Galois extension with ring of integers R and Galois group $G = \mathrm{Aut}(E)$. The action of G on E preserves R and permutes the prime ideals of R, so we have a G-action on $\mathrm{Spec}(R)$. Since G fixes each prime p in $\mathbb{Z}$, it follows that G acts on each fiber $\mathrm{Spec}(R/pR)$ of $\mathrm{Spec}(R)$ over $\mathrm{Spec}(\mathbb{Z})$.

Proposition 5.5 *The group G acts transitively on $\mathrm{Spec}(R/pR)$, for each prime $p \in \mathbb{Z}$.*

Proof: Suppose G does not act transitively on $\mathrm{Spec}(R/pR)$ for some prime $p \in \mathbb{Z}$. Then there are $P, Q \in X_p$ such that $Q \neq \sigma P$ for all $\sigma \in G$. Since primes in R are maximal, we can apply the Chinese Remainder Theorem: There exists $\alpha \in R$ such that

$$\alpha \equiv 0 \mod Q, \quad \text{and} \quad \alpha \equiv 1 \mod \sigma P \quad \forall\, \sigma \in G.$$

The product

$$N(\alpha) := \prod_{\sigma \in G} \sigma(\alpha) = \alpha \cdot \prod_{\sigma \neq e} \sigma(\alpha)$$

lies in Q because $\alpha \in Q$ and Q is an ideal. On the other hand $N(\alpha)$ is G-invariant, hence lies in $\mathbb{Q} \cap R = \mathbb{Z}$. Thus, $N(\alpha) \in Q \cap \mathbb{Z} = p\mathbb{Z}$. But $p\mathbb{Z} = P \cap \mathbb{Z}$, so we also have $N(\alpha) \in P$. Since P is prime we must have $\tau(\alpha) \in P$ for some $\tau \in G$, so $\alpha \in \tau^{-1}P$, contradicting the congruence $\alpha \equiv 1 \mod \sigma P$ for $\sigma = \tau^{-1}$. ■

It follows that the G-orbits in $\mathrm{Spec}(R)$ are precisely the fibers $\mathrm{Spec}(R/pR)$ and the map $\mathrm{Spec}(R) \to \mathrm{Spec}(\mathbb{Z})$ induces a bijection

$$G\backslash \mathrm{Spec}(R) \xrightarrow{\sim} \mathrm{Spec}(\mathbb{Z}).$$

The stabilizer of a prime $P \in \mathrm{Spec}(R)$ is the **decomposition group**

$$G_P = \{\sigma \in G : \ \sigma P = P\}.$$

[19] If we replace $\mathbb{Z}$ by $\mathbb{Z}_p$ we can avoid this assumption.

From Prop. 5.5 we have $[G : G_P] = |\operatorname{Spec}(R/pR)|$, and if $P, Q \in \operatorname{Spec}(R/pR)$ the subgroups G_P and G_Q are conjugate in G.

Let us now fix $P \in \operatorname{Spec}(R/pR)$. For each $\alpha \in R$ let $\bar{\alpha} = \alpha + P$ be the image of α in the finite field R/P. The decomposition group G_P preserves P, hence it acts on R/P, so we have a canonical homomorphism

$$\pi : G_P \longrightarrow \operatorname{Aut}(R/P) \qquad \sigma \mapsto \pi_\sigma, \quad \text{given by} \quad \pi_\sigma(\bar{\alpha}) = \overline{\sigma(\alpha)}.$$

The group $\operatorname{Aut}(R/P) \simeq C_r$ is cyclic of order $r = [R/P : \mathbb{F}_p]$, generated by the Frobenius automorphism $\phi_p \in \operatorname{Aut}(R/P)$ given by $\phi_p(x) = x^p$ for all $x \in R/P$.

Proposition 5.6 *The canonical homomorphism $\pi : G_P \to \operatorname{Aut}(R/P)$ is surjective.*

Proof: If $R/P = \mathbb{F}_p$ then $\operatorname{Aut}(R/P)$ is trivial, and so is the result. We may therefore assume $R/P \neq \mathbb{F}_p$. Choose $\beta \in R$ such that $R/P = \mathbb{F}_p(\bar{\beta})$. For example we could take $\bar{\beta}$ to be a generator of $(R/P)^\times$. Note that $\bar{\beta} \notin \mathbb{F}_p$ since $R/P \neq \mathbb{F}_p$. Let $g \in \mathbb{Z}[x]$ be the monic minimal polynomial of the algebraic integer β. Since G has a root in E, namely β, and $E/\mathbb{Q}$ is Galois, the polynomial g splits in $E[x]$ and all of the roots of g in E actually lie in R. These roots $\beta = \beta_1, \ldots, \beta_m \in R$ are permuted transitively by G, since g is irreducible in $\mathbb{Q}[x]$. The roots of $\bar{g}$ in R/P are $\bar{\beta} = \bar{\beta}_1, \ldots, \bar{\beta}_m$, and these are permuted, not necessarily transitively, by $\operatorname{Aut}(R/P) = \langle \phi_p \rangle$. Hence we have $\bar{\beta}^p = \bar{\beta}_i$ for some $1 \leq i \leq m$. Since G is transitive on $\{\beta_1, \ldots, \beta_m\}$ there exists $\sigma \in G$ such that $\sigma(\beta) = \beta_i$.

I claim that $\sigma \in G_P$. Suppose not. Then we have distinct maximal ideals $P \neq \sigma P$. By the Chinese Remainder Theorem, there exists $\alpha \in R$ such that

$$\alpha \equiv \beta \mod P, \quad \text{and} \quad \alpha \equiv 1 \mod \sigma P.$$

We then get two congruences in R/P:

$$\alpha^p \equiv \beta^p \mod P, \quad \text{and} \quad \sigma^{-1}(\alpha) \equiv 1 \mod P,$$

which imply

$$\beta = \sigma^{-1}(\beta_i) \equiv \sigma^{-1}(\beta^p) \equiv \sigma^{-1}(\alpha^p) = 1 \mod P.$$

This forces $\bar{\beta} = 1 \in \mathbb{F}_p$, a contradiction.

Therefore $\sigma \in G_P$, and we have

$$\pi_\sigma(\bar{\beta}) = \overline{\sigma(\beta)} = \bar{\beta}_i = \bar{\beta}^p = \phi_p(\bar{\beta}).$$

Since $\bar{\beta}$ generates R/P, it follows that $\pi_\sigma = \phi_p$ generates $\operatorname{Aut}(R/P)$, so π is surjective. ■

The **inertia group** I_P is the kernel of the canonical surjection $\pi : G_P \to \operatorname{Aut}(R/P)$. It fits into the exact sequence

$$1 \longrightarrow I_P \longrightarrow G_P \xrightarrow{\pi} \operatorname{Aut}(R/P) \longrightarrow 1.$$

If $P, Q \in \mathrm{Spec}(R)_p$ and $\sigma \in G$ is such that $\sigma P = Q$ then $\sigma G_P \sigma^{-1} = G_Q$ and $\sigma I_P \sigma^{-1} = I_Q$. Hence the degree r of R/P over $\mathbb{F}_p$ and the order e of I_P depend only on p and we have

$$|G| = e \cdot r \cdot s,$$

where

$$e = |I_P|, \quad r = [G_P : I_P], \quad s = [G : G_P] = |\,\mathrm{Spec}(R)_p|.$$

The number e is called the **ramification degree** of p. We say that p is **ramified in** E if $e > 1$ and **unramified in** E if $e = 1$. Equivalently, p is unramified in E exactly when the canonical surjection $\pi : G_P \to \mathrm{Aut}(G/P)$ is an isomorphism. In this case, we have a unique element $\sigma_P \in G_P$ such that $\pi(\sigma_P) = \phi_p$ is the Frobenius automorphism of R/P. One can check that $\tau \sigma_P \tau^{-1} = \sigma_{\tau(P)}$ for any $\tau \in G$. Thus for each unramified prime $p \in \mathbb{Z}$ we have a conjugacy class $\mathrm{Frob}_p \subset G$ given by

$$\mathrm{Frob}_p = \{\sigma_P : \ p \in P\}.$$

We will see that only a finite number of primes are ramified. As p varies among the all-but-finitely many unramified primes in $\mathbb{Z}$, the conjugacy class Frob_p varies among the conjugacy classes in G. The Chebotarev Density Theorem asserts that, statistically, each conjugacy class in G is visited by its fair share of primes.

Theorem 5.7 (Chebotarev Density Theorem) *Let $E/\mathbb{Q}$ be a Galois extension and let C be a conjugacy class in the Galois group $G = \mathrm{Aut}(E)$. Then we have*

$$\lim_{N \to \infty} \frac{|\{\textit{primes } p \leq N : \ \mathrm{Frob}_p = C\}|}{|\{\textit{all primes } p \leq N\}|} = \frac{|C|}{|G|}.$$

Proof: See [Neukirch, *Algebraic Number Theory* ,VII.13]. ■

Dedekind proved that that the ramified primes are exactly those which divide the discriminant $D_{E/\mathbb{Q}}$, defined in (32). [20] In the next section we will prove a weaker result with $D_{E/\mathbb{Q}}$ replaced by a polynomial discriminant D_f.

5.3 Frobenius classes in the Galois group of a polynomial

Let $f \in \mathbb{Z}[x]$ be a monic polynomial with $\deg f = d$. Let E be the splitting field of f over $\mathbb{Q}$ and let R be the ring of integers in E. Let $p \in \mathbb{Z}$ be a prime not dividing the discriminant D_f, let $\bar{f} \in \mathbb{F}_p[x]$ be the reduction of f modulo p, and let P be a prime ideal in R containing p.

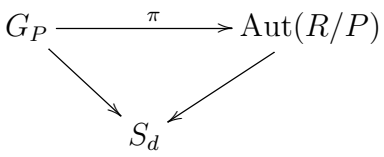
Since $p \nmid D_f$, and $\overline{D_f} = D_{\bar{f}}$ because D_f is an integral polynomial in the coefficients of f, it follows that both f and $\bar{f}$ have d-distinct roots in R and R/P respectively. If $\alpha_1, \ldots, \alpha_d$ are the distinct roots of f in R, then their images $\bar{\alpha}_1, \ldots, \bar{\alpha}_d$ in R/P are the distinct roots of $\bar{f}$ in R/P. Thus, we have homomorphisms

$$G_P \hookrightarrow S_d \longleftarrow \mathrm{Aut}(G/P),$$

where the left-hand map is the restriction of the injection $G \hookrightarrow S_d$.

[20] See for example, Neukirch *Algebraic Number Theory* III.2.

Proposition 5.8 *Assume that p does not divide the discriminant D_f. Then p is unramified in E. More precisely, the map $\pi : G_P \to \mathrm{Aut}(R/P)$ is an isomorphism making the following diagram commute:*



In particular, Frob_p *and* ϕ_p *belong to the same conjugacy class in* S_d*.*

Proof: Take $\sigma \in G_P$ and $1 \leq i \leq n$. Suppose $\sigma(\alpha_i) = \alpha_j$ Then $\pi_\sigma(\bar{\alpha}_i) = \overline{\sigma(\alpha_i)} = \bar{\alpha}_j$, so σ and π_σ induce the same permutation in S_d. ■

Proposition 5.9 *Assume $p \nmid D_f$. If $\bar{f} = \bar{f}_1 \dots \bar{f}_\ell$, with $\bar{f}_i$ irreducible in $\mathbb{F}_p[x]$, then the elements of* Frob_p *have cycle type $[d_1, d_2, \dots, d_\ell]$ in S_d, where $\bar{d}_i = \deg \bar{f}_i$.*

For example, Frob_p consists of d-cycles if and only if f is irreducible modulo p.

To apply Prop. 5.9, it is useful to have

Proposition 5.10 *[Jordan's Lemma] Let G be a finite group and let $H \leq G$ be a subgroup of G such that $H \cap C$ is nonempty for every conjugacy class C in G. Then $H = G$.*

Proof: We have

$$|G| = \left| \bigcup_{g \in G/H} gHg^{-1} \right| \leq 1 + [G : H](|H| - 1) = |G| - ([G : H] - 1),$$

so $[G : H] = 1$. ■

Example: Suppose $f \in \mathbb{Z}[x]$ is irreducible of degree five. Below we tabulate the transitive subgroups $G \leq S_5$ and the number of each cycle type in G.

G	$[5]$	$[41]$	$[32]$	$[311]$	$[221]$	$[2111]$	$[1^5]$
S_5	24	30	32	20	15	10	1
A_5	24	0	0	20	15	0	1
F_{20}	4	10	0	0	5	0	1
D_5	4	0	0	0	5	0	1
C_5	4	0	0	0	0	0	1

If there exists a prime p such that Frob_p has type $[32]$ then $G = S_5$, since no proper transitive subgroup of S_5 contains such a cycle type. Similarly, if Frob_p is of type $[311]$ for some p then G_f is either S_5 or A_5, which can be decided by a discriminant calculation.

Example: (Exercise in Lang) Let $f = x^6 + 22x^5 - 9x^4 + 12x^3 - 37x^2 - 29x - 15$. Reducing modulo $2, 3, 5$ we find cycle types $[6], [51], [21^4]$ in G_f, which implies that $G_f = S_6$.

Example: Let $f = x^6 - 10x^3 + 15x^2 - 6x + 1$. One can check that $(1-x)^6 f(1/(1-x)) = f(x)$. Hence if α is a root of f, so are $\alpha' = 1/(1-\alpha)$ and $\alpha'' = 1 - (1/\alpha)$. One checks that f is irreducible modulo 17, so $\alpha, \alpha', \alpha''$ are distinct. It follows that G_f centralizes a $[33]$-cycle in S_6. The centralizer $H = C_{S_6}([33])$ has structure $(C_3 \times C_3) \rtimes C_2$, with C_2 acting by permuting the factors and contains only elements of cycle types $[6], [3111], [33], [222], [1^6]$. To show $G_f = H$, it suffices to find elements in G_f of each of these cycle types.

class:	$[6]$	$[3111]$	$[33]$	$[222]$	$[1^6]$
smallest p :	17	11	5	13	127

This proves that $G_f = H$.

6 Cyclotomic extensions and abelian numbers

Fix an integer $n \geq 2$ and let $\mu_n = \{\alpha \in \mathbb{C}^\times : \alpha^n = 1\}$ be the group of n^{th}**-roots of unity** in $\mathbb{C}^\times$. These are the roots of $x^n - 1$ and are generated by the complex number $\zeta = e^{2\pi i/n}$. The **primitive** n^{th} **roots of unity** are the generators of μ_n; these are the powers ζ^k for k in the unit group $U(n) := (\mathbb{Z}/n\mathbb{Z})^\times$.

Since all of the roots of $x^n - 1$ are powers of ζ, the field $\mathbb{Q}(\zeta)$ is the splitting field of $x^n - 1$, so it is Galois over $\mathbb{Q}$. Let $G = \mathrm{Aut}(\mathbb{Q}(\zeta))$ be the Galois group. Each $\sigma \in G$ is determined by its effect on ζ and $\sigma(\zeta)$ must be another primitive n^{th} root of unity. Hence we have an injective homomorphism

$$\kappa : G \longrightarrow U(n), \quad \text{given by} \quad \sigma(\zeta) = \zeta^{\kappa(\sigma)}.$$

The n^{th} **cyclotomic polynomial**

$$\Phi_n(x) := \prod_{k \in U(n)} (x - \zeta^k)$$

has for roots exactly the primitive n^{th} roots of unity. As these are permuted by G, it follows that Φ_n is G-invariant, and hence has coefficients in $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.

Proposition 6.1 *$\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof: Let f be the minimal polynomial of ζ over $\mathbb{Q}$. Since $\zeta \in \bar{\mathbb{Z}}$ we have f monic in $\mathbb{Z}[x]$ and $f \mid x^n - 1$, so we may factor $x^n - 1 = fg$ in $\mathbb{Z}[x]$.

Let p be any prime not dividing n. Then ζ^p is another root of $x^n - 1$ so either $f(\zeta^p) = 0$ or $g(\zeta^p) = 0$. Suppose $g(\zeta^p) = 0$. Let $h(x) = g(x^p)$. Then $h(\zeta) = 0$ so $h = fq$ for some $q \in \mathbb{Z}[x]$. In $\mathbb{F}_p[x]$ we have

$$\bar{f} \cdot \bar{q} = \bar{h} = \bar{g}^p.$$

It follows that $\bar{f}$ and $\bar{g}$ have a common factor. But $x^n - 1$ has distinct roots modulo p, since $p \nmid n$. This contradiction shows that $g(\zeta_p) \neq 0$, so we must have $f(\zeta^p) = 0$.

This holds for all primes p not dividing n, hence $f(\zeta^k) = 0$ for all $k \in U(n)$. It follows that $f = \Phi_n$.

■

Recall that the order of $U(n)$ is given by the Euler function $\phi(n) = |U(n)|$.

Corollary 6.2 *We have $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ and the map $\kappa : G \to U(n)$ is an isomorphism.*

We now compute the classes $\mathrm{Frob}_p \subset G$ for each p not dividing n. Since G is abelian, each class Frob_p consists of a single element:

$$\mathrm{Frob}_p = \{\sigma_p\}.$$

Proposition 6.3 *For any prime p not dividing n, the element $\kappa(\sigma_p) \in U(n)$ is given by $\kappa(\sigma_p) \equiv p \mod n$.*

Proof: Let R be the ring of integers of $\mathbb{Q}(\zeta)$ and let P be a prime ideal of R containing p. Since $p \nmid n$, the reduction

$$\bar{\Phi}_n = \prod_{k \in U(n)} (x - \bar{\zeta}^k)$$

has distinct roots $\bar{\zeta}^k \in R/P$.

If $\sigma, \tau \in G$ are such that $\overline{\sigma(\zeta)} = \overline{\sigma(\tau)}$, we have $\kappa(\sigma) = \kappa(\tau)$, so $\sigma = \tau$ by the injectivity of κ. By the surjectivity of κ there is an element $\tau_p \in G$ such that $\kappa(\tau_p) = p$. That is, $\tau_p(\zeta) = \zeta^p$. But

$$\overline{\tau_p(\zeta)} = \bar{\zeta}^p = \overline{\sigma_p(\zeta)},$$

so in fact $\tau_p = \sigma_p$ as we wished to show. ■

For a given $k \in U(n)$ we have $\kappa(\sigma_p) = k$ if and only if $p \in k + n\mathbb{Z}$. Thus, Chebotarev's Theorem 5.7 reduces to Dirichlet's Theorem on primes in an arithmetic progression. [21]

Theorem 6.4 (Dirichlet's Theorem)

$$\lim_{N \to \infty} \frac{|\{p \leq N : \ p \in k + n\mathbb{Z}\}|}{|\{p < N\}|} = \frac{1}{\phi(n)}.$$

6.1 Gauss and Cyclotomy

In his *Disquisitiones* chapter VII, Gauss proposes to find the "Equations defining sections of a circle". Fix a prime $p \geq 3$ and cut the unit circle $|z| = 1$ into p equal parts, starting at $z = 1$. The cut points

[21] Historically Dirichlet's Theorem came first and inspired Chebotarev. See Serre's *Course in Arithmetic* for a direct proof of Dirichlet's Theorem.

$\zeta, \zeta^2, \ldots, \zeta^{p-1} = \bar{\zeta}$ all have minimal polynomial $\Phi_p = 1 + x + x^2 + \cdots + x^{p-1}$ and generate the field $\mathbb{Q}(\zeta)$.

The x-coordinates of the cut points, doubled, are $\zeta + \bar{\zeta},\ \zeta^2 + \bar{\zeta}^2, \ldots$. These have minimal polynomial Ψ_p given in equation (14) and generate the unique subfield $\mathbb{Q}(\zeta + \bar{\zeta})$ of degree $(p-1)/2$.

At the other extreme, the quadratic subfield of $\mathbb{Q}(\zeta)$ is generated by $\sqrt{\epsilon p}$, where $\epsilon \in \{\pm 1\}$ is given by $p \equiv \epsilon \mod 4$. We can see this as follows. The cyclic group $\mathbb{F}_p^\times$ has a unique subgroup of index two, namely $\mathbb{F}_p^{\times 2}$, so there is a unique nontrivial homomorphism

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \longrightarrow \{\pm 1\},$$

called the **Legendre symbol**, given by

$$\left(\frac{k}{p}\right) = \begin{cases} +1 & \text{if} \quad k \in \mathbb{F}_p^{\times 2} \\ -1 & \text{if} \quad k \notin \mathbb{F}_p^{\times 2}. \end{cases}$$

It can be shown [22] that the sum

$$\sum_{k \in \mathbb{F}_p^\times} \left(\frac{k}{p}\right) \zeta^k$$

squares to $\left(\frac{-1}{p}\right) p = \epsilon p$.

More generally, the subfields of $\mathbb{Q}(\zeta)$ are in bijection with subgroups of $\mathrm{Aut}(\mathbb{Q}(\zeta))$, and we have an isomorphism

$$\mathbb{F}_p^\times \xrightarrow{\sim} \mathrm{Aut}(\mathbb{Q}(\zeta)), \qquad \text{given by} \quad k \mapsto \sigma_k,$$

where σ_k is the automorphism of $\mathbb{Q}(\zeta)$ determined on the generator by $\sigma_k(\zeta) = \zeta^k$.

The group $\mathbb{F}_p^\times$ is cyclic of order $p-1$, so its subgroups correspond to divisors of $p-1$. Fix a divisor $d \mid (p-1)$ and let H_d be the unique subgroup of index d in $\mathbb{F}_p^\times$. Then $\mathbb{Q}(\zeta)^{H_d}$ is the unique subfield of $\mathbb{Q}(\zeta)$ of degree d over $\mathbb{Q}$. This field has a canonical generator, as follows.

Lemma 6.5 *We have $\mathbb{Q}(\zeta)^{H_d} = \mathbb{Q}(\alpha_d)$, where*

$$\alpha_d = \sum_{h \in H_d} \zeta^h.$$

Proof: By the Galois correspondence, $\mathbb{Q}(\alpha_d) = \mathbb{Q}(\zeta)^J$ for a unique subgroup $J \leq \mathbb{F}_p^\times$. Since α_d is clearly H_d-invariant, we have $\mathbb{Q}(\zeta)^J \subset \mathbb{Q}(\zeta)^{H_d}$, so $H_d \leq J$. It suffices to show that $J \leq H_d$. Given $s \in J$, we have

$$\sum_{h \in H_d} \zeta^h = \alpha_d = \sigma_s(\alpha_d) = \sum_{h \in H_d} \zeta^{hs}.$$

[22] Lang, VI.3

Since $\{\zeta^k : k \in \mathbb{F}_p^\times\}$ is a basis of $\mathbb{Q}(\zeta)$, it follows that $\zeta = \zeta^{hs}$ for some $h \in H_d$, so $hs = 1$ and this shows $s \in H_d$. ■

From Lemma 6.5, it follows that

$$[\mathbb{Q}(\alpha_d) : \mathbb{Q}] = [\mathbb{F}_p^\times : H_d] = d.$$

Gauss' problem becomes that of finding the minimal polynomial of α_d.

The polynomial

$$f_d(x) := \prod_{k \in \mathbb{F}_p^\times / H_d} (x - \sigma_k(\alpha_d))$$

is invariant under $\mathrm{Aut}(\mathbb{Q}(\zeta))$, has α_d as a root, and has degree d, so $f_d(x) \in \mathbb{Z}[x]$ is the minimal monic polynomial of α_d. It remains to find the coefficients of f_d.

Choose a generator g of $\mathbb{F}_p^\times$ and let $d' = (p-1)/d$. Then $H_d = \langle g^d \rangle$ and $\{1, g, g^2, \ldots, g^{d-1}\}$ is a set of coset representatives for $\mathbb{F}_p^\times / H_d$. The choice of g gives an isomorphism

$$\mathbb{F}_p^\times \xrightarrow{\sim} \mathbb{Z}/(p-1)\mathbb{Z}, \qquad g^j \mapsto j \mod (p-1)$$

sending $H_d \to \langle d \rangle$. The partition of $\mathbb{F}_p^\times$ into cosets of H_d corresponds to the partition

$$\mathbb{Z}/(p-1)\mathbb{Z} = \coprod_{i=0}^{d-1} C_d(i),$$

where $C_d(i) = \{dk + i : 0 \le k \le d'\}$. We have

$$\alpha_d = \sum_{k=1}^{d'} \zeta^{g^{dk}},$$

$$f_d(x) = \prod_{i=0}^{d-1} (x - \sigma_{g^i}(\alpha_d)),$$

and

$$\sigma_{g^i}(\alpha_d) = \sum_{\ell \in C_d(i)} \zeta^{g^\ell}. \tag{33}$$

The sums in (33) are called **Gauss periods**; they are the roots of f_d.

For explicit computations, we can make the periods into polynomials and treat them symbolically. Thus, we replace each $g^\ell \mod p$ by a representative $1 \le g^\ell \le p-1$ and define polynomials

$$A_i(t) = \sum_{\ell \in C_d(i)} z^{g^\ell} \in \mathbb{Z}[t],$$

and

$$F_d(t, x) = \prod_{i=0}^{d-1} (x - A_i(t)) \in R[x],$$

where $R = \mathbb{Z}[t]$. Now $f_d(x)$ is the polynomial remainder of $F_d(t)$ modulo $\Phi_p(t)$, taken in $R[t]$.

Example: Take $p = 13$, $d = 4$ and $g = 2$ as generator of $\mathbb{F}_{13}^\times$. The the partition of $\mathbb{F}_{13}^\times$ into cosets of H_4 and the periods are given by

$$\begin{array}{lll} \{2^4, 2^8, 2^{12}\} & \overset{\text{mod } 13}{\equiv} & \{3, 9, 1\} \qquad \alpha_4 = \zeta + \zeta^3 + \zeta^9 \\ \{2^{1+4}, 2^{1+8}, 2^{1+12}\} & \equiv & \{6, 5, 2\} \qquad \sigma_2(\alpha_4) = \zeta^6 + \zeta^5 + \zeta^2 \\ \{2^{2+4}, 2^{2+8}, 2^{2+12}\} & \equiv & \{12, 10, 4\} \quad \sigma_4(\alpha_4) = \zeta^{12} + \zeta^{10} + \zeta^4 \\ \{2^{3+4}, 2^{3+8}, 2^{3+12}\} & \equiv & \{11, 7, 8\} \qquad \sigma_8(\alpha_4) = \zeta^{11} + \zeta^7 + \zeta^8. \end{array}$$

We have

$$F_4(t, x) = (x - t - t^3 - t^9)(x - t^6 - t^5 - t^2)(x - t^{12} - t^{10} - t^4)(x - t^{11} - t^7 - t^8),$$

whose remainder modulo $\Phi_{13}(t)$ is

$$f_4(x) = x^4 + x^3 + 2x^2 - 4x + 3.$$

We can check this result using our analysis of quartic polynomials (cf. section 4.2.3), for the quartic $f = f_4$. Let's see if we get $G_f = C_4$.

The discriminant is $D_f = 3^2 \cdot 13^3$ so $G_f \not\leq A_4$.

The cubic resolvent is $x^3 - 2x^2 - 16x + 5 = (x - 5)(x^2 + 3x - 1)$, so $G_f \leq D_4$.

The quadratic resolvent (see (29)) has discriminant 13^2, so $G_f \leq C_4$, as it should be. And the quadratic subfield is $\sqrt{D_f} = \sqrt{13}$, again as it should be.

This method computes the minimal polynomial f_d of the canonical generator of the degree d- subfield of $\mathbb{Q}(\zeta)$ for any given p and $d \mid p-1$. Gauss found a general formula for f_3, in the following remarkable result.

Theorem 6.6 (Gauss) [23] *Let $p = 1 + 3k$ be a prime $\equiv 1 \mod 3$ and let $\zeta = e^{2\pi i/p}$. Then*

1. *There are unique integers A, B such that $4p = A^2 + 27B^2$ and $A \equiv 1 \mod 3$.*
2. *The generator α_3 of the cubic subfield of $\mathbb{Q}(\zeta)$ has minimal polynomial*

$$f_3 = x^3 + x^2 - kx - \frac{p(A+3) - 1}{27}$$

   of discriminant $D_{f_3} = (pB)^2$.

3. *The number of points in $\mathbb{P}^2(\mathbb{F}_p)$ lying on the curve $X^3 + Y^3 + Z^3 = 0$ is equal to $p + 1 + A$.*

[23] See Gauss *Disquisitiones* Art. 358, as well as Silverman-Tate *Rational points on elliptic curves* IV.2.

6.2 The Kronecker-Weber theorem and abelian numbers

A Galois extension E/F is *abelian* if the Galois group $\mathrm{Aut}(E/F)$ is abelian.

Theorem 6.7 (Kronecker-Weber) *Every abelian extension of $\mathbb{Q}$ is a subfield of $\mathbb{Q}(e^{2\pi i/n})$, for some positive integer n.*

The minimal such n is called the **conductor** of the abelian extension $E/\mathbb{Q}$. In the *Disquisitiones*, Gauss found the abelian extensions of $\mathbb{Q}$ of prime conductor.

In terms of polynomials, Kronecker-Weber asserts that if $f \in \mathbb{Q}[x]$ is a polynomial with abelian Galois group G_f, then the roots of f are polynomial expressions in $e^{2\pi i/n}$ for some n. I like to call such roots **abelian numbers**. The set $\mathbb{Q}^{ab}$ of all abelian numbers is a subfield of $\mathbb{C}$ and is an algebraic extension of $\mathbb{Q}$. Kronecker-Weber gives an explicit description of $\mathbb{Q}^{ab}$, as the union of all cyclotomic fields:

$$\mathbb{Q}^{ab} = \bigcup_{n \geq 1} \mathbb{Q}(e^{2\pi i/n}).$$

In group-theoretic terms, the Kronecker-Weber theorem says that every finite abelian quotient of $\mathrm{Aut}(\overline{\mathbb{Q}})$ factors through $\mathrm{Aut}(\mathbb{Q}(e^{2\pi i/n}))$, for some n. Today, the Kronecker-Weber theorem is regarded as a corollary of Class-Field Theory, which describes abelian extensions of a number field F in terms of the arithmetic of F. [24]

[24] See, for example, Neukirch *Algebraic Number Theory*.