

Field Theory

Notes taken by Yeheli Fomberg <yp@campus.technion.ac.il>

Based on lectures by Chen Meiri

Spring 2025

These notes are not endorsed by the lecturers. I have revised them outside lectures to incorporate supplementary explanations, clarifications, and material for fun. While I have strived for accuracy, any errors or misinterpretations are most likely mine.

Contents

0	Introduction	3
1	Field extensions and basic definitions	4
1.1	The field	4
1.2	Field extensions	5
1.3	Algebraic extensions	7
1.4	The multiplicative group of a finite field	11
1.5	Algebraically closed fields	11
2	Ruler and compass constructions	13
2.1	The system	13
2.2	Simple constructions	13
2.3	Lines and circles	16
3	Introduction to Galois theory	19
3.1	Splitting fields	19
3.2	The automorphism group of a field	22
3.3	The automorphism group of a field extension	23
3.4	Galois correspondence	26
4	Separable extensions	31
4.1	Separable polynomials and separable extensions	31
4.2	Finite fields	33
4.3	Embeddings of field extensions	34
5	Normal and Galois extensions	37
5.1	Normal extensions	37
5.2	Galois extensions	39
6	The Fundamental Theorem of Galois Theory	40
6.1	A different criterion for a finite Galois extension	40
6.2	The fundamental theorem of Galois theory	41
7	Corollaries from Galois theory	45
7.1	Ruler and compass constructions	45
7.2	Simple extensions and the primitive element theorem	47
7.3	The fundamental theorem of algebra	48
8	Solving equations using radicals	50
8.1	Radical extensions and Dedekind's lemma	50
8.2	Radical extensions and solvable Galois groups	52
8.3	Galois groups of polynomials of degree $n \leq 4$	54
9	Transcendence degree	57

0 Introduction

Definition 0.1 (Finite field extension). Let E and F be fields. We say that E/F is a finite field extension if

- (1) $F \subseteq E$
- (2) $\dim_F(E) < \infty$

Remark 0.1. Under certain conditions the fundamental theorem of Galois theory says that there exists a bijection between $\{F \subseteq L \subseteq E \mid L \text{ is a field}\}$ and the set of subgroups of the automorphism group $\text{Aut}(E/F) := \{\alpha \in \text{Aut}(E) \mid \alpha|_F = \text{id}_F\}$.

Remark 0.2. We can apply this theory when considering straightedge and compass constructions.

Example 0.1. Given a set of points in the plane so that $(0, 0) \in S$. We can

- (1) construct an edge between any two points in S ;
- (2) construct a circle with center $s \in S$.

We can construct points in the following ways:

- (1) intersection of two lines;
- (2) intersection of two circles;
- (3) intersection of a line and a circle.

Each point that we can construct in a finite sequence of these steps is called a constructable point (from S).

Question. Which points can be constructed from S ?

Remark 0.3. We will see that $(\sqrt{2}, 0)$ can be constructed from $S = \{(0, 0), (1, 0)\}$ but $(\sqrt[3]{2}, 0)$ cannot.

Remark 0.4. Let F be a field a characteristic 0. The roots of the polynomial $p(x) = x^2 + bx + c$ are given by

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

There exists a finite field extension so that

- (1) $\dim_F(E) = 2$;
- (2) there exists $a \in E$ so that $E = F(a)$;
- (3) $a^2 \in F$.
- (4) the polynomial splits into linear factors over E . This means that the roots of $p(x)$ are in E .

In fact (1) follows from (2) and (3).

Remark 0.5. Let F be a field with $\text{char}(F) = 0$ and let h be a polynomial of with $\deg(h) \leq 4$. Then there exists a finite field extension E/F , elements $a_1, \dots, a_k \in E$ and natural number $m_1, \dots, m_k$ so that

- (1) $h(x)$ splits into linear factors over E ;
- (2) $E = F(a_1, \dots, a_k)$;
- (3) for all $1 \leq k \leq i$ we have $a_i^{m_i} \in F$.

We will show that if $\deg(h) \geq 5$ then this property does not hold always.

1 Field extensions and basic definitions

1.1 The field

Definition 1.1 (Field). A field is triplet $(F, +, *)$ so that

- (1) $(F, +)$ is an abelian group, its unit is denoted by 0_F ;
- (2) $(F \setminus \{0\}, *)$ is a group, its unit is denoted by 1_F ;
- (3) the distributive property hold. For any $a, b, c \in F$ we have

$$a(b + c) = ab + ac.$$

Equivalently, a field is a commutative ring with unit where every nonzero element is a unit.

Remark 1.1. Another equivalent definition for a field, is a commutative ring with unit R , such that its only proper ideal is the zero ideal.

Example 1.1. We have that $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ and all of them are fields with the standard operations.

Example 1.2. The set $\mathbb{Q}(i) = \{x \in \mathbb{C} \mid \exists a, b \in \mathbb{Q} \text{ s.t. } x = a + bi\}$ is a field with the induced operations from $\mathbb{C}$. It is clear that $\mathbb{Q}(i)$ is a commutative ring so we can see it is a field by showing that every nonzero element is invertible. Indeed if $a + bi \neq 0$ then

$$a + bi \left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \right) = 1$$

which completes the proof.

Example 1.3. Let p be prime number. Then $F_p := \mathbb{Z}/(p)$ is a field with p elements where (p) is the ideal generated by p . Moreover, it is the unique field with p elements up to isomorphism.

Example 1.4. Let R be a commutative ring with unit and let $I \triangleleft R$. Then R/I is a field if and only if I is a maximal ideal.

Example 1.5. Let R be an integral domain. Then there exists a field $R \subseteq F$ so that $x \in F$ is of the form $\frac{a}{b}$ for $a, b \in R$ and F is called the field of fractions of R .

Definition 1.2 (Characteristic of a field). Let F be a field. The characteristic of F denoted $\text{char}(F)$ is defined to be the order of 1_F in the abelian group $(F, +)$ if the order is finite, or 0 if it is infinite.

Example 1.6. We have that

- (1) $\text{char}(\mathbb{Q}) = \text{char}(\mathbb{R}) = \text{char}(\mathbb{C}) = 0$;
- (2) $\text{char}(F_p) = p$.

Exercise 1.1. Let F be a field. Show that $\text{char}(F)$ is either 0 or a prime number.

Solution. Assume that $\text{char}(F) \neq 0$. It suffices to show that $\text{char}(F)$ is a prime number. By definition $\text{char}(F) < \infty$ and we may denote $\text{char}(F) = m$. Suppose next that $m = n_1 n_2$ for two natural numbers $n_1, n_2 \in \mathbb{Z}_+$. We now have that $0 = \text{char}(F) = n_1 n_2$ and since F is a field it is in particular an integral domain and thus $n_1 = 0$ or $n_2 = 0$. This is a contradiction which completes the proof.

Definition 1.3 (Subfield). Let E be a field. A subset $F \subseteq E$ is called a subfield if it is a field under the induced $(+, *)$ operations.

Proposition 1.1. *Let E be a subfield of F . Then $0_E = 0_F$ and $1_E = 1_F$ and $\text{char}(E) = \text{char}(F)$.*

Definition 1.4 (Generated subfield). Let F be a field and let $S \subseteq F$. The subfield generated by S is the intersection of all subsets of F that contain S . This intersection is not empty since $S \subseteq F$ and it is a field since an intersection of fields is a field.

Definition 1.5 (Prime subfield). Let F be a field. The prime subfield of F is defined to be the subfield generated by $\{1_F\}$.

Remark 1.2. Field isomorphisms, homomorphisms and endomorphisms are defined the same way they are defined for fields. In particular we require $\varphi(1_{F_1}) = 1_{F_2}$ and thus homomorphisms of fields are always injections.

Exercise 1.2. Let F be a field with $\text{char}(F) = p$. Show that the prime subfield of F is isomorphic to F_p . Moreover, show that if $\text{char}(F) = 0$ then the prime subfield is isomorphic to $\mathbb{Q}$.

Solution. Suppose that $\text{char}(F) = p < \infty$. Define a map $\varphi: \mathbb{Z} \rightarrow F$ by $\varphi: 1 \mapsto 1_F$ and extended so that

$$\varphi: n \mapsto \underbrace{1_F + \cdots + 1_F}_{n \text{ times}}.$$

Then since $\text{char}(F) = p$ we have that $\ker(\varphi) = p\mathbb{Z}$. Thus from the first isomorphism theorem

$$F_p := \mathbb{Z}/p\mathbb{Z} \cong \text{im}(\varphi) \subseteq F.$$

Since $F_p \cong \text{im}(\varphi)$ we obtain that $\text{im}(\varphi)$ is a subfield of F . Since its generated by 1, it is by definition the prime subfield of F , which completes this part of the proof.

Next suppose that $\text{char}(F) = 0$. Let P denote the prime subfield of F . Construct a similar homomorphism $\varphi: P \rightarrow \mathbb{Q}$ with $\varphi(1_F) = 1$ and extend the map so that it preserves addition and the inverse operation. Any homomorphism of fields is injective, and thus φ is injective. Since for any $\frac{a}{b} \in \mathbb{Q}$ we have

$$\varphi\left(\frac{\overbrace{1_F + \cdots + 1_F}^{a \text{ times}}}{\underbrace{1_F + \cdots + 1_F}_{b \text{ times}}}\right) = \frac{\varphi\left(\overbrace{1_F + \cdots + 1_F}^{a \text{ times}}\right)}{\varphi\left(\underbrace{1_F + \cdots + 1_F}_{b \text{ times}}\right)} = \frac{a}{b}$$

so it is clear that φ is surjective. Thus φ is an isomorphism which completes the proof.

1.2 Field extensions

Definition 1.6 (Field extension). Let F and E be fields. We say that E is a field extension of F and denote E/F if $F \subset E$.

Proposition 1.2. *Let E/F be a field extension. Then E is a vector space over F . In particular we have $+_F = +_E|_F$ and scalar multiplication is the restriction of $*$: $E \times E \rightarrow E$ to the set $F \times E$.*

Definition 1.7 (Degree of a field extension). Let E/F be a field extension. The degree of E/F is denoted $[E : F]$ and defined by $\dim_F(E)$. The extension is called a finite extension if $[E : F] < \infty$ and otherwise an infinite extension.

Example 1.7. We have that $[\mathbb{C} : \mathbb{R}] = 2$ and $[\mathbb{R} : \mathbb{Q}] = \infty$. The second follows from the fact $\mathbb{Q}$ is countable and thus any vector space of finite dimension over $\mathbb{Q}$ is countable.

Theorem 1.3. *Let F be a field and let $h(x) \in F[x]$ be a nonconstant polynomial. Then there exists a field extension E/F so that h has a root in E and $[E : F] \leq \deg(h)$.*

Proof. Let $g(x)$ be an irreducible factor of $h(x)$. It suffices to find a field extension E/F where $g(x)$ has a root and $[E : F] = \deg(g)$.

Since $F[x]$ is a PID and $g(x)$ is irreducible then $(g(x)) \triangleleft F[x]$ is a maximal ideal. In particular $E := F[x]/(g(x))$ is a field. Denote the quotient map $\rho: F[x] \rightarrow E$. The kernel of ρ is $(g(x))$ and in particular it doesn't contain any invertible elements. Thus $\rho|_F$ is an injection and then $\rho(F)$ is a subfield of E which is isomorphic to F . We may assume that F is a subfield of E and $\rho|_F = \text{id}_F$. We denote

$$g(x) = a_n x^n + \cdots + a_0 \in F[x]$$

where $a_n \neq 0$ and then

$$g(\rho(x)) = a_n \rho(x)^n + \cdots + a_1 \rho(x) + a_0 = \rho(a_n x^n + \cdots + a_0) = \rho(g(x)) = 0.$$

Thus $\rho(x) \in E$ is a root of g . We now need to show that $\rho(1), \rho(x), \dots, \rho(x^{n-1})$ is a basis of E over F where $n = \deg(g)$ which will show that $[E : F] = \deg(g)$.

Let $d(x) \in F[x]$. There exist $r, s \in F[x]$ so that $\deg(r) < n$ and

$$d(x) = s(x)g(x) + r(x)$$

and so we get that

$$\rho(d(x)) = \rho(r(x)) \in \text{span}_F \{\rho(1), \dots, \rho(x^{n-1})\}$$

and in particular $\{\rho(1), \dots, \rho(x^{n-1})\}$ spans E as a vector space over F . These elements are also linearly independent since if $b_0, \dots, b_{n-1} \in F$ and

$$b_0 \rho(1) + \cdots + b_{n-1} \rho(x^{n-1}) = 0$$

then

$$\rho(b_0 + \cdots + b_{n-1} x^{n-1}) = 0$$

which implies that $b_0 + \cdots + b_{n-1} x^{n-1} \in (g(x))$ but this is not possible since all the polynomials in $(g(x))$ are of degree greater or equal to n , which completes the proof. $\square$

Theorem 1.4. *Let $F \subseteq E \subseteq K$ be fields. Then $[K : F] = [K : E][E : F]$.*

Proof. Assume that $[E : F] = \infty$ or $[K : E] = \infty$ then obviously $[K : F] = \infty$. Assume now that $[E : F] = m$ and $[K : E] = n$ are finite. Let $\alpha_1, \dots, \alpha_m$ be a basis of E over F and $\beta_1, \dots, \beta_n$ be a basis of K over E . It suffices to show that the sequence

$$(a_i b_j)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

is a basis of K over F , which follows from linear algebra arguments. $\square$

Definition 1.8 (Finitely generated field extension). Let E/F be a field extension and let S be a subset of E . We denote $F(S)$ the smallest subfield of E generated by $S \cup F$. Suppose that $S = \{a_1, \dots, a_n\}$. We sometimes denote $F(a_1, \dots, a_n)$ instead of $F(S)$. We say that E/F is finitely generated if there exists a finite $S \subseteq E$ so that $E = F(S)$.

Exercise 1.3. Let E/F be a field extension and let $S = \{\alpha_1, \dots, \alpha_n\} \subseteq F$. Show that

$$F(S) = \left\{ \frac{p(s_1, \dots, s_n)}{q(s_1, \dots, s_n)} \mid p, q \in F[s_1, \dots, s_n] \text{ and } q \neq 0 \right\}.$$

1.3 Algebraic extensions

Definition 1.9 (Algebraic element). Let E/F be a field extension and let $\alpha \in E$. We say that α is algebraic over F if there exists a polynomial $g(x) \neq 0$ with coefficients in F so that $g(\alpha) = 0$.

Definition 1.10 (Transcendental number). Let E/F be a field extension and let $\alpha \in E$. We say that α is transcendental if it is not algebraic.

Remark 1.3. Since a polynomial of degree n there exist at most n roots and $\mathbb{Q}[x]$ is countable, there exist at most a countable amount of algebraic numbers of any field extension over $\mathbb{Q}[x]$ and in particular $\mathbb{C}$ contains transcendental numbers over $\mathbb{Q}$.

Definition 1.11 (Liouville number). An irrational real number x is said to be a Liouville number if for every integer $n \geq 1$ there exist integers p and $q \geq 2$ so that $\left|x - \frac{p}{q}\right| < \frac{1}{q^n}$.

Theorem 1.5 (Liouville's theorem). *Liouville numbers are transcendental.*

Proof. Let x be a Liouville number. Assume by contradiction that x is an algebraic number. Since x is a Liouville number, it is irrational so by a theorem not shown here there exists $c > 0$ and $n \in \mathbb{Z}_+$ so that

$$\left|x - \frac{p}{q}\right| \geq \frac{c}{q^n}$$

for every pair $p, q \in \mathbb{Z}$ with $q \neq 0$. Let $r \geq 1$ so that $2^r \geq c^{-1}$. Since x is a Liouville number there exist $p, q \in \mathbb{Z}$ with $q > 1$ so that

$$\left|x - \frac{p}{q}\right| < \frac{1}{q^{n+1}} \leq \frac{1}{2^r q^n} \leq \frac{c}{q^n}$$

which is a contradiction. Thus x is transcendental. □

Exercise 1.4. Show that Liouville's constant

$$\alpha = \sum_{k=1}^{\infty} 10^{-k!}$$

is transcendental over $\mathbb{Q}$.

Solution. We can show that Liouville's constant is a Liouville' number and thus by Theorem 1.5 it is transcendental.

Definition 1.12 (Minimal polynomial of an algebraic number). Let E/F be a field extension and let $\alpha \in E$ be an algebraic number. The minimal polynomial of α over F denoted $m_\alpha(x)$ is the minimal monic polynomial with respect to degree in $F[x]$ that vanishes at α .

Remark 1.4 (Degree of algebraic element). The degree of $m_\alpha(z)$ is called the degree of α over F and denoted by $\deg_F(\alpha)$ or $\deg(\alpha)$.

Remark 1.5. The minimal polynomial of α is unique and it generates the ideal

$$\{g(x) \in F[x] \mid g(\alpha) = 0\} \triangleleft F[x].$$

Assume that it is not unique, for example let f, g be monic polynomials of degree n that vanish at α . Then $f - g$ is a polynomial of degree $< n$ that with root α so there exists a monic polynomial of degree $< n$ which implies the uniqueness of the minimal polynomial.

Example 1.8. The minimal polynomial of $i \in \mathbb{C}$ over $\mathbb{Q}$ is $m_i(x) = x^2 + 1$.

Proposition 1.6. *Let E/F be a fields extension, let $\alpha \in E$ and let $g(x) \in F[x]$ be a monic polynomial that vanishes at α . Then $g(x)$ is the minimal polynomial of α over F if and only if $g(x)$ is irreducible.*

Theorem 1.7 (Eisenstein's criterion). *Suppose we have the following polynomial with integer coefficients:*

$$Q(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

If there exists a prime number p such that the following three conditions all apply:

- (1) p divides each a_i for $0 \leq i < n$;
- (2) p does not divide a_n ;
- (3) p^2 does not divide a_0 ;

then Q is irreducible over the rational numbers.

Corollary 1.8. *Let p be a prime number. Then the polynomial*

$$g(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 \in \mathbb{Z}[x].$$

is irreducible over $\mathbb{Q}[x]$.

Proof. We know that $f(x)$ is irreducible if and only if $f(x+1)$ is irreducible and indeed according to Theorem 1.7 the polynomial

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

is irreducible. □

Corollary 1.9. *Let p be a prime number. Then the minimal polynomial of $e^{\frac{2\pi i}{p}} \in \mathbb{C}$ over $\mathbb{Q}$ is $x^{p-1} + x^{p-2} + \cdots + x + 1$.*

Proposition 1.10. *Let E/F be a field extension and let $\alpha \in E$ be algebraic over F . Then*

- (1) $F(\alpha) \cong F[x]/(m_\alpha(x))$;
- (2) $[F(\alpha) : F] = \deg(\alpha)$.

Proof.

- (1) Define a homomorphism of rings with unit

$$\varphi: F[x] \rightarrow F(\alpha)$$

by saying it is the identity on F and setting $\varphi(x) = \alpha$. This homomorphism is the evaluation function at α . In this way we have $\ker(\varphi) = (m_\alpha(x))$ and since $m_\alpha(x)$ is irreducible the ideal $(m_\alpha(x))$ is maximal which implies that $F[x]/(m_\alpha(x))$ is a field. From the first isomorphism theorem we get that φ induces an isomorphism

$$\overline{\varphi}: F[x]/(m_\alpha(x)) \xrightarrow{\cong} \text{im}(\varphi) \subseteq F(\alpha).$$

We have that $\text{im}(\varphi)$ is a subfield of $F(\alpha)$ that contains F and α and thus is equal to $F(\alpha)$.

- (2) This follows from (1) since

$$\deg_F F[x]/(m_\alpha(x)) = \deg(m_\alpha(x))$$

□

Corollary 1.11. *Let E/F be a field extension and let α be algebraic over F of degree n . Then $1, \alpha, \dots, \alpha^{n-1}$ is a basis of $F(\alpha)$ as a vector space over F .*

Proof. We will show that $1, \alpha, \dots, \alpha^{n-1}$ are linearly independent over F . Let $c_0, \dots, c_{n-1} \in F$ be such that

$$c_0 1 + c_1 \alpha + \dots + c_{n-1} \alpha^{n-1} = 0$$

we can define a polynomial

$$g(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$$

and since $g(\alpha) = 0$ and $\deg(g) < \deg(m_{\alpha(x)})$ we get that $g(x)$ is the zero polynomial.

Next since that $[F(\alpha) : F] = n$ we have necessarily that $1, \alpha, \dots, \alpha^{n-1}$ is a basis which completes the proof. □

Proposition 1.12. *Let E/F be a field extension and $\alpha \in E$. Then α is algebraic over F if and only if $[F(\alpha) : F] < \infty$.*

Proof. We saw that if α is algebraic then $[F(\alpha) : F] = \deg(\alpha) < \infty$.

Next suppose that $[F(\alpha) : F] < \infty$. Then $1, \alpha, \dots, \alpha^n$ are necessarily linearly dependent over F , which means that there exist $b_0, \dots, b_n \in F$ not all zero such that

$$b_0 + b_1 \alpha + \dots + b_n \alpha^n = 0$$

and thus α is algebraic over F . □

Definition 1.13 (Algebraic and transcendental extensions). Let E/F be a field extension.

- (1) We say that E/F is an algebraic extension if every $x \in E$ is algebraic over F .
- (2) We say that E/F is a transcendental extension if it is not an algebraic extension.
- (3) We say that E/F is a pure transcendental extension if every $x \in E$ is transcendental over F .

Remark 1.6. The union of an increasing sequence of algebraic extensions (with respect to containment) is algebraic.

Proposition 1.13. *Let E/F be a field extension. Then the following conditions are equivalent:*

- (1) E/F is finite;
- (2) E/F is finitely generated and algebraic;
- (3) There exist algebraic numbers $\alpha_1, \dots, \alpha_k \in E$ over F so that $E = F(\alpha_1, \dots, \alpha_k)$.

Moreover, if (3) is satisfied and for all $1 \leq i \leq k$ we have $m_i = [F(\alpha_i) : F]$ then we also have that $[E : F] \leq m_1 m_2 \dots m_k$.

Proof.

- (1 $\rightarrow$ 2) Every finite extension is finitely generated (for example by the basis of E over F).
- (2 $\rightarrow$ 3) Obvious.
- (3 $\rightarrow$ 1) For all $1 \leq i \leq k$ we denote

- (a) $F_i = F(\alpha_1, \dots, \alpha_{i-1})$ and in particular $F_1 = F$;

(b) $m_i = [F(\alpha_i) : F]$ and $n_i = [F_i(\alpha_i) : F_i]$.

Since m_i is the degree of the minimal polynomial of α_i over F and n_i is the degree of the minimal polynomial over α_i over F_i , and since $F \subseteq F_i$, we get that $m_i \geq n_i$ for all $1 \leq i \leq n$. Thus we have

$$[E : F] = [E : F_k] \cdot [F_k : F_{k-1}] \cdots [F_2 : F_1] = n_1 \cdots n_k \leq m_1 \cdots m_k < \infty.$$

□

Corollary 1.14. *Let E/F be a field extension and let $\alpha, \beta \in E$ be algebraic over F so that $\beta \neq 0$. Then $\alpha \pm \alpha, \alpha\beta$ and $\frac{\alpha}{\beta}$ are all algebraic.*

Proof. The numbers $\alpha \pm \alpha, \alpha\beta$ and $\frac{\alpha}{\beta}$ are all elements in $F(\alpha, \beta)$ and by Theorem 1.13 we have that

$$[F(\alpha, \beta) : F] \leq \deg_F(\alpha) \deg_F(\beta),$$

which completes the proof

□

Corollary 1.15. *Let E/F be a field extension. Then the collection of algebraic elements of E over F is a subfield of E that contains F .*

Exercise 1.5. Denote $\overline{\mathbb{Q}}$ the set of complex numbers that are algebraic over $\mathbb{Q}$. Show that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$. Also show that $[\mathbb{R} : \mathbb{Q}] = \infty$.

Remark 1.7. By Theorem 1.15 the set $\overline{\mathbb{Q}}$ is a field. It is sometimes called the algebraic closure of $\mathbb{Q}$.

Corollary 1.16. *Let E/F and L/E be algebraic field extensions. Then L/F is algebraic.*

Proof. Let $\alpha \in L$. It suffices to show that $[F(\alpha) : F] < \infty$. Let

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

be the minimal polynomial of α over E . We denote $\{a_0, \dots, a_{n-1}\} A \subseteq E$. Since f is also the minimal polynomial of α over $F(A)$ we have that $[F(\{\alpha\} \cup A) : F(A)] = n$. Thus we obtain

$$[F(\alpha) : F] \leq [F(\{\alpha\} \cup A) : F] = \underbrace{[F(\{\alpha\} \cup A) : F(A)]}_{=n} \underbrace{[F(A) : F]}_{<\infty} < \infty$$

which completes the proof.

□

Definition 1.14 (Simple field extension). A field extension E/F is called simple if there exists an element $\alpha \in E$ so that $E = F(\alpha)$. In this case we call α the primitive element of the extension.

Definition 1.15. Let F be a field. The field of rational functions over F is denoted by $F(x)$ or equivalently the fraction field of $F[x]$.

Exercise 1.6. Let E/F be a simple field extension. Show that one of the following is always satisfied.

- (1) E/F is a finite algebraic extension;
- (2) There exists an isomorphism $\varphi : F(x) \rightarrow E$ which is the identity on F .

Exercise 1.7. Let $F(\alpha)/F$ be a simple field extension. Show that $F(\alpha)/F$ is finite if and only if $F(\alpha) = F[\alpha]$.

1.4 The multiplicative group of a finite field

Lemma 1.17. *Let G be a finite abelian group of order n . Suppose that G is not cyclic. Then there exists $0 < m < n$ so that for all $g \in G$ we have $g^m = 1$.*

Proof. From the classification theorem for finitely generated abelian groups there exists a finite sequence of natural numbers $1 < m_1 \mid m_2 \mid \cdots \mid m_k$ so that

$$G \cong C_{m_1} \times \cdots \times C_{m_k}.$$

Since G is not cyclic we get $k > 1$, and thus $|G| > m_k$. Since $g^{m_k} = 1$ for all $g \in G$ the proof is complete. $\square$

Corollary 1.18. *Let F be a field and let $G \leq F^\times$ be finite where $F^\times$ is the multiplicative group structure of the field. Then G is cyclic, and in particular the multiplicative group structure of a finite field is cyclic.*

Proof. Assume by contradiction that G is not cyclic and denote $|G| = n$. From Theorem 1.17 there exists $1 \leq m < n$ so that $g^m = 1$ for all $g \in G$. This means that each polynomial $x^m - 1$ has $m < n$ different roots which is a contradiction. $\square$

1.5 Algebraically closed fields

Definition 1.16 (Algebraically closed field). A field F is said to be an algebraically closed field if each nonconstant polynomial $f \in F[x]$ has a root in F .

Proposition 1.19. *Let F be a field. The following conditions are equivalent:*

- (1) F is an algebraically closed field;
- (2) every irreducible polynomial in $F[x]$ is of degree 1;
- (3) every nonconstant monic polynomial $f \in F[x]$ splits into linear factors $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ for $\alpha_1, \dots, \alpha_n \in F$.

Proof.

- (1 $\rightarrow$ 2) Let $f \in F[x]$. Suppose f is constant, then it is either invertible or the zero polynomial and thus it is not irreducible. Suppose $\deg f \geq 2$ then since F is an algebraically closed field it has a root $\alpha \in F$ and thus $f(x) = (x - \alpha)g(x)$ where $g(x) \in F[x]$ and $\deg g \geq 1$. In particular, f is not irreducible which completes the proof.
- (2 $\rightarrow$ 3) Since every irreducible polynomial in $F[x]$ is of degree 1 every polynomial $f(x)$ so that $\deg f \geq 2$ can be written as a product of nonconstant polynomials of smaller degrees. Thus we can prove (3) by induction on the degree of f .
- (3 $\rightarrow$ 1) Immediate.

$\square$

Remark 1.8. We have already seen proofs for the fundamental theorem of algebra in other courses such as topology, and complex analysis, and thus we omitted the proof of this theorem in class. However, we will not omit its following two corollaries.

Corollary 1.20. *Any real irreducible polynomial $f \in \mathbb{R}[x]$ is of degree $\deg f \leq 2$.*

Proof. Let $f \in \mathbb{R}[x]$ be irreducible. Let $\alpha \in \mathbb{C}$ be a root of f as a polynomial in $\mathbb{C}[x]$. Then we have

$$\deg f = [\mathbb{R}(\alpha) : \mathbb{R}] \leq [\mathbb{C} : \mathbb{R}] = 2$$

which completes the proof. $\square$

Corollary 1.21. *Every real polynomial is a product of real polynomials of degree at most 2. In particular, every real polynomial of an odd degree has a root.*

2 Ruler and compass constructions

2.1 The system

We start by setting $S = S_0 = \{(0, 0), (1, 0)\}$ which could be any two points in the plane because they only serve as giving as the unit distance.

Ruler: Given two different points in S we can draw a straight line between them of an arbitrary size.

Compass: Given three points in $p, q, r \in S$ so that $q \neq r$ we can draw the circle with center p and radius $|r - q|$.

Denote by S_1 the set points given from the following types of intersections:

- (1) intersection of two constructible straight lines;
- (2) intersection of two constructible circles;
- (3) intersection of a constructible line and a constructible circle.

The set S_1 is called the set of constructible points from S_0 in one step. For each $k \geq 1$ we denote S_k the set of constructible points from S_{k-1} in one step. We want to analyze the sets

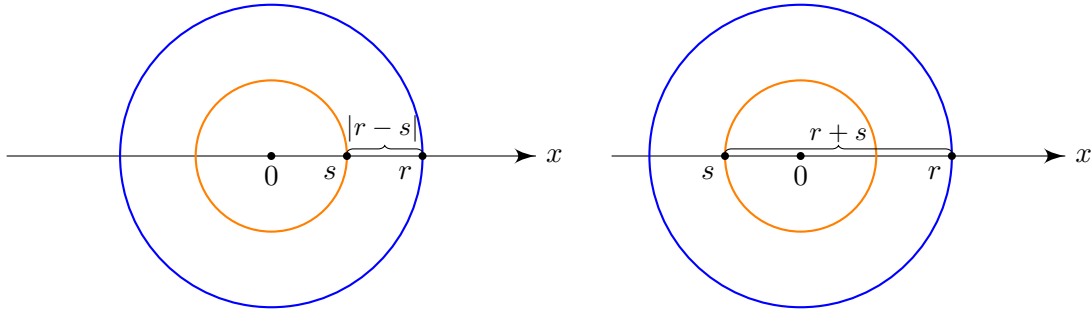
- (1) S_k and $T_k := \{|p - q| \mid p, q \in S_k\}$;
- (2) $S_\infty := \bigcup_{k \geq 0} S_k$ and $T_\infty := \{|p - q| \mid p, q \in S_\infty\}$;
- (3) $T_\infty^\pm := \{x \in \mathbb{R} \mid |x| \in T_\infty\} = \{x \in \mathbb{R} \mid (x, 0) \in S_\infty\}$.

2.2 Simple constructions

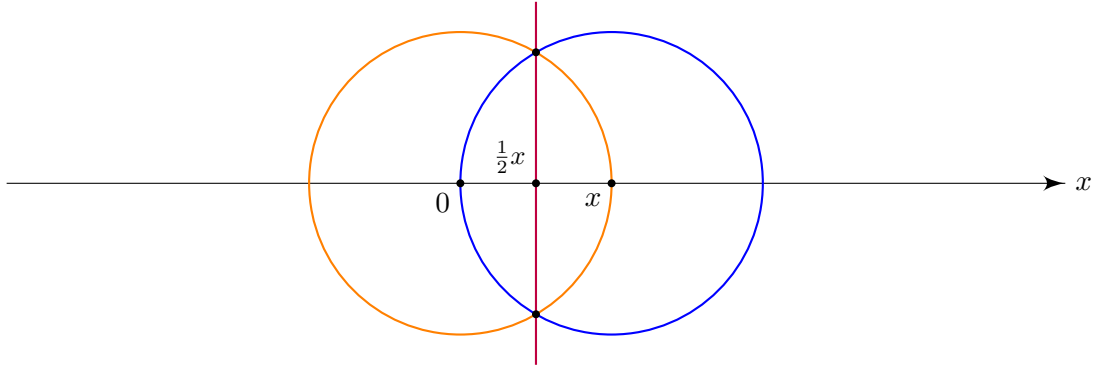
Remark 2.1. In the following constructions $0 := (0, 0)$ always denotes the origin.

Remark 2.2. Although I have drawn the x -axis, I can't use it to create points without justification since this was not part of the rules. The justification is simple: every time we want to use the x -axis, we "draw" an infinite line segment passing through $(0, 0)$ and $(1, 0)$.

Example 2.1. Let $r, s \in T_\infty$. Then $r + s, |r - s| \in T_\infty$. Without loss of generality assume $0 < s \leq r$.

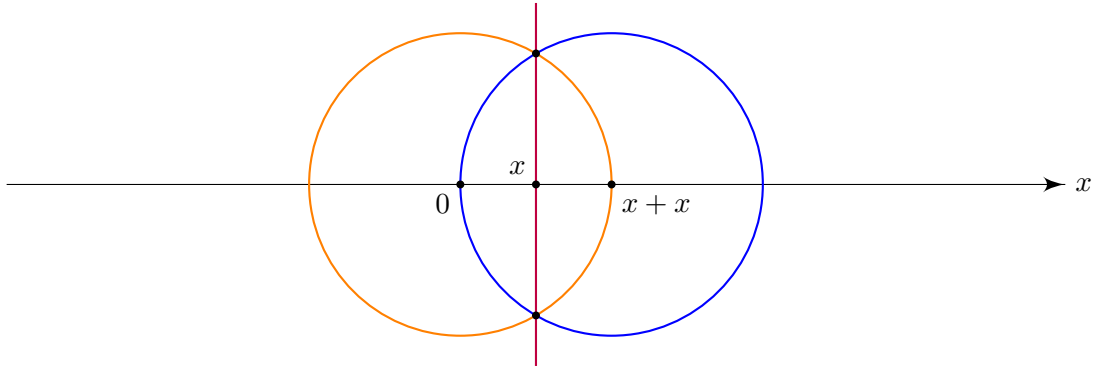


Example 2.2. Let $(x, 0) \in S_\infty$. Then $(\frac{1}{2}x, 0) \in S_\infty$.

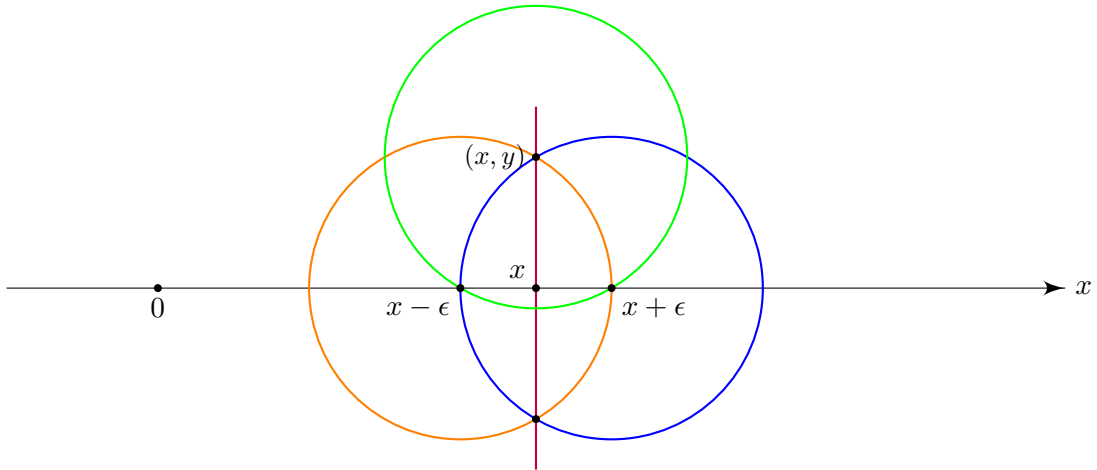


Example 2.3. Let $(x, y) \in S_\infty$. Then the line perpendicular to the x -axis that passes through (x, y) is constructible.

Suppose $y = 0$ and then $(x, y) = (x, 0)$. This case can either be shown directly or we can just you combine the results from Example 2.1 and Example 2.2.

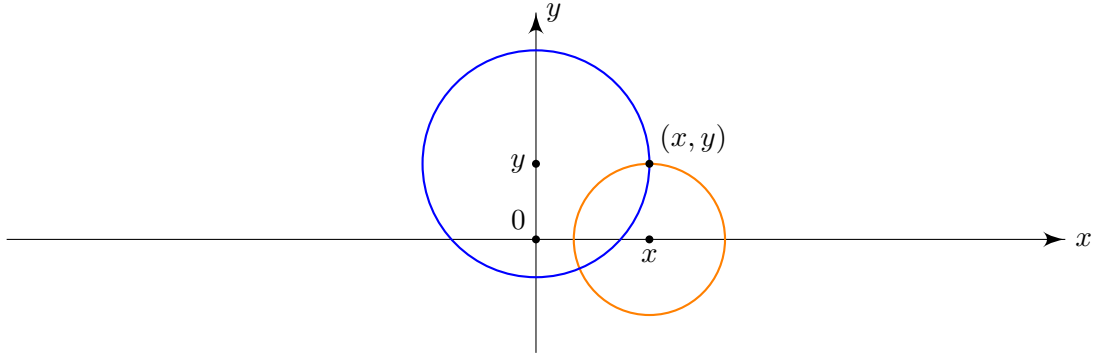


In the general case we can draw a circle around (x, y) with any radius greater than y , and then apply Example 2.2 on the two new points gained from the intersection with the x -axis.



Corollary 2.1. $S_\infty = T_\infty^\pm \times T_\infty^\pm$.

Proof. This is an immediate corollary to Example 2.3 since any point $(x, y) \in S_\infty$ implies $(x, 0), (0, y) \in S_\infty$ and thus $x, y \in T_\infty^\pm$. The other side of the inclusion follows from a simple construction. Let $(x, y) \in T_\infty^\pm \times T_\infty^\pm$. Then $(x, 0), (0, y) \in S_\infty$ and we can see that $(x, y) \in S_\infty$ by noticing that it is the intersection of the circle of radius $|x - 0|$ and center y and the circle of radius $|y - 0|$ and center x .

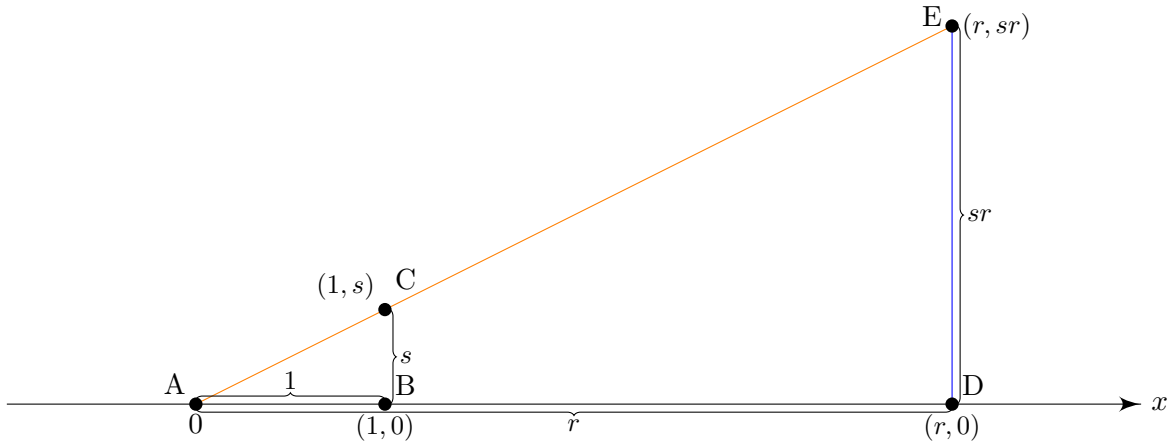


□

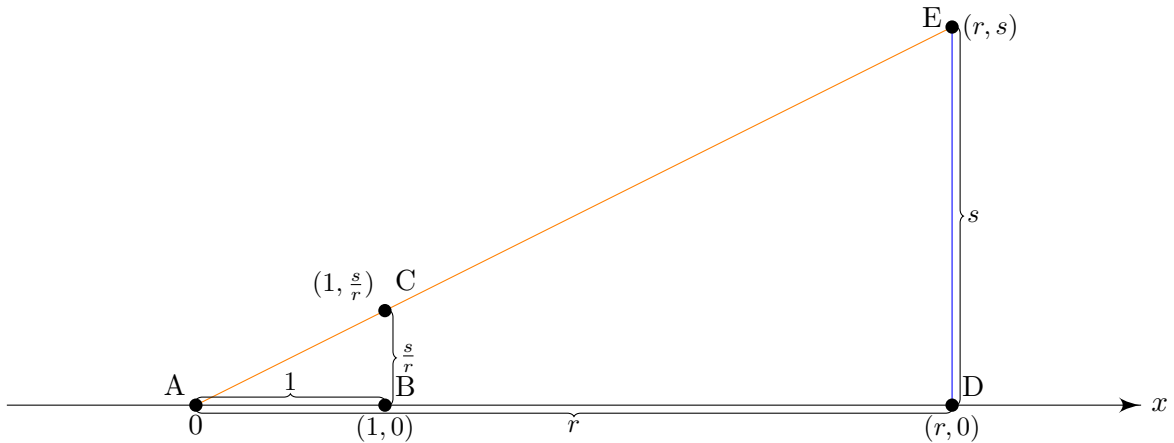
Example 2.4. Let $s, r \in T_\infty$. Then $rs \in T_\infty$ and if $r \neq 0$ then $\frac{s}{r} \in T_\infty$. We may assume that $s, r \neq 0$. From Example 2.1 and Example 2.2 and Example 2.3 we know that the points $A = (0, 0)$, $B = (1, 0)$, $C = (1, s)$ and $D = (r, 0)$ are constructible. We can now draw a line passing through A and C and a line perpendicular to the x -axis passing through D . We will denote their intersection point by E . The triangles $\triangle ABC$ and $\triangle ADE$ are similar, and so

$$\frac{AB}{BC} = \frac{AD}{DE} \implies \frac{1}{s} = \frac{r}{DE} \implies DE = rs$$

which completes the proof. Below is a diagram to visualize the process.

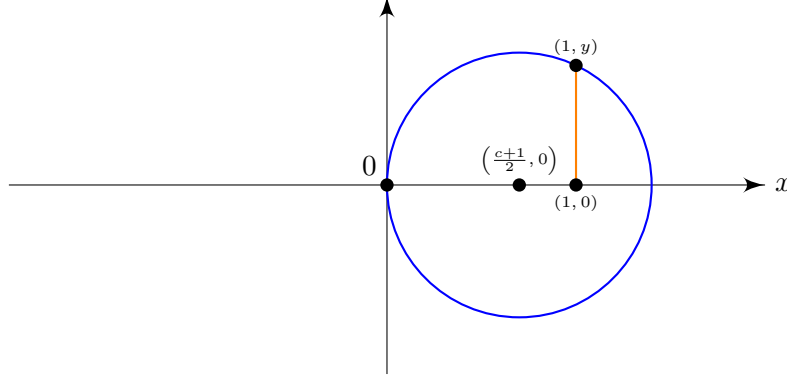


In order to show that $\frac{s}{r} \in T_\infty$ we use a very similar construction



which completes the proof.

Example 2.5. Let $c \in T_\infty$. Then $\sqrt{c} \in T_\infty$. From the Example 2.4 we can assume that $r < 1$ (we have already seen that if $1/t \in T_\infty$ then $t \in T_\infty$). We know from earlier examples that the point $(\frac{c+1}{2}, 0)$ can be constructed. We now construct the point $(1, y)$ by letting it be the intersection of the line perpendicular to the x -axis passing through $(1, 0)$ and the circle with radius $\frac{c+1}{2}$ and center $(\frac{c+1}{2}, 0)$. We can see this in the following diagram.



This shows that y is constructible and from the pythagorean theorem we have that

$$y^2 + \left(1 - \frac{c+1}{2}\right)^2 = \left(\frac{c+1}{2}\right)^2 \implies y^2 + 1 - (c+1) + \left(\frac{c+1}{2}\right)^2 = \left(\frac{c+1}{2}\right)^2 \implies y = \sqrt{c}$$

which completes the proof.

Corollary 2.2. $T_\infty^\pm$ is a field.

Proof. We have seen that $0, 1 \in T_\infty^\pm$ and we have shown in examples that if $r, s \in T_\infty^\pm$ then $r \pm s, rs \in T_\infty^\pm$ and if $r \neq 0$ that $s/r \in T_\infty^\pm$. $\square$

2.3 Lines and circles

Definition 2.1 (F -lines and F -circles). Let $F \subseteq \mathbb{R}$ be a field.

- (1) A line $L \subset \mathbb{R}^2$ is called an F -line if its equation is $x = a$ or $y = ax + b$ for $a, b \in F$.
- (2) A circle $C \subseteq \mathbb{R}^2$ is called an F -circle if its equation is $(x - a)^2 + (y - b)^2 = c$ for $a, b, c \in F$.

Remark 2.3. Let $S_0 \subseteq F \times F$ for some field F . Then each point that is constructible from S_0 in one step is either an intersection of two F -lines, an intersection of F -circles or an intersection of an F -line and an F -circle.

Lemma 2.3. Let $F \subseteq \mathbb{R}$ be a field, let $L_1 \neq L_2$ be F -lines and let $C_1 \neq C_2$ be F -circles. Then

- (1) $L_1 \cap L_2 = \emptyset$ or they intersect at one point in $F \times F$.
- (2) $L_1 \cap C_1 = \emptyset$ or they intersect at two points or less and there exists $0 < \alpha \in F$ so that each intersection point is an element of $F(\sqrt{\alpha}) \times F(\sqrt{\alpha})$.
- (3) $C_1 \cap C_2 = \emptyset$ or they intersect at two points or less and there exists $0 < \alpha \in F$ so that each intersection point is an element of $F(\sqrt{\alpha}) \times F(\sqrt{\alpha})$.

Proof. We are only going to prove case (2) under the assumption that the equation of L_1 is $y = ax + b$ for $a, b \in F$. The equation of C_1 is $(x - c)^2 + (y - d)^2 = e$ for $c, d, e \in F$. In order to solve for the intersection points we need to substitute y in $ax + b$ in the equation of the circle, and after some algebraic manipulations we see that intersection points must satisfy the equation

$$(a^2 + 1)x^2 - 2(c + a(d - b))x = e - c^2 - (d - b)^2$$

and so the intersection is nonempty if and only if this equation has a real solution, and in this case there exist $\alpha, \beta \in F$ so that $0 \leq \beta$ and the solutions are $\alpha \pm \sqrt{\beta}$. We conclude that

$$x = \alpha \pm \sqrt{\beta} \in F(\sqrt{\beta}) \text{ and } y = ax + b \in F(\sqrt{\beta})$$

which completes the proof. $\square$

Theorem 2.4. *Let $(0, 0), (1, 0) \in S_0 \subseteq \mathbb{R}^2$. We denote $F_0 := \mathbb{Q}(T_0)$. Then a real number $\alpha \in \mathbb{R}_{\geq 0}$ is constructible from S_0 if and only if there exists a tower of fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k \subseteq \mathbb{R}$ so that $\alpha \in F_k$ and for all $1 \leq i \leq k$ there exists $0 \leq \alpha_i \in F_{i-1}$ so that $F_i = F_{i-1}(\sqrt{\alpha_i})$.*

Proof. The previous lemma shows that this condition is necessary. Theorem 2.2 shows that the constructible numbers are a field and Example 2.5 shows that if elements of a field $E \subseteq \mathbb{R}$ are constructible and $0 \leq \alpha \in E$ then $\sqrt{\alpha}$ is constructible, and then from Theorem 2.2 we have that $E(\sqrt{\alpha})$ is a field. Thus we can use induction on k to show that for every $1 \leq i \leq k$ that the elements of F_i are constructible which completes the proof. $\square$

Corollary 2.5. *Let $S_0 = \{(0, 0), (1, 0)\}$. Then a necessary condition for some $\alpha \in \mathbb{R}_{\geq 0}$ to be constructible is that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k$ for some $k \geq 0$.*

Remark 2.4. In this stage we still don't know that if α is constructible from $S_0 = F_0 \times F_0$ then there exists a tower of fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_k = F(\alpha)$ so that for all $1 \leq i \leq k$ we have $[F_i : F_{i-1}] = 2$ but it is a corollary of Theorem 2.4.

Remark 2.5. In later sections we will see a concrete example of some $\alpha \in \mathbb{R}$ such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ but α is not constructible from $S_0 = \{(0, 0), (1, 0)\}$.

Example 2.6. We know that π is transcendental over $\mathbb{Q}$ and thus $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$. This implies that we can't construct using a ruler and a compass a square with area π .

Example 2.7. The polynomial $x^3 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein's criterion and thus it is the minimal polynomial of $\sqrt[3]{2} \in \mathbb{R}$. We get that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ which shows that we can't draw the edge of a cube with volume 2.

Definition 2.2 (Fermat number). A Fermat number is a number of the form $F_n = 2^{2^n} + 1$, where n is a positive integer.

Definition 2.3 (Fermat prime). Since if $2^k + 1$ is prime for a natural number $k > 0$ it follows that k itself is a power of two, any prime number of the form $2^k + 1$ is called a Fermat prime.

Remark 2.6. The only known Fermat primes are 3, 5, 17, 257 and 65537. Moreover, it is unknown whether there are finitely or infinitely many Fermat primes.

Example 2.8. Let p be an odd prime. We will show that if $\cos(2\pi/p)$ is constructible then p is a Fermat prime. We can see this by first denoting $\eta = e^{\alpha i}$ and $\alpha = \frac{2\pi}{p}$. We have seen earlier in Theorem 1.9 that $[\mathbb{Q}(\eta) : \mathbb{Q}] = p - 1$. We see that

$$\eta + \eta^{-1} = e^{\alpha i} + e^{-\alpha i} = 2 \cos(\alpha) \implies \eta^2 - 2 \cos(\alpha) \eta + 1 = 0$$

which means that η is a root of $x^2 - 2 \cos(\alpha)x + 1 \in \mathbb{Q}(\cos(\alpha))$, and thus $[\mathbb{Q}(\eta) : \mathbb{Q}(\cos(\alpha))] \leq 2$. On the other hand we have that $\mathbb{Q}(\cos(\alpha)) \subseteq \mathbb{R}$ and since $\eta \notin \mathbb{R}$ that $\mathbb{Q}(\eta) \subsetneq \mathbb{R}$ so finally $[\mathbb{Q}(\eta) : \mathbb{Q}(\cos(\alpha))] = 2$. We have that

$$\underbrace{[\mathbb{Q}(\eta) : \mathbb{Q}]}_{=p-1} = \underbrace{[\mathbb{Q}(\eta) : \mathbb{Q}(\cos(\alpha))]}_{=2} [\mathbb{Q}(\cos(\alpha)) : \mathbb{Q}]$$

which implies that $[\mathbb{Q}(\cos \alpha) : \mathbb{Q}] = \frac{p-1}{2}$. Thus if $\cos(\alpha)$ is constructible then there exists $0 \leq s$ so that $\frac{p-1}{2} = 2^s$ and thus $p = 2^{s+1} + 1$ which completes the proof.

Remark 2.7. We will see later that the other direction of the proposition also holds. If p is a Fermat prime then $\cos(2\pi/p)$ is constructible from $S_0 = \{(0, 0), (1, 0)\}$.

Exercise 2.1. Let p be an odd prime. Show that $\cos(2\pi/p)$ is constructible if and only if it is possible to construct the vertices of a regular p -sided polygon, or equivalently, if and only if p is a Fermat prime.

3 Introduction to Galois theory

3.1 Splitting fields

Definition 3.1 (Splitting over a field). Let F be a field and let $g(x) \in F[x]$ be a polynomial of degree n . Then g is said to split over F if there exist $\alpha_1, \dots, \alpha_n \in F$ not necessarily distinct so that

$$g(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Definition 3.2 (Splitting field). Let F be a field and let $g(x) \in F[x]$ of degree n . A field extension E/F is said to be a splitting field for g over F if

- (1) g splits in E ;
- (2) if $F \subseteq L \subsetneq E$ then g does not split in L .

Remark 3.1. Condition (2) in Definition 3.2 means that E is the minimal field where g splits, with respect to containment of fields.

Remark 3.2. The splitting field of a polynomial is unique up to isomorphism.

Proposition 3.1. Let F be a field and let $g(x) \in F[x]$ be a polynomial of degree n . Then there exists a field extension E/F that is a splitting field of g over F . Moreover, $[E : F] \leq n!$.

Proof. We will prove this by induction on n . When $n = 1$ then $g(x)$ is a linear polynomial and thus F is the splitting field of g over F . Assume that $2 \leq n$ and that the proposition holds for polynomials of degree less than n .

Let α be a root of g . We have seen in Theorem 1.3 that there exists a simple field extension L/F so that $L = F(\alpha)$ and $[L : F] \leq n$. We denote $h(x) = g(x)/(x - \alpha) \in L[x]$. From the induction hypothesis there exists a splitting field E of h over L and $[E : L] \leq (n - 1)!$, so we have that

$$[E : F] = [E : L][L : F] \leq n!,$$

and we want to show that E is a splitting field of g over F , so it is left to show that E is the minimal field where g splits. Assume, by way of contradiction, that $F \subseteq M \subsetneq E$ and g splits in M . Then M contains all the roots of g and in particular $\alpha \in M$. Since g splits over M , it follows that h splits in M . From the previous two statements, and from the fact E is the splitting field of h over $L = F(\alpha)$ it follows that $E \subseteq M$. This contradiction completes the proof. $\square$

Example 3.1. Let $f(x) = x^3 - 2 \in \mathbb{Q}[x]$. The roots of f in $\mathbb{C}$ are $\alpha, \alpha\omega, \alpha\omega^2$ where $\alpha = \sqrt[3]{2}$ and $\omega = e^{\frac{2\pi i}{3}}$. Thus $\mathbb{Q}(\alpha, \omega)$ is the splitting field of f over $\mathbb{Q}$. Notice that we have

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

From Eisenstein's criterion we have that $f(x) = x^3 - 2$ is irreducible and is the minimal polynomial of α so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Since ω is a root of $\frac{x^3-1}{x-1} = x^2 + x + 1 \in \mathbb{Q}(\alpha)[x]$ we get that $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)] \leq 2$ so since clearly $\omega \notin \mathbb{Q}(\alpha)$ we get

$$[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}(\alpha)]}_{=2} \underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}]}_{=3} = 6.$$

Definition 3.3 (Primitive n th root of unity). A primitive n th root of unity is a complex number ζ satisfying $\zeta^n = 1$ and $\zeta^k \neq 1$ for all $1 \leq k < n$.

Remark 3.3. Note that a primitive n th root of unity is not necessarily unique.

Example 3.2. Let E/F be a field extension so that $E = F(\alpha)$ and let α be a primitive n th root of unity. Then $\{1, \alpha, \dots, \alpha^{n-1}\}$ is the set of roots of the polynomial $x^n - 1$ and thus the splitting field of $x^n - 1$ is $F(\alpha)$ and $[F(\alpha) : F] \leq n$.

Example 3.3. We know that for any prime $p \in \mathbb{N}$ we have for all $1 \leq k \leq p-1$ that $p \mid \binom{p}{k}$. This implies an identity that is colloquially known as the “freshman’s dream” identity. It states that if F is a field of prime characteristic p then for any $a, b \in F$ we get

$$(a + b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

and in particular if $f(x) = x^p - a \in F[x]$ and $E = F(b)$ is a simple field extension of F where b is a root of f , then $b^p = a$, and thus $f(x) = x^p - b^p = (x - b)^p$. This implies that E is the splitting field of f .

Exercise 3.1. In example Example 3.3 show that if $b \notin F$ then f is irreducible over F and thus $[E : F] = p$.

Definition 3.4 (Algebraic closure). Let F be a field. An algebraic extension E/F is said to be an algebraic closure of F if

- (1) E/F is algebraic;
- (2) E is an algebraically closed field;

Exercise 3.2. Show that (1) + (2) imply that if $F \subsetneq L \subsetneq E$ then L is not algebraically closed.

Lemma 3.2. Let E/F be an algebraic extension. Suppose that every $f(x) \in F[x]$ splits over E . Then E is an algebraic closure of F .

Proof. It suffices to show that E is an algebraically closed field. Let $f(x) \in E[x]$ be a nonconstant polynomial. Let L/E be an algebraic extension of E so that f has a root $\alpha \in L$. Since L/E and E/F are algebraic extensions, the extension L/F is algebraic and in particular α is algebraic over F . Let $m(x) \in F[x]$ be the minimal polynomial of α over F , and let $h(x) \in E[x]$ be an irreducible element (over E) of $f(x)$ so that $h(\alpha) = 0$. Then $h(x)$ is the minimal polynomial of α over E . This means that $h(x)$ divides $m(x)$. From the assumption we get that $m(x)$ splits over E and thus $h(x)$ also splits over E and in particular $\alpha \in E$ and $f(x)$ has a root in E . $\square$

Proposition 3.3. Let F be a field. Then there exists an algebraic closure of F .

Proof. Let $\{f_\alpha \mid \alpha < \kappa\}$ be an indexing of the elements of $F[x]$. We may assume that κ is an infinite cardinal, and hence a limit ordinal. For all $\alpha \leq \kappa$ we define an extension of F in the following way:

- (1) $F_0 = F$;
- (2) if $\alpha = \beta + 1$ is a successor ordinal then F_α is the splitting field of f_β over F_β ;
- (3) if α is a limit ordinal then $F_\alpha = \bigcup_{\beta < \alpha} F_\beta$;

and we want to say that F_κ is the algebraic closure of F . From Theorem 3.2 it suffices to show that F_κ/F is an algebraic extension. We will show by transfinite induction that for all $\alpha \leq \kappa$ the extension F_α/F is an algebraic extension. For the base $\alpha = 0$ it is clear that $F_\alpha/F = F/F$ is algebraic. Suppose that α is a successor ordinal so that $\alpha = \beta + 1$. From the induction hypothesis F_β/F is algebraic. By definition of F_α , F_α/F_β is algebraic. Thus F_α/F is algebraic. Suppose that α is a limit ordinal. Then F_α/F is algebraic since an increasing union of algebraic extensions is an algebraic extension. This completes the proof. $\square$

Lemma 3.4. Let $\sigma: E \rightarrow L$ be an isomorphism of fields. Let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in E[x]$ be irreducible, and denote $g(x) = \sigma(f) = x^n + \sigma(a_{n-1})x^{n-1} + \cdots + \sigma(a_0) \in L[x]$. Let $E(a) = \bar{E}$ and $L(b) = \bar{L}$ be field extensions so that a is a root of f and b is a root of g . Then there exists a unique isomorphism $\bar{\sigma}: \bar{E} \rightarrow \bar{L}$ so that $\bar{\sigma}|_E = \sigma$ and $\bar{\sigma}(a) = b$. This could be summarized by the following commutative diagram:

$$\begin{array}{ccc} F & \xrightarrow{i_F} & F(a) \\ \sigma \downarrow & & \downarrow \exists! \bar{\sigma} \\ L & \xrightarrow{i_L} & L(b) \end{array}$$

Proof.

Uniqueness: We have that $\{1, a, \dots, a^{n-1}\}$ is a basis of $\bar{E}$ over E and thus $\bar{\sigma}|_E$ and $\bar{\sigma}(a)$ uniquely determine $\bar{\sigma}$.

Existence: There exist isomorphisms $\tau_1: \bar{E} \rightarrow E[x]/(f(x))$ so that for every $e \in E$ we have $\tau_1(e) := e + (f(x))$ and $\tau_1(a) = x + (f(x))$ and $\tau_2: \bar{L} \rightarrow L[x]/(g(x))$ defined similarly. Also we define $\tau_3: E[x]/(f(x)) \rightarrow L[x]/(g(x))$ by $h + (f(x)) \mapsto \sigma(h) + (g(x))$. In this way we have that $\tau_2^{-1} \circ \tau_3 \circ \tau_1$ is the desired isomorphism. □

Proposition 3.5. Let F be a field. Let E and L be algebraic closures of F . Then there exists some isomorphism (not necessarily unique) $\rho: E \rightarrow L$ so that $\rho|_F = \text{id}_F$.

Proof. Let $\{a_\alpha \mid \alpha < \kappa\}$ where κ is an infinite cardinal be an indexing of the elements of E . For all $\alpha \leq \kappa$ we inductively define a field $F \subseteq F_\alpha \subset E$ in the following way:

- (1) $F_0 := F$;
- (2) if $\alpha = \beta + 1$ then $F_\alpha = F_\beta(a_\beta)$;
- (3) if α is a limit ordinal then $F_\alpha = \bigcup_{\beta < \alpha} F_\beta$.

It is clear that $E = F_\kappa$. For every $\beta < \kappa$ we denote m_β the minimal polynomial of a_β over F_β . Then $\deg m_\beta = [F_{\beta+1} : F_\beta]$. We can now define an embedding $\rho_\alpha: F_\alpha \rightarrow L$ for every $\alpha \leq \kappa$ so that for all $\beta \leq \alpha \leq \kappa$ we have $\rho_\alpha|_{F_\beta} = \rho_\beta$ (this means that $\rho_\beta \subseteq \rho_\alpha$). If ρ_α has already been defined then we denote $L_\alpha = \text{im}(\rho_\alpha)$.

- (1) $\rho_0 = \text{id}_F$;
- (2) if $\alpha = \beta + 1$ is a successor ordinal then since L is algebraically closed we can choose $b_\beta \in L$ which is the root of the irreducible polynomial $\rho_\beta(m_\beta) \in L_\beta[x]$ (it is irreducible since $\rho_\beta|_{F_\beta}$ is an isomorphism and m_β is irreducible). From Theorem 3.4, there exists a unique extension of ρ_β to an isomorphism

$$\rho_\alpha: F_\alpha = F_\beta(a_\beta) \rightarrow L_\beta(b_\beta) \subseteq L$$

so that $\rho_\alpha(a_\beta) = b_\beta$;

- (3) if α is a limit ordinal then we let $\rho_\alpha = \bigcup_{\beta < \alpha} \rho_\beta$.

Denote $\rho := \rho_\kappa$. We get that $\rho: F_\kappa = E \rightarrow L$ is an embedding of E in L so that $\rho|_F = \text{id}_F$, which also respects the field operations. It is left to show that ρ is surjective. Let $b \in L$ and let g be the minimal polynomial of b over $\rho(E)$. We have that $\rho^{-1}(g)$ (we map x to x) splits over E (since E is algebraically closed), and thus g splits over $\rho(E)$ and in particular $b \in \rho(E)$. □

Exercise 3.3. Let $\sigma: F \rightarrow E$ be an isomorphism of fields. Let $g(x) \in F[x]$ and $h(x) = \sigma(g) \in E[x]$. Let L/F and M/E be the splitting fields of g and h . Then σ extends (not uniquely) to an isomorphism $\bar{\sigma}: M \rightarrow L$.

Corollary 3.6. Let F be a field. Let E/F and L/F be splitting fields of the same polynomial $f \in F[x]$. Then there exists an isomorphism $\sigma: E \rightarrow L$ so that $\sigma|_F = \text{id}_F$.

Remark 3.4. Let $p \in \mathbb{N}$ be prime and let E be a finite field of size p^n . Then the set $F = \{0, 1, 2, \dots, p-1\} \subseteq E$ is a subfield of E , and there exists a unique isomorphism $\rho: \mathbb{Z}/p\mathbb{Z} = F_p \rightarrow F$.

Lemma 3.7. Let p be prime. Let E be a field with p^n elements and identify F_p as a subfield of E . Then E is the splitting field (over F_p) of the polynomial $x^{p^n} - x \in F_p[x]$.

Proof. The multiplicative group $E^\times$ is of size $p^n - 1$, and thus from Cauchy's theorem for all $a \in E^\times$ we have $a^{p^n-1} = 1$. Since we also have that $0^{p^n-1} = 0$ it follows that all elements of E are roots of the polynomial $x(x^{p^n-1} - 1) = x^{p^n} - x \in F[x]$. Since $|E| = p^n$, and a polynomial of degree m has at most m roots, it follows that $x^{p^n} - x$ splits over E . We get that E is the splitting field of $x^{p^n} - x$ over F_p which completes the proof. $\square$

Corollary 3.8. Let $p \in \mathbb{N}$ be prime and $1 \leq n \in \mathbb{N}$. Then every two fields of order p^n are isomorphic.

Proof. The two fields are both splitting fields of $x^{p^n} - x$ over F_p , which is embedded uniquely in both of them. The result now follows directly from Theorem 3.6. $\square$

Remark 3.5. This shows that any field of size p^n is unique. In the next section we will show that there exists a field of size p^n for any prime p and natural number $n \geq 1$.

3.2 The automorphism group of a field

Definition 3.5 (Automorphism group). Let L be a field. The automorphism group of L is given by

$$\text{Aut}(L) := \{\sigma: L \rightarrow L \mid \sigma \text{ is an isomorphism}\}$$

with the group operation being function composition.

Example 3.4. We will show that $\text{Aut}(\mathbb{Q}) = \{\text{id}_{\mathbb{Q}}\}$. Let $\sigma \in \text{Aut}(\mathbb{Q})$. We must have $\sigma(0) = 0$ and $\sigma(1) = 1$ and thus for any $n \in \mathbb{N}$

$$\sigma(n) = \sigma(\underbrace{1 + 1 + \dots + 1}_{n \text{ times}}) = \underbrace{\sigma(1) + \dots + \sigma(1)}_{n \text{ times}} = \underbrace{1 + 1 + \dots + 1}_{n \text{ times}} = n,$$

and from other properties of isomorphisms we get $\sigma(-n) = -\sigma(n) = -n$. From this follows that for any $a/b \in \mathbb{Q}$ we have $\sigma(a/b) = \sigma(a)/\sigma(b) = a/b$, which implies that $\sigma = \text{id}_{\mathbb{Q}}$.

Example 3.5. Let $p \in \mathbb{N}$ be a prime number. Then $\text{Aut}(F_p) = \{\text{id}_{F_p}\}$.

Example 3.6. We want to find $\text{Aut}(\mathbb{R})$. Let $\sigma \in \text{Aut}(\mathbb{R})$. In particular $\sigma|_{\mathbb{Q}}$ is an isomorphism of $\mathbb{Q}$ and thus $\sigma|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$. We will show that σ preserves the order of the real numbers. Let $x, y \in \mathbb{R}$ so that $x \leq y$. There exists $m \in \mathbb{R}$ so that $y - x = m^2$. Hence

$$\sigma(y - x) = \sigma(m^2) \implies \sigma(y) - \sigma(x) = (\sigma(m))^2 \geq 0 \implies \sigma(y) \geq \sigma(x).$$

We will now show that $\sigma = \text{id}_{\mathbb{R}}$. Let $x \in \mathbb{R}$, and let $\{y_n\}_{n=1}^{\infty}, \{z_n\}_{n=1}^{\infty} \subset \mathbb{R}$ be sequences of rational numbers that converge to x from above and from below respectively. We then have that

$$\begin{aligned} y_n \leq x \leq z_n &\implies \sigma(y_n) \leq \sigma(x) \leq \sigma(z_n) \\ &\implies \lim_{n \rightarrow \infty} \sigma(y_n) \leq \sigma(x) \leq \lim_{n \rightarrow \infty} \sigma(z_n) \\ &\implies x \leq \sigma(x) \leq x \\ &\implies \sigma(x) = x. \end{aligned}$$

Definition 3.6 (Frobenius' endomorphism). Let L be a field of prime characteristic p . The map $\phi: L \rightarrow L$ given by $x \mapsto x^p$ is an embedding called Frobenius's endomorphism

Exercise 3.4. Verify that Frobenius' endomorphism is injective.

Example 3.7. Let F be a finite field. Then any injective function from F to F is surjective and thus $\phi \in \text{Aut}(F)$. If $|F| = p$ then from Fermat's little theorem we get that $\phi = \text{id}$, but when $|F| > p$ we have $\phi \neq \text{id}$ since there are exactly p elements that satisfy $x^p = x$, namely the elements of the prime subfield.

Example 3.8. Let $F = F_p(t)$ be a simple extension of the field with p elements. Then we get that $\phi(F) = F_p(t^p) \subsetneq F_p(t)$, so ϕ is not surjective.

3.3 The automorphism group of a field extension

Definition 3.7 (Automorphism group of a field extension). Let E/F be a field extension. The automorphism group of the extension E/F is given by

$$\text{Aut}(E/F) := \{\sigma \in \text{Aut}(E) \mid \sigma|_F = \text{id}_F\}.$$

Exercise 3.5. Verify that $\text{Aut}(E/F)$ is a subgroup of $\text{Aut}(E)$.

Example 3.9. Let us find the automorphism group $\text{Aut}(\mathbb{C}/\mathbb{R})$. The automorphism we may think about is the identity map $\text{id}: \mathbb{C} \rightarrow \mathbb{C}$. Indeed $\text{id} \in \text{Aut}(\mathbb{C}/\mathbb{R})$, but this doesn't really help us find the other automorphisms. In order to find the other automorphisms, we note that for $\sigma \in \text{Aut}(\mathbb{C}/\mathbb{R})$ we have $\sigma(x^2 + 1) = 0$ if and only if $x \in \{-i, i\}$, and since $\sigma(x^2 + 1) = (\sigma(x))^2 + 1$ for any $x \in \mathbb{C}$, we must have $\sigma(\{-i, i\}) = \{-i, i\}$. In the case $\sigma(i) = i$, we obtain $\sigma = \text{id}$, and in the case $\sigma(i) = -i$ we obtain $\sigma = \tau$, where τ is the complex conjugation map. Both of these are automorphisms of $\mathbb{C}$ that fix $\mathbb{R}$ and thus $\text{Aut}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \tau\}$.

Lemma 3.9. Let $E = F(\alpha)$ be a simple field extension. Then any $\sigma \in \text{Aut}(E/F)$ is uniquely determined by the image of α .

Proof. Let $\sigma, \tau \in \text{Aut}(E/F)$ be such that $\sigma(\alpha) = \tau(\alpha)$. Let $e \in E$, then there exist $f, g \in F[\alpha]$ so that $g(\alpha) \neq 0$ and $e = f(\alpha)/g(\alpha)$. We now have that

$$\sigma(e) = \frac{\sigma(f(\alpha))}{\sigma(g(\alpha))} = \frac{f(\sigma(\alpha))}{g(\sigma(\alpha))} = \frac{f(\tau(\alpha))}{g(\tau(\alpha))} = \frac{\tau(f(\alpha))}{\tau(g(\alpha))} = \tau(e),$$

which completes the proof. □

Exercise 3.6. Let $E = F(\alpha_1, \dots, \alpha_n)$ be a field extension. Then any $\sigma \in \text{Aut}(E/F)$ is determined uniquely by the images of $\alpha_1, \dots, \alpha_n$.

Lemma 3.10. Let $E = F(\alpha)$ be a simple algebraic field extension. Let $m(x) \in F[x]$ be the minimal polynomial of α over F . Then

- (1) for all $\sigma \in \text{Aut}(E/F)$, $\sigma(\alpha)$ is a root of $m(x)$;
- (2) for all roots $\beta \in E$ of $m(x)$ there exists a unique $\sigma \in \text{Aut}(E/F)$ so that $\sigma(\alpha) = \beta$.

Proof.

- (1) Since $m(x) \in F[x]$ we have $\sigma(m(x)) = m(\sigma(x))$, hence $0 = \sigma(0) = \sigma(m(\alpha)) = m(\sigma(\alpha))$.
- (2) Existence follows from Theorem 3.4 and the uniqueness follows from Theorem 3.9.

□

Corollary 3.11. *Let $E = F(\alpha)$ be a simple algebraic extension and let $m(x) \in F[x]$ be the minimal polynomial of α . Then*

- (1) *there exists a bijective correspondence between elements of $\text{Aut}(E/F)$ and the distinct roots of $m(x)$ in E (multiple roots count as a single root);*
- (2) *we have $|\text{Aut}(E/F)| \leq [E : F]$ and equality holds if and only if $m(x)$ splits into distinct linear factors over E .*

Proof.

- (1) This follows directly from Theorem 3.10.
- (2) We have that $[E : F] = \deg(m(x))$, and by Theorem 3.10, an automorphism $\sigma \in \text{Aut}(E/F)$ sends α (a root of $m(x)$) to another root of $m(x)$. We also know that σ is determined by where it sends α (remember, E/F is a simple extension), and therefore $|\text{Aut}(E/F)|$ is at most the number of distinct roots of $m(x)$ which is less or equal to $\deg(m(x)) = [E : F]$. Moreover, an equality holds if and only if all roots of $m(x)$ are in E , or in other words, when $m(x)$ splits into distinct linear factors over E .

□

Remark 3.6. Theorem 3.11 is very important for the development of Galois theory. We will later see that in what we call “Galois extensions” we always have the equality $|\text{Aut}(E/F)| = [E : F]$. That is because we explicitly require, in the case of this simple extension $F(a)$ for example, for the minimal polynomial $m(x)$ to split into distinct linear factors over E (in particular we require it does not have multiple roots).

Example 3.10. Consider the polynomial $p(x) = x^3 - 2 \in \mathbb{Q}[x]$. Its roots are $z_1 = \sqrt[3]{2}$ and two other complex roots $z_2, z_3 \in \mathbb{C} \setminus (\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. Since by Theorem 3.10 any automorphism in $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ must send z_1 to some root of p in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, and since $z_2, z_3 \in \mathbb{C} \setminus (\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$, we conclude that $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\text{id}\}$.

Remark 3.7. I suggest trying to visualize Example 3.10. Hold a mental image of $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{C}$ in your head, fix $\mathbb{Q}$ and see how $\mathbb{Q}(\sqrt[3]{2}) \setminus \mathbb{Q}$ is also fixed in place for all $\sigma \in \text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$. Now try to visualize how many embeddings of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ that fix $\mathbb{Q}$ are there in $\mathbb{C}$ in total (this time we can send $\sqrt[3]{2}$ to other roots as well because the embeddings are not required to be automorphisms of E).

Example 3.11. Let F_p be a field of prime characteristic p , and denote $F := F_p(t^p)$ for $t^p \notin F_p$. Now denote $E := F(t)$, and notice that $E = F_p(t)$. We have that $x^p - t^p = (x - t)^p \in F[x]$ is the minimal polynomial of t , and since E/F is simple we conclude $[E : F] = p$. However, since any $\sigma \in \text{Aut}(E/F)$ must send t to another root of $x^p - t^p = (x - t)^p$, it follows that $\sigma(t) = t$, and since $E = F(t)$, the automorphism is determined to be the identity map, and thus $|\text{Aut}(F_p(t)/F_p(t^p))| = |\{\text{id}\}| = 1 < n = [E : F]$.

Theorem 3.12. Let F be a field, let $g(x) \in F[x]$ and let E be the splitting field of g over F . Let $\alpha_1, \dots, \alpha_n$ be the distinct roots of g in E . Then

- (1) there exists an injective homomorphism $\rho: \text{Aut}(E/F) \rightarrow \text{Sym}\{\alpha_1, \dots, \alpha_n\} \cong S_n$;
- (2) $|\text{Aut}(E/F)|$ divides $n!$.

Proof.

- (1) Verify that the map $\varphi: \sigma \mapsto \sigma|_{\{\alpha_1, \dots, \alpha_n\}}$ is the desired homomorphism.
- (2) This part follows from (1) and from Lagrange's theorem since

$$|\text{Aut}(E/F)| = |\text{im } \varphi| \mid |S_n| = n!.$$

□

Remark 3.8. In the setting of Theorem 3.11 we had that $E = F(a)$ is a simple extension, and $m(a)$ is its minimal polynomial. Now in Theorem 3.12 we have that $g(x) \in F[x]$ is some polynomial and E is its splitting field. These are different settings because for example we saw in Example 3.10 that $\mathbb{Q}(\sqrt[3]{2})$ is not the splitting field of any polynomial $g(x) \in \mathbb{Q}[x]$.

Question. Theorem 3.12 is another step in developing Galois theory. We now require E to be the splitting field of a polynomial $g \in F[x]$. Under this extra condition g must split into linear factors (not necessarily distinct yet, so it could be of the form $g(x) = (x-1)^2$). However, if $g(x)$ does not have multiple roots, will the equality from Theorem 3.11 always hold?

Example 3.12. Let $E/\mathbb{Q}$ be the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$. Denote $\alpha = \sqrt[3]{2}$ and $w = e^{2\pi i/3}$. We know that $E = \mathbb{Q}(\alpha, w)$. We have seen in Example 3.1 that $[E : \mathbb{Q}] = 6$. The complex conjugation map τ satisfies

$$\begin{aligned}\tau(\alpha) &= \alpha, \\ \tau(\alpha w) &= \alpha \bar{w} = \alpha w^2, \\ \tau(\alpha w^2) &= \alpha \bar{w}^2 = \alpha w,\end{aligned}$$

so τ permutes the roots $\{\alpha, \alpha w, \alpha w^2\}$, and thus $\tau|_E \in \text{Aut}(E/\mathbb{Q})$. Similarly, by Theorem 3.4 we can show that exists automorphisms such that $\eta(\alpha) = \alpha w$ and $\iota(\alpha) = \alpha w^2$ (which unlike in Theorem 3.4 are not necessarily unique as the extension is not necessarily simple). Thus $\{\text{id}, \sigma, \eta, \iota\} \subset \text{Aut}(E/\mathbb{Q})$, and since by Theorem 3.12 we get that $\text{Aut}(E/\mathbb{Q})$ is isomorphic to a subgroup of S_3 we conclude that $\text{Aut}(E/\mathbb{Q}) \cong S_3$.

Exercise 3.7. Let $f \in \mathbb{Q}[x]$ and let E be the splitting field of f over $\mathbb{Q}$. Then $\tau|_E \in \text{Aut}(E/\mathbb{Q})$.

Remark 3.9. Let $E = F(\alpha)$ be a simple field extension such that α is a primitive n th root of unity. Then if $m_1 \equiv m_2 \pmod{n}$, we have $\alpha^{m_1} = \alpha^{m_2}$, and thus for any $m \in \mathbb{Z}/n\mathbb{Z}$, the expression α^m is well defined.

Exercise 3.8. Show that

$$\left\{ \alpha^m \mid m \in (\mathbb{Z}/n\mathbb{Z})^\times \right\} = \left\{ \beta \in E \mid \beta \text{ is a primitive } n\text{th root of unity} \right\}.$$

In particular, there are exactly $\phi(n)$ (Euler's totient function of n) primitive n th roots of unity.

Example 3.13. Let $E = F(\alpha)$ be a simple field extension such that α is a primitive n th root of unity and let $\sigma \in \text{Aut}(E/F)$. Then $\sigma(\alpha)$ is also a primitive n th root of unity, and we can define the map

$$\psi: \text{Aut}(E/F) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

by $\psi(\sigma) = m$ if and only if $\sigma(\alpha) = \alpha^m$. Since any $\sigma \in \text{Aut}(E/F)$ is determined by the image of α , it follows that ψ is injective, and since it is also a homomorphism, we get that $\text{Aut}(E/F)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Example 3.14. Let p be a prime number and let $\eta \in \mathbb{C}$ be a primitive p th root of unity. We have seen that the minimal polynomial of η over $\mathbb{Q}$ is

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 = \prod_{1 \leq k \leq p-1} (x - \eta^k).$$

In particular all roots of $\phi_p(x)$ are elements of $\mathbb{Q}(\eta)$. Thus,

$$p - 1 \leq |\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q})| \leq p - 1$$

where the first inequality follows from the existence of an automorphism that sends η to any other one of $p - 1$ roots, and the second inequality follows from the fact $\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q})$ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. Thus

$$|\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q})| = p - 1,$$

and

$$\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong C_{p-1}.$$

Example 3.15. Let $p \geq 3$ be a prime number and let η be defined like in Example 3.14. Since $\eta \notin \mathbb{R}$ and $\eta + \eta^{-1} \in \mathbb{R}$, we get that

$$\mathbb{Q}(\eta) \supsetneq \mathbb{Q}(\eta + \eta^{-1}).$$

On the other hand, η is a root of

$$f(x) = (x - \eta)(x - \eta^{-1}) = x^2 - (\eta + \eta^{-1})x + 1,$$

and thus $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta + \eta^{-1})] = 2$. Then since $\sigma \in \text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q})$ must send η to a root of its minimal polynomial we also have $\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q}) = \{\text{id}_{\mathbb{Q}(\eta)}, \tau\}$ where τ is the restriction of the complex conjugation map to $\mathbb{Q}(\eta)$.

3.4 Galois correspondence

Definition 3.8 (Galois correspondence). Let E/F be a field extension and let $G = \text{Aut}(E/F)$. For any subfield $F \subseteq M \subseteq E$, The Galois correspondence sends M to the group

$$\mathcal{G}(M) := \text{Aut}(E/M) \leq \text{Aut}(E/F).$$

For any subgroup $H \leq G := \text{Aut}(E/F)$, the Galois correspondence sends H to the fixed field of H

$$\mathcal{F}(H) := \{x \in E \mid (\forall \sigma \in H) \sigma(x) = x\}.$$

The correspondence is given by:

$$\{M \mid F \subseteq M \subseteq E \text{ is a subfield}\} \xrightleftharpoons[\mathcal{F}]{\mathcal{G}} \{H \mid H \leq G\}.$$

Example 3.16. Let $F = \mathbb{R}$ and $E = \mathbb{C}$. Then $G = \text{Aut}(E/F) = \{\text{id}, \tau\}$, and we have $\mathcal{F}(\{\text{id}\}) = \mathbb{C}$ and $\mathcal{F}(G) = \mathbb{R}$, and there aren't any more subfields. $\mathcal{G}(\mathbb{R}) = G$ and $\mathcal{G}(\mathbb{C}) = \{\text{id}\}$.

Proposition 3.13. *With regards to the notations above,*

- (1) $\mathcal{F}(H)$ is a field contained in E and containing F ;
- (2) $E = \mathcal{F}(\{\text{id}_E\})$;
- (3) if $H_1 \leq H_2$ then $\mathcal{F}(H_1) \supseteq \mathcal{F}(H_2)$.

Proof.

- (1) Any $\sigma \in G$ fixes the elements of F and thus $F \subseteq \mathcal{F}(H)$. For any $\sigma \in G$ and for all $x, y \in E$ if $\sigma(x) = x$ and $\sigma(y) = y$, then $\sigma(x \pm y) = x \pm y$ and $\sigma(xy) = xy$ and $\sigma(x/y) = x/y$ (if $y \neq 0$). We get that $\mathcal{F}(H)$ is closed under addition multiplication multiplication and division and contains 0 and 1, so $\mathcal{F}(H)$ is a subfield of E .
- (2) Immediate.
- (3) In particular $H_1 \subseteq H_2$, and thus $\mathcal{F}(H_1) \supseteq \mathcal{F}(H_2)$.

□

Exercise 3.9. With regards to the notations above,

- (1) $\mathcal{G}(M)$ is a subgroup of G ;
- (2) $\mathcal{G}(E) = \{\text{id}\}$ and $\mathcal{G}(F) = G$;
- (3) if $M_1 \subseteq M_2$ then $\mathcal{G}(M_1) \supseteq \mathcal{G}(M_2)$.

Remark 3.10. Notice that the exercise is almost symmetrical to Theorem 3.13, except that in part (2) of Theorem 3.13 we did not claim that $\mathcal{F}(G) = F$. Indeed, this claim is false.

Example 3.17. We see that $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\text{id}\}$ since $\sqrt[3]{2}$ is the only root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$. Thus we have $\mathcal{F}(\{\text{id}\}) = \mathcal{F}(G) = \mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}$.

Example 3.18. Let E/F be as in Example 3.11. We have seen that E is the splitting field of $x^p - t^p$ over F , and that $G := \text{Aut}(E/F) = \{\text{id}_E\}$. In particular we obtain that $\mathcal{F}(G) = E \neq F$.

Proposition 3.14. *With regards to the notations above,*

- (1) for any subfield M we have $M \subseteq \mathcal{F}(\mathcal{G}(M))$;
- (2) for any $H \leq G$ we have $H \subseteq \mathcal{G}(\mathcal{F}(H))$.

Proof.

- (1) Let $m \in M$. Then for any $\sigma \in \mathcal{G}(M)$, $\sigma(m) = m$, and thus $m \in \mathcal{F}(\mathcal{G}(M))$.
- (2) Let $\sigma \in H$. Then for any $a \in \mathcal{F}(H)$, $\sigma(a) = a$, and thus $\sigma \in \mathcal{G}(\mathcal{F}(M))$.

□

Exercise 3.10. Show that the following claims hold.

- (1) For any subfield M we have $\mathcal{G}(M) = \mathcal{G}(\mathcal{F}(\mathcal{G}(M)))$.
- (2) For any subfield $H \leq G$ we have $\mathcal{F}(M) = \mathcal{F}(\mathcal{G}(\mathcal{F}(H)))$.

Lemma 3.15. *Every quadratic extension $K/\mathbb{Q}$ is of the form $\mathbb{Q}(\sqrt{r})$ for some squarefree integer $r \in \mathbb{Z} \setminus \{0, 1\}$.*

Proof. Let K be a quadratic extension of $\mathbb{Q}$, this means that $[K : \mathbb{Q}] = 2$. Then there exists an element $\alpha \in K \setminus \mathbb{Q}$ such that $K = \mathbb{Q}(\alpha)$ and the minimal polynomial of α over $\mathbb{Q}$ has degree 2. Thus, the minimal polynomial has the form

$$f(x) = x^2 + bx + c \in \mathbb{Q}[x],$$

for some $b, c \in \mathbb{Q}$. The roots of this polynomial are

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Let $d = b^2 - 4c \in \mathbb{Q}$ be the discriminant. Then $\alpha \in \mathbb{Q}(\sqrt{d})$, so $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{d})$. Conversely, since $\sqrt{d} = \pm(2\alpha + b) \in \mathbb{Q}(\alpha)$, we have $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{d})$. It is left to show that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{r})$ for a squareless $r \in \mathbb{Z} \setminus \{0, 1\}$. Write $d = \frac{a}{b} \in \mathbb{Q}$ with $a, b \in \mathbb{Z}$ where b is a perfect square. Then

$$\sqrt{d} = \sqrt{\frac{a}{b}} = \frac{\sqrt{a}}{\sqrt{b}} \in \mathbb{Q}(\sqrt{a}),$$

so $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{a})$. Let r be the squarefree part of a , so $a = rs^2$ for some $s \in \mathbb{Z}$. Then

$$\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{r}),$$

since $\sqrt{a} = s\sqrt{r}$ with $s \in \mathbb{Q}$. Therefore, $K = \mathbb{Q}(\sqrt{r})$ for some squarefree integer $r \in \mathbb{Z} \setminus \{0, 1\}$. $\square$

Example 3.19. Let $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. We notice that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{6}) = \mathbb{Q}(\sqrt{3}, \sqrt{6})$.

- (I) Assume, by way of contradiction, that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Then $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$ and

$$3 = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

which implies that $ab = 0$, but since $3 \neq a^2$ for any $a \in \mathbb{Q}$ and $3 \neq 2b^2$ for any $b \in \mathbb{Q}$ we get a contradiction and thus $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. We get that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

and thus from Theorem 3.11 we get that $|\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| \leq 4$.

- (II) If $E = F(\alpha)$ is a field extension of degree 2 and $\alpha^2 \in F$ then the minimal polynomial of α over F is $x^2 - \alpha^2 = (x - \alpha)(x + \alpha)$, and thus there exists $\sigma \in \text{Aut}(E/F)$ so that $\sigma(\alpha) = -\alpha$ and $\text{Aut}(E/F) = \{\text{id}_E, \sigma\}$.
- (III) From (II) we get that there exists $\sigma \in \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})) \leq \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ such that $\sigma(\sqrt{3}) = -\sqrt{3}$ and $\sigma(\sqrt{2}) = \sqrt{2}$, and thus $\sigma(\sqrt{6}) = -\sqrt{6}$. Similarly, there exist $\tau, \eta \in \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ so that

$$\begin{aligned} \tau(\sqrt{2}) &= -\sqrt{2} \quad \text{and} \quad \tau(\sqrt{3}) = \sqrt{3} \quad \text{and} \quad \tau(\sqrt{6}) = -\sqrt{6}, \\ \eta(\sqrt{2}) &= -\sqrt{2} \quad \text{and} \quad \eta(\sqrt{3}) = -\sqrt{3} \quad \text{and} \quad \eta(\sqrt{6}) = \sqrt{6}, \end{aligned}$$

so necessarily from (I) we conclude $\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \eta\}$. Since all elements of the automorphism group $\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ are of order ≤ 2 , it is a *Boolean group*, and in particular it is an abelian group so it is the *inner direct product* of $\langle \sigma \rangle$ and $\langle \tau \rangle$.

$$\text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \langle \sigma \rangle \dot{\times} \langle \tau \rangle \cong C_2 \times C_2.$$

- (IV) If $\mathbb{Q} \subsetneq M \subsetneq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ then $M = \mathbb{Q}(\sqrt{r})$ for some squarefree integer $2 \leq r \in \mathbb{Z}$. We want to show that $r \in \{2, 3, 6\}$. Assume that $\sqrt{r} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then for any automorphism $\mu \in \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$, we have that $\mu(\sqrt{r}) = \pm\sqrt{r}$. There exist $a, b, c, d \in \mathbb{Q}$ so that

$$\sqrt{r} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}.$$

As we saw there exists $\text{id} \neq \mu \in \text{Aut}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{r}))$ so that $\mu(\sqrt{r}) = \sqrt{r}$. If $\mu = \sigma$ then

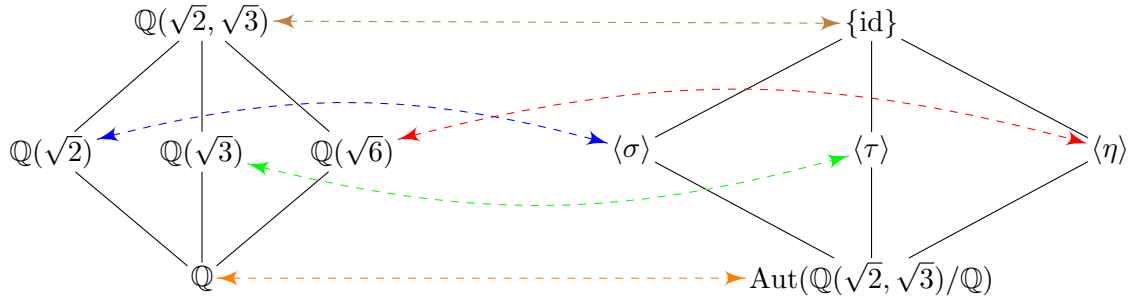
$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = \sqrt{r} = \mu(\sqrt{r}) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6} \implies c = d = 0,$$

which implies

$$\sqrt{r} = a + b\sqrt{2} \implies r = b^2 \cdot 2 \implies r = 2.$$

where the last step follows from the fact that r is squarefree. Similarly if $\mu = \tau$ then $r = 3$ and if $\mu = \eta$ then $r = 6$.

- (V) The subgroups and subfields form lattices, and the Galois correspondence gives a bijection between them. We can see this in the following diagram:



In this case, $\mathcal{F}$ and $\mathcal{G}$ are the inverse of each other and invert the containment order. Note that the fact these are all the subfield of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ follows from (V).

Example 3.20. Let $\eta \in \mathbb{C}$ be the primitive 5th root of unity.

- (o) We saw in Example 3.14 that $[\mathbb{Q}(\eta) : \mathbb{Q}] = 4$ and that

$$\text{Aut}(\mathbb{Q}(\eta) : \mathbb{Q}) \cong (\mathbb{Z}/5\mathbb{Z})^\times \cong C_4.$$

We will find a generator for $\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q})$. Let $\sigma \in \text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q})$ be the automorphism that satisfies $\sigma(\eta) = \eta^2$. Such an automorphism must exist since η^2 is a root of $\frac{x^5-1}{x-1}$ which is the minimal polynomial of η . We see that

$$\begin{aligned} \sigma(\eta) &= \eta^2, \\ \sigma^2(\eta) &= \eta^4, \\ \sigma^3(\eta) &= \eta^3, \\ \sigma^4(\eta) &= \eta, \end{aligned}$$

so $\langle \sigma \rangle = \text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q})$.

- (I) We have seen in Example 3.15 that

$$[\mathbb{Q}(\eta) : \mathbb{Q}(\eta + \eta^{-1})] = 2,$$

and thus from

$$4 = [\mathbb{Q}(\eta) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\eta) : \mathbb{Q}(\eta + \eta^{-1})]}_{=2} [\mathbb{Q}(\eta + \eta^{-1}) : \mathbb{Q}]$$

we get $[\mathbb{Q}(\eta + \eta^{-1}) : \mathbb{Q}] = 2$, so it is a quadratic extension and thus there exists a square-free integer $2 \leq r \in \mathbb{Z}$ so that

$$\mathbb{Q}(\sqrt{r}) = \mathbb{Q}(\eta + \eta^{-1}).$$

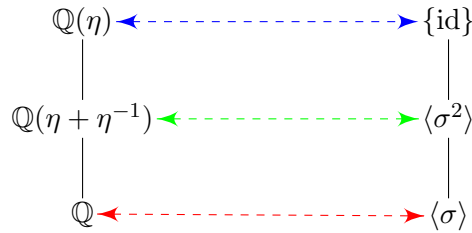
(II) We want to show that $\mathbb{Q}(\sqrt{r})$ is the only subfield that is properly contained in (not equal) $\mathbb{Q}(\eta)$ which contains $\mathbb{Q}$.

Let $\mathbb{Q} \subsetneq M \subsetneq \mathbb{Q}(\eta)$. Then

$$4 = [\mathbb{Q}(\eta) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\eta) : M]}_{1 <} \underbrace{[M : \mathbb{Q}]}_{1 <} \implies [M : \mathbb{Q}] = 2.$$

This implies that there exists a squarefree integer $s \neq 0, 1$ so that $N = \mathbb{Q}(\sqrt{s})$ (s may be negative). If $s \neq r$, then from the same arguments as in Example 3.19 (we didn't use the fact that the roots are real) we could obtain that $\text{Aut}(\mathbb{Q}(\eta)/\mathbb{Q}) \cong C_2 \times C_2$, which is a contradiction.

(III) In this case we also get that $\mathcal{F}$ and $\mathcal{G}$ are the inverse of each other:



Exercise 3.11. Show that the Galois correspondence induces a bijection between the lattice of the subgroups of $\text{Aut}(E/G)$ and the lattice of the subfields of E over $\mathbb{Q}$ where E is the splitting field of $x^3 - 2$ over $\mathbb{Q}$.

Remark 3.11. We have seen examples where $\mathcal{F}$ and $\mathcal{G}$ were the inverse of each other like Example 3.19 and Example 3.20, and examples where they weren't like Example 3.17 and Example 3.18. We want to figure out what was the difference between these examples.

- In Example 3.19 and Example 3.20 the extensions were the splitting fields of polynomials with distinct roots (all roots were simple - with multiplicity 1).
- In Example 3.17 the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not the splitting field of $x^3 - 2 \in \mathbb{Q}[x]$ since it does not contain the complex roots (although all roots of $x^3 - 2$ are distinct/simple).
- In Example 3.18 the extension was E/F where F is of prime characteristic p and $E = F(\alpha)$ for some $\alpha \notin F$ such that $\alpha^p \in F$. Here E is the splitting polynomial of $x^p - \alpha^p$, but all roots of $x^p - \alpha^p$ are equal - they are not distinct/simple.

4 Separable extensions

4.1 Separable polynomials and separable extensions

Definition 4.1 (Simple and multiple roots). Let E/F be the splitting field over F of a polynomial $0 \neq g(x) \in F[x]$. Let $\alpha \in E$ be a root of $g(x)$. The multiplicity of α is the maximal value of $k \geq 1$ so that $(x - \alpha)^k$ divides g (in $E[x]$). If the multiplicity of α is 1 then α is said to be a simple root. Otherwise it is said to be a multiple root.

Definition 4.2 (Separable polynomial). Let F be a field and $0 \neq g(x) \in F[x]$. Then g is called separable if there exists a splitting field E/F of g over F so that g doesn't have multiple roots.

Remark 4.1. If g is separable with regards to some splitting field, then g is separable in all fields in which it splits.

Definition 4.3 (Derivative). Let $g(x) = \sum_{i=0}^n a_i x^i \in F[x]$ be a polynomial. The derivative of g is

$$g'(x) = \sum_{i=1}^n i a_i x^{i-1}.$$

Remark 4.2. If $\text{char}(F) = 0$, then $\deg(g') = \deg(g) - 1$. If $\text{char}(F) > 0$ the degree might be smaller.

Example 4.1. When $g(x) = x^p \in F_p[x]$ we have $g'(x) = p x^{p-1} = 0$. Thus $\deg(g) = p$ but $\deg(g') = 0$.

Exercise 4.1. Show that the derivative is linear.

Solution. Let $g, h \in F[x]$ be so that $g(x) = \sum_{i=0}^n a_i x^i$ and $h(x) = \sum_{i=0}^n b_i x^i$ and let $c \in F$. We have that

$$(cg)'(x) = \sum_{i=1}^n i c a_i x^{i-1} = c \sum_{i=1}^n i a_i x^{i-1} = c(g')(x)$$

and

$$(g+h)' = \sum_{i=1}^n i(a_i + b_i)x^{i-1} = \sum_{i=1}^n i a_i x^{i-1} + \sum_{i=1}^n i b_i x^{i-1} = (g)' + (h)'.$$

This shows that the derivative is linear which completes the proof.

Lemma 4.1. Let F be a field, let $0 \neq g(x) \in F[x]$, let L be the splitting field of g over F and let $\alpha \in L$ be a root of g . Then α is a multiple root if and only if α is a root of g' .

Proof. Let $\alpha = \alpha_1, \dots, \alpha_r$ be the distinct roots of g in L and let $e_1, \dots, e_r$ be their multiplicities. Then there exists $0 \neq C \in F$ so that

$$g(x) = C \prod_{i=1}^r (x - \alpha_i)^{e_i},$$

and thus from the product rule:

$$g'(x) = C \sum_{i=1}^r \left(e_i (x - \alpha_i)^{e_i-1} \prod_{j \neq i} (x - \alpha_j)^{e_j} \right),$$

and so

$$g'(\alpha) = C \sum_{i=1}^r \left(e_i (\alpha_1 - \alpha_i)^{e_i-1} \prod_{j \neq i} (\alpha_1 - \alpha_j)^{e_j} \right) = C \left(e_1 (\alpha_1 - \alpha_1)^{e_1-1} \prod_{j \neq 1} (\alpha_1 - \alpha_j)^{e_j} \right)$$

so $g'(\alpha) = 0$ if and only if $e_1 > 1$. □

Remark 4.3. Let $g, h \in F[x]$ be polynomials. If E/F is a field extension of F , then when we apply Euclid's algorithm we would get the same polynomials in both fields, and thus $\gcd(g, h) = r$ in both $F[x]$ and $E[x]$.

Corollary 4.2. Let $g, h \in F[x]$ be polynomials and let E/F be a field extension of F . Then g and h are coprime over E if and only if they are coprime over F .

Exercise 4.2. Let F be a field and let $h, g \in F[x]$. Suppose that h splits in F . Then g and h are coprime if and only if they don't have a common root.

Solution. Suppose that g and h are coprime. Assume, by way of contradiction, that they have a common root $r \in F$. Then $(x - r)$ divides both g and h and thus it must divide $\gcd(g, h)$ in contradiction to $\gcd(g, h) = 1$.

Next suppose that g and h don't have a common root. Let $\gcd(g, h) = r$. Assume, by way of contradiction, that $r \neq 1$. Then since $r \mid h$ and h splits in F we get that r must split in F . Let $z \in F$ be a root of r , so that $p := (x - z) \mid r$. By properties of $\gcd$ it follows that $p \mid h$ and $p \mid g$ so they have a common root which is a contradiction.

Corollary 4.3. Let $0 \neq h \in F[x]$. Then h is separable if and only if h and h' are coprime in $F[x]$.

Proof. Let E be the splitting field of h over F . Then by definition h is separable if and only if h doesn't have multiple roots. Then h doesn't have multiple roots if and only if h and h' don't have common roots, so combining this with Exercise 4.2 we get that h is separable if and only if h and h' are coprime in E . From Theorem 4.2 we now get that h is separable if and only if h and h' are coprime in $F[x]$. $\square$

Corollary 4.4. Let F be a field of characteristic 0. Let $h \in F[x]$ be irreducible. Then h is separable.

Proof. Since h is irreducible every divisor of h of degree less than $\deg(h)$ is invertible. Since $\text{char} F = 0$ we obtain that $\deg(\gcd(h, h')) \leq \deg(h') = \deg(h) - 1 < \deg(h)$, so the greatest common divisor of h and h' is invertible. Hence $\gcd(h, h') = 1$ so h and h' are coprime. Then from Theorem 4.3 we obtain that h is separable, which completes the proof. $\square$

Example 4.2. Let F be a field of prime characteristic p and let $a \in F$ be so that there does not exist $b \in F$ so that $a = b^p$. We have seen in Exercise 3.1 that $h(x) = x^p - a$ is irreducible in $F[x]$. Since $h' = 0$ we get that h and h' are not coprime in $F[x]$. This shows that h is not separable.

Remark 4.4. Let F be a field of characteristic p . We want to understand the polynomials $g \in F[x]$ which are irreducible and nonseparable. Since g is irreducible, every polynomial of degree less than $\deg(g)$ that is not the zero polynomial is coprime to g . In particular if $g' \neq 0$ then g and g' are coprime, so Theorem 4.3 implies that g is separable, which is a contradiction. The implication is that all irreducible and nonseparable polynomials $g \in F[x]$ satisfy $g' = 0$, so they must be of the form

$$g(x) = \sum_{i=0}^n a_i x^{ip}.$$

If we denote $h(x) := \sum_{i=0}^n a_i x^i$, we can even write $g(x) = h(x^p)$. We can even show that $h(x)$ is irreducible. Assume, by way of contradiction, that there exist $h_1, h_2 \in F[x] \setminus F$ so that

$$h(x) = h_1(x)h_2(x).$$

Then $g(x) = h_1(x^p)h_2(x^p)$ where both $h_{1,2}(x^p) \in F[x] \setminus F$. However, g is irreducible, so we get a contradiction. Therefore all irreducible and nonseparable polynomials in a field of characteristic p are of the form $g(x) = h(x^p)$ for some irreducible polynomial $h(x) = \sum_{i=0}^n a_i x^i \in F[x]$.

Proposition 4.5. *Let F be a field of a prime characteristic p , and let $f \in F[x]$ be an arbitrary irreducible polynomial. Then there exists a number $e \geq 0$, and an irreducible, separable polynomial $h(x) \in F[x]$ so that*

- (1) $f(x) = h(x^{p^e})$;
- (2) the multiplicity of each of the roots of f is p^e .

Corollary 4.6. *Let F be a field and let $g \in F[x]$ be irreducible. Then any root r in some splitting field of g over F has the same multiplicity.*

4.2 Finite fields

Proposition 4.7. *Let p be a prime number. Then for all $n \geq 1$ there exists a unique (up to isomorphism) field F of order p^n .*

Proof. Let $n \geq 1$. We have seen that any field of order p^n is isomorphic to the splitting field of $x^{p^n} - x$ over F_p . We now prove existence. Denote $h(x) = x^{p^n} - x$. Let E be the splitting field of $h(x)$. Since $h'(x) = -1$ we conclude that h and h' are coprime and thus $h(x)$ is separable. By definition of separability we get that

$$L = \{a \in E \mid h(a) = 0\} \subseteq E$$

is a set of cardinality p^n . Notice that $0, 1 \in L$ and that it is closed under addition and multiplication, since for all $a, b \in L$ we have

$$\begin{aligned} h(a+b) &= (a+b)^{p^n} - (a+b) = a^{p^n} + b^{p^n} - a - b = 0 \\ h(a \cdot b) &= (a \cdot b)^{p^n} - (a \cdot b) = 0 \end{aligned}$$

A nonempty subset of a finite field that contains 0 and 1 and is closed under addition and multiplication is a subfield so L is a field of order p^n which completes the proof. $\square$

Remark 4.5. Notice that since $h(x)$ splits in L we actually have that $L = E$.

Definition 4.4 (Perfect field). A field F is said to be perfect if any irreducible polynomial $g(x) \in F[x]$ is separable.

Example 4.3. According to Theorem 4.4 any field of characteristic 0 is perfect.

Remark 4.6. The next proposition shows that any finite field is perfect and any field of rational functions $F(x)$ where $\text{char}(F) = p$ is not perfect.

Proposition 4.8. *Let F be a field of characteristic $p > 0$. Then F is perfect if and only if the endomorphism of Frobenius is surjective.*

Proof. Suppose that ϕ_p is not surjective, and let $b \in F \setminus \phi_p(F)$. We have seen in Example 4.2 that $x^p - b$ is irreducible and also nonseparable so F is not perfect.

Next suppose that ϕ_p is surjective. Let $g(x) \in F[x]$ be irreducible. Then from Theorem 4.5 there exists an irreducible and separable $h(x) \in F[x]$ and a number $e \geq 0$ so that $g(x) = h(x^{p^e})$. Denote $h(x) = \sum_{i=0}^n a_i x^i$. If we show that $p^e = 1$ then $g(x) = h(x)$ is separable which completes the proof. Since ϕ_p is surjective, for all $0 \leq i \leq n$ there exists $b_i \in F$ so that $(b_i)^{p^e} = a_i$. We get that

$$g(x) = h(x^{p^e}) = \sum_{i=0}^n a_i x^{ip^e} = \sum_{i=0}^n (b_i x^i)^{p^e} = \left(\sum_{i=0}^n b_i x^i \right)^{p^e},$$

where the last transition follows from the fact F has characteristic p . Since $g(x)$ is irreducible we get that $p^e = 1$, so $g(x) = h(x)$ is separable, which completes the proof. $\square$

Remark 4.7. Every finite field is perfect.

4.3 Embeddings of field extensions

Definition 4.5 (Separable element). Let E/F be an algebraic field extension. Then $\alpha \in F$ is said to be separable over F if its minimal polynomial is separable.

Definition 4.6 (Separable extension). A field extension E/F is said to be separable if all of its elements are separable.

Example 4.4. Let F be a field with characteristic 0. Then any algebraic extension of F is separable.

Definition 4.7. Let E/F be a finite extension, let $\varphi: F \rightarrow \Omega$ be an embedding of F in an algebraically closed field Ω . Denote

$$i_{\varphi, \Omega}(E/F) = \# \{ \hat{\varphi}: E \rightarrow \Omega \mid \hat{\varphi}|_F = \varphi \}.$$

Remark 4.8. We will soon see that $i_{\varphi, \Omega}(E/F)$ is not dependent on φ or Ω . It is only dependent on E/F .

Lemma 4.9. Let $E = F(a)$ be a finite simple field extension. Let Ω be an algebraically closed field and let $\varphi: F \rightarrow \Omega$ be an embedding. Let $m_a(x) \in F[x]$ be the minimal polynomial of a over F . Then $i_{\varphi, \Omega}(E/F)$ is equal to the number of different embeddings of E in the splitting field of m_a over F . In particular if E/F is a simple algebraic extension then

- (1) $i_{\varphi, \Omega}(E/F)$ is not dependent on φ or on Ω ;
- (2) $i_{\varphi, \Omega}(E/F) \leq [E : F]$;
- (3) in (2) there is equality if and only if $m_a(x)$ is separable.

Proof. We know that if $\hat{\varphi}: E \rightarrow \Omega$ is an extension of φ then $\hat{\varphi}(a)$ is a root of $\varphi(m_a)$ and that the number of different roots of $\varphi(m_a)$ in Ω is equal to the number of distinct roots of $m_a(x)$ in the splitting field of m_a over F . Theorem 3.4 shows that $\hat{\varphi}$ is determined by the image of a and that if $b \in \Omega$ is a root of $\varphi(m_a)$ then φ is extendable to an embedding $\hat{\varphi}: E \rightarrow \Omega$ so that $\hat{\varphi}(a) = b$.

Since each embedding is determined by $m_a(a)$, which must be a root of m_a , we immediately get $i_{\varphi, \Omega}(E/F) \leq \deg(m_a) = [E : F]$, and equality holds if and only if m_a has no multiple roots (is separable). $\square$

Remark 4.9 (Intuition for $i(E/F)$). We know that $i(E/F)$ is the number of F -embeddings of E in an algebraic closure of F which we denote Ω . For example, the inclusion map $i: E/F \rightarrow \Omega$ is always such an embedding (this may be the reason for the notation too). In general, if we have a simple field extension $F(a)/F$ (though this is true for nonsimple extensions as well), for example $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, and we want to understand what $i(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ is, we first find an algebraically closed field containing $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, for example $\mathbb{C}$. Then we notice the most important fact, that any F -embedding σ fixes F , so it must send roots of the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$ to other roots. Therefore, for any F -embedding σ we obtain $\sigma(\sqrt[3]{2}) \in \{z_1, z_2, z_3\}$, where z_1, z_2, z_3 are the roots of $x^3 - 2$. Since σ is determined by the value of $\sigma(\sqrt[3]{2})$ we get $i(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = 3$. Make sure you can visualize the embeddings, each as a union of $\mathbb{Q}$ and a “line” passing through a different root of $x^3 - 2$. Make sure you understand why there are 3 and not 6 embeddings (answer: because we can only send roots to roots).

Example 4.5. Since $x^2 + 1$ is separable and $[\mathbb{C} : \mathbb{R}] = 2$ we can use Theorem 4.9 to conclude that $i(\mathbb{C}/\mathbb{R}) = 2$, which are exactly the identity and complex conjugation (both interchange the roots of $x^2 + 1$).

Example 4.6. Recall Example 3.11. In that case, since any embedding sends a root of the minimal polynomial to another root of the minimal polynomial, and is determined by it, and the minimal polynomial only has one root t we conclude that $i(F_p(t)/F_p(t^p)) = 1$. However, $[F_p(t) : F_p(t^p)] = p$, because the minimal polynomial of t over $F_p(t^p)$ is $x^p - t^p = (x - t)^p$ of degree p . In this case we have $1 = i(F_p(t)/F_p(t^p)) < [F_p(t) : F_p(t^p)] = p$, since the point p is a multiple root of the minimal polynomial.

Proposition 4.10. *Let E/F be a finite field extension.*

(1) *Let $\varphi_1: F \rightarrow \Omega_1$ and $\varphi_2: F \rightarrow \Omega_2$ where Ω_1, Ω_2 are algebraically closed. Then $i_{\varphi_1, \Omega_1} = i_{\varphi_2, \Omega_2}$.*

(2) *If $F \subseteq L \subseteq E$ then*

$$i(E/F) = i(E/L) \cdot i(L/F).$$

(3) $1 \leq i(E/F) \leq [E : F]$.

Proof.

(1) + (2) The proof is by induction on $[E : F]$ such that the base case is $[E : F] = 2$ and in this case the extension is simple and thus (1) follows from the previous lemma (Theorem 4.9) and also if $F \subseteq L \subseteq E$ then $L = F$ or $L = E$ and the proposition is trivial.

Assume that $n = [E : F] > 2$ and we have shown the proposition holds for $k < n$. Suppose that there does not exist a subfield $F \subsetneq L \subsetneq E$ then E/F is a simple extension and the proof is like in the base case. Otherwise, there exists $F \subsetneq L \subsetneq E$. For all $1 \leq i \leq r$ let $\varphi_i: F \rightarrow \Omega_i$ be an embedding of F in an algebraically closed field Ω_i . For all $1 \leq i \leq r$ we denote

$$\begin{aligned} A_i &= \{ \hat{\varphi}: L \rightarrow \Omega \mid \hat{\varphi}|_F = \varphi_i \} \\ B_i &= \{ \hat{\varphi}: E \rightarrow \Omega \mid \hat{\varphi}|_F = \varphi_i \} \end{aligned}$$

For all $\psi \in A_i$ we denote

$$C_{\psi, i} = \{ \hat{\varphi}: E \rightarrow \Omega \mid \hat{\varphi}|_L = \psi \}$$

Then we have

$$B_i = \bigsqcup_{\psi \in A_i} C_{\psi, i}$$

Since $[E : F] > [E : L]$ from the induction hypothesis we know that $i_{\psi, \Omega_i}(E/L)$ is independent of ψ and Ω_i so we can simply write $i_{\psi, \Omega_i}(E/L) = i(E/L)$. Moreover, $|A_i|$ is independent of φ_i and Ω_i and it is simply equal to $i(L/F)$. Then using these observations we get

$$i_{\varphi_i, \Omega_i}(E/F) = \sum_{\psi \in A_i} i_{\psi, \Omega_i}(E/L) = \sum_{\psi \in A_i} i(E/L) = i(E/L) \cdot i(L/F),$$

which completes the proof.

(3) Suppose that $E = F(a_1, \dots, a_k)$ and for all $1 \leq j \leq k-1$ denote $L_j := F(a_1, \dots, a_j)$. Then from (2) we obtain that

$$i(E/F) = \underbrace{i(E/L_{k-1})}_{\geq 1} \cdots \underbrace{i(L_1/L)}_{\geq 1} \leq [E : L_{k-1}] \cdots [L_1 : L] = [E : F],$$

where the inequality follows from Theorem 4.9. This completes the proof. $\square$

Proposition 4.11. *Let E/F be a finite field extension. Then the following conditions are equivalent:*

- (1) *There exist $a_1, \dots, a_k \in E$ separable over F so that $E = F(a_1, \dots, a_k)$.*
- (2) *$i(E/F) = [E : F]$.*
- (3) *E/F is a separable extension.*

Proof.

- (1 $\rightarrow$ 2) For all $0 \leq i \leq k$ denote $L_i := F(a_1, \dots, a_i)$ and in particular denote $L_0 := F$. Since any a_i is separable over F , the minimal polynomial of a_i over F denoted by $m_{i,F}$ has no multiple roots. Also denote by $m_{i,L_{i-1}}$ the minimal polynomial of a_i over L_i . We get that $m_{i,L_{i-1}}$ divides $m_{i,F}$ so it must also have no multiple roots. Thus each a_i is separable over L_{i-1} so

$$i(E/F) = i(E/L_{k-1}) \cdots i(L_1/F) = [E : L_{k-1}] \cdots [L_1 : F] = [E : F],$$

where the second transition follows from part (3) of Theorem 4.9.

- (2 $\rightarrow$ 3) Assume, by way of contradiction, that there exists $\beta \in E$ which is not separable over F . Then, from Theorem 4.9 we get

$$i(E/F) = \underbrace{i(E/F(\beta))}_{\leq [E:F(\beta)]} \cdot \underbrace{i(F(\beta)/F)}_{< [F(\beta):F]} < [E : F(\beta)] \cdot [F(\beta) : F] = [E : F]$$

which is a contradiction to (2) which completes the proof.

- (3 $\rightarrow$ 1) Immediate. □

Corollary 4.12. *The splitting field of a separable polynomial is a separable extension.*

Proof. Let E be a splitting field of a separable polynomial $f \in F[x]$ and let a be a root of f . Then the minimal polynomial of a over F is separable, since it divides f which is separable. The result follows since $E = F(a_1, \dots, a_k)$ where $a_1, \dots, a_k$ are the roots of f in E . □

Corollary 4.13. *If E/L and L/F are finite extensions, then E/F is separable if and only if E/L and L/F are separable.*

Proof. Suppose that E/F is separable. If $a \in E$ is separable over F , then it is clearly separable over L . This implies that E/L and L/F are separable.

Suppose next that E/L and L/F are separable. This implies that

$$[E : F] = [E : L] \cdot [L : F] = i(E/L) \cdot i(L/F) = i(E/F).$$

Thus from Theorem 4.11 we get that E/F is separable, which completes the proof. □

Exercise 4.3. Prove Theorem 4.13 for E/L and L/F not necessarily finite.

Corollary 4.14. *A field is perfect if and only if all of its algebraic extensions are separable.*

5 Normal and Galois extensions

5.1 Normal extensions

Definition 5.1 (Normal extension). An algebraic field extension E/F is said to be normal if every irreducible polynomial (over F) which has a root in E , splits over E .

Example 5.1. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal since the minimal polynomial of $\sqrt[3]{2}$ has complex roots.

Example 5.2. The extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is normal.

Lemma 5.1. Every finite field extension E/F satisfies $|\text{Aut}(E/F)| \leq i(E/F)$.

Proof. Let Ω be an algebraic closure of E . Then

$$\text{Aut}(E/F) \subseteq \{\varphi: E \rightarrow \Omega \mid \varphi|_F = \text{id}_F\}$$

which is of size $i(E/F)$. □

Remark 5.1. Geometrically, it is healthy to visualize any element in $\text{Aut}(E/F)$, as an F -embedding σ of E in an algebraically closed Ω , such that $\sigma(E) = E$. Visualizing is also going to help in the following important proposition.

Proposition 5.2. Let E/F be a finite field extension. The following conditions are equivalent:

- (1) E/F is normal.
- (2) $|\text{Aut}(E/F)| = i(E/F)$.
- (3) E is the splitting field of some polynomial $g \in F[x]$.

Proof.

- (1 $\rightarrow$ 3) Suppose that $E = F(\alpha_1, \dots, \alpha_k)$. Denote the minimal polynomial of α_i over F by f_i for all $1 \leq i \leq k$. Then f_i is irreducible over F and has a root in E and thus splits in E . This means that E is the splitting field of the polynomial $f_1 \cdot f_2 \cdots f_k$.
- (3 $\rightarrow$ 2) Let $\alpha_1, \dots, \alpha_k$ be the roots of g . In particular $E = F(\alpha_1, \dots, \alpha_k)$. Let Ω be an algebraic closure of E . It suffices to show that if $\rho: E \rightarrow \Omega$ is an embedding such that $\rho|_F = \text{id}_F$, then $\rho \in \text{Aut}(E/F)$. Since $\rho(g) = g$ we get that ρ is a permutation on the roots of g , and thus

$$\rho(E) = \rho(F(\alpha_1, \dots, \alpha_k)) = F(\rho(\alpha_1), \dots, \rho(\alpha_k)) \subseteq E.$$

Moreover,

$$[E : F] = [\rho(E) : \rho(F)] = [\rho(E) : F]$$

and since $\rho(E) \subseteq E$ we get that $\rho(E) = E$ and therefore $\rho \in (\text{Aut}(E/F))$.

- (2 $\rightarrow$ 1) Assume, by way of contradiction, that there exists $g \in F[x]$ which is irreducible over F , has a root α in E , and does not split over E . Let Ω be an algebraic closure of E . We know that

$$\text{Aut}(E/F) \subseteq \{\varphi: E \rightarrow \Omega \mid \varphi|_F = \text{id}_F\},$$

and so in order to get a contradiction it suffices to show that there exists $\varphi: E \rightarrow \Omega$ so that $\varphi|_F = \text{id}_F$ and $\varphi(E) \neq E$.

Let $\beta \in \Omega \setminus E$ be a root of g . From Theorem 3.4 we know that there exists an isomorphism $\psi: F(\alpha) \rightarrow F(\beta)$ so that $\psi|_F = \text{id}$ and $\psi(\alpha) = \beta$. We can extend ψ to an embedding φ of E in Ω (since $1 \leq i_{\psi, \Omega}(E/F(\alpha))$). Now, $\varphi|_F = \psi|_F = \text{id}_F$ but $\varphi(E) \ni \varphi(\alpha) = \psi(\alpha) = \beta$ which implies that $\varphi(E) \neq E$, and completes the proof.

□

Corollary 5.3. *Let E/F be a finite normal extension and let $F \subseteq L \subseteq E$ be an intermediate field. Then E/L is normal.*

Proof. There exists $g(x) \in F[x]$ so that E is the splitting field of g over F . We know that E is also the splitting field of f over L and thus E/L is normal. □

Corollary 5.4. *Let $F \subseteq E \subseteq L$ be field extensions such that E/F is a normal finite extension. Then for every $\sigma \in \text{Aut}(L/F)$, we have $\sigma(E) = E$.*

Proof. Assume, by way of contradiction, that there exists $\sigma \in \text{Aut}(L/F)$ so that $\sigma(E) \neq E$. Since $[E : F] = [\sigma(E) : F]$ it is not possible that $\sigma(E) \subseteq E$ so there exists $\alpha \in E$ so that $\sigma(\alpha) \notin E$. Let $m_\alpha(x) \in F[x]$ be the minimal polynomial of α over F . Since $m_\alpha(x)$ is irreducible and has a root $\alpha \in E$ and E/F is normal, we get that $m_\alpha(x)$ splits in E . Let $\alpha_1, \dots, \alpha_k \in E$ be the roots of $m_\alpha(x)$. Since $m_\alpha(x) \in F[x]$ and $\sigma \in \text{Aut}(L/F)$ we get that

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

so $\sigma(\alpha)$ is a root of $m_\alpha(x)$, but all roots of $m_\alpha(x)$ are in E so $\sigma(\alpha) \in E$. This contradiction completes the proof. □

Example 5.3. Let $E/F := \mathbb{Q}(i, \sqrt{2})/\mathbb{Q}$ be a finite field extension. It is normal with minimal polynomial $m(x) = (x^2 + 1)(x^2 - 2)$, and it is also separable as the splitting field of a separable polynomial. From separability we get $i(E/F) = [E : F] = 4$, and from normality we get $|\text{Aut}(E/F)| = i(E/F)$, and thus $|\text{Aut}(E/F)| = 4$. By Theorem 5.4, we must have $\sigma(i) \in \{-i, i\}$ and $\sigma(\sqrt{2}) \in \{\sqrt{2}, -\sqrt{2}\}$ for all $\sigma \in \text{Aut}(E/F)$, and therefore these automorphisms form exactly the group $\text{Aut}(E/F)$, and it can easily be shown that $\text{Aut}(E/F) = C_2 \times C_2$.

Lemma 5.5. *Every quadratic field extension is normal.*

Proof. Let E/F be a quadratic field extension. That is, $[E : F] = 2$. Let $m(x)$ be an irreducible polynomial with a root $\alpha \in E \setminus F$. Since E/F is quadratic, we have $\deg(m) = 2$ so

$$m(x) = ax^2 + bx + c \in F[x].$$

Now, denote the other root of $m(x)$ by α' . We know that $\alpha + \alpha' = -b/a$ so $\alpha' = -\alpha - b/a \in E$. This means that $m(x)$ splits over E so E/F is normal. □

Question. Let E/L and L/F be normal extensions. Is E/F necessarily normal?

Answer. No! Let

$$F := \mathbb{Q} \quad \text{and} \quad L := \mathbb{Q}(\sqrt{2}) \quad \text{and} \quad E := \mathbb{Q}(\sqrt[4]{2}).$$

The extensions E/L and L/F are normal since by Theorem 5.5 any quadratic field extension is normal. However E/F is not normal since the minimal polynomial of $\sqrt[4]{2}$ over F is $x^4 - 2$ (irreducible from Eisenstein's criterion), and it has a root in E , but not all of its roots are in E since some of them are complex. Therefore E/F is not normal.

Remark 5.2. Note that when we consider $E/F := \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$, it becomes very easy to understand it is not a normal extension when we visualize things. The minimal polynomial of $\sqrt[4]{2}$ is $x^4 - 2$, and it has complex roots. We can see that we can embed $\mathbb{Q}(\sqrt[4]{2})$ in $\mathbb{C}$ by sending $\sqrt[4]{2}$ to one of the complex roots, so clearly $|\text{Aut}(E/F)| < i(E/F)$, so the extension is not normal.

5.2 Galois extensions

Definition 5.2 (Galois extension). A field extension E/F is said to be a Galois extension if it is separable and normal.

Remark 5.3. If E/F is a Galois extension then the automorphism group $\text{Aut}(E/F)$ is called the Galois group of E/F and we denote it by $\text{Gal}(E/F)$.

Remark 5.4. Note that a Galois extension is also implicitly required to be algebraic, since we require it to be normal.

Remark 5.5. Note that if $F \subseteq L \subseteq E$ are fields and E/F is a Galois extension, then by Theorem 4.13 and Theorem 5.3 we get that E/L is a Galois extension.

Proposition 5.6. Let E/F be a finite field extension. Then the following conditions are equivalent:

- (1) E/F is a Galois extension.
- (2) $|\text{Aut}(E/F)| = i(E/F) = [E : F]$.
- (3) E is the splitting field of a separable polynomial $g \in F[x]$.

Proof.

(1 $\leftrightarrow$ 2) We have seen in Theorem 4.11 and Theorem 5.2 that

$$1 \leq |\text{Aut}(E/F)| \leq i(E/F) \leq [E : F]$$

and that the second inequality is an equality if and only if E/F is normal, and the third inequality is an equality if and only if E/F is separable. This is the inequality at the center of all things.

- (3 $\rightarrow$ 1) Let $g \in F[x]$ be a separable polynomial so that E is the splitting field of g over F . Every splitting field is immediately a normal extension. If a is a root of g then the minimal polynomial of a over F divides g , and thus that minimal polynomial is separable and so a is a separable element. Since the extension E/F is generated by roots of g , and an extension generated by separable elements is separable, we conclude that E/F is normal and separable, thus it is Galois.
- (1 $\rightarrow$ 3) Assume that $E = F(\alpha_1, \dots, \alpha_k)$ and for all $1 \leq i \leq k$ denote m_i the minimal polynomial of α_i over F . Since E/F is separable we get that m_i is separable. Since E/F is normal and α_i is a root of the irreducible polynomial m_i then E contains all roots of m_i for all $1 \leq i \leq k$. By a reordering of the elements we can assume that there exists $1 \leq j \leq k$ so that $m_1, \dots, m_j$ are distinct and $\{m_1, \dots, m_k\} = \{m_1, \dots, m_j\}$. If $1 \leq r \neq s \leq j$ then m_r and m_s are distinct irreducible polynomials over F and thus they don't have a common root in E . We obtain that E is the splitting field of the separable polynomial $m_1 m_2 \cdots m_j$.

□

6 The Fundamental Theorem of Galois Theory

6.1 A different criterion for a finite Galois extension

Theorem 6.1 (Artin). *Let E be a field and let $G \leq \text{Aut}(E)$ be a finite group. Denote the fixed field of G by $F := \{x \in E \mid (\forall \sigma \in G)\sigma(x) = x\}$. Then $[E : F] = |G|$.*

Proof. Since by definition of F we have that $G \leq \text{Aut}(E/F)$ we can immediately obtain that $|G| \leq [E : F]$. It is left to show that $|G| \geq [E : F]$. Suppose that $G = \{\sigma_1, \dots, \sigma_m\}$ (so that $|G| = m$). We need to show that if $\alpha_1, \dots, \alpha_{m+1} \in E$ then there exist $x_1, \dots, x_{m+1} \in F$ not all 0 so that $\alpha_1 x_1 + \dots + \alpha_{m+1} x_{m+1} = 0$. (this is simply saying that $\alpha_1, \dots, \alpha_{m+1}$ are linearly dependent over F). Consider the system of equations:

$$\begin{cases} \sigma_1(\alpha_1)x_1 + \dots + \sigma_1(\alpha_{m+1})x_{m+1} = 0 \\ \sigma_2(\alpha_1)x_1 + \dots + \sigma_2(\alpha_{m+1})x_{m+1} = 0 \\ \vdots \\ \sigma_m(\alpha_1)x_1 + \dots + \sigma_m(\alpha_{m+1})x_{m+1} = 0 \end{cases}$$

This system of equations has a nontrivial solutions since there are more variables ($x_1, \dots, x_{m+1}$) than equations (m equations). Choose a nontrivial solution with the smallest number of nonzero coordinates, and denote it $(y_1, \dots, y_k, 0, \dots, 0)$ (without loss of generality we assume the nonzero entries are the first entries). We can multiply this solution by a scalar so that $y_1 = 1$ so we may assume $y_1 = 1$. If $y_2, \dots, y_k \in F$ then the proof is complete. We will show that necessarily $y_2, \dots, y_k \in F$ which will complete the proof. Assume, by way of contradiction, that there exists $2 \leq j \leq k$ so that $y_j \in E \setminus F$. Without loss of generality $y_2 \in E \setminus F$. By definition of F there exists $\sigma \in G$ so that $\sigma(y_2) \neq y_2$. We notice that $(\sigma(y_1), \sigma(y_2), \dots, \sigma(y_k), 0, \dots, 0)$ is also a solution to the system of equations, since for any $1 \leq i \leq m$ there exists $1 \leq j \leq m$ so that $\sigma^{-1}\sigma_i = \sigma_j$ so

$$\begin{aligned} \sigma_i(\alpha_1)\sigma(y_1) + \dots + \sigma_i(\alpha_{m+1})\sigma(y_{m+1}) &= \sigma\left(\sigma^{-1}(\sigma_i(\alpha_1)\sigma(y_1)) + \dots + \sigma^{-1}(\sigma_i(\alpha_{m+1})\sigma(y_{m+1}))\right) \\ &= \sigma\left(\sigma^{-1}(\sigma_i(\alpha_1))y_1 + \dots + \sigma^{-1}(\sigma_i(\alpha_{m+1}))y_{m+1}\right) \\ &= \sigma(\sigma_j(\alpha_1)y_1 + \dots + \sigma_j(\alpha_{m+1})y_{m+1}) \\ &= \sigma(0) = 0. \end{aligned}$$

Thus $(y_1 - \sigma(y_1), y_2 - \sigma(y_2), \dots, y_k - \sigma(y_k), 0, \dots, 0)$ is also a solution but $y_1 - \sigma(y_1) = 1 - 1 = 0$ and thus this solution has less than k nonzero entries in contradiction to the minimality of k . This contradiction implies that $y_2, \dots, y_k \in F$. This completes the proof. $\square$

Remark 6.1. If one pictures the lattices of subgroups and subfields as in Example 3.19 or Example 3.20, then if H is a subgroup corresponding to a subfield M , then Artin's theorem shows that $|H|$ is equal to $[E : M]$, and this is true for all corresponding subgroups and subfields.

Corollary 6.2 (Artin's criterion). *Let E/F be a finite field extension. Then E/F is a Galois extension if and only if F is the fixed field of $\text{Aut}(E/F)$.*

Proof. Denote the fixed field of $\text{Aut}(E/F)$ by $F \subseteq L \subseteq E$. Then

$$L = F \iff [E : L] = [E : F] \stackrel{(1)}{\iff} |\text{Aut}(E/F)| = [E : F] \stackrel{(2)}{\iff} E/F \text{ is Galois,}$$

where (1) follows from Theorem 6.1 and (2) follows from Theorem 5.6. $\square$

6.2 The fundamental theorem of Galois theory

Remark 6.2. Let E/F be a field extension and denote $G = \text{Aut}(E/F)$. Recall we have the Galois correspondence

$$\{M \mid F \subseteq M \subseteq E \text{ is a subfield}\} \xrightleftharpoons[\mathcal{F}]{\mathcal{G}} \{H \mid H \leq G\}.$$

with the functions

$$\begin{aligned} \mathcal{G}(M) &:= \text{Aut}(E/M) \leq \text{Aut}(E/F) \\ \mathcal{F}(H) &:= \{x \in E \mid (\forall \sigma \in H) \sigma(x) = x\}. \end{aligned}$$

Theorem 6.3 (Fundamental theorem of Galois theory, part A). *Let E/F be a finite Galois extension. Denote $G = \text{Gal}(E/F)$. Then the maps $\mathcal{F}$ and $\mathcal{G}$ are bijections, inverse of each other, and reverse the containment order. That is,*

- (1) *For every intermediate field $F \subseteq M \subseteq E$, we have that $\mathcal{F}(\mathcal{G}(M)) = M$.*
- (2) *For every subgroup $H \leq G$, we have that $\mathcal{G}(\mathcal{F}(H)) = H$.*
- (3) *If $M_1 \subseteq M_2$ are intermediate fields, then $\mathcal{G}(M_2) \subseteq \mathcal{G}(M_1)$.*
- (4) *If $H_1 \leq H_2$ are subgroups of G , then $\mathcal{F}(H_2) \subseteq \mathcal{F}(H_1)$.*
- (5) *If $M = \mathcal{F}(H)$, then $[E : M] = |H|$.*

Proof. We have already seen (3) + (4) earlier, and (5) follows from Artin's theorem. We will proceed to show (1) and (2).

- (1) Let $F \subseteq M \subseteq E$ be an intermediate field. We know that $M \subseteq \mathcal{F}(\mathcal{G}(M))$ so it suffices to show that $[E : M] = [E : \mathcal{F}(\mathcal{G}(M))]$. Indeed,

$$[E : M] \stackrel{(1)}{=} |\text{Gal}(E/M)| \stackrel{(2)}{=} [E : \mathcal{F}(\mathcal{G}(M))],$$

where (1) holds since E/M is a finite Galois extension, and (2) holds since we know that $\mathcal{G}(M)$ is finite which means we can use Artin's theorem.

- (2) Let $H \leq G$. Since E/F is a finite extension, its Galois group $G = \text{Gal}(E/F)$ is a finite group, and thus H is also finite. We know that $H \subseteq \mathcal{G}(\mathcal{F}(H))$ and thus it suffices to show that $|H| = |\mathcal{G}(\mathcal{F}(H))|$. Indeed,

$$|H| \stackrel{(1)}{=} [E : \mathcal{F}(H)] \stackrel{(2)}{=} |\text{Gal}(E/\mathcal{F}(H))| = |\mathcal{G}(\mathcal{F}(H))|,$$

where (1) follow from Artin's theorem (which is applicable since H is finite), and (2) holds since $E/\mathcal{F}(H)$ is a finite Galois extension. □

Corollary 6.4. *Let E/F be a finite Galois extension and let $H \leq G = \text{Gal}(E/F)$. Denote $M = \mathcal{F}(H)$. Then the degree of the extension M/F is equal to the index of H in G as groups. That is,*

$$[M : F] = [G : H].$$

Proof. We have

$$[M : F] = \frac{[E : F]}{[E : M]} = \frac{|G|}{|H|} = [G : H]$$

where the middle equality follows from Artin's theorem, which we can apply since L/M and L/K are finite Galois extensions. □

Lemma 6.5. *Let E/F be a field extension and let $G = \text{Aut}(E/F)$. For all $H \leq G$ and all $\sigma \in G$ we have $\mathcal{F}(\sigma H \sigma^{-1}) = \sigma(\mathcal{F}(H))$.*

Proof. Let $x \in L$. Then

$$\begin{aligned}
 x &\in \mathcal{F}(\sigma H \sigma^{-1}) \\
 &\Updownarrow \\
 \forall h \in H \quad \sigma h \sigma^{-1}(x) &= x \\
 &\Updownarrow \\
 \forall h \in H \quad h \sigma^{-1}(x) &= \sigma^{-1}(x) \\
 &\Updownarrow \\
 \sigma^{-1}(x) &\in \mathcal{F}(H) \\
 &\Updownarrow \\
 x &\in \sigma(\mathcal{F}(H)).
 \end{aligned}$$

□

Lemma 6.6. *Let E/F be a finite Galois extension with Galois group $G = \text{Gal}(E/F)$. Let $F \subseteq M \subseteq E$ be an intermediate field and denote $H = \mathcal{G}(M)$. Then M/F is normal if and only if for all $\sigma \in G$ we have $\sigma(M) = M$.*

Proof. We have seen in Theorem 5.4 that if E/F is a finite field extension (not necessarily Galois) and $F \subseteq M \subseteq E$ such that M/F is a normal extension then for all $\sigma \in \text{Aut}(E/F)$ we have $\sigma(M) = M$.

We now show the opposite direction. Assume, by way of contradiction, that M/F is not a normal extension and let Ω be an algebraic closure of E . We have seen in Theorem 5.2 that when M/F is not normal there exists an embedding $\rho: M \rightarrow \Omega$ so that $\rho|_F = \text{id}$ and $\rho(M) \neq M$. We also know that we can extend ρ to an embedding $\bar{\rho}: E \rightarrow \Omega$. Since E/F is a finite Galois extension, it is a finite normal extension, so we can recall Theorem 5.4 and similarly obtain that $\bar{\rho}(E) = E$ and thus $\bar{\rho} \in \text{Gal}(E/F)$. However, now for $\sigma := \bar{\rho} \in \text{Gal}(E/F)$ we have that $\sigma(M) = \rho(M) \neq M$, in contradiction to what was given. This contradiction implies that M/F is a normal extension which completes the proof. □

Theorem 6.7 (Fundamental theorem of Galois, part B). *Let E/F be a finite Galois extension with Galois group $G = \text{Gal}(E/F)$. Let $F \subseteq M \subseteq E$ be an intermediate field and let $H = \mathcal{G}(M)$. Then M/F is a Galois extension if and only if H is normal in G . Moreover, if $H \triangleleft G$ then the restriction homomorphism $\pi: \text{Gal}(E/F) \rightarrow \text{Gal}(M/F)$ which maps $\sigma \mapsto \sigma|_M$ is surjective, $\ker(\pi) = H$, and there exists an isomorphism which gives $\text{Gal}(M/F) \cong G/H$.*

Remark 6.3. Note that in Theorem 6.7 we have that M/F is a Galois extension if and only if H is normal in G . However since we know that E/F is separable, it follows that M/F is separable, so this statement is equivalent to saying that M/F is a normal extension if and only if H is normal in G .

Proof of Theorem 6.7.

$$\begin{aligned}
& H \triangleleft G \\
& \Updownarrow \\
& \forall \sigma \in G \quad \sigma H \sigma^{-1} = H \\
& \Updownarrow \text{ by Theorem 6.3} \\
& \forall \sigma \in G \quad \mathcal{F}(\sigma H \sigma^{-1}) = \mathcal{F}(H) \\
& \Updownarrow \text{ by Theorem 6.5} \\
& \forall \sigma \in G \quad \sigma(\mathcal{F}(H)) = \mathcal{F}(H) \\
& \Updownarrow \\
& \forall \sigma \in G \quad \sigma(M) = M \\
& \Updownarrow \text{ by Theorem 6.6} \\
& M/F \text{ is a normal extension}
\end{aligned}$$

Assume that M/F is normal. Then clearly π is a homomorphism and $\ker(\pi) = H$. We have that

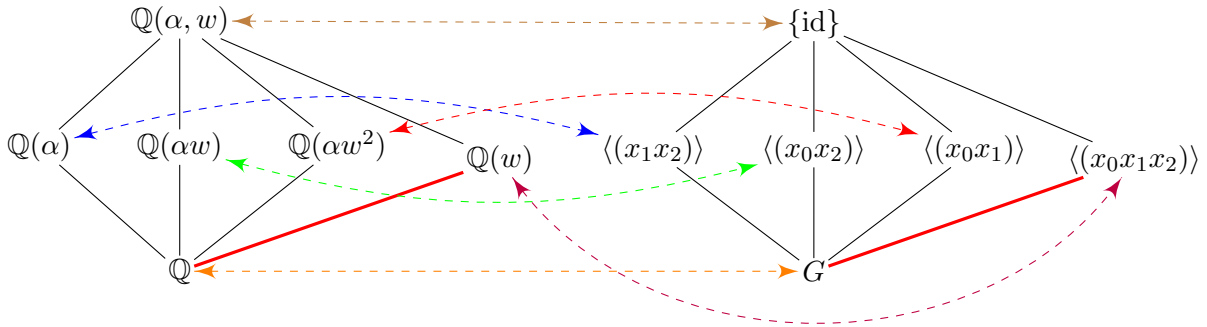
$$|\operatorname{im}(\pi)| = |G/H| = [G : H] \stackrel{(*)}{=} [M : F] = |\operatorname{Gal}(M/F)|.$$

where $(*)$ follows from Theorem 6.3. This implies that π is surjective. From the first isomorphism theorem for groups we get $G/H \cong \operatorname{Gal}(M/F)$ which completes the proof. $\square$

Example 6.1. Let $E/\mathbb{Q}$ be the splitting field of $x^3 - 2$ and let $G = \operatorname{Gal}(E/\mathbb{Q})$. Denote $w = e^{2\pi i/3}$ and $\alpha = \sqrt[3]{2}$ and

$$x_0 = \alpha \quad x_1 = \alpha w \quad x_2 = \alpha w^2.$$

We get the lattices



where the thick red lines mean that $N := \langle (x_0 x_1 x_2) \rangle \triangleleft G$ and that $\mathbb{Q}(w)/\mathbb{Q}$ is correspondingly a normal field extension. We can see that $G \cong S_3 \cong \operatorname{Sym}(\{x_0, x_1, x_2\})$, which implies that $N = A_3$. The notation $(x_1 x_2)$ etc. is the notation for permutations. For example $\langle (x_0 x_1) \rangle$ is all field automorphisms $\varphi \in \operatorname{Aut}(E/\mathbb{Q})$ such that exists $\sigma \in \langle (x_0 x_1) \rangle$ so that $\varphi(x_i) = \sigma(x_i)$.

Corollary 6.8. Denote $S_0 = \{(0, 0), (1, 0)\}$ and let p be an odd prime. Then we can construct from S_0 a perfect p -gon if and only if p is a Fermat prime.

Proof. We have seen in Example 2.8 that when p is an odd prime that the condition that p is a Fermat prime is necessary for a p -gon to be constructible. We will show that this condition is also sufficient. Let p be a Fermat prime, it suffices to show that $\cos(2\pi/p)$ is constructible.

Let $\eta \in \mathbb{C}$ be a primitive root of unity of order p . Thus, we have the identity $\eta + \eta^{-1} = 2 \cos(2\pi/p)$. We know that $\mathbb{Q}(\eta)/\mathbb{Q}$ is a Galois extension with a cyclic Galois group of order $p-1$. Denote $G_0 := \text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$. Since p is a Fermat prime there exists a tower of subgroups

$$1 = G_m \leq \cdots \leq G_1 \leq G_0,$$

so that for all $1 \leq i \leq m-1$ we have $G_{i-1}/G_i = \mathbb{Z}/2\mathbb{Z}$, and in particular $[G_{i-1} : G_i] = 2$. For all $1 \leq i \leq m$ denote $\mathcal{F}(G_i) := F_i$. Then from the fundamental theorem of Galois we get that

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m = \mathbb{Q}(\eta),$$

and from Artin's theorem we get that $[F_{i+1} : F_i] = 2$ for all $0 \leq i \leq m-1$. Also, since any cyclic group has at most one cyclic group of order 2, we can conclude that F_{m-1} is the unique subfield of $\mathbb{Q}(\eta)$ so that $[\mathbb{Q}(\eta) : F_{m-1}] = 2$. Since $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta + \eta^{-1})] = 2$ it follows that $F_{m-1} = \mathbb{Q}(\eta + \eta^{-1})$. Recall that $\mathbb{Q}(\eta + \eta^{-1}) = \mathbb{Q}(\cos(2\pi)/p)$, so we can write $F_{m-1} = \mathbb{Q}(\cos(2\pi)/p)$. Finally, we conclude that there is a tower of fields

$$F_0 \subseteq F_1 \subseteq \cdots \subseteq F_{m-2} \subseteq F_{m-1} = \mathbb{Q}(\cos(2\pi)/p)$$

and $[F_{i+1} : F_i] = 2$ for all $0 \leq i \leq m-2$. According to Theorem 2.4 we get that $\cos(2\pi/p)$ is constructible, which completes the proof. $\square$

Remark 6.4. In Theorem 6.8 we claimed that $[F_{i+1} : F_i] = 2$ follows from Artin's theorem without explaining too much. We will now show a more general claim.

Proposition 6.9. *Let E be a field and let $1 \leq H \leq G \leq \text{Aut}(E)$ be finite groups. Denote the fixed field of H and G by E^H and E^G respectively. Then $[E^H : E^G] = \frac{|G|}{|H|} = [H : G]$.*

Proof. By Artin's theorem we have $[E : E^H] = |H|$ and $[E : E^G] = |G|$. Now we simply have

$$[E^H : E^G] = \frac{[E : E^G]}{[E : E^H]} = \frac{|G|}{|H|} = [H : G],$$

which completes the proof. $\square$

7 Corollaries from Galois theory

7.1 Ruler and compass constructions

Remark 7.1. Let $S_0 = \{(0,0), (1,0)\}$. We have seen that a p -gon (for an odd prime number p) is constructible if and only if p is a Fermat prime. In this section we will generalize this, and find a necessary and sufficient condition for an n -gon to be constructible.

Definition 7.1 (Cyclotomic polynomial). Let $\eta \in \mathbb{C}$ be a primitive n th root of unity for some natural number $n \geq 1$, and let $A := \{\eta^d \mid d \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ be the set of all primitive n th roots of unity. Then the n th cyclotomic polynomial is given by:

$$\Phi_n(x) := \prod_{\alpha \in A} (x - \alpha) = \prod_{d \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \eta^d).$$

Remark 7.2. Our current goal is to show that $\Phi_n(x) \in \mathbb{Z}[x]$.

Lemma 7.1. Let $f, g \in \mathbb{Z}[x]$ be polynomials and suppose that g is monic, such that $g \mid f$ in $\mathbb{Q}[x]$. Then $f/g \in \mathbb{Z}[x]$.

Proof. We show this by induction on $k = \deg(f) - \deg(g)$. If $k = 0$ then $f = \alpha g$ for $\alpha \in \mathbb{Q}$. Since g is monic and $f \in \mathbb{Z}[x]$ it follows that $\alpha \in \mathbb{Z}$ and thus $f/g = \alpha \in \mathbb{Z}[x]$.

Suppose that $0 < k$ and that we have shown the lemma for values less than k . Write

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

so that $a_n \neq 0$. Define $h(x) := f(x) - a_n x^k g(x) \in \mathbb{Z}[x]$. We have $\deg(h) < n$ and $g \mid h$ in $\mathbb{Q}[x]$. Therefore we can use the induction hypothesis to obtain

$$\frac{f}{g} = \frac{a_n x^k g + h}{g} = a_n x^k + \frac{h}{g} \in \mathbb{Z}[x].$$

□

Lemma 7.2. For all $n \geq 1$ we have $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof. We will prove this by induction on n . We have that $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$. Assume that we have shown the lemma for values less than $n > 0$. We notice that

$$x^n - 1 = \prod_{\substack{\alpha \in \mathbb{C} \\ \alpha^n = 1}} (x - \alpha) = \prod_{d \mid n} \Phi_d(x) = \left(\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x) \right) \cdot \Phi_n(x).$$

By the induction hypothesis $\prod_{\substack{d \mid n \\ d < n}} \Phi_d(x)$ is a monic polynomial in $\mathbb{Z}[x]$, and then by Theorem 7.1 we get that $\Phi_n(x) \in \mathbb{Z}[x]$. □

Exercise 7.1. Let $f(x), g(x) \in \mathbb{Q}[x]$ be monic polynomials so that $f \cdot g \in \mathbb{Z}[x]$. Then $f, g \in \mathbb{Z}[x]$.

Theorem 7.3. The cyclotomic polynomials $\{\Phi_n(x)\}_{n=1}^\infty$ are irreducible over $\mathbb{Q}$.

Proof. Because $\Phi_n(x)$ is monic, Gauss's lemma shows that $\Phi_n(x)$ is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$. Denote some primitive n th root of unity by η . Let $g(x)$ be the minimal polynomial of η over $\mathbb{Q}$. We want to show that $g = \Phi_n$. We know that $g \mid \Phi_n$ over $\mathbb{Q}$ and that Φ_n is separable (because $x^n - 1$ is separable). Thus since g and Φ_n are monic, it suffices to show that every root of Φ_n is a root of g . In other words, we need to show that for each $1 \leq d \leq n$ that is coprime to n , that η^d is a root of g . Since d is a product of primes (not necessarily different), it suffices to show that for any prime p coprime to n , that η^p is a

root of g while only using the fact η is a root and a primitive n th root of unity. Then we could obtain that since η^{p_1} is an n th root of unity, and a root of g that $(\eta^{p_1})^{p_2}$ is also a root of g , and similarly that $n^d = (\eta^{p_1 \cdots p_k}) = ((\eta^{p_1})^{p_2})^{p_3}$ is a root of g .

Since $g \mid \Phi_n$ there exists $h(x) \in \mathbb{Q}[x]$ such that

$$\Phi_n(x) = g(x)h(x),$$

so from Exercise 7.1 we can conclude that $g, h \in \mathbb{Z}[x]$ are monic. Let p be a prime that is coprime to n . We will show that η^p is a root of $g(x)$. Since η^p is a root of $\Phi_n(x)$, it must be either a root of $h(x)$ or of $g(x)$. Assume, by way of contradiction, that η^p is a root of $h(x)$. The assumption implies that η is a root of $h(x^p)$. Thus by definition of g we get that $g(x) \mid h(x^p)$ over $\mathbb{Q}$, so by applying Theorem 7.1, we get that there exists $k(x) \in \mathbb{Z}[x]$ so that

$$h(x^p) = g(x)k(x).$$

If we consider this equation modulu p (by treating these functions as functions $\bar{h}, \bar{g}, \bar{k} \in F_p[x]$), we would get the following equation:

$$(\bar{h}(x))^p = \bar{h}(x^p) = \bar{g}(x)\bar{k}(x).$$

Since $F_p[x]$ is a principal ideal domain and in particular a unit factorization domain, there exists a common irreducible factor of $\bar{h}(x)$ and $\bar{g}(x)$ which we will denote by $\bar{l}(x)$. We get that

$$\bar{l}(x)^2 \mid \bar{h}(x)\bar{g}(x) = \bar{\Phi}_n(x).$$

This implies that $\bar{\Phi}_n(x)$ is nonseparable. However, $\bar{\Phi}_n(x) \mid x^n - 1 \in F_p[x]$ and thus $x^n - 1 \in F_p[x]$ is nonseparable. Since n and p are coprime we get that

$$\gcd(x^n - 1, (x^n - 1)') = \gcd(x^n - 1, nx^{n-1}) = 1,$$

which by Theorem 4.3 means that $x^n - 1 \in F_p[x]$ is separable so this is a contradiction to $x^n - 1$ being nonseparable. This contradiction completes the proof. $\square$

Corollary 7.4. *Let $n \geq 2$ and let $\eta \in \mathbb{C}$ be a primitive n th root. Then $\mathbb{Q}(\eta)/\mathbb{Q}$ is a Galois extension of degree $\varphi(n)$ where φ is Euler's function, and we have $\text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. The extension $\mathbb{Q}(\eta)$ is the splitting field of the separable cyclotomic polynomial $\Phi_n(x)$ and thus $\mathbb{Q}(\eta)/\mathbb{Q}$ is a Galois extension. Theorem 7.3 shows that $\Phi_n(x)$ is irreducible so

$$|\text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})| = [\mathbb{Q}(\eta) : \mathbb{Q}] = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Define the map $\Phi: \text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}) \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$ by $\Phi(\sigma) = [a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ where a is the exponent of η in $\sigma(\eta) = \eta^a$. This is a well defined group homomorphism, and since $|\text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})| = |(\mathbb{Z}/n\mathbb{Z})^\times|$, it suffices to show that it is injective. Indeed, it is injective since if $\Phi(\sigma) = \Phi(\tau)$ then $\sigma(\eta) = \tau(\eta)$, but since $\sigma, \tau \in \text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$, they are determined by their value at η , so $\sigma = \tau$. This shows that Φ is an automorphism and completes the proof. $\square$

Remark 7.3 (Group theory reminder). Let p be prime and let G be a finite group of order $1 < p^n$. Then $Z(G) \neq \{\text{id}\}$ and in particular there exists a sequence of normal subgroups

$$\{\text{id}\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_m = G$$

so that $[G_i : G_{i-1}] = p$ for all $1 \leq i \leq m$. This is a particular case of the Jordan–Hölder theorem.

Theorem 7.5 (Gauss–Wantzel). *Let $S = \{(0,0), (1,0)\}$. Then we can construct a perfect n -gon if and only if $n = 2^m \cdot p_1 \cdots p_k$ for $0 \leq m$ and $p_1, \dots, p_k$ are distinct Fermat primes.*

Proof. Denote $\eta := e^{2\pi i/n}$ so that $2 \cos(2\pi/n) = \eta + \eta^{-1}$. Recall an n -gon is constructible if and only if $\cos(2\pi/n)$ is constructible. We know that $\mathbb{Q}(\eta)/\mathbb{Q}$ is an abelian Galois extension (its Galois group is abelian), so every subgroup H of $\text{Gal}(\mathbb{Q}(\eta)/\mathbb{Q})$ is normal, so by the fundamental theorem of Galois the fixed field of H is a normal extension of $\mathbb{Q}$. In particular $\mathbb{Q}(\cos(2\pi/n))\mathbb{Q}$ is normal (and it is separable) so it is a Galois extension. Before continuing we will prove a short lemma.

Lemma 7.6. *Under the notations of the theorem so far, $\cos(2\pi/n)$ is constructible if and only if $[\mathbb{Q}(\eta) : \mathbb{Q}]$ is a power of 2.*

Proof. We will start by proving that $\cos(2\pi/n)$ is constructible if and only if $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ is a power of 2. One direction follows from Theorem 2.5, so we will only show that if $\cos(2\pi/n)$ is constructible then $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ is a power of 2.

Denote $G := \text{Gal}(\mathbb{Q}(\cos(2\pi/n))/\mathbb{Q})$ and suppose that $|G| = 2^m$. By Remark 7.3 there exists an increasing sequence of normal subgroups

$$\{\text{id}\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_m = G,$$

so that $[G_i : G_{i-1}] = 2$ for all $1 \leq i \leq m$. Therefore, by the fundamental theorem

$$\mathbb{Q} = \mathcal{F}(G_m) \subseteq \mathcal{F}(G_{m-1}) \subseteq \cdots \subseteq \mathcal{F}(G_0) = \mathbb{Q}(\cos(2\pi/n))$$

is a tower of fields so that $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq m$. Then by applying Theorem 2.4 we get that $\cos(2\pi/n)$ is constructible.

Now since $[\mathbb{Q}(\cos(2\pi/n)) : \mathbb{Q}]$ is a power of 2 if and only if $[\mathbb{Q}(\eta) : \mathbb{Q}]$ is a power of 2 (because $[\mathbb{Q}(\eta) : \mathbb{Q}(\cos(2\pi/n))] = [\mathbb{Q}(\eta) : \mathbb{Q}(\eta + \eta^{-1})] = 2$), we conclude that $\cos(2\pi/n)$ is constructible if and only if $[\mathbb{Q}(\eta) : \mathbb{Q}] = \varphi(n)$ is a power of 2, which completes the lemma. $\square$

Factorize n into its prime factors $n = 2^k \cdot p_1^{s_1} \cdots p_r^{s_r}$, and note that since φ is multiplicative we get

$$\varphi(n) = \varphi(2^k) \cdot \varphi(p_1^{s_1}) \cdots \varphi(p_r^{s_r}).$$

We know that $\varphi(2^k) = 2^{\max\{k-1, 0\}}$ so it is always a power of 2. We also know that $\varphi(p_i^{s_i}) = (p_i - 1)p_i^{s_i-1}$. Therefore $\varphi(n)$ is a power of two if and only if $(p_i - 1)p_i^{s_i-1}$ is a power of two for all $1 \leq i \leq r$, and this happens if and only if $s_i = 1$ and p_i is a Fermat prime for all $1 \leq i \leq r$. This completes the proof. $\square$

7.2 Simple extensions and the primitive element theorem

Theorem 7.7. *A finite field extension E/F is simple if and only if it has a finite amount of intermediate fields.*

Proof. Assume that E/F has a finite amount of intermediate fields. We will show that E/F is simple. If F is finite, then E is finite, and thus the multiplicative group of E is cyclic (see Theorem 1.18). If α is a generator of $E^\times$ then $E = F(\alpha)$. Therefore, we may assume that F is infinite. Since E/F is generated by a finite amount of elements over F it suffices to show that if $\alpha, \beta \in E$ then there exists $\gamma \in E$ so that $F(\alpha, \beta) = F(\gamma)$. For every $\delta \in F$ we know that $F(\alpha + \delta\beta)$ is an intermediate field of the extension. Since F is infinite, there exist distinct $\delta_1, \delta_2 \in F$ so that $L := F(\alpha + \delta_1\beta) = F(\alpha + \delta_2\beta)$. If we denote $\gamma_i := \alpha + \delta_i\beta$ for $i = 1, 2$ then by a simple arithmetic calculation we can obtain that

$$\beta = \frac{\gamma_2 - \gamma_1}{\delta_2 - \delta_1} \in L,$$

and thus clearly also $\alpha \in L$ and so $L = F(\gamma_1) = F(\alpha, \beta)$ which completes this part of the proof.

Assume next that $E = F(\alpha)$ is a simple extension. Let $g(x) \in F[x]$ be the minimal polynomial of α over F . We will show that there exists an injective map from the set of intermediate fields of E/F to the set of monic polynomials that divide $g(x)$, which is a finite set, which will complete the proof. Let $F \subseteq L \subseteq E$ be an intermediate field. Let $h \in L[X]$ be the minimal polynomial of α over L . Write it by

$$h(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_0.$$

Notice that since $E = L(\alpha)$ we have that $[E : L] = m$. Denote $M := F(b_{m-1}, \dots, b_0)$. Clearly $M \subseteq L$. However, $h(x) \in M[x]$ is irreducible and $E = M(\alpha)$. Therefore $[E : M] = m$. Thus we must have $M = L$. We conclude that every intermediate field $F \subseteq L \subseteq E$ is generated by the coefficients of a monic polynomial in $E[x]$ that divides $g(x)$. Thus the map that sends each intermediate field to its corresponding polynomial is injective which completes the proof. $\square$

Lemma 7.8. *Let E/F be a finite separable extension. Then there exists a field $E \subseteq M$ such that M/F is a finite Galois extension.*

Proof. Let $E = F(\alpha_1, \dots, \alpha_k)$ and let g_i be the minimal polynomial of α_i over F . Denote by M the splitting field of $g = h_1 h_2 \cdots h_l$ over F where $\{g_1, \dots, g_k\} = \{h_1, \dots, h_l\}$ for distinct h_i . Then M is a normal extension. We also have that M is separable since the roots of g are separable and M is finitely generated over F by the roots of g . $\square$

Corollary 7.9 (Primitive element theorem). *Every finite separable field extension is simple. In particular, every finite extension of a field of characteristic zero is simple.*

Proof. Let E/F be a finite separable extension. Let $E \subseteq M$ be so that M/F is a finite Galois extension (by Theorem 7.8). Then $\text{Gal}(M/F)$ is finite so it must have a finite amount of subgroups. From fundamental theorem of Galois theory, M/F has a finite amount of intermediate fields, which means that E/F has a finite amount of intermediate fields, so by Theorem 7.7 E/F is a simple extension. $\square$

Example 7.1. The simplest nonsimple algebraic extension is $K(x, y)/K(x^p, y^p)$ where K is an algebraically closed field of characteristic p . We notice that $[K(x, y) : K(x^p, y^p)] = p^2$ since a basis for $K(x, y)$ over $K(x^p, y^p)$ is given by the set

$$A := \left\{ x^i y^j \mid 0 \leq i, j \leq p-1 \right\}$$

and $|A| = p^2$. However, for each $\alpha \in K(x, y)$ we notice that $\alpha^p \in K(x^p, y^p)$. This implies that $[K(x^p, y^p)(\alpha) : K(x^p, y^p)] \leq p$, which means that it is not a simple extension. Then by the primitive element theorem we conclude that $K(x, y)/K(x^p, y^p)$ is nonsimple.

7.3 The fundamental theorem of algebra

Lemma 7.10. *The set of real number $\mathbb{R}$ does not have nontrivial extensions of an odd degree.*

Proof. Assume, by way of contradiction, that $E/\mathbb{R}$ is of an odd degree and let $\alpha \in E/\mathbb{R}$. Then

$$[\mathbb{R}(\alpha) : \mathbb{R}] = \deg(m_\alpha)$$

is odd. Therefore there exists an irreducible polynomial over $\mathbb{R}$ of an odd degree $p(x)$. Since $\deg(p)$ is odd it has a real root so it must be reducible. This contradiction completes the proof. $\square$

Lemma 7.11. *Let $f \in \mathbb{C}[x]$ be a polynomial of degree 2. Then f has a root in $\mathbb{C}$.*

Proof. Follows immediately from the quadratic formula and the fact every $\alpha \in \mathbb{C}$ has a root (otherwise the quadratic formula was not always defined). $\square$

Corollary 7.12. *The field of complex numbers $\mathbb{C}$ does not have extensions of degree 2*

Theorem 7.13 (First Sylow theorem, reminder). *Let G be a finite group, let p be a prime number, and let m be the maximal natural number so that $p^m \mid |G|$. Then G has a subgroup of order p^m .*

Theorem 7.14 (Fundamental theorem of algebra). *The field of complex numbers is algebraically closed.*

Proof. First we will show that every $f(x) \in \mathbb{R}[x]$ splits in $\mathbb{C}$. Let $f(x) \in \mathbb{R}[x]$ and let E be the splitting field of $(x^2 + 1)f(x)$ over $\mathbb{R}$. Since $i \in E$ the embedding $\mathbb{R} \hookrightarrow E$ extends to an embedding of $\mathbb{C}$ in E . We identify $\mathbb{C}$ as a subfield of E . The extension $E/\mathbb{R}$ is normal (since it is a splitting field) and it is separable since $\text{char}(\mathbb{R}) = 0$. Therefore $E/\mathbb{R}$ is a finite Galois extension. Denote $G := \text{Gal}(E/\mathbb{R})$. Then we have that $2 = [\mathbb{C} : \mathbb{R}] \mid [E : \mathbb{R}] = |G|$. Let P be a 2-Sylow subgroup of G and denote $M = \mathcal{F}(P)$. Since P is 2-Sylow we get that $[G : P] = [M : \mathbb{R}]$ is odd, but since by Theorem 7.10 $\mathbb{R}$ doesn't have nontrivial extensions of an odd degree, we get that $[G : P] = 1$ so $G = P$.

Recall that we want to show that $E = \mathbb{C}$ and from Galois correspondence it is equivalent to showing that $H := \mathcal{G}(\mathbb{C}) = \{\text{id}\}$. Assume, by way of contradiction, that $1 < |H|$. Since $H \leq P$ it is a 2-group (its order is a power of 2) which is nontrivial, so it has a subgroup $K \leq H$ of index 2. Now we get

$$2 = [H : K] = [\mathcal{F}(K) : \mathcal{F}(H)] = [\mathcal{F}(K) : \mathbb{C}],$$

which is a contradiction to Theorem 7.12. This completes the proof that every $f(x) \in \mathbb{R}[x]$ splits in $\mathbb{C}$.

Next we will show that any $f \in \mathbb{C}[x]$ splits in $\mathbb{C}$. Let $f(x) \in \mathbb{C}[x]$. Then $f \cdot \bar{f} \in \mathbb{R}[x]$. It follows from what we have shown that $f \cdot \bar{f}$ splits over $\mathbb{C}$, and in particular f splits over $\mathbb{C}$. This completes the proof. $\square$

8 Solving equations using radicals

8.1 Radical extensions and Dedekind's lemma

Definition 8.1 (Galois group of a polynomial). Let F be a field, and let $g(x) \in F[x]$ be a separable polynomial. Then the Galois group of g is defined to be $G_f := \text{Gal}(E_f/F)$, where E_f is the splitting field of g .

Remark 8.1. A finite Galois extension E/F is said to be abelian or cyclic if $\text{Gal}(E/F)$ is cyclic or abelian respectively.

Definition 8.2 (Radical extension). A finite field extension E/F is said to be a radical extension if there exist positive natural numbers $m_1, \dots, m_k$ and elements $a_1, \dots, a_k \in E$ so that $E = F(a_1, \dots, a_k)$ and for all $1 \leq i \leq k$ we have that $a_i^{m_i} \in F(a_1, \dots, a_{i-1})$.

Example 8.1. The extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is a radical extension.

Remark 8.2. It is possible for E/F to be a finite simple radical extension, so that there does not exist $a \in E$ so that $E = F(a)$ and $a^k \in F$ for some positive natural k . We will see this in the following example.

Example 8.2. Consider the extension $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})/\mathbb{Q}$. Since $\text{char}(\mathbb{Q}) = 0$ this extension is separable, and since it is finitely generated, by the primitive element theorem it must be simple. We can also verify easily that it is a radical extension. However, there does not exist an element $a \in \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$ so that $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) = \mathbb{Q}(a)$ and $a^k \in \mathbb{Q}$ for some positive natural k . That is because the Galois group of $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$ is isomorphic to $C_3 \times C_3$, and the Galois group of $\mathbb{Q}(a)$ would have to be isomorphic to C_9 . We will see this in the following theorem

Theorem 8.1. Let F be a field that contains a primitive n th root of unity and let $E = F(\alpha)$ be a simple extension such that $\alpha^n \in F$. Then E/F is a cyclic Galois extension of an order that divides n .

Proof. Let $\eta \in F$ be a primitive n th root of unity. Then

$$g(x) := \prod_{1 \leq i \leq n} (x - \eta^i \alpha) = x^n - \alpha^n \in F[x]$$

and E is the splitting field of g over F so E/F is a normal extension. Since g is separable we conclude that E/F is a Galois extension.

Now for all $\sigma \in \text{Gal}(E/F)$, we have that $\sigma(\alpha)$ is a root of $g(x)$, so there exists $1 \leq i \leq n$ so that $\sigma(\alpha) = \alpha \eta^i$. We get that there exists a map $\varphi: \text{Gal}(E/F) \rightarrow \langle \eta \rangle$ defined by $\varphi(\sigma) = \sigma(\alpha)/\alpha$. Since for any $\sigma, \tau \in \text{Gal}(E/F)$ so that $\varphi(\sigma) = \eta^i$ and $\varphi(\tau) = \eta^j$ we have that $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau) = \eta^{i+j}$, we get that φ is a homomorphism. Moreover, φ is injective since σ is determined by the image of α (recall that $\sigma \in \text{Gal}(E/F)$ and $E = F(\alpha)$). From the first isomorphism theorem we get that $\text{Gal}(E/F)$ is isomorphic to $\text{im}(\varphi)$ which is a subgroup of $\langle \eta \rangle$. Thus $\text{Gal}(E/F)$ is a cyclic group of an order that divides n . $\square$

Exercise 8.1. Using the notation from Theorem 8.1 show that if m is the minimal positive natural number so that $\alpha^m \in F$ then $[E:F] = m$.

Lemma 8.2 (Dedekind's lemma). Let F be a field, let G be a group, and let $\chi_1, \dots, \chi_k$ be distinct homomorphisms from G to $F^\times$. Then $\chi_1, \dots, \chi_k$ are linearly independent over F . That is, if $a_1, \dots, a_k \in F$ and for all $g \in G$ we have

$$a_1 \chi_1(g) + \dots + a_k \chi_k(g) = 0,$$

then $a_1 = \dots = a_k = 0$.

Proof. We prove this by induction over k . When $k = 1$ the lemma is obvious. Assume that $k \geq 2$ and that we have shown the proposition for all values $n < k$. Let $a_1, \dots, a_k \in F$ so that for all $g \in G$ we have

$$a_1\chi_1(g) + \dots + a_k\chi_k(g) = 0.$$

We need to show that $a_1 = \dots = a_k = 0$. By the induction hypothesis we may assume that all of the coefficients $a_1, \dots, a_k$ are nonzero so in particular $a_2 \neq 0$. Since $\chi_1 \neq \chi_2$ there exists $h \in G$ so that $\chi_1(h) \neq \chi_2(h)$. Thus for all $g \in G$ we have

$$0 = a_1\chi_1(hg) + \dots + a_k\chi_k(hg) = a_1\chi_1(h)\chi_1(g) + \dots + a_k\chi_k(h)\chi_k(g).$$

We now subtract from the equation the equation

$$0 = \chi_1(h) (a_1\chi_1(g) + \dots + a_k\chi_k(g)),$$

so that for all $g \in G$ we get

$$0 = a_2(\chi_2(h) - \chi_1(h))\chi_2(g) + \dots + a_k(\chi_k(h) - \chi_1(h))\chi_k(g).$$

However this is a contradiction to the induction hypothesis since $\{\chi_2, \dots, \chi_k\}$ is a linearly independent set of size $k-1$. This contradiction implies in particular that $a_2(\chi_2(h) - \chi_1(h)) = 0$ but since $\chi_1(h) \neq \chi_2(h)$ we can divide by $\chi_2(h) - \chi_1(h)$ and get that $a_2 = 0$. This completes the proof since as we mentioned at the beginning of the proof if $a_2 = 0$ the induction hypothesis immediately implies that $a_1 = a_3 = \dots = a_k = 0$ as well. $\square$

Theorem 8.3. *Let F be a field that contains a primitive n th root of unity, and let E/F be a cyclic Galois extension of order n . Then there exists $\alpha \in E$ so that $E = F(\alpha)$ and $\alpha^n \in E$.*

Proof. Let $\eta \in F$ a primitive n th root of unity. Let $\sigma \in \text{Gal}(E/F)$ so that $\langle \sigma \rangle = \text{Gal}(E/F)$. We will first show that there exists $\alpha \in E$ so that $\sigma(\alpha) = \alpha\eta^{-1}$. Notice that for all $\tau \in \text{Gal}(E/F)$ the restriction of τ to $E^\times$ is a homomorphism from $E^\times$ to $E^\times$. From Dedekind's lemma we get that

$$\sum_{i=1}^n \eta^i \sigma^i \neq 0.$$

Thus there exists $\gamma \in E^\times$ so that we can define

$$\alpha := \sum_{i=1}^n \eta^i \sigma^i(\gamma) \neq 0.$$

Now,

$$\sigma(\alpha) = \sum_{i=1}^n \sigma(\eta^i) \sigma^{i+1}(\gamma) \stackrel{\eta \in F}{=} \sum_{i=1}^n \eta^i \sigma^{i+1}(\gamma) = \eta^{-1} \sum_{i=1}^n \eta^{i+1} \sigma^{i+1}(\gamma) = \eta^{-1} \alpha.$$

We will now show that the minimal polynomial of α over F is $x^n - \alpha^n$ (in particular $\alpha^n \in F$) and that $E = F(\alpha)$.

For all $1 \leq i \leq n$,

$$\sigma(\alpha^i) = (\sigma(\alpha))^i = \alpha^i \eta^{-i}$$

so in particular $\sigma(\alpha^n) = \alpha^n$ and in particular when $1 \leq i \leq n$ we have

$$i = n \iff \alpha^i \in F = F(\langle \sigma \rangle) = \text{Fix}(\sigma).$$

This means that $x^n - \alpha^n \in F[x]$ so it suffices to show that $x^n - \alpha^n$ is irreducible to show that it is the minimal polynomial of α . Every monic polynomial of degree $1 \leq d < n$ that divides $g(x)$ is of the form

$$g(x) = (x - \alpha\eta^{i_1}) \dots (x - \alpha\eta^{i_d}) = x^d + \dots + \alpha^d \cdot \eta^j \notin F[x]$$

since $\alpha^d \notin F$ and $\eta^j \in F$. Since the minimal polynomial of α over F necessarily divides $g(x)$ and is in $F[x]$ it must be equal to $g(x)$. $\square$

Definition 8.3 (Commutator). Let G be a group, and let $g, h \in G$. The commutator of g and h is the element

$$[g, h] := g^{-1}h^{-1}gh.$$

Remark 8.3. The element $[g, h]$ is equal to the group's identity if and only if g and h commute, hence it is called the commutator of g and h .

Definition 8.4 (Commutator subgroup). Let G be a group. The commutator subgroup (or the derived group) of G is defined to be the subgroup *generated* by all commutators of G and we denote it by $[G, G]$.

Remark 8.4. We also define the following recursive sequence of groups

$$G^{(0)} := G \quad G^{(1)} := [G, G] \quad G^{(2)} := [G^{(1)}, G^{(1)}] \quad \dots \quad G^{(k+1)} := [G^{(k)}, G^{(k)}],$$

and so on.

Exercise 8.2.

- (1) Show that $G^{(1)} \triangleleft G$ and that $G/G^{(1)}$ is abelian.
- (2) Show that if $N \triangleleft G$ and G/N is abelian then $G^{(1)} \leq N$.

Definition 8.5 (Solvable group). A group G is said to be solvable if there exists a subgroup series

$$1 = G_k \leq G_{k-1} \leq \dots \leq G_1 \leq G_0 = G$$

so that for all $0 \leq i < k$ we have $G_{i+1} \triangleleft G_i$ and G_i/G_{i+1} is abelian.

Exercise 8.3. Let G be group.

- (1) Let G be a solvable group. Show that for all $0 \leq i \leq k$ we have $G^{(i)} \leq G_i$.
- (2) Show that G is solvable if and only if $G^{(k)} = 1$ for some natural k .
- (3) Let G be a group and let $N \triangleleft G$. Show that G is solvable if and only if G/N and N are solvable.

8.2 Radical extensions and solvable Galois groups

Lemma 8.4. Let F be a field, let $F \subseteq \Omega$ be an algebraically closed field, let $g \in F[x]$ and let $E := F(\alpha_1, \dots, \alpha_k) \subseteq \Omega$ be a splitting field of g over F . Suppose that $F \subseteq L \subseteq \Omega$ is an intermediate field. Then $L(\alpha_1, \dots, \alpha_k)$ is a splitting field of g over L and the restriction map $\rho: \text{Gal}(L(\alpha_1, \dots, \alpha_k)/L) \rightarrow \text{Gal}(E/F)$ is injective.

Proof. It is clear that $L(\alpha_1, \dots, \alpha_k)$ is a splitting field of g over L . Let $\sigma \in \text{Gal}(L(\alpha_1, \dots, \alpha_k)/L)$. Then $\sigma|_F = \text{id}_F$ and since E/F is normal we get that $\text{im}(\sigma|_E) \subseteq E$ so we can conclude that $\sigma|_E \in \text{Gal}(E/F)$ (since σ is an F -embedding of E into Ω , by definition of normality $\text{im}(E) \subseteq E$). Thus ρ is well defined and it is easy to verify that it is a homomorphism. In order to show that ρ is injective we will show that $\ker(\rho) = \{\text{id}\}$. Suppose that $\rho(\sigma) := \sigma|_E = \text{id}_E \in \text{Gal}(E/F)$. In particular we get that $\sigma|_{\{\alpha_1, \dots, \alpha_k\}} = \text{id}_{\{\alpha_1, \dots, \alpha_k\}}$ which means that σ fixes not only the elements of L (by definition) but it also fixes $\alpha_1, \dots, \alpha_k$, so clearly $\sigma = \text{id}_L$. $\square$

Lemma 8.5. Let F be a field and let E/F be a separable radical extension. Then E is contained in a radical Galois extension of F .

Proof. Since E/F is a radical extension, by definition we have

$$F := F_0 \subseteq F_0(\alpha_1) \subseteq F_1(\alpha_2) \subseteq \cdots \subseteq F_{k-1}(\alpha_k) = E$$

where we denote $F_0 := F$ and $F_n := F_{n-1}(\alpha_n)$, such that $\alpha_i^{r_i} \in F_{i-1}$ for all $1 \leq i \leq k$. Let m_i be the minimal polynomial of α_i over F , let Ω be an algebraic closure of E , and let $L \subseteq \Omega$ be a splitting field of $m_1 m_2 \cdots m_k$ over F . Then since L contains $\alpha_1, \dots, \alpha_k$ we get $E \subseteq L$. We notice that L is contained in any normal extension of F that contains E (since such an extension contains $\alpha_1, \dots, \alpha_k$ and thus the roots of $m_1, m_2, \dots, m_k$). Let $E \subseteq M \subseteq L$ be a normal extension of F which is maximal with respect to containment. We want to show that $M = L$. Assume, by way of contradiction, that $M \neq L$, then there exists $\sigma \in \text{Gal}(L/F)$ and $1 \leq i \leq k$ so that $\sigma(\alpha_i) \notin M$. Let $1 \leq j \leq k$ be the minimal index so that $\sigma(\alpha_j) \notin M$. We know that $\alpha_j^{r_j} \in F(\alpha_1, \dots, \alpha_{j-1})$ (if $j = 0$ then $F(\alpha_1, \dots, \alpha_{j-1}) = F$). Thus $\sigma(\alpha_j)^{r_j} \in F(\sigma(\alpha_1), \dots, \sigma(\alpha_{j-1}))$ (since $\sigma|_F = \text{id}_F$) and $F(\sigma(\alpha_1), \dots, \sigma(\alpha_{j-1})) \subseteq M$ from minimality of M . We get that

$$F \subseteq M \subseteq M(\sigma(\alpha_j)).$$

These are both radical extensions, so $M(\sigma(\alpha_j))/F$ is a radical extension that strictly contains M , which is a contradiction. This contradiction completes the proof. $\square$

Definition 8.6 (Solvable in radicals). Let F be a field and let $g(x) \in F[x]$. Then g is said to be solvable in radicals if there exists a radical extension E/F so that g splits in E .

Theorem 8.6. Let F be a field of characteristic 0. Let $h \in F[x]$. Then h is solvable in radicals if and only if G_h is solvable.

Proof. Let Ω be an algebraic closure of F . Denote the Galois group of h by G_h . Suppose that G_h is solvable and denote $n := (\deg h)!$. Let $\eta \in \Omega$ be a primitive n th root of unity, let $L := F(\eta)$, and let M be the splitting field of h over L . Theorem 8.5 shows that $\text{Gal}(M/L)$ has an embedding in $\text{Gal}(E/F)$ and thus is solvable. In particular there exists a sequence

$$1 \triangleleft G_k \triangleleft G_{k-1} \triangleleft \cdots \triangleleft G_0 = G$$

so that for all $1 \leq i \leq k$ we have that G_{i-1}/G_i is cyclic. For all $1 \leq i \leq k$ we denote $L_i = \mathcal{F}(G_i)$. From the fundamental theorem of Galois we get that

$$L = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_k = M.$$

Additionally, $G_i = \text{Gal}(M/L_i)$ for all $0 \leq i \leq k$. Since $G_i \triangleleft G_{i-1}$, part B of the fundamental theorem of Galois implies that for all $1 \leq i \leq k$ that L_i is a normal extension of L_{i-1} , and

$$\text{Gal}(L_i/L_{i-1}) \cong G_{i-1}/G_i.$$

and thus L_i/L_{i-1} is a cyclic Galois extension. Now since M is the splitting field over L of a polynomial of degree n ,

$$[L_i : L_{i-1}] \mid [M : L] \mid n!.$$

Since L contains the primitive n th root of unity it contains a primitive root of unity of order $[L_i : L_{i-1}]$. Thus from a theorem from the previous lecture there exists $\alpha_i \in L_i$ and a natural number r_i so that $L_i = L_{i-1}(\alpha_i)$ and $\alpha_i^{r_i} \in L_{i-1}$. We get that the sequence

$$F \subseteq \underbrace{F(\eta)}_{L_0} \subseteq L_1 \subseteq \cdots \subseteq L_k = M,$$

where L_k is the splitting field of h over L and thus contains a splitting field of h over F . This implies that h is solvable in radicals.

We proceed to show the other direction. Denote the splitting field of h over F by E and suppose that E is contained in a radical extension M . From Theorem 8.5 we can assume that M is a Galois extension of F . It suffices to show that there exists a Galois extension L/F so that $M \subseteq L$ and $\text{Gal}(L/F)$ is solvable (because $\text{Gal}(E/F)$ is a quotient of $\text{Gal}(L/F)$ and a quotient of a solvable group is solvable). Let

$$F = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M$$

where $M_0 := F$ and $M_n = M_{n-1}(\alpha_n)$ for $n > 1$ and $\alpha_i^{r_i} \in M_{i-1}$ for $i \geq 1$. A tower of fields implies solvability by radicals. Let Ω be an algebraic closure of M and let $\alpha_0 \in \Omega$ be a primitive root of unity of order

$$r_0 := r_1 \cdots r_k.$$

Note that the existence of α_0 follows from the fact $\text{char}(F) = 0$. Define $L = M(\alpha_0)$, so that L/F is a Galois extension. That is because if M is the splitting field of the polynomial $m(x)$ then L is the splitting field of $m(x)(x^r - 1)$. We know that L_0/F is an abelian Galois extension with a Galois group isomorphic to $(\mathbb{Z}/r_0\mathbb{Z})^\times$. Moreover, since for all $1 \leq i \leq r$ the field M_{i-1} contains a primitive r_i th root of unity, it follows that $\text{Gal}(L_i/L_{i-1})$ is cyclic. For all $-1 \leq i \leq k$ denote $G_i = \mathcal{G}(L_i)$, and then from the fundamental theorem of Galois theory, for all $0 \leq i \leq k$ we get $G_i \triangleleft G_{i-1}$ and that $G_{i-1}/G_i \cong \text{Gal}(L_i/L_{i-1})$ is abelian. This gives us a subnormal sequence

$$1 = G_k \triangleleft G_{k-1} \triangleleft \cdots \triangleleft G_0 \triangleleft G_{-1} = \text{Gal}(L/F),$$

with abelian quotients, and thus $\text{Gal}(L/F)$ is solvable. $\square$

Exercise 8.4. Show that A_5 is simple and not abelian. Conclude that it is not solvable. Conclude that S_5 is not solvable. Show that the groups S_2, S_3, S_4 are solvable.

Remark 8.5. In order to construct a polynomial which is not solvable in radicals, it suffices to construct a polynomial with a Galois group that is isomorphic to S_5 .

Exercise 8.5. Show that the only subgroup of S_5 that contains a transposition (ab) and a cycle of length 5 is S_5 .

Proposition 8.7. Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5 which has exactly 3 real roots. Then the Galois group of f is isomorphic to S_5 . Thus $\text{Gal}(L/F)$ is not solvable.

8.3 Galois groups of polynomials of degree $n \leq 4$

Let $f(x) \in \mathbb{Q}[x]$ be a separable polynomial of degree n and let $\alpha_1, \dots, \alpha_n$ be its roots in a splitting field E of f . We know that the action of $G_f := \text{Gal}(E/F)$ on the roots of f induces an embedding

$$\rho: G_f \hookrightarrow S_n.$$

We know that G_f is transitive if and only if f is irreducible. We would like to know when the image of this embedding is contained in A_n .

Definition 8.7 (Vandermonde product). Let $f \in F[x]$ be a polynomial. Then the Vandermonde product of f is defined to be the determinant of its associated Vandermonde matrix which is

$$\Delta(f) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$

Definition 8.8 (Discriminant). Let $f \in F[x]$ be a polynomial. Then its discriminant is defined by

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

Lemma 8.8. Let $f \in F[x]$ and let $\sigma \in G_f$. Then

$$\sigma(\Delta(f)) = \text{sgn}(\sigma) \cdot \Delta(f),$$

and in particular $\sigma(D(f)) = \sigma(\Delta(f))^2 = D(f)$.

Proof. From multiplicity of the sign and since transpositions of the form $\begin{pmatrix} i & i+1 \end{pmatrix}$ generate S_n , it suffices to show the statement in the case $\sigma = \begin{pmatrix} i & i+1 \end{pmatrix}$. In this case we get,

$$\sigma(\Delta(f)) = \left(\prod_{\substack{1 \leq j < l \leq n \\ (j,l) \neq (i,i+1)}} (\alpha_j - \alpha_l) \right) \cdot (\alpha_{i+1} - \alpha_i) = -\Delta(f),$$

which completes the proof. $\square$

Corollary 8.9. The following propositions hold:

- (1) $D(f) \in \mathcal{F}(Gf) = \mathbb{Q}$.
- (2) $G_f \subseteq A_n$ if and only if $\Delta(f) \in \mathbb{Q}$.

Remark 8.6. In what follows we show that $D(f)$ is a polynomial in the coefficients of f . We will additionally show how to compute the Galois groups of (almost) any polynomial in $\mathbb{Q}[x]$ of degree $n \leq 4$.

Example 8.3 (Polynomials of degree 2). Let $f(x) = x^2 + bx + a \in \mathbb{Q}[x]$. Denote the roots of f by α_1 and α_2 . Then

$$(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-b)^2 - 4c = b^2 - 4c,$$

where the second transition follows from that fact that the sum of the roots is $-b/a$ and $a = 1$. This is the exactly the discriminant $\Delta(f)$. Now we have that

$$\Delta(f) \notin \mathbb{Q} \iff D(f) \notin \mathbb{Q}^2 \iff f \text{ is irreducible} \iff G_f \text{ transitive} \iff G_f = S_2.$$

Example 8.4 (Polynomials of degree 3). Let $f(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$. We know that f is reducible over f if and only if it has a rational root of the form $\frac{r}{s} \in \mathbb{Q}$ where $\gcd(r, s) = 1$. We want to show that we can deduce whether f is irreducible. Suppose $\frac{r}{s}$ is a root of f , then $r \mid d$ and $s \mid a$. That is because

$$0 = a \left(\frac{r}{s} \right)^3 + b \left(\frac{r}{s} \right)^2 + c \left(\frac{r}{s} \right) + d \iff 0 = ar^3 + br^2s + crs^2 + ds$$

(this is the rational root theorem). Suppose f is irreducible. Then G_f is isomorphic to a transitive subgroup of S_3 , so $G_f \cong S_3$ or $G_f \cong A_3$. We will try to classify these cases.

By change of a variable $y = rx + s$ and a multiplication by a scalar we can assume that $f(x) = x^3 + bx + c$ (a linear change in variables does not change the Galois group) where $b, c \in \mathbb{Q}$. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of f . We have

$$D(f) = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha_3)^2(\alpha_3 - \alpha_1)^2 = ((\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1))^2.$$

Notice that

$$(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) = \underbrace{(\alpha_1^2\alpha_3 + \alpha_2^2\alpha_1 + \alpha_3^2\alpha_2)}_v - \underbrace{(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1)}_u.$$

Since $\alpha_1 + \alpha_2 + \alpha_3$ is the coefficient of the quadratic term we get that $\alpha_1 + \alpha_2 + \alpha_3 = 0$. We also know that $\alpha_1\alpha_2 + \alpha_2\alpha_1 + \alpha_3\alpha_1 = b$ and $\alpha_1\alpha_2\alpha_3 = -c$. Notice that

$$u + v = \sum_{1 \leq i < j \leq 3} \alpha_i \alpha_j (\alpha_i + \alpha_j) = \sum_{\substack{1 \leq i < j \leq 3 \\ k \neq i, j}} \left(\alpha_i \alpha_j \underbrace{(\alpha_i + \alpha_j + \alpha_k)}_{=0} - \underbrace{\alpha_i \alpha_j \alpha_k}_{=c} \right) = -3c.$$

Similarly, we can show that $uv = b^3 + 9c^2$. Thus

$$D(f) = (v - u)^2 = (v + u)^2 - 4uv = -27c^2 - 4b^3.$$

This allows us to conclude that $G_f \subseteq A_3$ if and only if $D(f) = -27c^2 - 4b^3$ is a square in $\mathbb{Q}$.

Example 8.5 (Polynomials of degree 4). Let $E/\mathbb{Q}$ be a splitting of a polynomial $f \in \mathbb{Q}[x]$ of degree 4 which is irreducible. Let $\alpha_1, \dots, \alpha_4 \in E$ be the roots of f . Denote

$$u := \alpha_1\alpha_2 + \alpha_3\alpha_4$$

$$v := \alpha_1\alpha_3 + \alpha_2\alpha_4$$

$$w := \alpha_1\alpha_4 + \alpha_2\alpha_3$$

Since

$$u - v = \alpha_1(\alpha_2 - \alpha_3) + \alpha_4(\alpha_3 - \alpha_2) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) \neq 0,$$

we obtain that $u \neq v$, and similarly we can show that u, v , and w are distinct. Denote

$$V := \{\text{id}, (12)(34), (13)(24), (14)(23)\}.$$

Then $V \triangleleft S_4$ and $S_4/V \cong S_3$ (home exercise). Denote $M = \mathbb{Q}(u, v, w)$. We can verify directly that $\mathcal{G}(M) = G_f \cap V$. Now we can deduce from $V \triangleleft S_4$ that $G_f \cap V \triangleleft G_f$. From the fundamental theorem of Galois theory $M/\mathbb{Q}$ is a normal extension and

$$\text{Gal}(M/\mathbb{Q}) \cong G_f/\mathcal{G}(M).$$

Denote $g(x) = (x - u)(x - v)(x - w) \in M[x]$. We can express the coefficients of $g(x)$ using the coefficients of $f(x)$ (home exercise). By Example 8.4 we can find $G_f/\mathcal{G}(M)$. Since f is irreducible, G_f acts transitively, and $4 \mid |G_f|$, we can simply classify all subgroups of S_4 that satisfy these conditions. The options are:

G_f	$ \mathcal{G}(M) $	$ G_f/\mathcal{G}(M) = [M : F]$
S_4	4	6
A_4	4	3
V	4	1
D_4	4	2
C_4	2	2

We can conclude that unless $|G_f/\mathcal{G}(M)| = 2$, we can determine G_f . How can we differentiate between D_4 and C_4 ? We know that $G_f \cap V$ is transitive if and only if $G_f = D_4$ if and only if $f \in M[x]$ is irreducible, and we will not get into it but there is a way to determine this.

9 Transcendence degree

Definition 9.1 (Algebraically independent elements). Let E/F be a field extension. We say that $a_1, \dots, a_k \in E$ are algebraically independent over F if for all $0 \neq g \in F[x_1, \dots, x_n]$ we have $g(a_1, \dots, a_n) \neq 0$.

Example 9.1. An element $\alpha \in \mathbb{R}$ is algebraically independent if and only if it is transcendental.

Remark 9.1. Notice that if $a_1, \dots, a_k$ are algebraically independent then $F(a_1, \dots, a_n) \cong F(x_1, \dots, x_n)$.

Lemma 9.1. Let E/F be a field extension. Let $a_1, \dots, a_k \in F$ be algebraically independent over F , and suppose that $a_1, \dots, a_{k+1} \in F$ are algebraically dependent over F . Then a_{k+1} is algebraic over $F(a_1, \dots, a_k)$.

Proof. There exists $0 \neq g \in F[x_1, \dots, x_{k+1}]$ such that $g(a_1, \dots, a_{k+1}) = 0$. Write

$$g = \sum_{i=0}^m g_i(x_1, \dots, x_k) x_{k+1}^i.$$

Since $g \neq 0$, there exists $0 \leq j \leq m$ so that $g_j \neq 0$. Since $a_1, \dots, a_k$ are algebraically independent over F we get $g_j(a_1, \dots, a_k) \neq 0$ and thus

$$0 \neq h(x) = \sum_{i=0}^m g_i(a_1, \dots, a_k) x^i \in F(a_1, \dots, a_k)[x],$$

and $h(a_{k+1}) = 0$, which completes the proof. $\square$

Corollary 9.2. Let E/F be a finitely generated field extension. Then if E/F is not an algebraic extension, there exist algebraically independent elements $a_1, \dots, a_k \in E$ so that $E/F(a_1, \dots, a_k)$ is algebraic.

Lemma 9.3 (Steinitz exchange lemma). Let E/F be a finitely generated non algebraic field extension. Let $k \in \mathbb{N}^+$ be the minimal number so that there exist $a_1, \dots, a_k \in E$ algebraically independent over F , so that $E/F(a_1, \dots, a_k)$ is algebraic. Let $b \in E$ be transcendental over F , and let $1 \leq j \leq k$ be minimal so that $a_1, \dots, a_j, b$ are algebraically dependent over F . Then $a_1, \dots, a_{j-1}, b, a_{j+1}, \dots, a_k$ are algebraically independent over F and E/L is algebraic where $L = F(a_1, \dots, a_{j-1}, b, a_{j+1}, \dots, a_k)$.

Proof. By definition of j , we get that $a_1, \dots, a_j, b$ are algebraically dependent over F , and that $a_1, \dots, a_{j-1}, b$ are algebraically independent over F . By Theorem 9.1 we conclude that a_j is algebraic over $F(a_1, \dots, a_{j-1}, b)$. We now have that $L(a_j)/L$ and $E/L(a_j)$ are algebraic extensions, and thus E/L is algebraic as well. Finally, if $a_1, \dots, a_{j-1}, b, a_{j+1}, \dots, a_k$ are algebraically dependent, then from the previous lemma we can conclude that L/M is algebraic where $M = F(a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_k)$. Since E/L and L/M are algebraic extensions we conclude that E/M is an algebraic extension, which is a contradiction to the minimality of k . This contradiction completes the proof. $\square$

Proposition 9.4. Let E/F be a finitely generated non algebraic field extension. Let $k \in \mathbb{N}$ be the minimal natural number so that there exist $a_1, \dots, a_k \in E$ algebraically independent over F so that E/L is algebraic where $L = F(a_1, \dots, a_k)$. If $b_1, \dots, b_m$ are algebraically dependent then $m \leq k$. Moreover, $m = k$ if and only if E/M is algebraic where $M = F(b_1, \dots, b_m)$.

Proof. First, we will prove that for all $1 \leq j \leq \min\{m, k\}$ there exist $1 \leq i_{1,j} < i_{2,j} < \cdots < i_{k-j,j}$ so that $b_1, \dots, b_j, a_{i_{1,j}}, \dots, a_{i_{k-j,j}}$ are algebraically independent over F and the extension $E/F(b_1, \dots, b_j, a_{i_{1,j}}, \dots, a_{i_{k-j,j}})$ is algebraic.

The case $j = 1$ follows from the previous lemma. Assume that we have shown the statement for $1 \leq j < k$ and show it for $j + 1$. This follows from applying the previous lemma for $b_1, \dots, b_j, a_{i_{1,j}}, \dots, a_{i_{k-j,j}}$ and the element b_{j+1} .

We now continue to prove the theorem. What we have shown implies that

- (1) $m \leq k$ since otherwise b_{k+1} is algebraic over $b_1, \dots, b_k$.
- (2) If $k = m$ then E is algebraic over $F(b_1, \dots, b_m)$.
- (3) If $m < k$ then there exists $1 \leq i \leq k$ so that a_i is transcendental over $F(b_1, \dots, b_m)$ and in particular $E/F(b_1, \dots, b_m)$ is not algebraic.

This completes the proof. $\square$

Definition 9.2 (Transcendence degree). Let E/F be a finitely generated field extension. The transcendence degree of E/F is the minimal k so that there exist $a_1, \dots, a_k \in E$ that are algebraically independent over F so that $E/F(a_1, \dots, a_k)$ is an algebraic extension.

Definition 9.3 (Transcendence basis). Let E/F be a finitely generated field extension of transcendence degree $k \geq 1$. Then any set of k algebraically independent elements over F so that $E/F(a_1, \dots, a_k)$ is an algebraic extension is called a transcendental basis of E over F .

Example 9.2. Let F be a field and let $E = F(x_1, \dots, x_n)$ be the field of rational functions over F in n variables. Then the transcendence degree of E over F is n . Let G be some subgroup of S_n . Then we define an embedding $\rho: G \rightarrow \text{Aut}(E/F)$ in the following way: For each $\sigma \in G$ we define

$$\rho(\sigma)(x_i) := x_{\sigma(i)},$$

for all $1 \leq i \leq n$. Denote $H = \rho(G)$ and $L = \mathcal{F}(H)$. From Artin's theorem it follows that E/F is a Galois extension and $\text{Gal}(E/L) \cong H$.

Example 9.3. Recall Example 9.2 and consider the case $G = S_n$. For all $1 \leq k \leq n$ define:

$$p_1 = \sum_{1 \leq i \leq n} x_i \quad p_2 = \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2} \quad \cdots \quad p_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \cdots x_{i_k}$$

Note that for all $\sigma \in S_n$ and for all $1 \leq i \leq k$ we have $\rho(\sigma)(p_i) = p_i$. Like in Example 9.2, denote $H = \rho(G)$, $L = \mathcal{F}(H)$, and also denote $M = F(p_1, \dots, p_n)$. We have that $M \subseteq L$, and we want to show that $L = M$. Since the transcendence degree of L is n , we get that L is isomorphic to $F(x_1, \dots, x_n)$. The isomorphism is the map $\varphi: F(x_1, \dots, x_n) \rightarrow F(p_1, \dots, p_n)$ given by $\varphi(x_i) = p_i$.

We know that $M \subseteq L$ and that $[E : F] = |S_n| = n!$. In order to show that $M = L$ it suffices to show that $[E : M] \leq n!$. Define

$$M[t] \ni g(t) := t^n - p_1 t^{n-1} + \cdots + (-1)^{n-1} p_{n-1} t + (-1)^n p_n = (t - x_1)(t - x_2) \cdots (t - x_n).$$

Thus, E is the splitting field of g over M , and in particular $[E : M] \leq n!$.

Exercise 9.1. Let E/F be an extension of transcendence degree k .

- (1) Suppose that $F \subseteq L \subseteq E$ and E/L is an algebraic extension, then the transcendence degree of L/F is k .
- (2) Suppose that $E = F(a_1, \dots, a_k)$ and that E/F has transcendence degree k . Then E is isomorphic to the ring of rational functions in k variables over F , and $a_1, \dots, a_k$ form a transcendence basis of E/F .