Fields and Galois Theory
Fall 2004
Professor Yu-Ru Liu

CHRIS ALMOST

Contents

1 Introduction

Galois Theory is the interplay between fields and groups.

1.1 Motivation

Consider the following historical problems.

- Construct an arbitrary regular n-gon using only a ruler and a compass. We know how to construct a triangle and square, but what about 5-gon, etc.?
- Square the circle using only a ruler and compass (i.e. construct a square of area π).
- Solve an arbirary polynomial using only algebraic means (i.e. plus, minus, times, divides, and n^{th}root). The quadratic formula gives a solution for quadratic equations. Cubic and quartic equations can be solved similarily. e.g. if $x^3 + px = q$ then

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}$$

- For which quintic equations do we have radical solutions? If we know there is such a solution, what does the solution look like?

How can we solve these problems? The main steps in applying the theory that we develope in this course are as follows:

1. Associate the solution of interest, say $\alpha = \sqrt{\pi}$ or $\alpha =$ the root of some quintic, with the field $\mathbb{Q}(\alpha)$.
2. Associate $\mathbb{Q}(\alpha)$ with the group of isomorphisms of $\mathbb{Q}(\alpha)$ that fix $\mathbb{Q}$, $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$. If α is algebraic then $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is finite. If α is constructable then the order of $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ is in certain forms.

Hard Question: How many intermediate fields between $\mathbb{Q}$ and $\mathbb{Q}(\alpha)$? There is a 1-1 correspondence between the intermediate fields and the subgroups of $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\alpha))$ (this is the Fundemental Theorem of Galois theory.)

1.2 Brief Review of Ring Theory

For this course we will be dealing with commutative rings with identity.

1.1 Example. Let R be a ring. We denote by $R[x]$ the polynomial ring over R in indeterminant x. The degree of a polynomial is the exponent on the leading term. By convention, $\deg 0 = -\infty$. If a polynomial has leading coefficient 1 then it is called "monic".

A ring R is called a domain if it has no zero divisors. An element $u \in R$ is called a unit if it is invertible. A field is a commutative ring in which each non-zero element is a unit and $0 \neq 1$.

1.2 Example. If F is a field, then $F[x]$ is a domain (it is sufficient that F be a domain) and for $f, g \in F[x]$, $\deg(fg) = \deg(f) + \deg(g)$. This degree function actually makes $F[x]$ into a Euclidean domain.

The rational (function) field over a field F is denoted $F(x)$ and consists of all quotients of polynomials (with non-zero denominator) from $F[x]$. It is the smallest field that contains $F[x]$.

An ideal I of a ring R is a (not necessarily unital) subring of R that is absorbing with respect to multiplication by elements of R. We can now construct R/I, the quotient ring modulo I.

I is said to be maximal if $I \neq R$ and for any ideal J we have $I \subseteq J \subseteq R \Rightarrow I = J \vee J = R$. I is said to be prime if $I \neq R$ and $ab \in I \Rightarrow a \in I \vee b \in I$. Notice that every maximal ideal is prime, and in PIDs every prime ideal is maximal. Fields have only trivial ideals.

1.3 Theorem. *Let I be a proper ideal of R. Then*

1. *R/I is a field if and only if I is maximal*
2. *R/I is a domain if and only if I is prime*

1.4 Theorem. *(First Isomorphism Theorem) If $\varphi : R \to S$ is a ring homomorphism and $\ker\varphi = I$ then there is an isomorphism*

$$\alpha : R/I \to Im\,\varphi : r + I \mapsto \varphi(r)$$

2 Field extensions

2.1 Definition. If E is a field containing another field F then E is said to be a field extension of F, denoted by E/F

2.1 Degree of a Field Extention

If E/F is a field extension then we can view E as a vector space over F.

- Addition is given to agree with the field addition
- Scalar multiplication is given to agree with the field multiplication

2.2 Definition. The dimension of E viewed as a vector space over F is called the degree of E over F and is denoted $[E : F]$. If this quantity happens to be finite, then E/F is said to be a finite extension, otherwise it is an infinite extension.

2.3 Example.
1. $\mathbb{C} \cong \mathbb{R} \oplus i\mathbb{R}$, so $[\mathbb{C} : \mathbb{R}] = 2$
2. $[\mathbb{R} : \mathbb{Q}] = \infty$
3. Let F be a field. The rational field is an infinite extension. An infinite linearly independent set is $\{\ldots, x^{-1}, 1, x, x^2, \ldots\}$

2.4 Theorem. *If E/K and K/F are finite field extensions, then E/F is finite and*

$$[E : F] = [E : K][K : F]$$

PROOF: Let $\{a_1, \ldots, a_m\}$ be a basis for E over K and $\{b_1, \ldots, b_n\}$ be a basis for K over F. It suffices to prove $\alpha := \{a_i b_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ is a basis for E over F. Every element of E is a linear combination of elements of α since each element of E is a linear combination of elements of $\{a_1, \ldots, a_m\}$, and each of the a_i's (being elements of K) can be written as a linear combination of elements from $\{b_1, \ldots, b_n\}$. α is linearly independent over F, for otherwise if $\sum_{i=1}^{m}\sum_{j=1}^{n} c_{i,j} b_j a_i = 0$, then $\{a_1, \ldots, a_m\}$ a basis implies that $\sum_{j=1}^{n} c_{i,j} b_j = 0$ for all i. Since $\{b_1, \ldots, b_n\}$ is also a basis, we get that $c_{i,j} = 0$ for all i and j. □

2.5 Definition. Let E/F be a field extension. If K is a subfield of E that contains F then we say that K is an intermediate field of E/F.

2.6 Corollary. *If E/F is a finite extension and K is an intermediate field then $[E : K]$ and $[K : F]$ are divisors of $[E : F]$.*

2.2 Algebraic and Transcendental Numbers

2.7 Definition. Let E/F be a field extension and $\alpha \in E$. We say that α is algebraic over F if there is $f(x) \in F[x]$ such that $f \neq 0$ and $f(\alpha) = 0$. Otherwise α is said to be transcendental over F.

In particular, for $\alpha \in \mathbb{C}$ and α algebraic (transcendental) over $\mathbb{Q}$, we say that α is an algebraic (transcendental) number. For example, all rational numbers are algebraic, as are $\sqrt{2}$, $\sqrt[3]{2} + i$, etc. The real numbers e (Hermite 1873) and π (Lindemann 1882) are transcendental numbers.

2.8 Theorem. *(Liouville 1884) Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be a root of a polynomial $f(x) \in \mathbb{Q}[x]$ of degree n. Then there exists a constant $c > 0$ such that for any rational number $\frac{p}{q}$ with $q > 0$*

$$\left| \alpha - \frac{p}{q} \right| > \frac{c}{q^n}$$

PROOF: Without loss of generality, we can assume $|\alpha - \frac{p}{q}| < 1$ and that $f(x) \in \mathbb{Z}[x]$ and f is irreducible. Then $f(\alpha) = 0$ and $f(\frac{p}{q}) \neq 0$. By the Mean Value theorem, $|f(\frac{p}{q})| = |f(\alpha) - f(\frac{p}{q})| \leq M|\alpha - \frac{p}{q}|$, where $M = \sup |f'(x)|$ for $|x - \alpha| < 1$. Since α is irrational, $\deg(f) \geq 2$ and $M \neq 0$. Furthermore, $|f(\frac{p}{q})| \geq 1/q^n$, and thus $|\alpha - \frac{p}{q}| \geq \frac{1}{M}\frac{1}{q^n}$, so take $c = \frac{1}{M}$. □

Remark. Liouville's Theorem says that algebraic numbers are "harder" to approximate by rational numbers than transcendental numbers. Thue (1909) and Siegel (1921) improved the above theorem by replacing n with $\frac{n}{2} + 1$ and $2\sqrt{n}$, respectively. In 1955, Roth improved the above theorem to $|\alpha - \frac{p}{q}| > \frac{c'}{q^{2+\epsilon}}$. This won him the Fields medal in 1958.

2.9 Example. $z = \sum_{n \geq 1} \frac{1}{10^{n!}}$ is trancendental.

Suppose that z is algebraic and is a root of a polynomial of degree n. Then there is a constant $c > 0$ such that for any rational number $\frac{p}{q}$ with $q > 0$

$$\left| z - \frac{p}{q} \right| > \frac{c}{q^n}$$

Consider $\sum_{n=1}^{s} \frac{1}{10^{n!}} = \frac{p}{10^{s!}}$, $q = 10^{s!}$ We have

$$\frac{c}{q^n} < \left| z - \frac{p}{q} \right| = \sum_{n=s+1}^{\infty} \frac{1}{10^{n!}} < \frac{1}{10^{(s+1)!-1}}$$

It follows that

$$0 < c < \frac{10^{n \cdot s!}}{10^{(s+1)!-1}} \longrightarrow 0$$

as $s \to \infty$. This implies that $c = 0$, a contradiction.

2.3 Simple Extensions

Let E/F be a field extension and $\alpha \in E$. Let $F[\alpha]$ denote the smallest subring of E containing F and α and $F(\alpha)$ denote the smallest sufield of E containing F and α.

2.10 Definition. If $E = F(\alpha)$ then we say that E is a simple extension of F.

$[E : F]$ can be either ∞ or finite depending on whether α is transcendental or algebraic over F.

2.11 Definition. If R and R' are two rings containing a field F, then a ring homomorphism $\psi : R \to R'$ such that $\psi(c) = c \ \forall\, c \in F$ is said to be an F-homomorphism.

2.12 Theorem. *Let E/F be a field extension and $\alpha \in E$. If α is transcendental over F then $F[\alpha] \cong F[x]$ and $F(\alpha) \cong F(x)$. In particular, $F[\alpha] \ncong F(\alpha)$.*

PROOF: The F-homomorphism $\alpha \mapsto x$ is clearly the desired isomorphism in each case. □

2.13 Theorem. *Let E/F be a field extension and $\alpha \in E$. If α is algebraic over F then there is a unique monic irreducible polynomial $p(x) \in F[x]$ such that there is an F-isomorphism*

$$\psi : F[x]/\langle p(x)\rangle \to F[\alpha]$$

with $\psi(x) = \alpha$. From this we conclude that $F[\alpha] = F(\alpha)$.

PROOF: Let $\psi : F[x] \to F(\alpha)$ be the unique F-homomorphism with $\psi(x) = \alpha$. Thus, $\operatorname{Im}\psi = F[\alpha]$ and let $I = \ker\psi$. Since α is algebraic, $I \neq 0$. We have $F[x]/I \cong \operatorname{Im}\psi$, a subring of a field, so it is a (principal ideal) domain. Therefore I is a prime ideal, so it must be generated by some irreducible polynomial $p(x)$. We may assume that $p(x)$ is monic without loss of generality. It follows that $F[x]/\langle p(x)\rangle \cong F[\alpha]$ is a field. $F(\alpha)$ is also a field, and since it is the smallest field that contains $F[\alpha]$, we must have $F[\alpha] = F(\alpha)$. □

2.14 Definition. The monic irreducible in the last theorem is called the minimal polynomial of α over F.

2.15 Theorem. *Let E/F be a field extension and $\alpha \in E$.*

1. *α is transcendental over F if and only if $[F(\alpha) : F] = \infty$*
2. *α is algebraic over F if and only if $[F(\alpha) : F] < \infty$*

If $p(x)$ is the minimal polynomial of α over F then we have $[F(\alpha) : F] = \deg p$ and $\{1, \alpha, \ldots, \alpha^{\deg p - 1}\}$ is a basis of $F(\alpha)/F$.

2.16 Example. Let p be a prime and ζ_p be the primitive p^{th} root of unity. It is a root of the cyclotomic polynomial $\Phi_p(x)$. From the assignment, this polynomial is irreducible over $\mathbb{Q}$ and it is monic, so it is the minimal polynomial of ζ_p. Thus $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. $\mathbb{Q}(\zeta_p)$ is called the p^{th} cyclotomic extension of $\mathbb{Q}$.

2.4 Algebraic Extensions

2.17 Theorem. *Let E/F be a field extension. If $[E : F] < \infty$ there exists $\{\alpha_1, \ldots, \alpha_n\} \subseteq E$ such that $F \subsetneqq F(\alpha_1) \subsetneqq F(\alpha_1, \alpha_2) \subsetneqq \cdots F(\alpha_1 \ldots, \alpha_n) = E$*

PROOF: By induction on $[E : F]$. If $[E : F] = 1$, $E = F$ and we are done. Suppose that $[E : F] > 1$. Then there is $\alpha_1 \in E \setminus F$ such that $[E : F] = [E : F(\alpha_1)][F(\alpha_1) : F]$. Since $[F(\alpha_1) : F] > 1$, we get that $[E : F(\alpha_1)] < [E : F]$. Applying the induction hypothesis to $[E : F(\alpha_1)]$, there is $\{\alpha_2, \ldots, \alpha_n\} \subseteq E$ such that $F(\alpha_1) = F_1 \subsetneqq F_1(\alpha_2) \subsetneqq \cdots \subsetneqq F_1(\alpha_2 \ldots, \alpha_n) = E$. It follows that $E = F(\alpha_1)(\alpha_2 \ldots, \alpha_n) = F(\alpha_1 \ldots, \alpha_n)$. □

2.18 Definition. A field extension E/F is algebraic if every $\alpha \in E$ is algebraic over F. Otherwise the extension is transcendental.

2.19 Theorem. *Let E/F be a field extension. If $[E : F] < \infty$ then E/F is algebraic.*

PROOF: Suppose that $[E : F] = n$. For $\alpha \in E$ the elements $\{1, \alpha, \ldots, \alpha^n\}$ are not linearly independent over F. Thus there exist $c_i \in F$, not all zero, such that

$$\sum_{i=0}^{n} c_i \alpha^i = 0$$

Hence α is a root of the polynomial $\sum_{i=0}^{n} c_i x^i \in F[x]$. □

2.20 Theorem. *Let E/F be a field extension. Define the set of algebraic elements to be*

$$L := \{\alpha \in E \mid [F(\alpha) : F] < \infty\}$$

Then L is an intermediate field.

PROOF: If $a, b \in L$, then $[F(a) : F] < \infty$ and $[F(b) : F] < \infty$. Consider the field $F(a, b)$. By assignment 1, we have $[F(a, b) : F(a)] \leq [F(b) : F]$. It follows that

$$[F(a, b) : F] = [F(a, b) : F(a)][F(a) : F] \leq [F(b) : F][F(a) : F] < \infty$$

Thus $F(a, b)/F$ is algebraic, so $a \pm b$, ab, and a/b $(b \neq 0)$ are all in L, so L is a field. □

2.21 Definition. Let E/F be a field extension. The set

$$\overline{F} = \{\alpha \in E \mid [F(\alpha) : F] < \infty\}$$

is called the algebraic closure of F in E.

2.22 Example. Let $\overline{\mathbb{Q}}$ be the algebraic closure of $\mathbb{Q}$ over $\mathbb{C}$. Then $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$ (See assignment 2). In particular, the converse of Theorem 2.19 is false.

2.23 Definition. A field F is said to be algebraically closed if for any algebraic extension E/F, then $E = F$.

Bonus Question: Let F be a field with characteristic p, and assume that $F \subseteq E$, where E is algebraically closed. Is there such a field E/F such that $[E : F] < \infty$?

3 Splitting Fields

3.1 Definition. For a field F, we consider the polynomial ring $F[x]$. For $f(x) \in F[x]$ and a field extension E/F, we say that $f(x)$ splits over E if it is a product of linear factors in $E[x]$. In other words, E contains all roots of $f(x)$. If furthermore there is no proper subfield of E that $f(x)$ splits over, then we say that E is a splitting field of $f(x)$ in E.

3.1 Existence of splitting fields

3.2 Theorem. *Let $p(x) \in F[x]$ be irreducible. The quotient ring $F[x]/\langle p(x)\rangle$ is a field containing F and a root of $p(x)$.*

PROOF: Since $p(x)$ is irreducible, the ideal $I = \langle p(x)\rangle$ is maximal. Hence $E := F[x]/I$ is a field. Consider the map

$$\psi : F \to E : a \mapsto a + I$$

This map is injective since $\ker \psi$ is an ideal of the field F (and hence trivial). By identifying F with $\psi(F)$, F is a subfield of E. Moreover, let $\alpha = x + I \in E$.

Claim. α is a root of $p(x)$

Write $p(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, so $p(x) = (a_0+I) + (a_1+I)x + \cdots + (a_n+I)x^n \in E[x]$. Thus we have

$$p(\alpha) = (a_0+I) + (a_1+I)(x+I) + \cdots + (a_n+I)(x+I)^n = p(x) + I = 0$$

in E. Thus $\alpha = x + I \in E$ is a root of $p(x)$. □

3.3 Theorem. *(Kronecker) Let $f(x) \in F[x]$. There exists a field E/F such that $f(x)$ splits over E*

PROOF: By induction on $\deg f$. If $\deg f = 1$, then $E = F$. If $\deg f > 1$ then write $f(x) = p(x)g(x)$ where $p(x)$ is irreducible. By the previous theorem there is a field K/F containing a root α of $p(x)$. Hence $f(x) = (x-\alpha)h(x)g(x) \in K[x]$, for some $h(x) \in K[x]$. Since $\deg(hg) < \deg f$, by induction there is a field E/K over which gh is a product of linear factors. It follows that $f(x)$ splits over E/F. □

3.4 Theorem. *Every $f(x) \in F[x]$ has a splitting field that is a finite extension of F.*

PROOF: For $f(x) \in F[x]$, there exists a field E/F such that $f(x)$ splits over E. Say $a_1, \ldots, a_n$ are the roots. Consider the algebraic extension $F(a_1, \ldots, a_n)$. This extension is finite, and $f(x)$ splits over $F(a_1, \ldots, a_n)$. Moreover, $f(x)$ does not split over any proper subfield of $F(a_1, \ldots, a_n)$, since any such subfield will omit at least one of the a_i's. Therefore $F(a_1, \ldots, a_n)$ is a splitting field of $f(x)$ in E. □

3.2 Uniqueness of the splitting field

3.5 Lemma. *Let $\varphi : R \to R_1$ be a ring homomorphism. Then there is a unique ring homomorphism $\Phi : R[x] \to R_1[y]$ such that $\Phi|_R = \varphi$ and $\Phi(x) = y$. We say that Φ extends the map φ.*

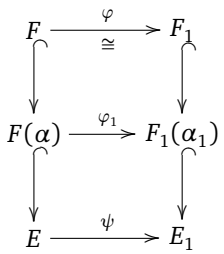
PROOF: Trivial. □

3.6 Theorem. *Let $\varphi : F \to F_1$ be an isomorphism of fields, and $f(x) \in F[x]$. Let $\Phi : F[x] \to F_1[x]$ be the unique ring isomorphism which extends φ and maps x to x. Let $f_1(x) = \Phi(f(x))$ and E/F and E_1/F_1 be splitting fields of f and f_1, respectively. Then there exists an isomorphism $\psi : E \to E_1$ which extends φ.*

PROOF: By induction on $[E : F]$. If $[E : F] = 1$, f is a product of linear factors in $F[x]$. Thus $E = F$ and $E_1 = F_1$. Take $\psi = \varphi$ and we are done. If $[E : F] > 1$ then let $p(x)$ be an irreducible factor of $f(x)$ with $\deg p \geq 2$. Write $p_1(x) = \Phi(p(x))$. Let $\alpha \in E$ and $\alpha_1 \in E_1$ be roots of p and p_1, respectively. Then we have an F-isomorphism $F(\alpha) \cong F[x]/\langle p(x)\rangle$ and an F_1-isomorphism $F_1(\alpha_1) \cong F_1[x]/\langle p_1(x)\rangle$. Consider the isomorphism Φ. Since $p_1(x) = \Phi(p_1(x))$ there must exist a field isomorphism

$$\Phi_1 : F[x]/\langle p(x)\rangle \to F_1[x]/\langle p_1(x)\rangle \cong F_1(\alpha_1)$$

which extends φ. It follows that there exists a field isomorphism $\varphi_1 : F(\alpha) \to F_1(\alpha_1)$ which extends φ and sends α to α_1.



By induction, since $[E : F(\alpha)] < [E : F]$, there exists $\psi : E \to E_1$ which extends φ_1, and thus extends φ. □

3.7 Corollary. *Any two splitting fields of a non-zero polynomial $f(x) \in F[x]$ over F are F-isomorphic.*

3.8 Corollary. *(E.H. Moore) Any two finite fields of order p^n for some prime p are isomorphic.*

PROOF: Any finite field F of order p^n is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ □

3.9 Theorem. *Let F be a field and $f(x) \in F[x]$ have degree $n \geq 1$. Let E/F be a splitting field of $f(x)$. Then $[E : F]$ divides $n!$.*

PROOF: By induction on $\deg f$. If $\deg f = 1$ then $[E : F] = 1$ and it's trivial. Suppose $\deg f > 1$. If f is irreducible and $\alpha \in E$ is a root of f, then there exists a simple extension $F(\alpha)/F$ such that $F(\alpha) \cong F[x]/\langle f(x)\rangle$ and $[F(\alpha) : F] = \deg f = n$. Write $f(x) = (x - \alpha)g(x) \in F(\alpha)[x]$ and $\deg g = n - 1$. By induction, $[E : F(\alpha)]$ is a divisor of $(n-1)!$. It follows that $[E : F] = [E : F(\alpha)][F(\alpha) : F]$ divides $n!$. If $f(x)$ is not irreducible, write $f = g \cdot h$, where $\deg g = m$ and $\deg h = k$. Let K be a splitting field of g over F. By induction, $[K : F]$ divides $m!$. Also, $[E : K]$ divides $k!$ (E is a splitting field of h over K). Thus $[E : F]$ divides $m!k!$, which is a factor of $n!$. □

4 Separable Polynomials

4.1 Prime Fields

4.1 Definition. The prime field of a field F is the intersection of all of the subfields of F.

4.2 Theorem. *If F is a field, then its prime field is isomorphic to $\mathbb{Q}$ or to $\mathbb{F}_p$ for some prime p.*

PROOF: Consider the ring map

$$\chi : \mathbb{Z} \to F : n \mapsto \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}}$$

Let $I = \ker \chi$. Then $\mathbb{Z}/I$ is a domain (since it is isomorphic to the image of $\chi(\mathbb{Z})$, a subring of F). Hence I is a prime ideal of $\mathbb{Z}$, and so either is $\langle 0\rangle$ or $\langle p\rangle$ for some prime p. If $I = \langle 0\rangle$ then $\mathbb{Z} \subseteq F$. It follows that all subfields of F contain $\mathrm{Frac}(F) = \mathbb{Q}$, and so the prime field of F is $\mathbb{Q}$. If $I = \langle p\rangle$ then by the first isomorphism theorem,

$$\mathbb{F}_p \cong \mathbb{Z}/\langle p\rangle \cong \operatorname{Im}\chi \subseteq F$$

and so the prime field of F is $\mathbb{F}_p$. □

4.3 Definition. Given a field F, if the prime field is isomorphic to $\mathbb{Q}$ then we say that F has characteristic 0, denoted $\operatorname{ch} F = 0$. On the other hand, if the prime field is isomorphic to $\mathbb{F}_p$ then we say $\operatorname{ch} F = p$. Notice that if $\operatorname{ch} F = p$ then $(a + b)^p = a^p + b^p$.

4.2 Formal Derivative and Repeated Roots

4.4 Definition. If F is a field, the monomials $\{1, x, x^2, \dots\}$ form an F-basis for $F[x]$. Define the linear operator $\mathrm{D} : F[x] \to F[x]$ by $\mathrm{D}1 = 0$ and $\mathrm{D}x^n = nx^{n-1}$. D is called the formal derivative, and is also denoted with a prime.

The formal derivative has all the usual algebraic properties of the differential operator from calculus, in particular

1. $\mathrm{D}(f + g) = \mathrm{D}f + \mathrm{D}g$
2. $\mathrm{D}(fg) = (\mathrm{D}f)g + f(\mathrm{D}g)$

4.5 Theorem. *Let F be field and $f(x) \in F[x]$.*

1. *If $\mathrm{ch}F = 0$ and $Df = 0$ then $f(x) = c$ for some $c \in F$*
2. *If $\mathrm{ch}F = p$ and $Df = 0$ then $f(x) = g(x^p)$ for some $g(x) \in F[x]$*

PROOF: Trivial. □

4.6 Definition. Let E/F be a field extension and $f(x) \in F[x]$. We say that $\alpha \in E$ is a repeated root of $f(x)$ if $f(x) = (x-\alpha)^2 g(x)$ for some $g(x) \in E[x]$.

4.7 Lemma. *If $E[x]$, α is a repeated root of $f(x)$ if and only if $x - \alpha$ divides both f and Df.*

PROOF: If $f(x) = (x-\alpha)^2 g(x)$ then $\mathrm{D}f(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 \mathrm{D}g(x)$, so $x-\alpha$ is a common factor of f and $\mathrm{D}f$. Suppose conversely that $x-\alpha$ divides both f and $\mathrm{D}f$. Write $f(x) = (x-\alpha)h(x)$, for some $h(x) \in E[x]$. Then $\mathrm{D}f(x) = h(x) + (x-\alpha)\mathrm{D}h(x)$. $\mathrm{D}f(\alpha) = 0$ implies that $h(\alpha) = 0$, and so we are done. □

4.8 Theorem. *Let $f(x) \in F[x]$. Then f has no repeated roots in any extension of F if and only if* $\gcd(f, Df) = 1$ *in $F[x]$*

Notice that the condition of repeated roots depends on the extension of F, while the gcd condition involves only F.

PROOF: Let $g = \gcd(f, \mathrm{D}f)$. Write $g = sf + t\mathrm{D}f$ for some polynomials $s(x), t(x) \in F[x]$ ($F[x]$ is a Euclidean domain). Suppose $f(x)$ has a repeated root α in some extension E/F. Then clearly $x-\alpha$ is a common factor of f and $\mathrm{D}f$, and so $g \neq 1$. Suppose now that $g \neq 1$. Then there is an extension E/F such that E contains a root α of g. Then $x-\alpha$ divides both f and $\mathrm{D}f$, and so α is a repeated root of f. □

4.3 Separable Polynomials

4.9 Definition. Let F be a field and $f(x) \in F[x]$ not zero. If $f(x)$ is irreducible, then we say $f(x)$ is separable over F if it has no repeated roots in any extension of F. If $f(x)$ is not irreducible, then we say it is separable if all of it's irreducible factors are separable.

4.10 Example. Consider the polynomial $f(x) = x^t - a \in F[x]$, with $t \geq 2$. If $a = 0$, then f is clearly separable, as the only irreducible factor of f is x. A linear polynomial is always separable. Now we assume that $a \neq 0$. Note that $\mathrm{D}f(x) = tx^{t-1}$.

1. If $\mathrm{ch}F = 0$ then $\gcd(f, \mathrm{D}f) = 1$, so f is separable.
2. If $\mathrm{ch}F = p$ and $\gcd(p, t) = 1$ then $\gcd(f, \mathrm{D}f) = 1$, so f is separable.
3. If $\mathrm{ch}F = p$ and $t = p$ then $\mathrm{D}f = 0$, so $\gcd(f, \mathrm{D}f) \neq 1$. However, it is still possible that all of the irreducible factors $p(x)$ have the property that $\gcd(p, \mathrm{D}p) = 1$. To decide, we need to find the irreducible factors of f. Define $F^p = \{a^p \mid a \in F\}$, a subfield of F. If $a \in F^p$ then there is some $b \in F$ such that $a = b^p$, and so $f(x) = (x-b)^p$, and f is separable. There is another case, although it only comes up if F is an infinite field of characteristic p. If $a \notin F^p$ then we claim that $f(x) = x^p - a$ is irreducible. Assume that we may write $x^p - a = g(x)h(x)$, where $g, h \in F[x]$ are monic. Let E/F be a extension such that $x^p - a$ has a root $\beta \in E$. Then $\beta^p = a$, and so $\beta \notin F$. We have

$$x^p - a = x^p - \beta^p = (x-\beta)^p$$

Thus $g(x) = (x-\beta)^r$ and $h(x) = (x-\beta)^s$ for some $r+s = p$. Write $g(x) = x^r + r\beta x^{r-1} + \cdots$. Then since $r\beta \in F$, $r = 0$ in F. Thus $r = kp$ for some k. This shows that either $r = 0$ or $s = 0$, and so $x^p - a$ is irreducible over F. Therefore $x^p - a$ is not separable in this case. We say that f is purely inseparable since all of the roots of f are the same.

4.4 Perfect Fields

4.11 Definition. A field F is called perfect if every irreducible polynomial $f(x) \in F[x]$ is separable.

4.12 Theorem. *Let F be a field.*

1. *If $\mathrm{ch}F = 0$ then F is perfect.*
2. *If $\mathrm{ch}F = p$ and $F^p = F$ then F is perfect.*

PROOF: Let $r(x) \in F[x]$ be irreducible. Then either $\gcd(r, \mathrm{D}r) = 1$ or $\gcd(r, \mathrm{D}r) = r$.

1. Let $\mathrm{ch}\,F = 0$. Suppose that r is not separable, that is, $\gcd(r, \mathrm{D}r) = r$. Then $\mathrm{D}r = 0$, and so $\deg r = 0$, a contradiction. Therefore r is separable and F is perfect.
2. Let $\mathrm{ch}\,F = p$. Suppose that r is not separable, that is, $\gcd(r, \mathrm{D}r) = r$. Then $\mathrm{D}r = 0$ in $F[x]$. Write

$$r(x) = a_0 + a_1 x^p + \cdots + a_m x^{mp},\ a_i \in F$$

Since $F^p = F$, we can write $a_i = b_i^p$ for some $b_i \in F$. Thus

$$r(x) = b_0^p + b_1^p x^p + \cdots + b_m^p x^{mp} = (b_0 + b_1 x + \cdots + b_m x^m)^p$$

which is a contradiction since r is irreducible. Thus r is separable and F is perfect. □

4.13 Corollary. *Every finite field is perfect. (Assignment 3)*

Recall that if E/F is a finite extension then there exist $\alpha_1, \ldots, \alpha_n \in E$ such that

$$F \subsetneqq F(\alpha_1) \subsetneqq \cdots \subsetneqq F(\alpha_1, \ldots, \alpha_n) = E$$

4.14 Theorem. *If $\mathrm{ch}F = 0$ and E/F is a finite extension then E/F is a simple extension.*

PROOF: Since $E = F(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in E$, it suffices to consider the case when $E = F(\alpha, \beta)$. The general case follows by induction. Let $E = F(\alpha, \beta)$. Our goal is to find $\gamma \in E$ such that $E = F(\gamma)$. It suffices to find $\lambda \in F$ such that $\gamma = \alpha + \lambda\beta$ and $\beta \in F(\gamma)$ because then we will have $F(\alpha, \beta) \subseteq F(\gamma)$ (the reverse containment is clear).

Let $a(x)$ and $b(x)$ be the minimal polynomials of α and β over F, respectively. Choose $\lambda \in F$ such that

$$\lambda \neq \frac{\tilde{\alpha} - \alpha}{\tilde{\beta} - \beta}$$

where $\tilde{\alpha}$ runs over all the roots of a in E, and $\tilde{\beta}$ runs over all of the roots of b in E that are not β. We can do this because there are infinitely many elements in F, but only finitely many excluded choices. Let $\gamma = \alpha + \lambda\beta$. Consider $h(x) = a(\gamma - \lambda x) \in F(\gamma)[x]$. Then β is a root of h. However, for all $\tilde{\beta} \neq \beta$, since

$$\gamma - \lambda\tilde{\beta} = \alpha + \lambda(\beta - \tilde{\beta}) \neq \tilde{\alpha}$$

by the choice of λ, we have that $h(\tilde{\beta}) \neq 0$. Thus h and b have β as a common root, but no others in any extension of $F(\gamma)$. The minimal polynomial of β in $F(\gamma)$, call it $b_1(x)$, must divide h and b. Since $\mathrm{ch}\,F = 0$ and b_1 is irreducible, b_1 has distinct roots. The roots of b_1 are also roots of b and h. Since β is the only common root, $b_1(x) = x - \beta$, and so $\beta \in F(\gamma)$. □

Remark. This a special case of a more general result called the Primative Element Theorem that we will see later.

5 Automorphism Groups

5.1 Automorphism Groups

5.1 Definition. If E is a field, we say that a map $\psi : E \to E$ is an automorphism if it is an isomorphism of E. If E/F is a field extension and $\psi : E \to E$ is an automorphism which fixes F, we say that ψ is an F-automorphism of E. By map composition, the set

$$\mathrm{Aut}_F(E) = \{\psi : E \to E \mid \psi \text{ is an } F\text{-automorphism}\}$$

is called the automorphism group of E/F. It may also be denoted $\mathrm{Aut}(E/F)$.

5.2 Lemma. *Let $f(x) \in F[x]$ and $\alpha \in E$ a root of $f(x)$. For $\psi \in \mathrm{Aut}_F(E)$, $\psi(\alpha)$ is also a root of $f(x)$. Notice that E does not have to be the splitting field of $f(x)$.*

PROOF: If $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ then we have

$$\begin{aligned} f(\psi(\alpha)) &= a_0 + a_1\psi(\alpha) + \cdots + a_n\psi(\alpha)^n \\ &= \psi(a_0) + \psi(a_1\alpha) + \cdots + \psi(a_n\alpha^n) \\ &= \psi(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \psi(0) = 0 \end{aligned}$$

Thus $\psi(\alpha)$ is a root of $f(x)$. □

5.3 Lemma. *Let $E = F(\alpha_1, \ldots, \alpha_n)$ be a field extension. For $\psi_1, \psi_2 \in \mathrm{Aut}_F(E)$, if $\psi_1(\alpha_i) = \psi_2(\alpha_i)$ for all $i = 1, \ldots, n$ then $\psi_1 = \psi_2$.*

PROOF: Trivial. □

5.4 Corollary. *If E/F is a finite extension then $\mathrm{Aut}_F(E)$ is a finite group.*

5.2 Automorphism Groups of Polynomials

5.5 Definition. Let F be a field and $f(x) \in F[x]$. The automorphism group of $f(x)$ over F is defined to be the group $\mathrm{Aut}_F(E)$, where E is a splitting field of $f(x)$. Notice that this definition does not depend on the choice of E. By a previous theorem all splitting fields of $f(x)$ are isomorphic, and hence their automorphism groups are isomorphic.

5.6 Theorem. *Let E/F be a splitting field of a non-zero polynomial $f(x) \in F[x]$. Then $|\mathrm{Aut}_F(E)| \leq [E : F]$, and equality holds if and only if $f(x)$ is separable over F.*

PROOF: Assignment 3. □

5.7 Example.

1. Let F be a field with $\mathrm{ch}\, F = p$. Let $a \in F \setminus F^p$ and E/F a splitting field of the polynomial $f(x) = x^p - a$. We have seen before that $x^p - a = (x - \beta)^p$, for some $\beta \in E \setminus F$. Thus $E = F(\beta)$, and since β can only map to β, $\mathrm{Aut}_F(E)$ is the trivial group. Notice that $|\mathrm{Aut}_F(E)| = 1$ while $[E : F] = p$.
2. Consider $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is the splitting field of $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. $f(x)$ is separable, so $|\mathrm{Aut}_F(E)| = [E : F] = 4$. It follows that $\mathrm{Aut}_F(E)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, as $\mathrm{Aut}_F(E)$ has not elements of order 4.

3. Consider the irreducible polynomial $x^3-2 \in \mathbb{Q}[x]$. Let $\zeta_3 = e^{2\pi i/3}$. The roots of x^3-2 are $\{\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2\}$, and thus the splitting field of x^3-2 is

$$E = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

Let $L = \mathbb{Q}(\sqrt[3]{2})$ be a subfield of E containing $\mathbb{Q}$. We consider $\mathrm{Aut}_{\mathbb{Q}}(L)$ and $\mathrm{Aut}_{\mathbb{Q}}(E)$. L contains only one root of x^3-2 since it is a real field, and so $\mathrm{Aut}_{\mathbb{Q}}(L)$ is the trivial group. E is the splitting field of a separable polynomial, so $|\mathrm{Aut}_{\mathbb{Q}}(E)| = [E:\mathbb{Q}] = 6$. By the next theorem, we see that it is a subgroup of $\mathfrak{S}_3$, so $\mathrm{Aut}_{\mathbb{Q}}(E) \cong \mathfrak{S}_3$. We notice from this example that the automorphism group is not always Abelian.

Open Problem: Does every finite group occur as the automorphism group over $\mathbb{Q}$ of the splitting field of some polynomial? It is known that every finite Abelian group does occur.

5.8 Theorem. *If $f(x) \in F[x]$ has n distinct roots in its splitting field E then $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup of the symmetric group $\mathfrak{S}_n$. In particular, $|\mathrm{Aut}_F(E)|$ divides $n!$.*

PROOF: Let $X = \{\alpha_1, \ldots, \alpha_n\}$ be the distinct roots of $f(x)$ in E. If $\psi \in \mathrm{Aut}_F(E)$, then $\psi(X) = X$. From this observation and the fact that ψ is uniquely determined by its action on X, it is clear that $\mathrm{Aut}_F(E)$ is isomorphic to a subgroup of the symmetric group on X, which itself is isomorphic to $\mathfrak{S}_n$, with an injective homomorphism given by $\psi \mapsto \psi|_X$. □

5.3 Fixed Fields

5.9 Definition. Let E/F be a field extension and $\varphi \in \mathrm{Aut}_F(E)$. Define

$$E^{\varphi} = \{a \in E \mid \varphi(a) = a\}$$

which is necessarily a subfield of E that contains F. We usually call E^{φ} the fixed field of φ. Let G be a subgroup of $\mathrm{Aut}_F(E)$. The fixed field of G is defined to be

$$E^G = \bigcap_{\psi \in G} E^{\psi} = \{a \in E \mid \psi(a) = a \ \forall\, \psi \in G\}$$

5.10 Theorem. *Let $f(x) \in F[x]$ be a separable polynomial and E/F its splitting field. Then $E^{\mathrm{Aut}_F(E)} = F$.*

PROOF: Let $G = \mathrm{Aut}_F(E)$ and $L = E^G$. Clearly $F \subseteq L$, and thus $\mathrm{Aut}_L(E) \subseteq \mathrm{Aut}_F(E)$. If $\psi \in \mathrm{Aut}_F(E) = G$ then for all $a \in L$, $\psi(a) = a$. That is, $\psi \in \mathrm{Aut}_L(E)$, and thus $\mathrm{Aut}_L(E) = \mathrm{Aut}_F(E)$. Because $f(x)$ is separable over F and splits over E, $f(x)$ is also separable over L and has E as its splitting field over L. It follows that $[E:L] = |\mathrm{Aut}_L(E)| = |\mathrm{Aut}_F(E)| = [E:F]$ Since $[E:F] = [E:L][L:F]$, it follows that $[L:F] = 1$ and so $L = F$. □

6 Galois Extensions

6.1 Separable Extensions

6.1 Definition. Let E/F be an algebraic field extension. For $\alpha \in E$, let $p(x) \in F[x]$ be the minimal polynomial of α. We say that α is separable over F if $p(x)$ is separable. If α is separable for all $\alpha \in E$ then we say that the extension E/F is separable.

6.2 Theorem. *Let E/F be a splitting field of $f(x) \in F[x]$. If $f(x)$ is separable then E/F is a separable extension.*

PROOF: If $\operatorname{ch} F = 0$ then F is perfect and every extension is separable. If $\operatorname{ch} F = p$ then consider $\alpha \in E$. Let $p(x) \in F[x]$ be the minimal polynomial of α. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the distinct roots of $p(x)$ that are contained in E. We claim that $p(x) = (x - \alpha_1) \cdots (x - \alpha_n)$. It suffices to show that

$$\tilde{p}(x) := (x - \alpha_1) \cdots (x - \alpha_n)$$

is in $F[x]$, since $p(x)$ is the minimal polynomial of α and $\tilde{p}(x)$ has α as a root. Let $\psi \in \operatorname{Aut}_F(E)$. ψ permutes $\alpha_1, \ldots, \alpha_n$ and the coefficients of $\tilde{p}$ are symmetric with respect to $\alpha_1, \ldots, \alpha_n$, so each coefficient of $\tilde{p}(x)$ is fixed with respect to ψ. Therefore $\tilde{p}(x) \in E^{\psi}[x]$. Since ψ was arbitrary, $\tilde{p}(x) \in E^{\operatorname{Aut}_F(E)}[x] = F[x]$. □

6.3 Corollary. *Let E/F be a finite extension and $E = F(\alpha_1, \ldots, \alpha_n)$. If each α_i is separable over F then E/F is separable.*

PROOF: For $1 \leq i \leq n$, let $p_i(x) \in F[x]$ be the minimal polynomial of α_i. Let $f(x) = \prod_{i=1}^{n} p_i(x)$. Then $f(x)$ is separable. Let L be the splitting field of f, so that L/F is separable. Since $E = F(\alpha_1, \ldots, \alpha_n)$ is a subfield of L, E is also separable. □

6.4 Corollary. *Let E/F be an algebraic extension and L be the set of all $\alpha \in E$ that are separable over F. Then L is an intermediate field.*

6.2 Normal extensions

6.5 Definition. Let E/F be an algebraic extension. We say that E/F is a normal extension if given any irreducible polynomial $p(x) \in F[x]$, either $p(x)$ has no root in E or E contains all of the roots of $p(x)$. In other words, if $p(x)$ has a root in E then $p(x)$ splits over E.

6.6 Example. Let $\alpha \in \mathbb{R}$ such that $\alpha^4 = 5$ and let $\beta = (1 + i)\alpha$. Consider the field extension $\mathbb{Q}(\beta)/\mathbb{Q}$. Notice that $\beta^2 = 2i\alpha^2$, and so $\beta^4 = -20$. Hence the minimal polynomial of β over $\mathbb{Q}$ is $x^4 + 20$ and $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. The roots of $x^4 + 20$ are $\pm\beta, \pm i\beta$. It is sufficient to show that $\alpha \notin \mathbb{Q}(\beta)$ to show that $i\beta \notin \mathbb{Q}(\beta)$. The minimal polynomial of α is $x^4 - 5$, and so we have that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Notice that if $\alpha \in \mathbb{Q}(\beta)$ then $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, and this is impossible since $\mathbb{Q}(\alpha)$ is a real field while $\mathbb{Q}(\beta)$ is not. It follows that the prime factorization of $x^4 + 20$ over $\mathbb{Q}(\beta)$ is $(x - \beta)(x + \beta)(x^2 + \beta^2)$, and hence it does not split over $\mathbb{Q}(\beta)$, so $\mathbb{Q}(\beta)$ is not a normal extension of $\mathbb{Q}$.

6.7 Theorem. *A finite extension E/F is normal if and only if it is the splitting field of some polynomial $f(x) \in F[x]$.*

PROOF: Suppose that E/F is a finite extension and is normal. Let $E = F(\alpha_1, \ldots, \alpha_n)$. For each i, let $p_i(x)$ be the minimal polynomial of α_i. Define $f(x) = \prod_{i=1}^{n} p_i(x)$. Since E/F is normal, each $p_i(x)$ splits over E, say $\alpha_{i,1}, \ldots, \alpha_{i,r_i}$ are the roots of $p_i(x)$ over E. Thus

$$E = F(\alpha_1, \ldots, \alpha_n) = F(\alpha_{1,1}, \ldots, \alpha_{1,r_i}, \alpha_{2,1}, \ldots, \alpha_{n,r_i})$$

Therefore E is a splitting field of $f(x)$ over F.

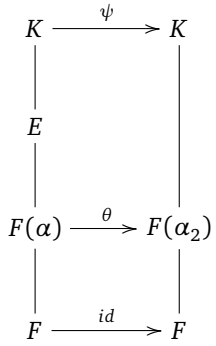
Now suppose that E/F is the splitting field of $f(x) \in F[x]$. Let $p(x) \in F[x]$ be an irreducible polynomial with a root $\alpha \in E$. Let K/E be a splitting field of $p(x)$ over E. Write

$$p(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$$

where $0 \neq c \in F$ and $\alpha = \alpha_1, \ldots, \alpha_n \in K = E(\alpha_1, \ldots, \alpha_n)$. Define an F-isomorphism

$$\theta : F(\alpha) \to F(\alpha_2) : \alpha \mapsto \alpha_2$$

Note that $p(x) \in F(\alpha)[x], F(\alpha_2)[x]$. Hence we can view K as a splitting field of $p(x)f(x)$ over $F(\alpha)$ and $F(\alpha_2)$ respectively. Thus there exists an isomorphism $\psi : K \to K$ which extends θ.

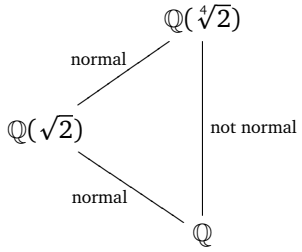


Since $\psi \in \mathrm{Aut}_F(K)$, ψ permutes the roots of $f(x)$. Since E is generated over F by the roots of $f(x)$, we have $\psi(E) = E$. It follows that for $\alpha \in E$, $\alpha_2 = \psi(\alpha) \in E$. Since the choice of α_2 was arbitrary, $\alpha_i \in E$ for all i. Therefore $K = E$ and $p(x)$ splits over E and E is normal. □

6.8 Example. Every quadratic extension is normal. Let E/F be a quadratic extension. For $\alpha \in E \setminus F$, $E = F(\alpha)$. Let $p(x) = x^2 + ax + b$ be the minimal polynomial of α over F. Then $-a - \alpha \in F(\alpha)$ is the other root of p, and so E is the splitting field of p. Therefore E/F is normal.

$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal since the irreducible polynomial $x^4 - 2$ does not split over $\mathbb{Q}(\sqrt[4]{2})$ despite having a root in $\mathbb{Q}(\sqrt[4]{2})$. Note that the extension $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is made up of two quadratic extensions

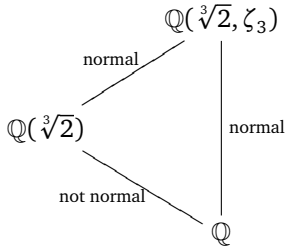
$$\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2}) \text{ and } \mathbb{Q}(\sqrt{2})/\mathbb{Q}$$



6.9 Proposition. *If E/F is a normal extension and K is an intermediate field then E/K is normal.*

PROOF: Let $p(x) \in K[x]$ be irreducible and have a root $\alpha \in E$. Let $f(x) \in F[x]$ be the minimal polynomial of α over F. Then $f(x)$ splits over E since E/F is normal, and $p(x)|f(x)$. It follows that $p(x)$ splits over E as well, so E/K is a normal extension. □

Remark. K/F is not always normal. Take $F = \mathbb{Q}, K = \mathbb{Q}(\sqrt[3]{2}), E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Then E/F is normal but K/F is not.



6.3 Conjugates

6.10 Definition. Let E/F be a field extension and $\alpha, \beta \in E$. If α and β have the same minimal polynomial then they are said to be *conjugate* over F.

It is clear that a field extension E/F is normal if and only if for every $\alpha \in E$, E contains all of the conjugates of α over F.

6.11 Proposition. *Let E/F be a finite normal extension and $\alpha, \beta \in E$. Then the following are equivalent*

1. *α and β are conjugate over F*
2. *there exists $\psi \in \mathrm{Aut}_F(E)$ such that $\psi(\alpha) = \beta$*

PROOF: Suppose that $p(x) \in F[x]$ is the minimal polynomial of both α and β. Then

$$F(\alpha) \cong F[x]/\langle p(x) \rangle \cong F(\beta)$$

and so there is an F-isomorphism $\theta : F(\alpha) \to F(\beta) : \alpha \mapsto \beta$. Now E/F is a finite normal extension, so by an above theorem, E is the splitting field of some polynomial $f(x) \in F[x]$. We can also view E as a splitting field of $f(x)$ over $F(\alpha)$ and $F(\beta)$ respectively. Thus, there exists an isomorphism $\psi : E \to E$ which extends θ. It follows that $\psi \in \mathrm{Aut}_F(E)$ and $\psi(\alpha) = \beta$.

Now suppose that there is $\psi \in \mathrm{Aut}_F(E)$ with $\psi(\alpha) = \beta$. Let $p(x) \in F[x]$ be the minimal polynomial of α over F. Then

$$p(\beta) = p(\psi(\alpha)) = \psi(p(\alpha)) = \psi(0) = 0$$

so β is a root of $p(x)$. Therefore $p(x)$ must be the minimal polynomial of β as well. □

6.12 Definition. A normal closure of a finite extension E/F is a finite normal extension N/F which has the following properties

1. E is a subfield of N
2. If L is any intermediate field of N/E and L is normal over F then $L = N$.

6.13 Theorem. *Every finite extension E/F has a normal closure N/F. Moreover, N is unique up to E-isomorphism.*

PROOF: (Existence) Write $E = F(\alpha_1, \ldots, \alpha_n)$. Let $p_i(x) \in F[x]$ be the minimal polynomial of α_i, and let $f(x) = \prod_{i=1}^{n} p_i(x)$. Let N/E be the splitting field of $f(x)$ over E. Then N is a normal extension of F (since is it also the splitting field of $f(x)$ over F) that contains E. If $N \supset L \supset E$ is normal then $f(x)$ splits over L since each irreducible factor of $f(x)$ has a root in L. Thus $L = N$, so N is a normal closure of E/F.

(Uniqueness) Let N_1 be another normal closure of E/F. Since N_1 is normal over F and contains $\alpha_1, \ldots, \alpha_n$, N_1 must contain a splitting field N_2 of $f(x)$ over F with $E \subseteq N_2$. Since N_2 is normal over F, we must have $N_1 = N_2$. Therefore N_1 are N are splitting fields of $f(x)$ over F, and hence over E, so they are E-isomorphic by Theorem 3.6. □

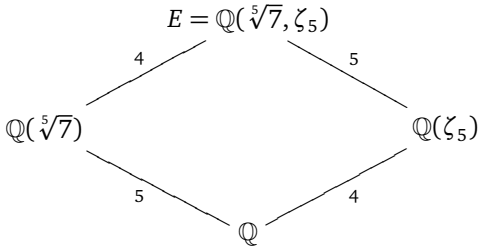
6.4 Galois Extensions

6.14 Definition. An algebraic extension E/F is Galois if it is normal and separable. If E/F is a Galois extension then the Galois group of E over F is defined to be $\mathrm{Aut}_F(E)$, denoted $\mathrm{Gal}_F(E)$.

Remark.
1. Notice that by the last two sections, the finite Galois extensions of F are exactly the splitting fields of separable polynomials in $F[x]$.
2. If E/F is a finite Galois extension then $|\mathrm{Gal}_F(E)| = [E : F]$

3. If E/F the splitting field of a separable polynomial $f(x)$ of degree n then $\mathrm{Gal}_F(E)$ is a subgroup of $\mathfrak{S}_n$.

6.15 Example. Let E be the splitting field of x^5-7 over $\mathbb{Q}$. Then $E=\mathbb{Q}(\sqrt[5]{7},\zeta_5)$. The minimal polynomials of $\sqrt[5]{7}$ and ζ_5 over $\mathbb{Q}$ are x^5-7 and $x^4+x^3+x^2+x+1$, respectively. Since $[\mathbb{Q}(\sqrt[5]{7}):\mathbb{Q}]=5$ and $[\mathbb{Q}(\zeta_5):\mathbb{Q}]=4$ are divisors of $[E:\mathbb{Q}]$, $[E:\mathbb{Q}]$ is divisible by 20. Since $[E:\mathbb{Q}]=[E:\mathbb{Q}(\zeta_5)][\mathbb{Q}(\zeta_5):\mathbb{Q}]$ and $\mathbb{Q}(\zeta_5):\mathbb{Q}]=4$, we may conclude that $[E:\mathbb{Q}(\zeta_5)]\geq 5$. Also, $E=\mathbb{Q}(\sqrt[5]{7},\zeta_5)=\mathbb{Q}(\zeta_5)(\sqrt[5]{7})$ and the minimal polynomial of $\sqrt[5]{7}$ over $\mathbb{Q}(\zeta_5)$ is a factor of x^5-7. Thus $[E:\mathbb{Q}(\zeta_5)]\leq 5$, and so $[E:\mathbb{Q}(\zeta_5)]=5$.



Then for $\psi\in\mathrm{Gal}_{\mathbb{Q}}(E)$, ψ is determined by its action on the roots of x^5-7, so denote $\psi=\psi_{k,s}$ with $1\leq s,k\leq 5$ if $\psi(\sqrt[5]{7})=\sqrt[5]{7}\zeta_5^k$ and $\psi(\zeta_5)=\zeta_5^s$. We have the following identity (Check this)

$$\psi_{k_1,s_1}\circ\psi_{k_2,s_2}=\psi_{k_1+s_1k_2,s_1s_2}$$

There are two ways to view $\mathrm{Gal}_{\mathbb{Q}}(E)$

1. $\mathrm{Gal}_{\mathbb{Q}}(E)$ can be viewed as a group of permutations of the roots of x^5-7. Identity the roots of x^5-7 with the elements of $\{1,2,3,4,5\}$ as $\ell\longleftrightarrow\sqrt[5]{7}\zeta_5^{\ell}$. Then, for example, we may view $\psi_{2,3}$ as (5 2 3 1).
2. We can also understand $\mathrm{Gal}_{\mathbb{Q}}(E)$ in terms of matrix groups. notice that

$$\begin{pmatrix}s_1&k_1\\0&1\end{pmatrix}\cdot\begin{pmatrix}s_2&k_2\\0&1\end{pmatrix}=\begin{pmatrix}s_1s_2&k_1+s_1k_2\\0&1\end{pmatrix}$$

Thus we can associate $\psi_{k,s}\in\mathrm{Gal}_{\mathbb{Q}}(E)$ with the matrix

$$\begin{pmatrix}s&k\\0&1\end{pmatrix}\in GL_2(\mathbb{F}_5)$$

and the map composition law in $\mathrm{Gal}_{\mathbb{Q}}(E)$ is preserved by the matrix mulitplication. Thus we have that

$$\mathrm{Gal}_{\mathbb{Q}}(E)\cong\left\{\begin{pmatrix}s&k\\0&1\end{pmatrix}\,\middle|\,s\in\mathbb{F}_5^*,k\in\mathbb{F}_5\right\}$$

6.5 Artin's Theorem

6.16 Theorem. *(E. Artin) Let E be a field and G a finite subgroup of* $\mathrm{Aut}(E)$*. Then E/E^G is a finite Galois extension with $G=Gal_{E^G}(E)$. In particular, $[E:E^G]=|G|$.*

PROOF: Let $n=|G|$ and $F=E^G$. For any $\alpha\in E$, consider the G-orbit of α, that is, the set

$$\{\psi(\alpha)\mid\psi\in G\}=\{\alpha=\alpha_1,\ldots,\alpha_m\}$$

where the α_i are distinct and $m \leq n$. Let $f(x) = (x-\alpha_1)\dots(x-\alpha_m)$. For any $\psi \in G$, ψ permutes the roots $\{\alpha_1,\dots,\alpha_m\}$. Thus $f(x) \in E^G[x] = F[x]$. Let $g(x)$ be a factor of $f(x)$. Without loss of generality, we may write $g(x) = (x-\alpha_1)\dots(x-\alpha_\ell)$ for some $\ell \leq m$. If $\ell \neq m$, choose $\psi \in G$ such that $\{\alpha_1,\dots,\alpha_m\} \neq \{\psi(\alpha_1),\dots,\psi(\alpha_m)\}$. It follows that $\psi(g(x)) = (x-\psi(\alpha_1))\dots(x-\psi(\alpha_\ell)) \neq g(x)$. Thus, if $\ell \neq m$ then $g(x) \notin F[x]$. Thus $f(x)$ is irreducible over F, and so is the minimal polynomial of α over F. Since $f(x)$ is separable and splits over E, this shows that E/F is Galois.

Now consider $[E:F]$. We show first that $[E:F] \leq n$. If $[E:F] > n = |G|$ then we can choose $\alpha_1,\dots,\alpha_{n+1} \in E$ which are linearly independent over F. Consider the system

$$\psi(\alpha_1)v_1 + \dots + \psi(\alpha_{n+1})v_{n+1} = 0 \text{ as } \psi \text{ ranges over } G$$

of linear equations in $n+1$ variables $v_1,\dots,v_{n+1}$. It has a non-trivial solution in $(\beta_1,\dots,\beta_{n+1})$ in E. Assume that $(\beta_1,\dots,\beta_{n+1})$ has the minimal number of non-zero coordinates, say r. Clearly, $r > 1$ and without loss of generality we may assume that $\beta_1,\dots,\beta_r \neq 0$ and $\beta_{r+1},\dots,\beta_{n+1} = 0$. Furthermore, we may assume that $\beta_r = 1$. Thus

$$\psi(\alpha_1)\beta_1 + \dots + \psi(\alpha_r)\beta_r = 0 \text{ for all } \psi \in G \qquad (*)$$

and taking $\psi = id_E$ we get that $\alpha_1\beta_1 + \dots + \alpha_r\beta_r = 0$, so we may assume that $\beta_1 \notin F$ since $\alpha_1,\dots,\alpha_{n+1}$ are linearly independent in F. Choose $\phi \in G$ such that $\phi(\beta_1) \neq \beta_1$. Applying ϕ to $(*)$ yeilds

$$(\phi\circ\psi)(\alpha_1)\phi(\beta_1) + \dots + (\phi\circ\psi)(\alpha_r)\phi(\beta_r) = 0 \text{ for all } \psi \in G$$

But $\beta_r = 1$, so $\phi(\beta_r) = \beta_r$, and subtracting this equation from (1) gives us a solution with strictly fewer non-zero coordinates. This contradiction shows that $[E:F] \leq n$. We have seen that E/F is a finite Galois extension, thus E is a splitting field of some separable polynomial $g(x) \in F[x]$. Also, since $F = E^G$, G is a subgroup of $\mathrm{Gal}_F(E)$. But then $n = |G| \leq |\mathrm{Gal}_F(E)| = [E:F] \leq n$. Therefore $[E:F] = n$ and $G = \mathrm{Gal}_F(E)$. □

Remark. Let E/F be a Galois extension with Galois group G. For $\alpha \in E$ let $\{\alpha = \alpha_1,\dots,\alpha_n\}$ be the G-orbit of α. This is the set of all conjugate roots of α. Then the minimal polynomial of α over F is $(x-\alpha_1)\dots(x-\alpha_n)$.

6.17 Example. Let $E = F(t_1,\dots,t_n)$ be the function field in n variables over F. Consider the symmetric group $\mathfrak{S}_n$ as a subgroup of $\mathrm{Aut}_F(E)$ which permutes the variables $t_1,\dots,t_n$. We would like to find $E^{\mathfrak{S}_n}$. The $\mathfrak{S}_n$-orbit of t_1 is $\{t_1,\dots,t_n\}$. It follows that the minimal polynomial of t_1 over $E^{\mathfrak{S}_n}$ is

$$f(x) = (x-t_1)\dots(x-t_n)$$

Recall the the elementary symmetric functions in $t_1,\dots,t_n$ are

$$\begin{aligned} s_0 &= 1 \\ s_1 &= t_1 + \dots + t_n \\ s_1 &= \sum_{1\leq i<j\leq n} t_i t_j \\ &\vdots \\ s_n &= t_1 \dots t_n \end{aligned}$$

Thus $f(x) = \sum_{i=0}^{n} (-1)^{n-i} s_{n-i} x^i$. Define $L = F(s_1,\dots,s_n) \subseteq E^{\mathfrak{S}_n}$. We have $f(x) \in L[x]$ and E is a splitting field of $f(x)$ over L. Since $\deg f \leq n$, $[E:L] \leq n!$. On the other hand, $[E:E^{\mathfrak{S}_n}] = |\mathfrak{S}_n| = n!$ by Artin's theorem. Since $L \subseteq E^{\mathfrak{S}_n}$, we have $n! = [E:E^{\mathfrak{S}_n}] \leq [E:L] \leq n!$, and so $E^{\mathfrak{S}_n} = L$.

6.18 Example. Let $E = F(t)$ be the function field in one variable over F. Let G be the subgroup of $\mathrm{Aut}_F(E)$ generated by involutions σ and τ defined by

$$\sigma : g(t) \mapsto g\left(\frac{1}{t}\right) \text{ and } \tau : g(t) \mapsto g(1-t)$$

Let $\rho = \sigma\tau$. Then $\rho(g(t)) = g(\frac{1}{1-t})$, $\rho^2(g(t)) = g(\frac{t-1}{t})$, and $\rho^3(g(t)) = g(t)$. Hence $\rho^3 = 1$ in G. We have $G = \langle \sigma, \tau \rangle = \langle \rho, \sigma \rangle \cong \mathfrak{S}_3$. To consider E^G, notice that the G-orbit of t is

$$\begin{array}{ccccc} t & \xrightarrow{\rho} & \frac{1}{1-t} & \xrightarrow{\rho} & \frac{t-1}{t} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ \frac{1}{t} & & 1-t & & \frac{t}{t-1} \end{array}$$

Hence the minimal polynomial of t in $E^G[x]$ is

$$\begin{aligned} f(x) &= (x-t)\left(x-\frac{1}{1-t}\right)\left(x-\frac{t-1}{t}\right)\left(x-\frac{1}{t}\right)\left(x-\frac{t}{t-1}\right)(x-(1-t)) \\ &= x^6 - 3x^5 + (6-h)(x^4+x^2) + (2h-7)x^3 - 3x + 1 \end{aligned}$$

where $h = \frac{(t^2-t+1)^3}{t^2(t-1)^2}$. Now $h \in E^G$ (check this) and we have that $F \subseteq F(h) \subseteq E^G \subseteq E$. Since

$$(t^2-t+1)^3 - ht^2(t-1)^2 = 0$$

$t \in E$ is a root of $g(x) = (x^2-x+1)^3 - hx^2(x-1)^2 \in F(h)[x]$. Since $\deg g = 6$ and $E = F(h)(t)$, $[E : F(h)] \leq 6$. Also, $[E : E^G] = |G| = 6$ by Artin's theorem. Since $6 = [E : E^G] \leq [E : F(h)] \leq 6$, we have that $E^G = F(h)$ and $g(x)$ is the minimal polynomial of t over $F(h)$.

7 The Galois Correspondence

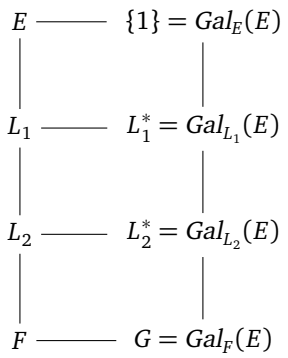
7.1 The Fundemental Theorem

7.1 Theorem. *(Fundemental Theorem of Galois Theory) Let E/F be a finite Galois extension and $G = Gal_F(E)$. Then there is an order reversing bijection between the intermediate fields of E/F and the subgroups of G. More precisely, let $Int(E/F)$ denote the set of intermediate fields of E/F and $Sub(G)$ the set of subgroups of G. Then the maps*

- $Int(E/F) \to Sub(G) : L \mapsto L^* := Gal_L(E)$
- $Sub(G) \to Int(E/F) : H \mapsto H^* := E^H$

are inverses of each other and reverse the inclusion relation. In particular, for $L_1 \supseteq L_2 \in Int(E/F)$ and $H_1 \subseteq H_2 \in Sub(G)$ then we have

$$[L_1 : L_2] = [L_2^* : L_1^*] \text{ and } [H_1 : H_2] = [H_2^* : H_1^*]$$



PROOF: Recall the following theorems:

1. If $f(x) \in F[x]$ is separable and E/F is its splitting field then $E^{\mathrm{Aut}_F(E)} = F$.
2. If E is a field and G is finite subgroup of $\mathrm{Aut}(E)$ then E/E^G is a finite Galois extension and $\mathrm{Gal}_{E^G}(E) = G$.
3. If E/F is Galois and L is an intermediate field then E/L is also Galois.

Let $L \in \mathrm{Int}(E/F)$ and let $H \in \mathrm{Sub}(G)$. Then

$$E^{\mathrm{Gal}_L(E)} = L \text{ so } (L^*)^* = (\mathrm{Gal}_L(E))^* = L$$

Also,

$$\mathrm{Gal}_{E^H}(E) = H \text{ so } (H^*)^* = (E^H)^* = H$$

Hence we have

$$H \mapsto H^* \mapsto (H^*)^* = H \text{ and } L \mapsto L^* \mapsto (L^*)^* = L$$

so the maps $L \mapsto L^*$ and $H \mapsto H^*$ are inverses of each other. For $L_1, L_2 \in \mathrm{Int}(E/F)$, E/L_1 and E/L_2 are also Galois. If $L_2 \subseteq L_1$ then we have $\mathrm{Gal}_{L_1}(E) \subseteq \mathrm{Gal}_{L_2}(E)$. Thus $L_2 \subseteq L_1 \implies L_1^* \subseteq L_2^*$. Also,

$$[L_1 : L_2] = \frac{[E : L_2]}{[E : L_1]} = \frac{|\mathrm{Gal}_{L_2}(E)|}{|\mathrm{Gal}_{L_1}(E)|} = \frac{|L_2^*|}{|L_1^*|} = [L_2^* : L_1^*]$$

For $H_1, H_2 \in \mathrm{Sub}(G)$, if $H_2 \subseteq H_1$ then we have $E^{H_1} \subseteq E^{H_2}$. Thus $H_2 \subseteq H_1 \implies H_1^* \subseteq H_2^*$. Also,

$$[H_1 : H_2] = \frac{|H_1|}{|H_2|} = \frac{|\mathrm{Gal}_{E^{H_1}}(E)|}{|\mathrm{Gal}_{E^{H_2}}(E)|} = \frac{[E : E^{H_1}]}{[E : E^{H_2}]} = [E^{H_2} : E^{H_1}] = [H_2^* : H_1^*]$$

□

Remark. Given a finite Galois extension E/F, we can ask how many intermediate fields are between E and F. Without the Fundemental Theorem of Galois Theory, this would be a hard question to answer. In particular, since $\mathrm{Gal}_F(E)$ is finite for finite Galois extensions, there are only finitely many intermediate fields. This is exactly the spirit of Galois theory: transform a question of infiniteness (fields), which is hard to answer, to a question of finiteness (groups), which is easier to understand.

7.2 Applications

7.2 Lemma. *Let E/F be a finite Galois extension with Galois group G. Let L be an intermediate field. For $\psi \in G$, we have*

$$Gal_{\psi(L)}(E) = \psi Gal_L(E)\psi^{-1}$$

PROOF: For any $\alpha \in \psi(L)$, $\psi^{-1}(\alpha) \in L$. If $\phi \in \mathrm{Gal}_L(E)$, we have $\phi \circ \psi^{-1}(\alpha) = \psi^{-1}(\alpha)$. That is to say, $\psi \circ \phi \circ \psi^{-1} \in \mathrm{Gal}_{\psi(L)}(E)$ for any $\phi \in \mathrm{Gal}_L(E)$. Thus $\psi \mathrm{Gal}_L(E)\psi^{-1} \subseteq \mathrm{Gal}_{\psi(L)}(E)$. Since the groups have the same order we conclude that they are the same. □

7.3 Theorem. *Let E/F, L, G be defined as in the last theorem. Then L/F is Galois if and only if L^* is a normal subgroup of G. In this case*

$$Gal_F(L) \cong G/L^*$$

PROOF:

$$\begin{aligned} L/F \text{ is normal} &\iff \psi(L) = L \ \forall \psi \in \mathrm{Gal}_F(E) \\ &\iff \mathrm{Gal}_{\psi(L)}(E) = \mathrm{Gal}_L(E) \ \forall \psi \in \mathrm{Gal}_F(E) \\ &\iff \psi \mathrm{Gal}_L(E)\psi^{-1} = \mathrm{Gal}_L(E) \ \forall \psi \in \mathrm{Gal}_F(E) \\ &\iff L^* = \mathrm{Gal}_L(E) \text{ is a normal subgroup of } G \end{aligned}$$

If L/F is a Galois extension, the restriction map $\psi \mapsto \psi|_L$ from G to $\mathrm{Gal}_F(L)$ is well-defined. Moreover, it is surjective and has kernel L^*. We are done by the first isomorphism theorem. □

7.4 Example. For a prime p, let $q = p^n$. Consider $\mathbb{F}_q$, which is an extension of $\mathbb{F}_p$ of degree n. The Frobenius Automorphism of $\mathbb{F}_q$ is defined by

$$\sigma_p : \mathbb{F}_q \to \mathbb{F}_q : \alpha \mapsto \alpha^p$$

Notice that the above map is really an automorphism (see assignment 3). For all $\alpha \in \mathbb{F}_q$, we have that $\sigma_p^n(\alpha) = \alpha^{p^n} = \alpha$. Thus $\sigma_p^n = 1$. For $1 \leq m < n$, $\sigma_p^m(\alpha) = \alpha$ implies that α is a root of $x^{p^m} - x$, which has at most p^m roots. Therefore $\sigma_p^m \neq 1$. Hence σ_p^n has order n. It follows that

$$n = |\langle \sigma_p \rangle| \leq |\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)| = [\mathbb{F}_q : \mathbb{F}_p] = n$$

Thus $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q) = \langle \sigma_p \rangle$.

Consider a subgroup H of $\mathrm{Gal}_{\mathbb{F}_p}(\mathbb{F}_q)$ of order d. Then $d|n$ and $[G : H] = \frac{n}{d}$. By the Fundemental Theorem, we have

$$\frac{n}{d} = [G : H] = [H^* : G^*] = [\mathbb{F}_q^H : \mathbb{F}_p]$$

and thus $H^* = \mathbb{F}_{p^{\frac{n}{d}}}$.

7.3 Brief Review of Group Theory

7.5 Theorem. *(Cauchy) Let p be prime and G a finite group. If p divides $|G|$ then G contains an element of order p.*

7.6 Definition. Let p be prime. A group in which every element has order a power of p is called a p-group. It follows by Cauchy's theorem that a finite group G is a p-group if and only if $|G|$ is a power of p.

7.7 Theorem. *(First Sylow Theorem) Let G be a group with order $p^n m$ where p is prime, $n > 0$, and $\gcd(p, m) = 1$. Then G contains a subgroup of order p^i for each $1 \leq i \leq n$ and every subgroup of G of order p^i for $i < n$ is normal in some subgroup of order p^{i+1}.*

7.8 Definition. A subgroup P of a group G is a Sylow p-subgroup if P is a maximal p-subgroup of G. By the first Sylow theorem, if $|G| = p^n m$ (as in the theorem) then $|P| = p^n$.

7.9 Theorem. *(Second Sylow Theorem) If H is a p-subgroup of a finite group G and P is any Sylow p-subgroup of G, then there exists $g \in G$ such that $H \subseteq gPg^{-1}$. In particular, any two Sylow p-subgroups of G are conjugate.*

7.10 Theorem. *(Third Sylow Theorem) Let G be a finite group and p be a prime. Then the number of Sylow p-subgroups of G divides $|G|$ and is of the form $1 + kp$ for some $k \geq 0$.*

7.11 Example. Determine the lattice of subfields of the splitting field of $x^5 - 7$.

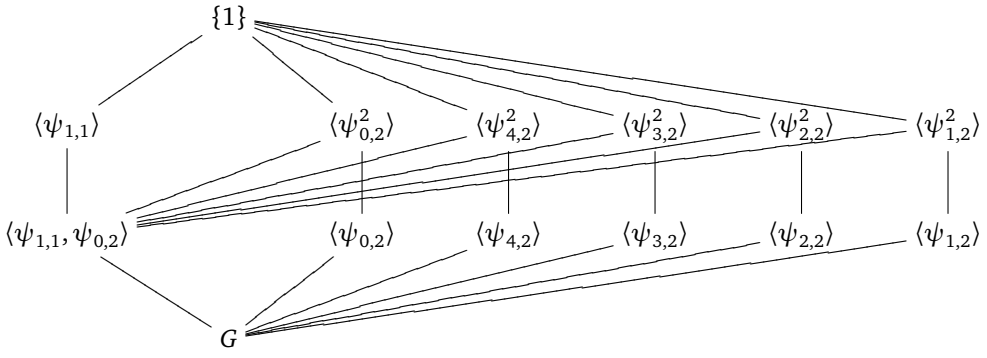
We have seen in the previous section that the splitting field of $x^5 - 7$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \zeta_5)$ where $\alpha = \sqrt[5]{7}$. We already know that $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ and $[E : \mathbb{Q}(\zeta_5)] = 5$. It follows that $[E : \mathbb{Q}] = 20$ and $\mathrm{Gal}_{\mathbb{Q}}(E)$ is a subgroup of $\mathfrak{S}_5$ of order 20. Also, for each $\psi \in \mathrm{Gal}_{\mathbb{Q}}(E)$, we write $\psi = \psi_{k,s}$ if $\psi(\alpha) = \alpha\zeta_5^k$ and $\psi(\zeta_5) = \zeta_5^s$. Define

$$\sigma : \alpha \mapsto \alpha\zeta_5 : \zeta_5 \mapsto \zeta_5 \text{ and } \tau : \alpha \mapsto \alpha : \zeta_5 \mapsto \zeta_5^2$$

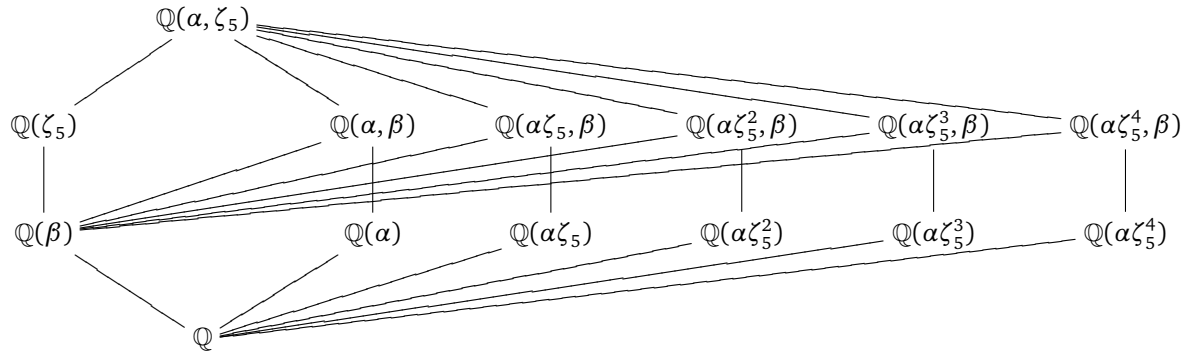
So $\sigma = \psi_{1,1}$ and $\tau = \psi_{0,2}$. It can be checked that $\tau\sigma = \sigma\tau^2$. We have

$$G := \mathrm{Gal}_{\mathbb{Q}}(E) = \langle \sigma, \tau \mid \sigma^5 = \tau^4 = 1, \tau\sigma = \sigma\tau^2 \rangle$$

Since $|G| = 20$, the possible subgroups of G are of orders $1, 2, 4, 5, 10, 20$. Since $20 = 4 \cdot 5$, by the first Sylow theorem, G has Sylow 2-subgroups and Sylow 5-subgroups. By the third Sylow theorem, there must be only one Sylow 5-subgroup, and it is normal by the second Sylow theorem. Using the same argument, the number of Sylow 2-subgroups of G is either 1 or 5. But if there is only one Sylow 2-subgroup then it would be normal and hence we would have that $G \cong \mathbb{Z}_5 \oplus \mathbb{Z}_4$, a contradiction since G is not Abelian. Hence there must be 5 Sylow 2-subgroups, and they must all be cyclic (since $\langle\tau\rangle$ is cyclic and all Sylow 2-subgroups are conjugate). Notice that all the elements of G are of the form $\sigma^a\tau^b$. Conjugating τ gives $\sigma^a\tau\sigma^a$, and using the relation $\tau\sigma = \sigma\tau^2$ we get $\langle\sigma\tau\sigma^{-1}\rangle = \langle\sigma^4\tau\rangle = \langle\psi_{4,2}\rangle$



The corresponding diagram of subfields is



where $\beta = \zeta_5 + \zeta_5^{-1}$ (notice that $\beta^2 + \beta - 1 = 0$).

7.4 The Primitive Element Theorem

Given a field extension E/F, we may ask

1. Is it simple? That is, is $E = F(\alpha)$ for some $\alpha \in E$? If this is the case, we say that α is a primitive element of E.
2. Are there infinitely many intermediate fields?

We have see that in characteristic zero every finite extension is simple. However, in characteristic p there are finite extensions which are not simple.

7.12 Example. Let F be a field with $\mathrm{ch}(F) = p$ and let $F(s,t)$ be the rational function field in two variables. We have $F(s^p,t^p) \subseteq F(s,t^p) \subseteq F(s,t)$ Since t is a root of the irreducible polynomial $x^p - t^p \in F(s,t^p)[x]$ (note that $t^p \notin F(s,t^p)^p$) we have that $[F(s,t) : F(s,t^p)] = p$, and similarily $[F(s,t^p) : F(s^p,t^p)] = p$. Thus $F(s,t)$ is a finite extension of $F(s^p,t^p)$ of degree p^2. Let $u \in F(s,t)$. Notice that $u^p \in F(s^p,s^p)$. Thus $[F(s^p,t^p)(u) : F(s^p,t^p)] \leq p$ since u is a root of $x^p - u^p \in F(s^p,t^p)[x]$. Hence the extension cannot be simple.

7.13 Theorem. *A finite extension E/F is simple if and only if it has finitely many intermediate fields.*

PROOF: Suppose that $E = F(\alpha)$ is a simple extension. Let K be any intermediate field. We denote by $f(x)$ and $g(x)$ the minimal polynomials of α over F and K respectively. Thus $g(x)$ is a monic factor of $f(x)$ in $E[x]$. Write $g(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_0$, where $c_i \in K$. Let $L = F(c_0,\ldots,c_{m-1})$, a subfield of K. Then $g(x) \in L[x]$. Notice that $E = F(\alpha) = L(\alpha) = K(\alpha)$. We have

$$m = [E : K] \leq [E : L] = [L(\alpha) : L] \leq m$$

Hence $K = L = F(c_0,\ldots,c_{m-1})$, so K is completely determined by $g(x)$, a factor of $f(x)$. There are only finitely many choices for $g(x)$, so there can only be finitely many different intermediate fields.

Suppose conversly that E/F has only finitely many intermediate fields. Since E/F is a finite extension, $E = F(\alpha_1,\ldots,\alpha_n)$. Without loss of generality, we may assume that $E = F(\alpha,\beta)$ (the general case follows by induction).

Claim. There exists $\lambda \in F$ such that $F(\alpha + \lambda\beta) = F(\alpha,\beta)$

Since we undertand completely a finite extension of a finite field, we may assume that F is an infinite field. By assumption there are only finitely many intermediate fields, so we can find some $\lambda, \lambda' \in F$ such that $\lambda \neq \lambda'$ and $F(\alpha + \lambda\beta) = F(\alpha + \lambda'\beta)$. Hence $\alpha + \lambda\beta, \alpha + \lambda'\beta \in F(\alpha + \lambda\beta)$, so $\beta \in F(\alpha + \lambda\beta)$ (since $\lambda - \lambda' \neq 0$). Thus $E = F(\alpha, \beta) \subseteq F(\alpha + \lambda\beta)$. The other inclusion is clear, so $E = F(\alpha + \lambda\beta)$. □

7.14 Theorem. *(Primitive Element Theorem) Every finite separable extension is simple.*

PROOF: Exercise. □

8 Ruler and Compass Constructions

8.1 Constructible Points

Consider the Euclidean plane $\mathbb{R}^2$. Let $O, I \in \mathbb{R}^2$ be two distinct points. We take the distance OI as the unit of length. Introduce an orthogonal coordinate system in $\mathbb{R}^2$ with the origin O and I on the x-axis with coordinates $(1, 0)$

8.1 Definition. Let S be any set of points in $\mathbb{R}^2$. We call a line L an S-line if $|S \cap L| \geq 2$. We call a circle C an S-circle if the centre of C is in S and the radius of C is equal to the distance between two points in S.

Notation. We denote by S' the set of points which are either in S or lie in the intersection of two distinct S-lines, two distinct S-circles, or an S-line and an S-circle.

8.2 Definition. A point $P \in \mathbb{R}^2$ is constructible if there exists a finite sequence of points $\{P_1, \ldots, P_n\}$ such that $P_n = P$ and $P_i \in \{O, I, P_1, \ldots, P_{i-1}\}' \ \forall\, 1 \leq i \leq n$.

8.3 Lemma. *All rational numbers (i.e. points in $\mathbb{Q} \times \{0\}$) are constructible.*

PROOF: Exercise. □

8.4 Theorem. *For a point $P = (\alpha, \beta) \in \mathbb{R}^2$, the following are equivalent*

1. *P is constructible*
2. *there exists a tower of fields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subset \mathbb{R}$ such that $\alpha, \beta \in F_n$ and $[F_i : F_{i-1}] \leq 2$ for all $1 \leq i \leq n$*

PROOF: Suppose that P is constructible. Then there exists a finite sequence of points $\{P_1, \ldots, P_n\}$ such that

$$P_n = P \text{ and } P_i \in \{O, I, P_1, \ldots, P_{i-1}\}' \ \forall\, 1 \leq i \leq n$$

Write $P_i = (\alpha_i, \beta_i)$ and define $F_0 = \mathbb{Q}$ and $F_i = F_{i-1}(\alpha_i, \beta_i)$. Let $S = \{O, I, P_1, \ldots, P_{i-1}\}$, so that $P \in S'$. There are two cases

Case 1: If $P_i \in S$ then $F_i = F_{i-1}$

Case 2: Suppose $P_i \in S' \setminus S$. Then P_i is the intersection point of two S-lines, two S-circles, or an S-line and an S-circle. Notice that given two points $(a, b), (c, d)$, the equation of the line that contains them is

$$(b - d)x + (c - a)y(ad - bc) = 0$$

Similarily, given the center of a circle (a, b) and a radius r then the equation of the circle is

$$(x - a)^2 + (y - b)^2 = r^2$$

There are three subcases

(a) If P_i is on the intersection of two S-lines then we may clearly use the equations of these lines to solve for the coordinates P_i, and see that $F_i = F_{i-1}$.
(b) If P_i is on the intersection of an S-line and an S-circle then α_i and β_i are solutions to a equation of degree at most two. Hence $[F_i : F_{i-1}] \leq 2$.
(c) Suppose P_i is on the intersection of two S-circles. By subtracting the equations of the circles we get a linear equation that is satisfied by α_i and β_i, so we may use the last case to see that $[F_i : F_{i-1}] \leq 2$.

Now suppose that (2) holds. We prove that P is constructible by induction on n. If $n = 0$ then $\alpha, \beta \in \mathbb{Q}$, so P is constructible by the last lemma. Suppose that for all $P = (\alpha, \beta)$ with $\alpha, \beta \in F_{n-1}$ are constructible. Consider F_n.

1. $F_n = F_{n-1}$ trivially implies that P is constructible.
2. $[F_n : F_{n-1}] = 2$ implies that $F_n = F_{n-1}(\sqrt{\gamma})$ for some $\gamma \in F_{n-1}$, $\gamma > 0$. $\sqrt{\gamma}$ is constructible (see diagram). In general, for $\alpha \in F_n$, $\alpha = a + b\sqrt{\gamma}$ with $a, b \in F_{n-1}$. Since all of these are constructible so is α. Therefore P is constructible. □

8.2 Constructible Numbers

8.5 Definition. For $\alpha \in \mathbb{R}$, α is constructible if the point $P = (\alpha, 0)$ is constructible. For $\gamma = \alpha + i\beta \in \mathbb{C}$, γ is constructible if the point $P = (\alpha, \beta)$ is constructible.

8.6 Corollary. *If $\alpha \in \mathbb{R}$ is constructible then α is algebraic and the degree of the minimal polynomial polynomial of α over $\mathbb{Q}$ is a power of 2.*

Remark. The converse of this corollary is false, as we shall see later.

8.7 Lemma. *Let $\gamma = \alpha + i\beta$. Suppose there is a real field $L \subseteq \mathbb{Q}(\gamma)$ such that $[\mathbb{Q}(\gamma) : L] = 2$. If all elements of L are constructible then γ is constructible.*

PROOF: Since $[\mathbb{Q}(\gamma) : L] = 2$, γ is a root of a polynomial $ax^+bx + c \in L[x]$ where $a \neq 0$. Then

$$\gamma = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

so that

$$\alpha = \begin{cases} \frac{-b \pm \sqrt{b^2-4ac}}{2a} & \text{if } b^2 - 4ac \geq 0 \\ \frac{-b}{2a} & \text{otherwise} \end{cases} \quad \text{and} \quad \beta = \begin{cases} 0 & \text{if } b^2 - 4ac \geq 0 \\ \frac{\pm\sqrt{4ac-b^2}}{2a} & \text{if } b^2 - 4ac < 0 \end{cases}$$

Recall that if $\delta \in \mathbb{R}$ is constructible, then so is $\sqrt{\delta}$. □

8.3 Applications

8.8 Example. 1. The regular pentagon is constructible. It is enough to show that ζ_5 is constructible. The minimal polynomial of ζ_5 is $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$. Let $\beta = \zeta_5 + \zeta_5^{-1} = \frac{\sqrt{5}-1}{2}$, a real number. The minimal polynomial of β is $x^2 + x - 1$, so $\mathbb{Q} \subseteq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\zeta)$ is a tower of fields such that the increase of degree at each step is 2.

2. The regular 9-gon is not constructible. Consider ζ_9 and $\lambda = \zeta_9 + \zeta_9^{-1}$. Then ζ_9 is a root of the polynomial $x^2 - \lambda x + 1 \in \mathbb{Q}(\lambda)[x]$. Therefore $[\mathbb{Q}(\zeta_9) : \mathbb{Q}(\lambda)] = 2$, so ζ_9 is constructible if and only if λ is constructible. Since $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$ the minimal polynomial of ζ_9 is $x^6 + x^3 + 1$. Notice that

$$\begin{aligned}\lambda^3 &= (\zeta_9 + \zeta_9^{-1})^3 \\ &= \zeta_9^3 + \zeta_9^{-3} + 3(\zeta_9 + \zeta_9^{-1}) \\ &= \zeta_9^3 + \zeta_9^6 + 3\lambda \\ &= -1 + 3\lambda\end{aligned}$$

   Therefore λ is a root of the irreducible polynomial $x^3 - 3x + 1$, so λ cannot be constructible since 3 is not a power of 2.

   Consequently, the angle of $\frac{2\pi}{3}$ can not be trisected by ruler and compass.
3. The cicle cannot be squared. Specifically, $\sqrt{\pi}$ is not constructible. It is sufficient to show that π is not constructible. But π is not algebraic, so it is not constructible.
4. The unit cube cannot be doubled. Specifically, $\sqrt[3]{2}$ is not constructible. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$, which is of degree 3, not a power of two.

8.9 Theorem. *Let $\alpha \in \mathbb{R}$ be an algebraic number and $p(x)$ its minimal polynomial over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be the splitting field of $p(x)$. Then α is constructible if and only if $\mathrm{Gal}_{\mathbb{Q}}(E)$ is a 2-group.*

PROOF: Assume that α is constructible. Let

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{R}$$

be a tower of real quadratic extensions and $\alpha \in F_n$. Since we are in characteristic zero, there is $\beta \in F_n$ such that $F_n = \mathbb{Q}(\beta)$. Let $p_\beta(x) \in \mathbb{Q}[x]$ be the minimal polynomial of β. Let $\beta = \beta_1, \ldots, \beta_m$ be the roots of $p_\beta(x)$. Let $E_\beta = \mathbb{Q}(\beta_1, \ldots, \beta_m)$, which is a Galois extension. For each $i = 1, \ldots, m$, define $\psi_i : \mathbb{Q}(\beta) \to \mathbb{Q}(\beta_i) : \beta \mapsto \beta_i$ such that ψ_i fixes $\mathbb{Q}$. This is a field isomorphism. We have

$$\begin{aligned}\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n &= \mathbb{Q}(\beta) \\ &= \mathbb{Q}(\beta)(\psi_2(F_0)) \subseteq \mathbb{Q}(\beta)(\psi_2(F_1)) \subseteq \cdots \subseteq \mathbb{Q}(\beta)(\psi_2(F_n)) = \mathbb{Q}(\beta_1, \beta_2) \\ &= \mathbb{Q}(\beta_1, \beta_2)(\psi_3(F_0)) \subseteq \cdots \subseteq \mathbb{Q}(\beta_1, \beta_2, \beta_3) \\ &\vdots \\ &\subseteq \mathbb{Q}(\beta_1, \ldots, \beta_m) = E_\beta\end{aligned}$$

which is a chain of quadratic extensions. Therefore $[E_\beta : \mathbb{Q}]$ is a power of 2. Since $\alpha \in \mathbb{Q}(\beta) \subseteq E_\beta$ and E_β is Galois, all of the conjugates of α are in E_β. It follows that E is a subfield of E_β, and so the degree of E over $\mathbb{Q}$ is a power of 2. Hence $|\mathrm{Gal}_{\mathbb{Q}}(E)|$ is a power of 2.

Conversely, let $G = \mathrm{Gal}_{\mathbb{Q}}(E)$. If $|G| = 2^n$ for some n, by the first Sylow theorem there exists a subgroup $H_{n-1} \subseteq G$ of order 2^{n-1}. Applying the Sylow theorem repeatedly, we get a chain of subgroups of G

$$\{1\} = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_{n-1} \subseteq H_n = G$$

Let $H_i^* = E^{H_i}$. By the Fundemental Theorem of Galois Theory,

$$E = H_0^* \supseteq H_1^* \supseteq \cdots \supseteq H_{n-1}^* \supseteq H_n^* = G^* = \mathbb{Q}$$

where $[H_{i-1}^* : H_i^*] = 2$ for $i = 1, \ldots, m$. Since $\alpha \in E$, α is constructible. □

9 Cyclotomic Extensions

9.1 Cyclotomic Polynomials

For a prime p, the p^{th} cyclotomic polynomial

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

is irreducible. However, for general n the polynomial $\frac{x^n-1}{x-1}$ is not irreducible if n is not prime. To generalize the definition of cyclotomic polynomial to general n, we notice that

$$\Phi_p(x) = (x - \zeta_p)(x - \zeta_p^2)\ldots(x - \zeta_p^{p-1})$$

For each $k = 1, \ldots, p-1$ we have that $\gcd(k, p) = 1$. Hence

$$\Phi_p(x) = \prod_{\substack{1 \le k \le p \\ (k,p)=1}} (x - \zeta_p^k)$$

Thus, a natural way to define $\Phi_n(x)$ is

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ (k,n)=1}} (x - \zeta_n^k)$$

9.1 Definition. Let $n \in \mathbb{N}$ and $\zeta_n = e^{\frac{2\pi i}{n}}$. For any $k \in \mathbb{N}$ with $(k, n) = 1$, we call ζ_n^k a primitive n^{th} root of unity in $\mathbb{C}$.

9.2 Proposition. $x^n - 1 = \prod_{d|n} \Phi_d(x)$, *where d runs through all positive divisors of n.*

9.3 Example. $x^6 - 1 = (x-1)(x+1)(x^2+x+1)(x^2-x+1)$, so the sixth cyclotomic polynomial is $\Phi_6(x) = x^2 - x + 1$.

Notice that if $\psi \in \text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n))$ then $\psi(\zeta_n) = \zeta_n^k$, where $(k, n) = 1$. It follows that $\Phi_n(x) \in \mathbb{Q}[x]$.

9.4 Theorem. *The polynomial $\Phi_n(x)$ has integer coefficients and is irreducible over $\mathbb{Q}$.*

PROOF: The following statement is an application of Gauß's Lemma.

Claim. Let $h(x) \in \mathbb{Z}[x]$ be monic and $h(x) = f(x)g(x)$, where $f(x), g(x) \in \mathbb{Q}[x]$. If $f(x), g(x)$ are both monic then $f(x), g(x) \in \mathbb{Z}[x]$.

Now let ζ_n be a primitive n^{th} root of unity and $f(x)$ be the minimal polynomial of ζ_n over $\mathbb{Q}$. Then $x^n - 1 = f(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. Since $f(x)$ is monic, $g(x)$ is monic, so $f(x), g(x) \in \mathbb{Z}[x]$. Let p be a prime with $(n, p) = 1$. Reduce the above equation modulo p to get $x^n - \overline{1} = \overline{f}(x)\overline{g}(x)$ in $\mathbb{F}_p$. Since $(n, p) = 1$, $x^n - \overline{1}$ has no multiple roots in any extension of $\mathbb{F}_p$. In particular, $\overline{f}(x)$ and $\overline{g}(x)$ are relatively prime.

Notice that $f(\zeta_n^p)g(\zeta_n^p) = (\zeta_n^p)^n - 1 = 0$. Suppose that $g(\zeta_n^p) = 0$. Since $f(x)$ is the minimal polynomial of ζ_n and $g(\zeta_n^p) = 0$, we have $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Then $\overline{g}(x)^p = \overline{g(x^p)} = \overline{f}(x)\overline{h}(x)$, and this is a contradiction because if $\overline{r}(x)$ is an irreducible factor of $\overline{f}(x)$ then $\overline{r}(x)$ divides $\overline{g}(x)$, contradicting that $\overline{f}(x)$ and $\overline{g}(x)$ are relatively prime. Therefore $f(\zeta_n^p) = 0$. Now for $1 \le k \le n$ with $(k, n) = 1$, let $k = p_1 \ldots p_s$ it's prime factorization (where the p_i's are not necessarily distinct). Notice that if ζ_n is a primitive root, then ζ_n^p with $(p, n) = 1$ is also a primitive root. Hence we have

$$0 = f(\zeta_n) = f(\zeta_n^{p_1}) = \cdots = f(\zeta_n^{p_s}) = f(\zeta_n^{p_1 p_2}) = \cdots = f(\zeta_n^k)$$

Thus all primitive n^{th} roots ζ_n^k are roots of $f(x)$, so $\Phi_n(x) | f(x)$. The other direction is obvious, so $\Phi_n(x) = f(x)$ is the minimal polynomial of ζ_n over $\mathbb{Q}$. □

9.2 Cyclotomic Fields

9.5 Definition. The n^{th} cyclotomic field is $\mathbb{Q}(\zeta_n)$, a splitting field of $x^n - 1$.

9.6 Theorem. *The Galois group of $x^n - 1$ over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_n^*$, the group of invertible elements of $\mathbb{Z}_n$. It follows that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, where φ is the Euler function.*

PROOF: Exercise. □

9.7 Theorem. *Every quadratic extension of $\mathbb{Q}$ in $\mathbb{C}$ is contained in some cyclotomic extension $\mathbb{Q}(\zeta_n)$.*

PROOF: Every quadratic extension is of the form $\mathbb{Q}(\sqrt{D})$, where $D \neq 1$ square-free integer. Notice that for distinct primes p_1 and p_2, if $\mathbb{Q}(\sqrt{p_1}) \subseteq \mathbb{Q}(\zeta_{n_1})$ and $\mathbb{Q}(\sqrt{p_2}) \subseteq \mathbb{Q}(\zeta_{n_2})$ then $\mathbb{Q}(\sqrt{p_1 p_2}) \subseteq \mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}) \subseteq \mathbb{Q}(\zeta_{n_1 n_2})$. Hence it is enough to consider $\mathbb{Q}(\sqrt{\pm p})$ for prime p.

If $p = 2$, since $(1+i)^2 = 2i$ and $1 + i \in \mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$, we have $\sqrt{2i} \in \mathbb{Q}(\zeta_4)$. Also, $i \in \mathbb{Q}(\zeta_4)$, so $\sqrt{i} \in \mathbb{Q}(\zeta_8)$. It follows that $\sqrt{2}, \sqrt{-2} \in \mathbb{Q}(\zeta_8)$, and so $\mathbb{Q}(\sqrt{\pm 2}) \subseteq \mathbb{Q}(\zeta_8)$.

Let p be an odd prime. Consider $\mathbb{Q}(\zeta_p)$. The minimal polynomial of ζ_p over $\mathbb{Q}$ is

$$\Phi_p(x) = \prod_{1 \leq k < p} (x - \zeta_p^k)$$

The discriminant of $\Phi_p(x)$ is

$$D(\Phi_p) = \prod_{1 \leq i < j < p} (\zeta_p^i - \zeta_p^j)^2$$

It can be shown that $D(\Phi_p) = (-1)^{\frac{p-1}{2}} p^{p-2}$. Thus we have

$$\prod_{1 \leq i < j < p} (\zeta_p^i - \zeta_p^j) = \pm p^{\frac{p-3}{2}} \sqrt{(-1)^{\frac{p-1}{2}} p}$$

Since $\frac{p-3}{2} \in \mathbb{Z}$ and $\prod_{1 \leq i < j < p} (\zeta_p^i - \zeta_p^j) \in \mathbb{Q}(\zeta_p)$, if $p \equiv 1 \pmod 4$ then $\sqrt{p} \in \mathbb{Q}(\zeta_p)$ and $\sqrt{-p} \in \mathbb{Q}(\zeta_{4p})$. Otherwise, if $p \equiv 3 \pmod 4$ then $\sqrt{-p} \in \mathbb{Q}(\zeta_p)$ and $\sqrt{p} \in \mathbb{Q}(\zeta_{4p})$.

Hence in all cases, $\mathbb{Q}(\sqrt{\pm p}) \subseteq \mathbb{Q}(\zeta_{4p})$. □

Remark. Notice that $\text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{D})) \cong \{1\}$ or $\mathbb{Z}_2$, which are Abelian groups. We call these type of extensions Abelian extensions. It turns out that all Abelian extensions of $\mathbb{Q}$ in $\mathbb{C}$ are contained in some cyclotomic extension (Kronecker-Weber). The proof of this theorem is beyond the scope of this course. The proof of the converse is not too difficult.

9.3 Abelian Extensions

9.8 Lemma. *Let p be prime and $m \geq 1$ with $p \nmid m$. Let $\Phi_m(x) \in \mathbb{Z}[x]$ be the m^{th} cyclotomic polynomial and $a \in \mathbb{Z}$. Then $p | \Phi_m(a)$ if and only if a is not divisible by p and $\overline{a}$ has order m in $\mathbb{F}_p^*$.*

PROOF: Assume $p | \Phi_m(a)$. Then since m and p are coprime, $x^m - \overline{1} \in \mathbb{F}_p[x]$ has no multiple roots in any extension of $\mathbb{F}_p$. Write

$$x^m - \overline{1} = \prod_{d|m} \overline{\Phi_d}(x) = \overline{\Phi_m}(x) \prod_{\substack{d|m \\ d<m}} \overline{\Phi_d}(x) \in \mathbb{F}_p[x]$$

We have $p|\Phi_m(a)$, so $\overline{\Phi_m}(\overline{a}) = 0$, and hence $(\overline{a})^m = \overline{1}$. It follows that $p \nmid a$. Since $p \nmid m$, $x^m - \overline{1} \in \mathbb{F}_p[x]$ has no multiple roots in any extension. We have already seen that the order of $\overline{a}$ divides m. Assume $d < m$ is the order of $\overline{a}$. Then $\overline{a}^d - \overline{1} = 0$, so $\overline{a}$ is a root of $\overline{\Phi}_{d'}$ for some $d'|d$. But then $d'|m$, and so $\overline{a}$ is a double root of $x^m - \overline{1}$, a contradiction. Therefore the order of $\overline{a}$ is m in $\mathbb{F}_p^*$.

Suppose conversely. If $d|m$ and $d < m$ then $\overline{a}^d - \overline{1} \neq 0$ so $\overline{\Phi}_d(\overline{a}) \neq 0$ either. Since $\overline{a}^m - \overline{1} = 0$, we must have $\overline{\Phi}_m(\overline{a}) = 0$, so $p|\Phi_m(a)$. □

We have all seen Euclid's theorem that there are infinitely many primes. We may generalize this slightly and say that there are infinitely many primes congruent to 1 modulo 2. Can we generalize this further?

9.9 Lemma. *If $f(x) \in \mathbb{Z}[x]$ is a monic polynomial and $\deg f \geq 1$, the set of prime divisors of the non-zero integers in the sequence $f(1), f(2), f(3), \ldots$ is infinite.*

PROOF: Suppose $p_1, \ldots, p_k$ are the prime divisors of the non-zero integers in the sequence $f(1), f(2), f(3), \ldots$. Choose $s \in \mathbb{Z}$ such that $m = f(s) \neq 0$. Define $g(x) = \frac{1}{m} f(s + mp_1 \ldots p_k x)$. Notice that $g(0) = \frac{1}{m} f(s) = 1$. Also, since all terms involving x in $f(s + mp_1 \ldots p_k x)$ have m in the coefficients, $g(x) \in \mathbb{Z}[x]$. Moreover, for any $n \in \mathbb{Z}$, $g(n) \equiv 1 \pmod{p_1 \ldots p_k}$. Choose $n \in \mathbb{Z}$ such that $|g(n)| > 1$. Since $p_i | g(n) - 1$ and $|g(n)| > 1$ it follows that $p_i \nmid g(n)$ for all $i = 1, \ldots, k$. Hence $g(n)$ has a prime divisor $p \notin \{p_1, \ldots, p_k\}$, and so $p | f(s + mp_1 \ldots p_k n)$, a contradiction. Therefore there are infinitely many divisors of this sequence. □

9.10 Theorem. *(Dirichlet's Theorem, weak version) Let m be a positive integer. Then there are infinitely many primes p such that $p \equiv 1 \pmod{m}$.*

PROOF: Consider $\Phi_m(x) \in \mathbb{Z}[x]$, which has degree at least 1. By the above lemma there are infinitely many prime divisors p of $\Phi_m(1), \Phi_m(2), \ldots$. If $p|\Phi_m(a)$ for some $a > 1$ then $\overline{a}$ has order m in $\mathbb{F}_p^*$. Since $\mathbb{F}_p^*$ has order $p - 1$, $m|p - 1$, so $p \equiv 1 \pmod{m}$. □

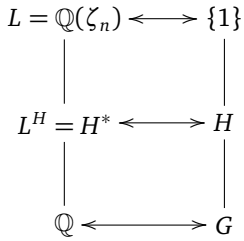
Remark. The actual statement of Dirichlet's Theorem is much stronger. Considering modulo m, for almost all primes p, $p \equiv k \pmod{m}$ where $(k, m) = 1$. There are $\varphi(m)$ equivalence classes for each m. Let $\pi(x)$ denote the number of primes less than or equal to x. Consider $\pi(x, k, m)$, the number of primes less than or equal to m and congruent to k modulo m. Dirichlet's Theorem says that $\pi(x, k, m) = \frac{1}{\varphi(m)} \pi(x) + \text{error}$.

9.11 Theorem. *Given a finite Abelian group A, there is a subfield E of a cyclotomic field with $Gal_{\mathbb{Q}}(E) \cong A$.*

PROOF: We have $A \cong C_{k_1} \times \cdots \times C_{k_s}$ where C_k is the cyclic group of order k. Choose odd primes $p_1 < \cdots < p_s$ such that $p_1 \equiv 1 \pmod{k_1}, \ldots, p_s \equiv 1 \pmod{k_s}$. Such primes exist by Dirichlet's Theorem. Let $n = p_1 \ldots p_s$ and consider the n^{th} cyclotomic field $L = \mathbb{Q}(\zeta_n)$. Then

$$\begin{aligned} G = \text{Gal}_{\mathbb{Q}}(L) &\cong \mathbb{Z}_n^* \\ &\cong (\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_s})^* \\ &\cong C_{p_1 - 1} \times \cdots \times C_{p_s - 1} \end{aligned}$$

Write $p_1 - 1 = k_1 d_1, \ldots, p_s - 1 = k_s d_s$. Since $C_{p_i - 1}$ is cyclic, there exists a subgroup D_{d_i} of $C_{p_i - 1}$ which is of order d_i. Moreover, $C_{p_i - 1} / D_{d_i} \cong C_{k_i}$. Define $H \cong D_{d_1} \times \cdots \times D_{d_s}$, which is a normal subgroup of G. Also, $G/H \cong C_{k_1} \times \cdots \times C_{k_s} \cong A$.



Let $E = H^* = L^H$. Since H is normal, by Theorem 7.3, $E/\mathbb{Q}$ is Galois. Also, $\mathrm{Gal}_{\mathbb{Q}}(E) \cong G/H \cong A$. □

9.4 Constructible n-gons

9.12 Definition. A Fermat prime is a Fermat number $F_n = 2^{2^n} + 1$ which is prime.

Remark. 1. Fermat conjectured in 1650 that every Fermat number is prime. The conjecture is false since $F_5 = 2^{2^5} + 1 = 641 \cdot 6700417$.

2. Are there infinitely many Fermat primes? This question is still open. The only Fermat primes known to date are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$.

9.13 Theorem. *(Gauss) The regular n-gon is constructible if and only if $n = 2^k p_1 \dots p_m$ where $k \geq 0$ and the p_i are distinct Fermat primes.*

PROOF: Let ζ_n be a primative n^{th} root of unity. We have seen that the minimal polynomial of ζ_n has degree $\varphi(n)$. By Corollary 8.6, the regular n-gon is constructible if and only if $\varphi(n)$ is a power of 2. Write $n = 2^k p_1^{d_1} \dots p_r^{d_r}$ where $k \geq 0$, $d_i \geq 1$, and p_i are distinct odd primes. Then $\varphi(n) = \varphi(2^k)\varphi(p_1^{d_1}) \dots \varphi(p_r^{d_r})$. Now $\varphi(2^k)$ is always a power of 2. $\varphi(p_i^{d_i}) = p_i^{d_i - 1}(p_i - 1)$, and so is a power of 2 if and only if $d_i = 1$ and $p_i - 1$ is a power of 2. Write $p_i = 2^{r_i} + 1$. Notice that if q is an odd prime dividing r then $2^r + 1 = (2^{\frac{r}{q}} + 1)(2^{\frac{r}{q}(q-1)} - 2^{\frac{r}{q}(q-2)} + \dots \pm 1)$. Thus since p_i is prime, it must be the case that r_i is a power of 2 as well. □

10 Galois Groups of Polynomials

10.1 Discriminant

10.1 Definition. Let F be a field and $f(x) \in F[x]$ a separable polynomial. Let E be the splitting field of $f(x)$ over F. The Galois group of $f(x)$ is $\mathrm{Gal}_F(E)$. We denote it by $\mathrm{Gal}_F(f)$.

10.2 Definition. Let F be a field and let $f(x) \in F[x]$ be a square-free separable polynomial of degree n. Let $\alpha_1, \dots, \alpha_n$ be the n distinct roots of $f(x)$ in some splitting field E of F. The discriminant $D(f)$ of $f(x)$ is

$$D(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

Remark. We do not lose generality by assuming that $f(x)$ is square-free. If $p(x)^2 | f(x)$, the splitting field of $f(x)$ is the same as the splitting field of $\frac{f(x)}{p(x)}$.

10.3 Proposition. *Let F be a field of characteristic not 2. Let $f(x) \in F[x]$ be a square-free separable polynomial of degree n. Let $D(f)$ be the discriminant of $f(x)$, $d^2 = D(f)$, and $G = Gal_F(f)$. Then*

1. *$D(f) \in F$*
2. *For each $\psi \in G \subseteq \mathfrak{S}_n$, $\psi(d) = \pm d$, and moreover ψ is even if and only if $\psi(d) = d$.*
3. *In the Galois correspondence of subgroups of G with intermediate fields of E/F (E is a splitting field of $f(x)$ over F) we have*
$$F(d)^* = G \cap A_n$$
In particular, G consists of even permutations if and only if $d \in F$ (which is to say that $D(f)$ is a square in F).

PROOF: Assignment 6. □

10.2 Cubic Polynomials

Let F be a field of characteristic not 2. A general cubic polynomial in $F[x]$ is of the form

$$\tilde{p}(x) = x^3 + \tilde{a}x^2 + \tilde{b}x + \tilde{c} \in F[x]$$

If $\mathrm{ch}(F) \neq 3$, by replacing x with $(x - \frac{\tilde{a}}{3})$ it suffices to consider

$$p(x) = x^3 + bx + c$$

If $p(x)$ is separable and square-free, say $\alpha_1, \alpha_2, \alpha_3$ are the distinct roots of $p(x)$. Then

$$D(p) = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2 = -4b^3 - 27c^2$$

Since $\deg p = 3$, $\mathrm{Gal}_F(p) \subseteq \mathfrak{S}_3$. By Propostion 10.3 we get

10.4 Theorem. *Let F be a field with $ch(F) \neq 2, 3$. Let $p(x) = x^3 + bx + c \in F[x]$ be an irreducible polynomial and $D(p)$ its discriminant. Then*

$$Gal_F(p) = \begin{cases} A_3 \cong C_3 & \text{if } D(p) \text{ is a square in } F \\ \mathfrak{S}_3 & \text{otherwise} \end{cases}$$

10.5 Definition. A subgroup G of the symmetric group $\mathfrak{S}_n$ is *transitive* if for any $1 \leq i \neq j \leq n$, there is $\psi \in G$ such that $\psi(i) = j$.

10.6 Lemma. *Let F be a field and $f(x) \in F[x]$. Let $G = Gal_F(f)$. If $f(x)$ is an irreducible separable polynomial of degree n then G is isomorphic to a transitive subgroup of $\mathfrak{S}_n$ and n divides the order of G.*

PROOF: Let $\alpha = \alpha_1, \ldots, \alpha_n$ be distinct roots of $f(x)$ and $E = F(\alpha_1, \ldots, \alpha_n)$ be the splitting field. Since $F(\alpha) \subseteq E$, $[F(\alpha) : F]$ is a divisor of $[E : F]$. Hence $n = [F(\alpha) : F]$ divides $|G| = [E : F]$.

For any $i \neq j$ there is a field isomorphism $\sigma : F(\alpha_i) \to F(\alpha_j) : \alpha_i \mapsto \alpha_j$ such that $\sigma|_F = id_F$. Since E is a splitting field of $f(x)$ over $F(\alpha_i)$ and $F(\alpha_j)$ there is $\psi : E \to E$ which extends σ. Clearly ψ is an automorphism of E that maps α_i to α_j. Hence $\mathrm{Gal}_F(f)$ is a transitive subgroup of $\mathfrak{S}_n$. □

10.3 Quartic Polynomials

Now we consider a quartic polynomial. Let F be a field of characteristic not 2. A general quartic polynomial in $F[x]$ is of the form

$$\tilde{p}(x) = x^4 + \tilde{a}x^3 + \tilde{b}x^2 + \tilde{c}x + \tilde{d} \in F[x]$$

By replacing x with $(x - \frac{\tilde{a}}{4})$ it suffices to consider

$$p(x) = x^4 + bx^2 + cx + d$$

If $p(x)$ is irreducible and separable, by the above theorem $G = \mathrm{Gal}_F(f)$ is a transitive subgroup of $\mathfrak{S}_4$, the order of which is divisible by 4. The possibilities are $\mathfrak{S}_4$, A_4, D_4, V, and C_4. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of $p(x)$. Set

$$u = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$v = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$w = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

Notice that u, v, w are all distinct. Every $\psi \in \mathrm{Gal}_F(p)$ permutes the roots of $p(x)$, and so permutes $\{u, v, w\}$. Hence we have

$$g_p(x) := (x-u)(x-v)(x-w) \in F[x]$$

It can be computed that

$$g_p(x) = x^3 - bx^2 - 4dx + 4bd - c^2$$

Notice that

$$\begin{aligned} u - v &= (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) \\ v - w &= (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) \\ w - u &= (\alpha_1 - \alpha_3)(\alpha_4 - \alpha_2) \end{aligned}$$

and hence $D(g_p) = D(p)$. We call g_p the resolvent cubic of $p(x)$.

10.7 Lemma. *Let F be a field of characteristic not 2. Let $p(x) = x^4 + bx^2 + cx + d \in F[x]$ be irreducible and separable and g_p be its resolvent cubic (as above). Let*

$$E = F(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \text{ and } L = F(u, v, w)$$

be the splitting fields of p and g_p respectively. Under the Galois correspondence for $G = Gal_F(p) = Gal_F(E)$, L corresponds to the subgroup $G \cap V$. It follows that

$$Gal_F(g_p) = Gal_F(L) \cong G/G \cap V$$

PROOF: (Sketch) Since all elements of V fix u, v, w, we have $G \cap V \subseteq L^* = \mathrm{Gal}_F(L)$. Hence to show that $G \cap V = L^*$ it suffices to show that all elements of $G \setminus V$ move at least one of u, v, w. Just check all 20 possibilities (or check 5 representatives from the cosets of $\mathfrak{S}_4/V$). Notice that V is a normal subgroup of $\mathfrak{S}_4$ and so is G, so $G \cap V$ is normal. By Theorem 7.3 L is a Galois extension of F and $\mathrm{Gal}_F(L) \cong G/G \cap V$. □

Let $m = |\mathrm{Gal}_L(E)| = |G/G \cap V|$. We have the following table

G	$\mathfrak{S}_4$	A_4	D_4	V	C_4
$G \cap V$	V	V	V	V	C_2
$G/G \cap V$	$\mathfrak{S}_3$	C_3	C_2	C_1	C_2
m	6	3	2	1	2

In the case $m = 2$, $g_p(x)$ has exactly one root in F, say $u \in F$ and $v, w \notin F$. Since either $G \cong D_4$ or C_4 and both D_4 and C_4 contain a 4-cycle, there is an element in G of order 4. Since $u = \alpha_1\alpha_2 + \alpha_3\alpha_4$ we have $\sigma = (1\ 2\ 3\ 4) \in G$ and $\sigma^2 = (1\ 2)(3\ 4) \in G$. Consider

$$x^2 - ux + d = (x - \alpha_1\alpha_2)(x - \alpha_3\alpha_4)$$

Notice that

$$(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) + (\alpha_1\alpha_2 + \alpha_3\alpha_4) = b$$

Hence we have

$$x^2 + (b - u) = (x - (\alpha_1 + \alpha_2))(x - (\alpha_3 + \alpha_4))$$

since the roots sum to zero. Assume that $G \cong C_4 = \langle\sigma\rangle$. Then $\mathrm{Gal}_L(E) = G \cap V = \langle\sigma^2\rangle$. Also, σ^2 fixes $\alpha_1\alpha_2, \alpha_3\alpha_4, \alpha_1 + \alpha_2, \alpha_3 + \alpha_4$. Hence $x^2 - ux + d, x^2 + b - u \in F[x]$ and they split over L.

Conversely, if $x^2 - ux + d, x^2 + b - u$ split over L then $\alpha_1 + \alpha_2, \alpha_1\alpha_2 \in L$. Since α_1 is a root of $x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2$, we have $[L(\alpha_1) : L] = 2$. Consider $L(\alpha_1)$. Since $\alpha_1 + \alpha_2 \in L$, we have $\alpha_2 \in L$. Also, $v, w \in L$ give a system of linear equations for α_3, α_4 which can be solved in L. Hence $L(\alpha_1) = E$. Hence $[E : L] = 2$ and $[L : F] = m = 2$ we have $[E : F] = 4$. Thus $G \cong C_4$. We have proven

10.8 Theorem. *Let F be a field of characteristic not 2. Let $p(x) = x^4 + bx^2 + cx + d \in F[x]$ be irreducible and separable and $g_p = x^3 - bx^2 - 4dx + 4bd - c^2$ be its resolvent cubic. Let $m = |Gal_F(g_p)|$. Then*

$$Gal_F(p) \cong \begin{cases} \mathfrak{S}_4 & \text{if } m = 6 \\ A_4 & \text{if } m = 3 \\ D_4 \text{ or } C_4 & \text{if } m = 2 \\ V & \text{if } m = 1 \end{cases}$$

In the case of $m = 2$, let u be the root of g_p that belongs to F. We have $Gal_F(p) \cong C_4$ if and only if the polynomials $x^2 - ux + d$ and $x^2 + (b - u)$ split over L, the splitting field of g_p.

10.9 Example. The polynomial $p(x) = x^4 - 2x - 2 \in \mathbb{Q}[x]$ is irreducible by Eisenstein's criterion. Its resolvent cubic is $g_p(x) = x^3 + 8x - 4$ and is irreducible over $\mathbb{Q}$. We have $D(g_p) = -4(8^3) - 27(-4)^2 = -155 \cdot 4^4$, which is not a square in $\mathbb{Q}$. Hence by Theorem 10.4 we have $\mathrm{Gal}_{\mathbb{Q}}(g_p) \cong \mathfrak{S}_3$, i.e. $m = 6$. Hence by Theorem 10.8 we have $\mathrm{Gal}_{\mathbb{Q}}(p) \cong \mathfrak{S}_4$.

Remark. We have seen that $\alpha \in \mathbb{R}$ is constructible only if the minimal polynomial of α has degree a power of 2. The converse of this is false. For example, let α be a real root of $p(x) = x^4 - 2x - 2$. If E is the splitting field of $p(x)$ then $\mathrm{Gal}_{\mathbb{Q}}(E) \cong \mathfrak{S}_4$. By Theorem 8.9, α is constructible if and only if $\mathrm{Gal}_{\mathbb{Q}}(E)$ is a 2-group. Hence α is not constructible even though it's minimal polynomial has degree 4, a power of 2.

10.10 Example.

1. Consider the irreducible polynomial $p(x) = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$. Its resolvent cubic is $g_p(x) = x^3 + 10x^2 - 4x - 40 = (x + 10)(x - 2)(x + 2)$. Hence $\mathrm{Gal}_{\mathbb{Q}}(g_p)$ is trivial and so $\mathrm{Gal}_{\mathbb{Q}}(p) \cong V$.
2. Consider the irreducible polynomial $p(x) = x^4 + 5x + 5 \in \mathbb{Q}[x]$. Its resolvent cubic is $g_p(x) = x^3 - 20x - 25 = (x - 5)(x^2 + 5x + 5)$. Hence $m = 2$. Let L be the splitting field of g_p. Since the roots of g_p are $5, \frac{-5 \pm \sqrt{5}}{2}$, we have $L = \mathbb{Q}(\sqrt{5})$. Hence $\mathrm{Gal}_p(p) \cong C_4$.

11 Solvability by Radicals

11.1 Cardano's Formula

For simplicity, we will assume that F is a field of characteristic not 2 or 3. We all know the quadratic formula: the roots of $x^2 + bx + c \in F[x]$ are $\frac{-b \pm \sqrt{b^2 - 4c}}{2}$. An expression of this type, involving only $+, -, \times, \div$, and $\sqrt[n]{\cdot}$ is called a radical. We consider the cubic equation $x^3 + bx + c = 0 \in F[x]$. Set $x = u + v$, where u and v are indeterminates. We obtain

$$\begin{aligned} 0 &= x^3 + bx + c \\ &= (u + v)^3 + b(u + v) + c \\ &= u^3 + v^3 + (3uv + b)(u + v) + c \\ &= u^3 + v^3 + c \end{aligned}$$

by imposing the condition that $uv = \frac{-b}{3}$. Letting $\alpha = u^3$ and $\beta = v^3$ we have $\alpha + \beta = -c$ and $\alpha\beta = \left(\frac{-b}{3}\right)^3$. Hence α and β are roots of the quadratic

$$y^2 + cy - \left(\frac{b}{3}\right)^3 = 0$$

Thus by the above formula we have

$$\alpha, \beta = \frac{-c \pm \sqrt{c^2 + 4(b/3)^3}}{2} = \frac{-c}{2} \pm \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}$$

There seems to be 3 choices for each of u and v, but the imposed conditions narrow them down to just 3. We have proven

11.1 Theorem. *(Tartaglia, del Ferro, Fontana) The solutions fo the cubic equation $x^3 + bx^2 + c = 0$ are of the form*

$$\alpha_1 = \sqrt[3]{\frac{-c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \sqrt[3]{\frac{-c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}}$$

$$\alpha_2 = \zeta_3 \sqrt[3]{\frac{-c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \zeta_3^2 \sqrt[3]{\frac{-c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}}$$

$$\alpha_3 = \zeta_3^2 \sqrt[3]{\frac{-c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \zeta_3 \sqrt[3]{\frac{-c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}}$$

Where the cubic roots are chosen such that

$$\sqrt[3]{\frac{-c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} \cdot \sqrt[3]{\frac{-c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} = \frac{-b}{3}$$

Consider $x^4 + bx^2 + cx + d \in F[x]$. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots. We have seen before the that resolvent cubic is defined to be $g(x) = x^3 - bx^2 - 4dx + 4bd - c^2$ where the roots of g are

$$u = \alpha_1\alpha_2 + \alpha_3\alpha_4$$
$$v = \alpha_1\alpha_3 + \alpha_2\alpha_4$$
$$w = \alpha_1\alpha_4 + \alpha_2\alpha_3$$

Applying the Cardano formula for cubics, we can obtain u, v, w. Notice that

$$\begin{aligned} u + v = -(\alpha_1 + \alpha_4)^2 &\quad\longleftrightarrow\quad \alpha_1 + \alpha_4 = \pm\sqrt{u+v} \\ v + w = -(\alpha_1 + \alpha_2)^2 &\quad\longleftrightarrow\quad \alpha_1 + \alpha_2 = \pm\sqrt{v+w} \\ w + u = -(\alpha_1 + \alpha_3)^2 &\quad\longleftrightarrow\quad \alpha_1 + \alpha_3 = \pm\sqrt{w+u} \end{aligned}$$

It appears as though there are 8 choices for the signs. However, we know that

$$(\alpha_1 + \alpha_4)(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3) = -c$$

and this cuts down the choices. Now

$$(\alpha_1 + \alpha_4) + (\alpha_1 + \alpha_2) + (\alpha_1 + \alpha_3) = 2\alpha_1$$

and we can get similar expressions for the other roots. We have almost proven

11.2 Theorem. *(Ferrari) The solutions of the quartic equation $x^4 + bx^2 + cx + d = 0$ are of the form*

$$\alpha_1 = \frac{1}{2}\left(\sqrt{-u-v} + \sqrt{-v-w} + \sqrt{-w-u}\right)$$

$$\alpha_2 = \frac{1}{2}\left(-\sqrt{-u-v} - \sqrt{-v-w} + \sqrt{-w-u}\right)$$

$$\alpha_3 = \frac{1}{2}\left(-\sqrt{-u-v} + \sqrt{-v-w} - \sqrt{-w-u}\right)$$

$$\alpha_4 = \frac{1}{2}\left(\sqrt{-u-v} - \sqrt{-v-w} - \sqrt{-w-u}\right)$$

where the square roots are chosen such that

$$(\sqrt{-u-v})(\sqrt{-v-w})(\sqrt{-w-u}) = -c$$

11.2 Solvable groups

11.3 Definition. If G is a group and N is a subgroup of G then N is normal if $gNg^{-1} = N$ for all $g \in G$. We write $N \lhd G$. A group G is solvable if there is a tower

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$$

where $G_{i+1} \lhd G_i$ and G_i/G_{i+1} is Abelian for $i = 0, \ldots, m-1$.

11.4 Example. The symmetric group $\mathfrak{S}_4$ is solvable. Notice that A_4 and V are normal subgroups of $\mathfrak{S}_4$.

$$\mathfrak{S}_4 \supseteq A_4 \subseteq V \supseteq \{1\}$$

and $\mathfrak{S}_4/A_4 \cong C_2$ and $A_4/V \cong C_3$. These quotients are Abelian, so $\mathfrak{S}_4$ is solvable.

11.5 Theorem. *(Second Isomorphism Theorem) If H, N are subgroups of G with $N \lhd G$ then*

$$H/H \cap N \cong NH/N$$

11.6 Theorem. *(Third Isomorphism Theorem) If G a group and $H, N \lhd G$ such that $N \subseteq H$ then $H/N \lhd G/N$ and*

$$(G/N)/(H/N) \cong G/H$$

11.7 Theorem. *If G is a solvable group, then every subgroup and every quotient group of G is solvable. Conversely, if $N \lhd G$ and both N and G/N are solvable then G is solvable.*

PROOF: Suppose that G is a solvable group with tower

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$$

where $G_{i+1} \lhd G_i$ and G_i/G_{i+1} is Abelian for $i = 0, \ldots, m-1$.

Let H be a subgroup of G. Define $H_i = h \cap G_i$. Since $G_{i+1} \lhd G_i$ we have $H_{i+1} \lhd H_i$ for $i = 0, \ldots, m-1$ and

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$

Notice that H_i and G_{i+1} are subgroups of G_i and $H_{i+1} = H \cap G_{i+1} = H_i \cap G_{i+1}$. Applying the second isomorphism theorem to G_i, we have

$$H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \cong H_i G_{i+1}/G_{i+1} \subseteq G_i/G_{i+1}$$

Since G_i/G_{i+1} is Abelian, so is H_i/H_{i+1}. It follows that H is solvable.

Let N be a normal subgroup of N. We want that G/N is normal. Mulitplying by N, we have a tower

$$G = G_0N \supseteq G_1N \supseteq \cdots \supseteq G_mN = N$$

taking the quotient gives

$$G/N = G_0N/N \supseteq G_1N/N \supseteq \cdots \supseteq G_mN/N = \{1\}$$

Since $G_{i+1} \lhd G_i$ and $N \lhd G$, we have $G_{i+1}N \lhd G_iN$, which implies that $G_{i+1}N/N \lhd G_iN/N$. By the third isomorphism theorem, we have

$$(G_{i+1}N/N)/(G_iN/N) \cong G_{i+1}N/G_iN$$

Apply the second isomorphism theorem to get

$$G_{i+1}N/G_iN \cong G_i/G_i \cap G_{i+1}N$$

Since $G_{i+1} \subseteq G_i \cap G_{i+1}N$, there is a natural injection

$$G_i/G_i \cap G_{i+1}N \longrightarrow G_i/G_{i+1} : g + (G_i \cap G_{i+1}N) \longmapsto g + G_{i+1}$$

G_i/G_{i+1} is Abelian, so as is $G_i/G_i \cap G_{i+1}N$. Thus $(G_{i+1}N/N)/(G_iN/N)$ is Abelian and hence G/N is solvable.

Let N be a normal subgroup of G and suppose that N and G/N are solvable. Since N is solvable there is a tower

$$N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_m = \{1\}$$

where $N_{i+1} \lhd N_i$ and N_i/N_{i+1} is Abelian for $i = 0, \ldots, m-1$. For a subgroup $H \subseteq G$ with $N \subseteq H$, we denote $\overline{H} = H/N$. Since G/N is solvable, we have a tower

$$G/N = \overline{G}_0 \supseteq \overline{G}_1 \supseteq \cdots \supseteq \overline{G}_r = \{\overline{1}\}$$

where $\overline{G}_{i+1} \lhd \overline{G}_i$ and $\overline{G}_i/\overline{G}_{i+1}$ is Abelian for $i = 0, \ldots, r-1$. Let $\sigma : G \to G/N, H \to H/N$. For all $i = 0, \ldots, r$, define $G_i = \sigma^{-1}(\overline{G}_i)$. Since $N \lhd G$ and $\overline{G}_{i+1} \lhd \overline{G}_i$, we have $G_{i+1} \lhd G_i$. Moreover, by the third isomorphism threorem, $G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1}$ is Abelian. It follows that we have the tower

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_r = N = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_m = \{1\}$$

which shows that G is solvable. □

11.8 Example. Since $\mathfrak{S}_2 \subseteq \mathfrak{S}_3 \subseteq \mathfrak{S}_4$, we have that $\mathfrak{S}_2$ and $\mathfrak{S}_3$ are solvable.

11.9 Corollary. *If G is a finite solvable group then there is a tower*

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_m = \{1\}$$

$G_{i+1} \lhd G_i$ and G_i/G_{i+1} is cyclic of prime order for $i = 0, \ldots, m-1$.

11.10 Definition. A group G is simple if it is not the trivial group and it has no normal subgroups other than G and $\{1\}$.

The alternating group A_5 is simple, hence is not solvable. By Theorem 11.7, we conclude that $\mathfrak{S}_5$ is not solvable. Hence for all $n \geq 5$, since $\mathfrak{S}_n$ contains a subgroup isomorphic to $\mathfrak{S}_5$, so $\mathfrak{S}_n$ is not solvable.

Given a polynomial $f(x) \in F[x]$ of degree n, its Galois group $\mathrm{Gal}(f)$ is a subgroup of $\mathfrak{S}_n$. We will prove later that $f(x)$ has radical solutions if and only if $\mathrm{Gal}(f)$ is solvable. It follows (as had already been proven) that any polynomial of degree 2, 3, or 4 has radical solutions. Since $\mathfrak{S}_n$ is not solvable for $n \geq 5$, there are no radical solutions for a general polynomial of degree n.

11.3 Cyclic Extensions

11.11 Definition. A Galois extension E/F is *Abelian/cyclic/solvable* if $\mathrm{Gal}_F(E)$ has the corresponding property.

11.12 Lemma. *(Dedekind's Lemma) Let E and F be fields and $\psi_i : F \to E$ be distinct homomorphisms for $1 \leq i \leq n$. If $c_i \in E$ and*

$$c_1\psi_1(\alpha) + \cdots + c_n\psi_n(\alpha) = 0 \ \forall\, \alpha \in F$$

then $c_1 = \cdots = c_n = 0$.

PROOF: Suppose conversely. Let $m \geq 2$ be the smallest positive integer such that

$$c_1\psi_1(\alpha) + \cdots + c_m\psi_m(\alpha) = 0 \ \forall\, \alpha \in F$$

for some $c_1, \ldots, c_m \in E$ non-zero. Choose $\beta \in F$ such that $\psi_1(\beta) \neq \psi_2(\beta)$ and $\psi_1(\beta) \neq 0$. We have

$$c_1\psi_1(\beta\alpha) + \cdots + c_m\psi_m(\beta\alpha) = 0 \ \forall\, \alpha \in F$$

Dividing by $\psi_1(\beta)$ gives

$$c_1\psi_1(\alpha) + \frac{c_2}{\psi_1(\beta)}\psi_2(\beta\alpha) + \cdots + \frac{c_m}{\psi_1(\beta)}\psi_m(\beta\alpha) = 0 \ \forall\, \alpha \in F$$

Subtracting this equation from the original equation gives us

$$c_2\left(1 - \frac{\psi_2(\beta)}{\psi_1(\beta)}\right)\psi_2(\beta\alpha) + \cdots + c_m\left(1 - \frac{\psi_m(\beta)}{\psi_1(\beta)}\right)\psi_m(\beta\alpha) = 0 \ \forall\, \alpha \in F$$

a contradiction (since not all of these coefficients are zero). □

11.13 Theorem. *Let F be a field and n be a positive integer. Suppose that $ch(F) = 0$ or p, where $p \nmid n$. Assume that $x^n - 1$ splits over F.*

1. *If the Galois extension E/F is cyclic of degree n then $E = F(\alpha)$ for some $\alpha \in E$ and $\alpha^n \in F$. It follows that $x^n - \alpha^n$ is the minimal polynomial of α over F.*
2. *If $E = F(\alpha)$ and $\alpha^n \in F$ then E/F is a cyclic extension of degree d, where $d|n$ and $\alpha^d \in F$. It follows that $x^d - \alpha^d$ is the minimal polynomial of α over F.*

PROOF: Let $\zeta_n \in F$ be a primitive n^{th} root of unity.

1. Let $G = \mathrm{Gal}_F(E) = \langle\psi\rangle \cong C_n$. Apply Dedekind's lemma to domain and codomain E, $\psi_i = \psi^{i-1}$, $1 \leq i \leq n$, and $c_i = \zeta_n^{1-i}$. There exists $u \in E$ such that

   $$\alpha := u + \zeta_n^{-1}\psi(u) + \cdots + \zeta_n^{-(n-1)}\psi^{n-1}(u) \neq 0$$

   We have

   $$\psi(\alpha) = \psi(u) + \zeta_n^{-1}\psi^2(u) + \cdots + \zeta_n^{-(n-1)}\psi^n(u) = \alpha\zeta_n$$

   Since $\zeta_n \in F$ it follows that $\psi^i(\alpha) = \alpha\zeta_n^i$. Also, $\psi(\alpha^n) = \alpha^n$, so $\alpha^n \in E^G = F$ (since ψ generates G). Therefore $\alpha, \alpha\zeta_n, \ldots, \alpha\zeta_n^{n-1}$ are roots of $x^n - \alpha^n \in F[x]$. If $p(x) \in F[x]$ is the minimal polynomial of α, then all of the conjugates of α are also roots of $p(x)$, so we must have $p(x) = x^n - \alpha^n$. Moreover, since $F(\alpha) \subseteq E$ and $[F(\alpha) : F] = \deg p = n = [E : F]$ we must have $E = F(\alpha)$.

2. Let $p(x) \in F[x]$ be the minimal polynomial of α over F. Since $\alpha^n \in F$, α is a root of $x^n - \alpha^n \in F[x]$. Thus $p(x) | x^n - \alpha^n$, and the roots of $p(x)$ are of the form $\alpha\zeta_n^i$ for some i and ζ_n a primitive n^{th} root of unity in F. We have $p(0) = \pm\alpha^d\zeta_n^k$ for some k and $d = \deg p$. Since $p(0), \zeta_n^k \in F$, it follows that $\alpha^d \in F$, and so α is a root of $x^d - \alpha^d \in F[x]$. This polynomial has the same degree as p and is monic, so $p(x) = x^d - \alpha^d$. $d|n$ because if $n = qd + r$ for $r < d$ then we have $\alpha^r = \alpha^{n-qd} = \alpha^n(\alpha^{-d})^q \in F$, a contradiction unless $r = 0$ (since otherwise α would be a root of $x^r - \alpha^r \in F[x]$, contradicting that α has degree d over F). Write $n = md$, and the roots of p are $\alpha, \alpha\zeta_n^m, \ldots, \alpha\zeta_n^{(d-1)m}$. If $\psi \in G$ satisfies $\psi(\alpha) = \alpha\zeta_n^m$, then $G = \langle\psi\rangle$ is cyclic of order d. □

11.14 Theorem. *Let F be a field of characteristic p.*

1. *If $x^p - x - a \in F[x]$ is irreducible, then its splitting field E/F is cyclic of degree p.*
2. *Theo converse of (1) is also true, that is, every cyclic extension of F of degree p is the splitting field of some irreducible polynomial $x^p - x - a \in F[x]$.*

PROOF: Assignment. □

11.4 Radical Extensions

For simplicity, we assume in this section that F is a field of characteristic 0.

11.15 Definition. A finite extension E/F is called a radical extension if there exists a tower of subfields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = E$$

and $\alpha_i \in F_i$, $i = 1, \ldots, k$, such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some integer $d_i \geq 1$.

Notice in particular that every constructible extension is a radical extension. In this case, $d_i = 1$ or 2 for each i.

11.16 Lemma. *If E/F is a radical extension, then its normal closure N/F is also a radical extension.*

PROOF: Since $\text{ch}(F) = 0$ and E/F is a finite extension, by Theorem 4.14, E/F is a simple extension. Write $E = F(\alpha)$. Since E/F is a radical extension, there is a tower of subfields

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = E$$

and $\alpha_i \in F_i$, $i = 1, \ldots, k$, such that $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$ for some integer $d_i \geq 1$. Let $p(x) \in F[x]$ be the minimal polynomial of α and N/E a splitting field of $p(x)$ over E. Then N/F is a splitting field of $p(x)$ over F and is a normal closure of E/F. Let $\alpha = \alpha_1, \ldots, \alpha_n$ be the roots of p in N. There is a field isomorphism $\sigma_i : F(\alpha) \to F(\alpha_i)$ such that $\sigma_i|_F = id$ and $\alpha \mapsto \alpha_i$ for $i = 2, \ldots, n$. Since N can be viewed as a splitting field of p over $F(\alpha)$ and $F(\alpha_i)$ respectively, there is $\psi_i : N \to N$ which extends σ_i. Hence $\psi_i \in \text{Gal}_F(N)$ and $\psi_i(\alpha) = \alpha_i$. We have

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = E = F(\alpha) = F(\alpha_1)\psi_2(F_0) \subseteq$$
$$F(\alpha_1)\psi_2(F_1) \subseteq \cdots \subseteq F(\alpha_1)\psi_2(F_k) = F(\alpha_1, \alpha_2) \subseteq \cdots \subseteq F(\alpha_1, \ldots, \alpha_n) = N$$

Notice that since $F_i = F_{i-1}(\beta_i)$ and $\beta_i^{d_i} \in F_{i-1}$ for some $\beta \in F_i \setminus F_{i-1}$, we have

$$F(\alpha_1, \ldots, \alpha_{j-1})\psi_j(F_i) = F(\alpha_1, \ldots, \alpha_{j-1})\psi_j(F_{i-1}(\beta_i)) = F(\alpha_1, \ldots, \alpha_{j-1})\psi_j(F_{i-1})\psi_j(\beta_i)$$

and $(\psi_j(\beta_i))^{d_i} = \psi_j(\beta_i^{d_i}) \in \psi_j(F_{i-1})$. This shows that N/F is a radical extension. □

11.5 Solving polynomials by Radicals

11.17 Definition. Let $f(x) \in F$. We say that f is solvable by radicals if there is a radical extension E/F such that f splits over E. It follows that the equation $f(x) = 0$ has radical solutions.

11.18 Lemma. *If K, L are intermediate fields of E/F with K/F a finite Galois extension, then KL is a finite Galois extension over L and $Gal_L(KL)$ is isomorphic to a subgroup of $Gal_F(K)$.*

PROOF: Suppose that K is the splitting field of $f(x) \in F[x]$ over F. Then KL is a splitting field of $f(x)$ over L. Hence KL/L is a finite Galois extension. Consider

$$\Gamma : \mathrm{Gal}_L(KL) \to \mathrm{Gal}_F(K) : \psi \mapsto \psi|_K$$

This map is well defined since K is normal. Moreover, if $\psi|_K = id_K$ then ψ is trivial on K and L, so must be equal to id_{KL}. Thus Γ is an injection. Therefore $\mathrm{Gal}_L(KL)$ is isomorphic to a subgroup of $\mathrm{Gal}_F(K)$. □

11.19 Theorem. *Let F be a field of characteristic zero and let $f(x) \in F[x]$ with $f \neq 0$. Then $f(x)$ is solvable by radicals if and only if its Galois group $Gal(f)$ is a solvable group.*

PROOF: Assume that $G = \mathrm{Gal}(f)$ is solvable. Let E/F be a splitting field of f over F. Let $n = |G|$ and L/E be a splitting field of $x^n - 1$ over E (so that $L = E(\zeta_n)$ for some primative n^{th} root of unity). Let $K = F(\zeta_n)$ be the splitting field of $x^n - 1$ over F. We have $L = KE$. Since E/F is a finite Galois extension, by the previous lemma L/K is a finite Galois extension and $H = \mathrm{Gal}_K(L)$ is isomorphic to a subgroup of G. Hence H is solvable since G is solvable. Write

$$H = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_m = \{1\}$$

where $H_{i+1} \lhd H_i$ and $H_i/H_{i+1} \cong C_{d_i}$ (cyclic of order d_i). Let $K_i = H_i^* = L^{H_i}$ for $i = 0, \ldots, m$. Then $\mathrm{Gal}_{K_i}(L) \cong H_i$, so we have a tower of fields

$$F \subseteq F(\zeta_n) = K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L = E(\zeta_n)$$

Since $H_{i+1} \lhd H_i$, K_{i+1}/K_i is Galois and the Galois group is isomorphic to $H_i/H_{i+1} \cong C_{d_i}$. By Theorem 11.13 there is $\alpha_{i+1} \in K_{i+1}$ such that $K_{i+1} = K_i(\alpha_{i+1})$ and $\alpha_{i+1}^{d_{i+1}} \in K_i$. It follows that L/F is a radical extension. Since all the roots of f are in E and hence in L, we conclude that f is solvable by radicals.

Suppose $f(x)$ is solvable by radical, so that f splits over some extension E/F with

$$F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = E$$

where $F_i = F_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1}$. By lemma 11.16 we may assume that E/F is Galois. Let $n = \prod_{i=1}^m d_i$ and let L/E be the splitting field of $x^n - 1$ over E. Set $K = F(\zeta_n)$ and we have $L = E(\zeta_n) = KE$. Define $K_i = F_i(\zeta_n) = KF_i$, so that $K_i = K_{i-1}(\alpha_i)$ and $\alpha_i^{d_i} \in F_{i-1} \subseteq K_{i-1}$. Since $\alpha_i^{d_i} \in K_{i-1}$, K_i is a splitting field of $x^{d_i} - \alpha^{d_i}$ over K_{i-1}. Then K_i/K_{i-1} is cyclic, and so we have

$$F \subseteq F(\zeta_n) = K \subseteq K_1 \subseteq \cdots \subseteq K_m = F_m(\zeta_n) = L$$

Notice that L is a splitting field of $f(x)(x^n - 1)$ over F, hence L/F is Galois. Each K_i is an intermediate field of L/F, so K_i is Galois. Applying the Galois correspondence we have

$$G = \mathrm{Gal}_F(L) \supseteq \mathrm{Gal}_K(L) \supseteq \mathrm{Gal}_{K_1}(L) \supseteq \cdots \supseteq \mathrm{Gal}_{K_m}(L) = \{1\}$$

For each $\sigma \in \mathrm{Gal}_{K_i}(L)$, $\psi \in \mathrm{Gal}_{K_{i+1}}(L)$, we have

$$\sigma\psi\sigma^{-1}\Big|_{K_{i+1}} = id_{K_{i+1}}$$

Hence $\mathrm{Gal}_{K_{i+1}}(L) \lhd \mathrm{Gal}_{K_i}(L)$, and moreover we have $\mathrm{Gal}_{K_i}(L)/\mathrm{Gal}_{K_{i+1}}(L) \cong \mathrm{Gal}_{K_i}(K_{i+1})$, which is cyclic (and hence Abelian). Also, $\mathrm{Gal}_F(L)\mathrm{Gal}_{K_0}(L) \cong \mathrm{Gal}_F(F(\zeta_n))$, which is also Abelian. Therefore $\mathrm{Gal}_F(L)$ is solvable. Since $\mathrm{Gal}_F(E) \cong \mathrm{Gal}_F(L)/\mathrm{Gal}_E(L)$, $\mathrm{Gal}(f) = \mathrm{Gal}_F(E)$ is solvable as well. □

11.20 Proposition. *Let $f(x) \in \mathbb{Q}[x]$ be irreducible of prime degree p. If $f(x)$ contains precisely two non-real roots in $\mathbb{C}$ then $\mathrm{Gal}(f) \cong \mathfrak{S}_p$.*

PROOF: Recall that the symmetric group $\mathfrak{S}_n$ is generated by $(1\ 2)$ and $(1\ 2\ \ldots\ n)$. Hence to show that $\mathrm{Gal}(f)$ is isomorphic to $\mathfrak{S}_p$ it suffices to find a 2-cycle and a p-cycle. Since f is irreducible with degree p, p divides the order of $\mathrm{Gal}(f)$. By Cauchy's Theorem there is an element of $\mathrm{Gal}(f)$ of order p – a p-cycle. Complex conjugation will juxtapose the non-real roots of f and leave all other (real) roots fixed. Hence complex conjugation is a 2-cycle in $\mathrm{Gal}(f)$. □

Consider $f(x) = x^5 + 2x^3 - 24x - 2 \in \mathbb{Q}[x]$, which is irreducible by Eisensteins's criterion. Since $f(-1) = 19$, $f(1) = -23$, $\lim_{x\to\infty} f(x) = \infty$, and $\lim_{x\to-\infty} f(x) = -\infty$, f has at least three real roots. Let $a_1, \ldots, a_5$ be the roots of $f(x)$. We have $a_1 + \cdots + a_5 = 0$ and $\sum_{i<j} a_i a_j = 2$. From the first sum,

$$0 = \left(\sum_{i=1}^{5} a_i\right)^2 = \sum_{i=1}^{5} a_i^2 + 2\sum_{i<j} a_i a_j$$

so $\sum_{i=1}^{5} a_i^2 = -4$, and not all of the roots of f can be real. Therefore f has exactly three real roots and two non-real roots. By the above proposition, $\mathrm{Gal}(f) \cong \mathfrak{S}_5$. Since $\mathfrak{S}_5$ is not solvable, the equation

$$x^5 + 2x^3 - 24x - 2 = 0$$

does not have radical solutions.

11.21 Theorem. *(Abel) The general polynomial equation $f(x) = 0$ with $\deg f \geq 5$ is not solvable by radical solutions. In other words, we have radical solutions for $f(x) = 0$ if and only if $f(x) \leq 4$.*

11.6 Probabilistic Galois Theory

(Extra Section)

Indeed, for almost all $f(x) \in \mathbb{Z}[x]$ with degree n, $\mathrm{Gal}(f) \cong \mathfrak{S}_n$. Since $\mathfrak{S}_n$ is not solvable for $n \geq 5$, by Theorem 11.19, f is not solvable by radicals for almost all $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 5$. The study of "density" of polynomials $f(x)$ of degree n with $\mathrm{Gal}(f)$ isomorphic to certain subgroups of $\mathfrak{S}_n$ is called probabilistic Galois theory.

Notation. Let $f(x)$ and $g(x)$ be two functions. If there exists a constant C such that $|f(x)| \leq Cg(x)$ when x is sufficiently large, we write $f(x) \ll g(x)$ or $f(x) = O(g(x))$.

For example, since $\lim_{x\to\infty} \frac{x^{n-1}(\log x)^r}{x^n} = 0$ we have $x^{n-1}(\log x)^r \ll x^n$ for any r.

Consider $E_n(N) = \#\{f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \mid |a_i| \leq N, \mathrm{Gal}(f) \subsetneqq \mathfrak{S}_n\}$. Notice that if $a_0 = 0$ then $f(x) = x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$. Since $x = 0 \in \mathbb{Q}$, $\mathrm{Gal}(f) = \mathrm{Gal}(f/x) \subseteq \mathfrak{S}_{n-1} \subsetneqq \mathfrak{S}_n$. For each $a_{n-1}, \ldots, a_1$ with $|a_i| \leq N$ there are $2N+1$ choices for each of them, so there are $(2N+1)^{n-1}$ polnomials with $a_0 = 0$ and Galois group a proper subgroup of $\mathfrak{S}_n$. If follows that

$$E_n(N) \geq (2N+1)^{n-1} = 2^{n-1}N^{n-1} + O(N^{n-2}) >> N^{n-1}$$

11.22 Conjecture. *(van der Waerden) $E_n(N) \ll N^{n-1}$.*

This question remains open today. The best result known for this problem is due to Gallagher, who proves that $E_n(N) \ll N^{n-\frac{1}{2}}(\log N)$ by the large sieve method. In any case (i.e. whether the conjecture is true or not), since there are $(2N+1)^n$ many polynomials of the form $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ with $|a_i| \leq N$, we have

$$\#\{f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x] \mid |a_i| \leq N, \mathrm{Gal}(f) \cong \mathfrak{S}_n\} = (2N+1)^n + O(N^{n-\frac{1}{2}}(\log N))$$

Since

$$\lim_{N\to\infty} \frac{(2N+1)^n + O(N^{n-\frac{1}{2}}(\log N))}{(2N+1)^n} = 1$$

we conclude that for almost all (i.e. with probability 1) $f(x) \in \mathbb{Z}[x]$ of degree n, $\mathrm{Gal}(f) \cong \mathfrak{S}_n$.

Consider the special case of the Galois group of cubics. Define

$$E_3(N) = \{f(x) = x^3 + bx^2 + cx + d \in \mathbb{Z}[x] \mid H(f) \leq N, \mathrm{Gal}(f) \subsetneqq \mathfrak{S}_3\}$$

where $H(f) =$ height of $f = \max\{|b|, |c|, |d|\}$. Our goal is prove that $E_3(N) \ll N^{2+\varepsilon}$.

11.23 Theorem. *(van der Waerden)*

$$\#\{f(x) = x^3 + bx^2 + cx + d \in \mathbb{Z}[x] \mid H(f) \leq N, f \text{ is reducible}\} \ll N^2$$

Hence, to prove $E_3(N) \ll N^{2+\varepsilon}$ it suffices to consider irreducible polynomials. Let $f(x) = x^3 + bx^2 + cx + d$ be irreducible. If $\mathrm{Gal}(f) \subsetneqq \mathfrak{S}_3$, then $\mathrm{Gal}(f) \cong A_3$. We recall that the discriminant $D(f)$ is $b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd$. By Theorem 10.4, $\mathrm{Gal}(f) \cong A_3 \iff D(f) = z^2$ for some $z \in \mathbb{Z}$. Hence, to compute $E_3(N)$ if suffices to compute the number of $z \in \mathbb{Z}$ such that $b^2c^2 - 4c^3 - 4b^3d - 27d^2 + 18bcd = z^2$. That is,

$$27(d)^2 + (4b^3 - 18bc)d + z^2 + (4c^3 - b^2c^2) = 0 \tag{1}$$

11.24 Theorem. *Suppose that $Q(x,y) = \tilde{a}x^2 + \tilde{b}xy + \tilde{c}y^2 + \tilde{d}x + \tilde{e}y + \tilde{f}$ is a quadratic polynomial with coefficients in $\mathbb{Z}$. Assume that the absolute values of all coefficients of $Q(x,y)$ are bounded by N. Then*

$$\#\{(x,y) \in \mathbb{Z}^2 \mid Q(x,y) = 0, |x|, |y| \leq M\} \ll (MN)^\varepsilon$$

Consider equation (1). Since $|d| \leq N$ and $|z| \leq N^2$, for fixed b, c, the number of choices of d and z is $\ll (NN^2)^\varepsilon \ll N^\varepsilon$. It follows that $E_3(N) \ll N^{2+\varepsilon}$.