

Galois Theory

Ikhan Choi

March 24, 2022

Contents

I	Group theory	3
1	Extension theory	4
1.1	Semidirect product	4
1.2	Extensions	5
1.3	Subnormal series	6
2	The Sylow theorems	7
2.1	The Sylow theorems	7
2.2	Classification of small groups	9
3	Group presentation	12
3.1	Free groups	12
II	Field extentsions	13
4	Algebraic extensions	14
4.1	Fields	14
4.2	Algebraic elements	14
4.2.1	Conjugates	17
4.3	Algebraic extensions	18
4.4	Algebraic closures	20
4.4.1	Algebraically closed fields	20
4.4.2	Uniqueness and existence	22
5	Separable extensions	24
5.1	Separable polynomials	24
5.2	Separable extensions	26
5.3	Separable closures	26

6	Normal extensions	27
6.1	Normal extensions	27
6.2	Galois correspondence	27
III	Galois groups	28
7	Generators of Galois groups	29
8	Invariants of Galois groups	30
8.1	Resultants	30
8.2	Resolvent polynomials	30
9	Reduction of Galois groups	32
9.1	Finite fields	32
9.2	Ramification theory	33
9.3	The Dedekind theorem	33
IV	Insolvability of the quintic	34
10	Cyclic extensions	35
11	Cyclotomic extensions	36
11.1	Cyclotomic polynomials	36
11.2	Kummer theory	36
12	Radical extensions	37

Part I

Group theory

Chapter 1

Extension theory

1.1 Semidirect product

Definition 1.1.1 (External semidirect product). Suppose we have three data: groups $(N, +)$, (H, \cdot) and a group homomorphism $\varphi : H \rightarrow \text{Aut}(N)$. The *semidirect product* $N \rtimes_{\varphi} H$ is a group defined on the set $N \times H$ by

$$(n, h)(n', h') = (n + \varphi(h)n', hh').$$

The motivation of the group structure of semidirect product is shown in the following theorem.

Theorem 1.1.1 (Internal semidirect product). Let N, H be subgroups of G such that

$$N \trianglelefteq G, \quad N \cap H = 1, \quad NH = G.$$

Then, $G \cong N \rtimes_{\varphi} H$, where the action φ is given by conjugation

$$\varphi(h) : N \rightarrow N : n \mapsto hnh^{-1}.$$

Lemma 1.1.2. Let N, H be groups. Let $\varphi_1, \varphi_2 : H \rightarrow \text{Aut}(N)$ be group actions. If there are $\nu \in \text{Aut}(N)$ and $\eta \in \text{Aut}(H)$ such that a diagram

$$\begin{array}{ccc} H & \xrightarrow{\varphi_1} & \text{Aut}(N) \\ \downarrow \eta & & \downarrow \nu \cdot \nu^{-1} \\ H & \xrightarrow{\varphi_2} & \text{Aut}(N) \end{array}$$

commutes, then a map

$$N \rtimes_{\varphi} H \rightarrow N \rtimes_{\varphi'} H : (n, h) \mapsto (\nu(n), \eta(h))$$

is an isomorphism.

Lemma 1.1.3. *Let Z, G be finite groups. If Z is cyclic, then two group actions $\varphi, \varphi' : Z \rightarrow \text{Aut}(G)$ induces the isomorphic semidirect products if and only if their images are conjugate.*

1.2 Extensions

Proposition 1.2.1. *Let N and H be groups. Then, the following objects have one-to-one correspondences among each other:*

- (a) *isomorphic types of groups G such that a sequence*

$$0 \rightarrow N \rightarrow G \rightarrow H \rightarrow 0$$

is exact and right split,

- (b) *isomorphic types of groups G such that $N \trianglelefteq G \geq H$ with $G = NH$ and $N \cap H = 1$,*
(c) *group actions $H \rightarrow \text{Aut}(N)$ preserving the group structure of N .*

Definition 1.2.1. The group G in the previous proposition is called the *semidirect product* of N and H .

$$0 \rightarrow F \rightarrow E \rightarrow G \rightarrow 0.$$

Four data $G, F, \varphi : G \rightarrow \text{Aut}(F), c : G \times G \rightarrow F$ completely determine the extension E .

Suppose we have an extension $F \rightarrow E \rightarrow G$. There is a *set-theoretic section* $s : G \rightarrow E$. The number of s is $|G||F|$.

Definition of action φ : For two sections s and s' , $s(g)$ and $s'(g)$ acts on F equivalently. Thus, we can define a *group homomorphism* $\varphi : G \rightarrow \text{Aut}(F)$ independently on sections.

Definition of 2-cocycle c : It is a *set-theoretic function* $c : G \times G \rightarrow F$ defined by $c(g, g') = s(g)s(g')s(gg')^{-1}$ for a section s . Actually, c depends on the section s , and c measures how much s fails to be a group homomorphism. It requires the cocycle condition for the associativity of group operation, i.e.

$$c(g, h)c(gh, k) = \varphi_g(c(h, k))c(g, hk)$$

should be satisfied. Conversely, a map $G \times G \rightarrow F$ satisfying the condition the cocycle condition gives a associative group operation on G .

If F is abelian, then the set of cocycles forms an abelian group, and is denoted by $Z^2(G, F)$. The boundaries are also defined in abelian F case.

- (a) φ, c is trivial \iff direct product,
- (b) c is trivial $\iff s$ is a homomorphism \iff semidirect product,
- (c) φ is trivial \iff central extension.

Group cohomology is defined for a group G and G -module A (three data: G, A, φ). What is important is that the cohomology depends on the action of G on A .

If φ is trivial so that A is just an abelian group, then the universal coefficient theorem can be applied.

1.3 Subnormal series

Chapter 2

The Sylow theorems

2.1 The Sylow theorems

2.1 (The Sylow theorems). Let G be a finite group of order $n = p^a m$ for a prime $p \nmid m$. A *Sylow p -subgroup* is a subgroup of order p^a . Denote $\text{Syl}_p(G)$ the set of Sylow p -subgroups and $n_p(G)$ its cardinality.

- (a) $n_p \geq 1$.
- (b) $n_p \equiv 1 \pmod{p}$.
- (c) $n_p \mid m$.

Proof. (a) Suppose $\text{Syl}_p(G) \neq \emptyset$ for all finite groups G such that $|G| < n$. The class equation for the action of G on G by conjugation is

$$n = |Z(G)| + \sum_{i=1}^r |G : C_G(g_i)|,$$

where r is the number of non-trivial orbits.

If $p \mid |Z(G)|$, then, by the Cauchy theorem for abelian groups, $Z(G)$ has a normal subgroup P_p of order p , and so is a normal subgroup of G . For $Q \in \text{Syl}_p(G/P_p)$, the inverse image of Q under the projection $G \rightarrow G/P_p$ is a Sylow p -subgroup of G . If $p \nmid |Z(G)|$, then we have $p \nmid |G : C_G(g)|$ for some $g \in G$, and with this g , we have $\text{Syl}_p(C_G(g)) \subset \text{Syl}_p(G)$. Then, we are done by induction.

(b) For $P \in \text{Syl}_p(G)$, the class equation for the action of P on $\text{Syl}_p(G)$ by conjugation is

$$n_p = f + \sum_{i=1}^r |P : N_P(P_i)|,$$

where f is the number of fixed points and r the number of non-trivial orbits.

If $P_i \in \text{Syl}_p(G)$ is fixed, then P normalizes P_i so that $P < N_G(P_i)$, and by passing P through the projection $N_G(P_i) \rightarrow N_G(P_i)/P_i$ we can show $P = P_i$. Therefore, P is the only fixed point, so it follows that $n_p \equiv 1 \pmod{p}$ from

$$n_p = 1 + \sum_{i=1}^r |P : N_P(P_i)|.$$

(c) Suppose there are $P, P' \in \text{Syl}_p(G)$ that are not conjugate. The class equations for actions of P and P' on $\text{Orb}_G(P) \subset \text{Syl}_p(G)$ are

$$|\text{Orb}_G(P)| = 1 + \sum_{i=1}^r |P : N_P(P_i)| = \sum_{i=1}^{r'} |P' : N_{P'}(P_i)|,$$

because only P can fix P as shown in the part (b). It deduces $|\text{Orb}_G(P)| \equiv 0, 1 \pmod{p}$ simultaneously, which is a contradiction. Therefore, the action of G on $\text{Syl}_p(G)$ by conjugation is transitive and its class equation is

$$n_p = |G : N_G(P)|$$

for all $P \in \text{Syl}_p(G)$. □

- (a) every pair of two Sylow p -subgroup is conjugate.
- (b) every p -subgroup is contained in a Sylow p -subgroup.
- (c) a Sylow p -subgroup is normal if and only if $n_p = 1$.

Investigation of a group of a given order is divided into two main parts: the existence of a subgroup of particular orders and the measurement of the size of conjugate subgroups.

In order to show the existence of subgroups of particular orders:

- (a) p -groups always exist,
- (b) extension theory, (what can subgroups of subgroups do?)
- (c) normalizers,
- (d) Poincare theorem: kernel of permutation representation

In order to find the size of conjugacy classes:

- (a) measure the order of normalizers, (find some groups normalize a subgroup)
- (b) count elements,

2.2 Classification of small groups

2.2 (Classification of groups of order pq).

2.3 (Classification of groups of order p^2).

2.4 (Classification of groups of order pqr).

2.5 (Conjugacy classes of $\text{GL}_2(\mathbb{F}_p)$). The conjugacy classes are classified by the Jordan normal forms. There are four cases: for some a and b in \mathbb{F}_p ,

(a) $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$: $\binom{p-1}{2} = \frac{(q-1)(q-2)}{2}$ classes of size $\frac{|G|}{(q-1)^2} = q(q+1)$.

(b) $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$: $q-1$ classes of size 1.

(c) $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$: $q-1$ classes of size $\frac{|G|}{q(q-1)} = q^2-1$.

(d) otherwise, the eigenvalues are in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. In this case, the number of conjugacy classes is same as the number of monic irreducible quadratic polynomials over \mathbb{F}_p ; $\frac{|\mathbb{F}_{p^2}| - |\mathbb{F}_p|}{2} = \frac{p(p-1)}{2}$ classes. Their size is $\frac{p(p-1)}{2}$.

2.6 (Classification of groups of order p^2q). Let p and q be distinct primes.

(a) If $p+2 \leq q$, there are

$$\begin{cases} 2 & \text{if } v_p(q-1) = 0, \\ 4 & \text{if } v_p(q-1) = 1, \\ 5 & \text{if } v_p(q-1) \geq 2 \end{cases}$$

non-isomorphic groups of order p^2q .

(b) If $p > q$, there are

$$\begin{cases} 5 & \text{if } q = 2, \\ \frac{q+9}{2} & \text{if } q \neq 2, q \mid p-1, \\ 3 & \text{if } q \neq 2, q \mid p+1 \\ 2 & \text{otherwise} \end{cases}$$

non-isomorphic groups of order p^2q

(c) There are five non-isomorphic groups of order 12.

Proof. (a) Let G be a finite group of order p^2q . Sylow's theorem implies $n_q = 1$. For $P \in \text{Syl}_p(G)$ and $Q \in \text{Syl}_q(G)$, we have

$$P \cong Z_{p^2} \text{ or } Z_p^2, \quad \text{and} \quad Q \cong Z_q.$$

Consider actions of the form

$$\varphi : Z_{p^2} \rightarrow \text{Aut}(Z_q) \cong Z_{q-1}.$$

There are $1 + \min\{v_p(q-1), 2\}$ subgroups of Z_{q-1} that can be the image of φ , up to conjugation, that is, there are $1 + \min\{v_p(q-1), 2\}$ distinct groups of the form $Z_q \rtimes Z_{p^2}$.

Consider actions of the form

$$\varphi : Z_p \times Z_p \rightarrow \text{Aut}(Z_q) \cong Z_{q-1}.$$

Similarly, there are $1 + \min\{v_p(q-1), 1\}$ distinct groups of the form $Z_q \rtimes Z_p^2$.

(b) Sylow's theorem implies $n_p = 1$.

Consider actions of the form

$$\varphi : Z_q \rightarrow \text{Aut}(Z_{p^2}) \cong Z_{p(p-1)}.$$

There are $1 + \min\{v_q(p-1), 1\}$ distinct groups of the form $Z_{p^2} \rtimes Z_q$.

Let $Z_p^2 \rtimes Z_q$, and consider actions of the form

$$\varphi : Z_q \rightarrow \text{Aut}(Z_p \times Z_p) \cong \text{GL}_2(\mathbb{F}_p).$$

Note that $|\text{GL}_2(\mathbb{F}_p)| = (p^2-1)(p^2-p) = (p-1)^2p(p+1)$ so that $q \mid p-1$ or $q \mid p+1$. Denote 1 a generator of Z_q , and let $\varphi(1) \neq 1_{2 \times 2}$ so that the action is not trivial.

If $q = 2$, then $\varphi(1)$ is one of the followings

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

up to conjugation, and they generate distinct subgroups of $\text{GL}_2(\mathbb{F}_p)$ up to conjugation.

If $q \neq 2$ and $q \mid p+1$, then there is an element $A \in \text{GL}_2(\mathbb{F}_p)$ of order q exists. Let $\lambda^{\pm 1} \in \overline{\mathbb{F}_p}$ be eigenvalues of A . Then, λ^i is a root of $x^q - 1 = 0$ for each integer i , and the polynomial $x^q - 1$ has q distinct roots λ^i for $0 \leq i < q$. It means that the eigenvalues of $\varphi(1)$ must be $\lambda^{\pm i}$ for some integer i , the image of φ is always conjugate to the subgroup generated by A . Therefore, there is a unique subgroup of order q in $\text{GL}_2(\mathbb{F}_p)$ up to conjugation.

If $q \neq 2$ and $q \mid p-1$, then since the number of one-dimensional linear subspaces of \mathbb{F}_p^2 is $q+1$ and the number of symmetric subspaces is 2 in \mathbb{F}_q^2 , we have $\frac{(q+1)-2}{2} + 2 = \frac{q+3}{2}$ conjugacy classes of subgroups of order q in $\text{GL}_2(\mathbb{F}_p)$. (Need more detail!)

To sum up, there are

$$\begin{cases} 2 & \text{if } q = 2 \\ 1 & \text{if } q \neq 2, q \mid p+1, \\ \frac{q+3}{2} & \text{if } q \neq 2, q \mid p-1, \\ 0 & \text{otherwise} \end{cases}$$

non-abelian groups of the form $Z_p^2 \rtimes Z_q$.

(c)

□

2.7 (Classification of groups of order p^3).

$ G = p^2q \ (p < q)$	12	20	28	44	45	52	63
# of groups	5	5	4	4	2	5	4

$ G = p^2q \ (p > q)$	18	50	75
# of groups	5	5	3

$ G = pqr$	30	42
# of groups	4	6

$ G = \prod^4 p$	16	24	40	54	56	36	60
# of groups	14	15	14	15	13	14	13

$ G = \prod^{5 \text{ or } 6} p$	32	48	64
# of groups	51	52	267

Exercises

2.8. Alternative proof for existence of p -groups.

Proof. Let $|G| = p^{a+b}m$. Let \mathcal{P}_{p^a} be the set of all subsets of G with size p^a . Give $G \rightarrow \text{Sym}(\mathcal{P}_{p^a})$ by left multiplication. Since $v_p(|\mathcal{P}_{p^a}|) = v_p\left(\binom{p^a(p^b m)}{p^a}\right) = b$, there is an orbit \mathcal{O} such that $v_p(|\mathcal{O}|) \leq b$. We have transitive action $G \rightarrow \text{Sym}(\mathcal{O})$ and the stabilizer H satisfies $p^a \mid |G|/|\mathcal{O}| = |H|$. Since $H \rightarrow \text{Sym}(\mathcal{O})$ trivially, $H \rightarrow \text{Sym}(A)$ for $A \in \mathcal{O} \subset \mathcal{P}_{p^a}$. It is only possible when $H \subset A$, hence $|H| = p^a$. □

Chapter 3

Group presentation

3.1 Free groups

Part II

Field extensions

Chapter 4

Algebraic extensions

4.1 Fields

4.1 (Field homomorphisms).

4.2 (Vector space structures and degree).

4.3 (Finite extensions).

4.4 (Simple extensions).

straightedge and compass construction

4.2 Algebraic elements

4.5 (Algebraic elements). Let E/F be a field extension. An element $\alpha \in E$ is called *algebraic over F* if there is a non-zero polynomial $f \in F[x]$ such that $f(\alpha) = 0$. If α is not algebraic over F , we call it *transcendental over F* . For $\alpha \in E$, the following statements are all equivalent:

- (a) The element α is algebraic over F .
- (b) The ring $F[\alpha]$ is a field.
- (c) The equality $F(\alpha) = F[\alpha]$ holds.
- (d) The simple extension $F(\alpha)/F$ is finite.

Proof. (a) \Rightarrow (b) Note $F[\alpha] = F$ is a field if $\alpha = 0$. Let $\alpha \neq 0$. Define a ring homomorphism

$$\text{eval}_\alpha : F[x] \rightarrow F[\alpha] : f(x) \mapsto f(\alpha),$$

which is called *evaluation*. The kernel of eval_α contains α , hence is non-zero, and it is a prime ideal because the quotient

$$F[x]/\ker(\text{eval}_\alpha) \cong \text{im}(\text{eval}_\alpha) = F[\alpha]$$

is an integral domain. Since $F[x]$ is a principal ideal domain so that every non-zero prime ideal is maximal, the quotient $F[\alpha]$ is a field.

(b) \Rightarrow (c) We clearly have $F[\alpha] \subset F(\alpha)$. Since $F(\alpha)$ is defined as the intersection of all subfields of E containing F and α , $F(\alpha) \subset F[\alpha]$.

(c) \Rightarrow (a) There is $g \in F[x]$ such that $\alpha^{-1} = g(\alpha)$. Then, $f \in F[x]$ defined by $f(x) = xg(x) - 1$ satisfies $f(\alpha) = 0$.

(a), (c) \Rightarrow (d) Let $f \in F[x]$ be non-zero with $f(\alpha) = 0$. For an element $g(\alpha)$ of $F(\alpha) = F[\alpha]$ for some $g \in F[x]$, there are $q, r \in F[x]$ such that $g = qf + r$ and $\deg r < \deg f$ by the Euclidean algorithm, so $g(\alpha) = r(\alpha)$. Since $r(\alpha)$ is a linear combination of $\{1, \alpha, \dots, \alpha^{\deg f - 1}\}$ over F , we get $[F(\alpha) : F] \leq \deg f$.

(d) \Rightarrow (a) Since $[F(\alpha) : F] < \infty$, we can find a linearly dependent finite subset of a set $\{1, \alpha, \alpha^2, \dots\} \subset F(\alpha)$ over F . The coefficients on the linear dependency relation construct the polynomial. \square

Since the ideal $\ker(\text{eval}_\alpha) \subset F[x]$ for algebraic $\alpha \in E$ is maximal, the following definition makes sense:

Definition 4.2.1. Let E/F be a field extension and $\alpha \in E$ is algebraic. The unique monic irreducible polynomial $\mu_{\alpha, F} \in F[x]$ satisfying

$$\mu_{\alpha, F}(\alpha) = 0$$

is called the *minimal polynomial* of α over F .

Theorem 4.2.1. Let E/F be a field extension and $\alpha \in E$ is algebraic. Then,

$$F(\alpha) \cong F[x]/(\mu_{\alpha, F}).$$

In particular, $[F(\alpha) : F] = \deg \mu_{\alpha, F}$.

Proof. The kernel of $\text{eval}_\alpha : F[x] \rightarrow F(\alpha)$ is characterized as the principal ideal generated by $\mu_{\alpha, F}$, so we find the isomorphism $F[x]/(\mu_{\alpha, F}) \cong F(\alpha)$.

Now we claim the dimension of $F[x]/(f)$ over F is the degree of $f \in F[x]$. It is enough to show $\{1, x, \dots, x^{d-1}\}$ is a basis where $d = \deg f$. We can check this with the Euclidean algorithm. \square

Example 4.2.1. Consider a field extension \mathbb{C}/\mathbb{Q} . The minimal polynomial of $\sqrt{2} \in \mathbb{C}$ over \mathbb{Q} is

$$\mu_{\sqrt{2}, \mathbb{Q}}(x) = x^2 - 2$$

since it is monic irreducible and has a root $\sqrt{2}$. Similarly, the minimal polynomial of $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ over \mathbb{Q} is

$$\mu_{\omega, \mathbb{Q}}(x) = x^2 + x + 1.$$

Example 4.2.2. We can compute the degree of a field extension by finding minimal polynomial. Since the minimal polynomial $\sqrt{2} + \sqrt{3}$ over \mathbb{Q} is

$$\mu_{\sqrt{2}+\sqrt{3}, \mathbb{Q}}(x) = x^4 - 10x^2 + 1,$$

we have

$$[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = \deg(x^4 - 10x^2 + 1) = 4.$$

On the other hand, we have

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

Since $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ implies $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and the dimensions as vector spaces are equal, we get $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. We can also directly check

$$\sqrt{2} = \frac{1}{2} \left(\alpha - \frac{1}{\alpha} \right) \quad \text{and} \quad \sqrt{3} = \frac{1}{2} \left(\alpha + \frac{1}{\alpha} \right),$$

where $\alpha = \sqrt{2} + \sqrt{3}$. This kind of *dimension argument* is one of powerful tools to attack field theory. It will be discovered later that the dimension argument has an analogy with computation of group orders in finite group theory.

Example 4.2.3. The base field is important: we have

$$\mu_{\sqrt{2}, \mathbb{Q}}(x) = x^2 - 2, \quad \text{but} \quad \mu_{\sqrt{2}, \mathbb{Q}(\sqrt{2})}(x) = x - \sqrt{2}.$$

Example 4.2.4. Although $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1 + \sqrt{2})$, the minimal polynomials of $\sqrt{2}$ and $1 + \sqrt{2}$ over \mathbb{Q} are $x^2 - 2$ and $(x - 1)^2 - 2$ respectively. Polynomials are usually used in order to be provided as a computational tool, so we frequently want to find a suitable minimal polynomial for a given field extension. However, note that a finite simple extension does not specify only one minimal polynomial as the above example. It is enough to find only one minimal polynomial that is effective in computation.

4.2.1 Conjugates

Definition 4.2.2. Let E/F be a field extension and $\alpha, \beta \in E$ be algebraic over F . They are said to be *conjugate over F* if they share a common minimal polynomial over F .

In other words, conjugates share the maximal ideal $\ker(\text{eval})$, hence we get that $F(\alpha)$ and $F(\beta)$ are isomorphic. For the practical isomorphism map, we have the following theorem. It is also useful when we compute field automorphisms explicitly.

Theorem 4.2.2 (Conjugation isomorphism). *Let E/F be a field extension. Two elements $\alpha, \beta \in E$ are conjugate over F iff there is a field isomorphism $\phi : F(\alpha) \rightarrow F(\beta)$ such that*

$$\phi : \alpha \mapsto \beta \quad \text{and} \quad \phi|_F = \text{id}|_F.$$

Proof. (\Rightarrow) Let $\mu \in F[x]$ be the common minimal polynomial of α and β over F and define a map

$$\phi : F(\alpha) \xrightarrow{\sim} F[x]/(\mu) \xrightarrow{\sim} F(\beta) : \alpha \mapsto x + (\mu) \mapsto \beta.$$

Since it is clearly a field homomorphism and we can define the inverse in the same manner, so is an isomorphism. It is easy to check $\phi(\alpha) = \beta$ and $\phi|_F = \text{id}_F$. In particular, the two conditions uniquely determine ϕ .

(\Leftarrow) Suppose $\phi : F(\alpha) \rightarrow F(\beta) : \alpha \mapsto \beta$ is a field homomorphism fixing F . Then, ϕ commutes with a polynomial function with coefficients in F . From

$$\mu_{\alpha, F}(\beta) = \mu_{\alpha, F}(\phi(\alpha)) = \phi(\mu_{\alpha, F}(\alpha)) = \phi(0) = 0,$$

we get $\mu_{\beta, F} \mid \mu_{\alpha, F}$. The irreducibility of $\mu_{\alpha, F}$ implies $\mu_{\alpha, F} = \mu_{\beta, F}$. \square

Corollary 4.2.3. *Let $\phi : F \rightarrow F$ is a field automorphism. Then, α and $\phi(\alpha)$ are always conjugates.*

Example 4.2.5. The base fields are important. There are two conjugates of $\sqrt{2} \in \mathbb{C}$ over \mathbb{Q} : $\{\pm\sqrt{2}\}$. However, there is only one conjugate of $\sqrt{2}$ over $\mathbb{Q}(\sqrt{2})$ or \mathbb{C} : itself $\{\sqrt{2}\}$.

Example 4.2.6. There are two conjugates of $\omega = \frac{-1+\sqrt{-3}}{2} \in \mathbb{C}$ over \mathbb{Q} : $\{\omega, \bar{\omega} = \omega^{-1}\}$. It implies that there are at most two field automorphisms on $\mathbb{Q}(\omega)$ fixing \mathbb{Q} . In fact, there are exactly two; one is identity, and the other is the complex conjugation.

Example 4.2.7. For almost every case in applications, the number of conjugates is same as the degree of its minimal polynomial. However, there are counterexamples; two field isomorphisms $\phi_1 : \alpha \mapsto \beta_1$ and $\phi_2 : \alpha \mapsto \beta_2$ may be the same even for $\beta_1 \neq \beta_2$. See Section 3 for the detailed discussion.

Example 4.2.8. The isomorphism does not have to be an automorphism. There are four conjugates of $\sqrt[4]{2}$ over \mathbb{Q} : $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. However, $\mathbb{Q}(\sqrt[4]{2}) \neq \mathbb{Q}(i\sqrt[4]{2})$ even though they are isomorphic. See Section 4.

4.3 Algebraic extensions

Algebraic extension is a generalization of finite extensions, for instance, every finite extension is algebraic. In Galois theory, which will be studied later, we will not care elements that are not algebraic. Therefore, it is natural to think of a field extension that only consists of algebraic elements, which is called also algebraic. The main interests in Galois theory will be restricted to algebraic extensions. To people who know the category theory, an algebraic extension is just a direct limit of finite simple extensions.

Definition 4.3.1. A field extension E/F is called *algebraic* if all elements $\alpha \in E$ are algebraic over F .

The easiest example of an algebraic extension is a finite extension. The relations between finite extensions and algebraic extension are as follows.

Proposition 4.3.1. *For finite extensions and algebraic extensions, we have:*

- (a) *a finite extension is algebraic,*
- (b) *a simple algebraic extension is finite.*

Proof. Easy. □

Now, we are going to get some basic criteria for determining or constructing algebraic extensions. If summarized, we can just say any basic operations of algebraic extensions are algebraic. Before that, we introduce a good notion about algebraic extensions: the set of all algebraic elements in a given field.

In the rest of this subsection, assume that we have fixed a sufficiently large ambient field L . Restricting the “domain of discourse” by assuming a large entire field is a greatly helpful idea in order not to be confused in the theory of extensions.

For example, if we do not fix such a field L , we might be able to consider useless large fields which may grow without limits. Moreover, we cannot think about the number of field extensions satisfying particular properties.

Note that the following definition *depends on the choice of L* , and we will use it *only in this subsection*.

Definition 4.3.2. Let \overline{F} denote the set of all algebraic elements in L over F .

Proposition 4.3.2. The set \overline{F} of F in L is always a field.

Proof. An element is algebraic over F if and only if it is contained in a finite extension E/F because $\alpha \in E$ is equivalent to $F(\alpha) \leq E$.

Let $\alpha, \beta \in L$ be nonzero algebraic elements over a field F . Since $\alpha + \beta$, $\alpha\beta$, and α^{-1} are all in $F(\alpha, \beta)$, which is a finite extension of F with degree $\deg_F(\alpha)\deg_F(\beta)$, the set of algebraic elements over F in L is a field. \square

Remark. The field \overline{F} is called the *relative algebraic closure of F in L* . Since we have not defined algebraic closures yet, we will only adopt the notation. The reason of the word “relative” is explained later. Also, honestly, the notation \overline{F} is not so good that it is often used to represent an algebraic closure, not a relative one. We, however, proceed with this notation to grasp concepts of algebraic extensions.

Lemma 4.3.3. Let L be any field containing two fields E, F . Then,

- (a) $F \leq E$ implies $\overline{F} \leq \overline{E}$,
- (b) $\overline{\overline{F}} = \overline{F}$.

Proof. (a) Suppose $\alpha \in \overline{F}$ so that there is $f \in F[x]$ such that $f(\alpha) = 0$. Since $f \in F[x] \subset E[x]$, the element α is also algebraic over E , hence $\alpha \in \overline{E}$.

(b) It is enough to show $\overline{\overline{F}} \subset \overline{F}$. Let $\alpha \in \overline{\overline{F}}$ so that we can find $f \in \overline{F}[x]$ such that

$$f(\alpha) = \sum_{i=0}^n a_i \alpha^i = 0.$$

If we consider the field $E = F(a_0, \dots, a_n)$ of coefficients, then $f \in E[x]$. In other words, α is algebraic over E .

The field extension E/F is finite since all generators a_i are algebraic over F , and $E(\alpha)/E$ is also finite since α is algebraic over E . Therefore, the field extension $E(\alpha)/F$ is finite, and $F(\alpha)/F$ is also finite, hence the algebraicity of α over F . \square

Theorem 4.3.4. Let E/F be a field extension.

- (a) Fix any $L \geq E$. Then, E/F is algebraic iff $\overline{E} = \overline{F}$.
- (b) Let $F \leq K \leq E$. Then, E/F is algebraic iff E/K and K/F are algebraic.
- (c) The compositum E_1E_2/F is algebraic if E_1/F and E_2/F are algebraic.

Proof. (a) If E/F is algebraic, then $F \leq E \leq \overline{F}$ implies $\overline{F} \leq \overline{E} \leq \overline{\overline{F}} = \overline{F}$. Conversely, if $\overline{E} = \overline{F}$, then $\alpha \in E$ implies $\alpha \in E \leq \overline{E} = \overline{F}$, hence E is algebraic over F .

(b) Choose a big L . Since $\overline{E} \geq \overline{K} \geq \overline{F}$, we have $\overline{E} = \overline{F}$ iff $\overline{E} = \overline{K}$ and $\overline{K} = \overline{F}$.

(b') A direct proof uses the argument in the proof of above lemma as follows: if we take $\alpha \in E$ that is algebraic over K , and if a_i denotes the coefficients of $\mu_{\alpha, K}$, then the field extension $F(a_1, \dots, a_n, \alpha)/F$ is finite, so α is algebraic over F .

(c) Choose a big L . Since $E_1, E_2 \leq \overline{F}$, we have $E_1E_2 \leq \overline{F}$, so $\overline{E_1E_2} = \overline{F}$. \square

Remark. An algebraic extension is a direct limit of finite extensions. In other words, a field E is algebraic over F if and only if there is a tower of fields $\{K_\alpha\}_\alpha$ such that K_α/F are all finite and the ascending union is E . We skip the proof.

Example 4.3.1. For a transcendental number such as π , the extension $\mathbb{Q}(\pi)/\mathbb{Q}$ is not algebraic since it contains an element that is not algebraic. It is also because a simple extension is algebraic if and only if it is finite but $[\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$.

Example 4.3.2. Finite extensions are not only the algebraic extensions. For examples,

$$\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \dots), \quad \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)$$

are infinite algebraic extensions.

4.4 Algebraic closures

Algebraic closure is intuitively a maximal algebraic extension. It is well described using the notion of algebraically closed fields. Although the existence will be proved later, we give definitions.

4.4.1 Algebraically closed fields

Definition 4.4.1. A field F is called *algebraically closed* if it has no proper algebraic extension.

Proposition 4.4.1. For a field F , the following statements are all equivalent:

- (a) F is algebraically closed,
- (b) every polynomial in $F[x]$ has a root in F ,
- (c) every polynomial in $F[x]$ is linearly factorized in F ; every root is in F .

Proof. (a) \Rightarrow (b) If $f \in F[x]$ does not have root in F , then the proper finite extension $(F[x]/(f))/F$ shows that F is not algebraically closed.

(b) \Rightarrow (c) If f has a root α , then we can inductively apply this theorem for a new polynomial $f(x)/(x - \alpha)$ of a lower degree to make the complete linear factorization.

(c) \Rightarrow (a) If F is not algebraically closed so that there is a proper algebraic extension E/F , then the minimal polynomial $\alpha \in E \setminus F$ should be irreducible with degree bigger than 1. \square

Remark. In particular, this proposition implies that algebraically closedness can be described in itself by factorizations. Namely, it is an internal property; it is preserved under isomorphisms.

Definition 4.4.2. A field \bar{F} is called an *algebraic closure* of a field F if \bar{F} is algebraically closed field and \bar{F}/F is algebraic.

Proposition 4.4.2. Let E/F be a field extension with E algebraically closed. Then the set of all algebraic elements in E over F is the only algebraic closure of F contained in E .

Proof. For a while in this proof, let \bar{F} denote the set of all algebraic elements of F in E .

Step 1: Algebraic closure. We will show that \bar{F} is algebraically closed because the extension \bar{F}/F is clearly algebraic. Let $f \in \bar{F}[x]$ and take a root $\alpha \in E$. Since both $\bar{F}(\alpha)/\bar{F}$ and \bar{F}/F are algebraic, α is algebraic over F . Thus we have $\alpha \in \bar{F}$, and by the previous proposition, \bar{F} is algebraically closed.

Step 2: Uniqueness. Suppose K is an algebraic closure of F in E . We have $\bar{F} \leq K$ since every algebraic element α with $f(\alpha) = 0$ for $f \in F[x] \subset K[x]$ should be contained in K . Also, K/\bar{F} is algebraic because K/F is algebraic. Since \bar{F} is algebraically closed, $K = \bar{F}$. \square

This is a relation with relative algebraic closure: the relative algebraic closure in an algebraically closed field is really an algebraic closure. The proposition allows us to choose a standard algebraic closure when provided a large superfield like \mathbb{C} . In number theory, it is convenient for all algebraically closed fields to be considered that they are in \mathbb{C} .

Example 4.4.1. The set of all complex numbers \mathbb{C} is an algebraically closed field by the fundamental theorem of algebra.

Example 4.4.2. The set of all algebraic numbers (over \mathbb{Q}) is an algebraically closed field by the proposition above and is a subfield of \mathbb{C} .

4.4.2 Uniqueness and existence

Here is a useful lemma that allows to apply the axiom of choice to field theory.

4.6 (Isomorphism extension theorem). Let E/F be an algebraic extension. Let $\phi : F \cong F'$ be a field isomorphism. Let \overline{F}' be an algebraic closure of F' . Then, there is an embedding $\tilde{\phi} : E \rightarrow \overline{F}'$ which extends ϕ .

$$\begin{array}{ccc} & & \overline{F}' \\ & & \downarrow \\ E & \xrightarrow{\tilde{\phi}} & \\ \downarrow & & \downarrow \\ F & \xrightarrow{\phi} & F' \end{array}$$

Proof. Let S be the set of all pairs (K, ψ) of a subfield $K \leq E$ and a field homomorphism $\psi : K \rightarrow \overline{F}'$ which extends ϕ . The set S is nonempty since $\phi \in S$. It also satisfies the chain condition since the increasing union defines the upper bound of chain. Use the Zorn lemma on S to obtain a maximal element $\tilde{\phi} : K \rightarrow \overline{F}'$. We now claim $K = E$.

Suppose K is a proper subfield of E and let $\alpha \in E \setminus K$. Let $\alpha' \in \overline{F}'$ be a root of the pushforward polynomial $\phi_*(\mu_{\alpha, F}) \in F'[x]$. Then, we can construct a field homomorphism $K(\alpha) \rightarrow \overline{F}' : \alpha \mapsto \alpha'$. It leads a contradiction to the maximality of $\tilde{\phi}$. Therefore, $K = E$. \square

4.7 (Uniqueness of algebraic closure). Algebraic closure is unique up to isomorphism.

Proof. Suppose there are two algebraic closures $\overline{F}_1, \overline{F}_2$ of a field F . By the isomorphism extension theorem, we have a field homomorphism $\phi : \overline{F}_1 \rightarrow \overline{F}_2$ which extends the identity map on F . Since the image $\phi(F_1)$ is also algebraically closed and the field extension $\overline{F}_2/\phi(F_1)$ is algebraic, we must have $\phi(F_1) = \overline{F}_2$ by the definition of algebraically closedness. Thus, ϕ is surjective so that it is an isomorphism. \square

4.8 (Existence of algebraic closure). Every field has an algebraic closure.

Proof. Let F be a field.

Step 1: Construct an algebraically closed field containing F . At first we want to construct a field $K_1 \geq F$ such that every $f \in F[x]$ has a root in K_1 . This is satisfied by $K_1 := R/\mathfrak{m}$, where a ring R and its maximal ideal \mathfrak{m} is defined as follows: Let S be the set of all nonconstant irreducibles in $F[x]$. Define $R := F[\{x_f\}_{f \in S}]$. Let I be an ideal in R generated by $f(x_f)$ as f runs through all S . It has a maximal ideal $\mathfrak{m} \supset I$ in R since I does not contain constants. If $f \in F[x]$, then $\alpha = x_f + \mathfrak{m} \in K_1$ satisfies $f(\alpha) = f(x_f) + \mathfrak{m} = \mathfrak{m}$.

Construct a sequence $\{K_n\}_n$ of fields inductively such that every nonconstant $k \in K_n[x]$ has a root in K_{n+1} . Define $K := \lim_{\rightarrow} K_n$ as the inductive limit. It is in other word just the directed union of K_n through all $n \in \mathbb{N}$. Then, K is easily checked to be algebraically closed.

Step 2: Construct the algebraic closure of F . Let \overline{F} be the set of all algebraic elements of K over F . Then, this is an algebraic closure. \square

Remark. In fact, this K_1 is already algebraically closed, but it is hard to prove directly, so we are going to construct another algebraically closed field, K .

Exercises

4.9 (Minimal polynomials in a simple extension). Let $F(\alpha)/F$ be a finite simple extension of a field F and let $\beta \in F(\alpha)$. In light of elementary linear algebra,

Chapter 5

Separable extensions

5.1 Separable polynomials

Definition 5.1.1. Let F be a field. A polynomial $f \in F[x]$ is called *separable* if it is square-free in $\overline{F}[x]$. An element $\alpha \in \overline{F}$ is called *separable* over F if its minimal polynomial $\mu_{\alpha,F}$ is separable.

The separability of a polynomial does not depend on coefficient fields, but their characteristic. We can consider the algebraic closure of the smallest field containing coefficients of the polynomial and its characteristic when we check separability of a polynomial.

5.1 (Formal derivatives). Let $f \in F[x]$ for a field F such that

$$f(x) = \sum_{i=0}^n a_i x^i$$

The *formal derivative* of f is defined as a polynomial $f' \in F[x]$ such that

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

- (a) Formal derivatives satisfies the Leibniz rule.
- (b) If f is separable, then f and f' are coprime in F .
- (c) If f and f' are coprime in F , then f is separable.

Proof. (a)

(b) Suppose f and f' are not coprime in F so that they have a common factor, and let $\alpha \in \overline{F}$ be a root of the common factor. If we write

$$f(x) = (x - \alpha)g(x), \quad f'(x) = g(x) + (x - \alpha)g'(x)$$

for $g \in \overline{F}[x]$, then $g(\alpha) = 0$ implies $(x - \alpha) \mid g(x)$ in $\overline{F}[x]$. Hence $(x - \alpha)^2 \mid f(x)$ in $\overline{F}[x]$, so f is not separable.

(c) Suppose f is not separable. Then, there is $\alpha \in \overline{F}$ such that

$$f(x) = (x - \alpha)^m g(x), \quad f'(x) = m(x - \alpha)^{m-1}g(x) - (x - \alpha)^m g'(x)$$

for an integer $m \geq 2$ and $g \in \overline{F}[x]$. Since $f(\alpha) = f'(\alpha) = 0$, we get $\mu_{\alpha, F}(x) \mid \gcd(f(x), f'(x))$ in $F[x]$. \square

5.2 (Perfect fields). A *perfect field* is a field over which every irreducible is separable. Let F be a field of characteristic p .

(a) If $p = 0$, then F is perfect.

(b) If $p > 0$, then F is perfect if and only if the Frobenius homomorphism is an automorphism.

Proof. (a) Let $f \in F[x]$ be an irreducible of degree n . Notice that f and g are not coprime iff $f \mid g$. Since F has characteristic 0, f' has degree $n - 1$ and is nonzero, so we have $f \nmid f'$. Hence f is separable.

(b) (\Leftarrow) Let $f \in F[x]$ be an inseparable irreducible. Since we must have $f' = 0$ by the irreducibility of f , we can find $g \in F[x]$ such that $f(x) = g(x^p)$. The coefficients of g are p -powers of elements of F , so there is $h \in F[x]$ such that $g(x^p) = h(x)^p$. It is a contradiction to the irreducibility of f . \square

Proposition 5.1.1. Let F be a field of characteristic $p > 0$. For an irreducible $f \in F[x]$, there is a unique separable irreducible $f_{\text{sep}} \in F[x]$ such that $f(x) = f_{\text{sep}}(x^{p^k})$ for some k .

Example 5.1.1. The Frobenius endomorphism is not surjective in the field of rational functions $\mathbb{F}_p(t)$, where t is not algebraic over \mathbb{F}_p . For example, t is not in the image of $\mathbb{F}_p(t) \rightarrow \mathbb{F}_p(t) : x \mapsto x^p$. Then, the polynomial $x^p - t \in \mathbb{F}_p(t)[x]$ is inseparable irreducible since it is factorized as

$$x^p - t = (x - t^{\frac{1}{p}})^p$$

in $\overline{\mathbb{F}_p(t)}[x]$.

5.2 Separable extensions

Definition 5.2.1. A field extension E/F is called *separable* if all elements in E is separable over F .

Theorem 5.2.1 (Primitive element theorem). *A finite separable extension is simple.*

5.3 Separable closures

Definition 5.3.1. Let E/F be a field extension. The *separable degree* of E/F is the number $[\bar{F}^{\text{sep}} : F]$.

Theorem 5.3.1. *The separable degree of a field extension E/F is the number of field embeddings $E \hookrightarrow \bar{F}$ fixing F .*

Lemma 5.3.2. *All roots of an irreducible polynomial has same multiplicity.*

Proof.

□

Theorem 5.3.3. *Let K be an intermediate field of a finite extension E/F . Then,*

$$[E : F]_{\text{sep}} \mid [E : F]$$

Proof.

□

Theorem 5.3.4. *A finite field extension E/F is separable if and only if*

$$[E : F]_{\text{sep}} = [E : F].$$

Proof.

□

multiplication formula

Chapter 6

Normal extensions

6.1 Normal extensions

6.2 Galois correspondence

6.1 (Automorphism groups). (a) $|\text{Aut}(E/F)| \leq [E : F]$.

6.2 (Fixed fields). Galois descent..?

(a) $[E : \text{Fix}_E(H)] \leq |H|$.

6.3 (Galois correspondence). Let E/F be an algebraic extension and $G := \text{Aut}(E/F)$. Define a map

$$\begin{aligned} \text{Aut}(E/-) : \{ \text{subextensions of } E/F \} &\rightarrow \{ \text{subgroups of } G \} \\ K &\mapsto \text{Aut}(E/K) \end{aligned}$$

(a) $K \leq \text{Fix}_E(\text{Aut}(E/K))$ and $H \leq \text{Aut}(E/\text{Fix}_E(H))$.

(b) The map $\text{Aut}(E/-)$ is surjective onto finite subgroups of G .

(c) The map $\text{Aut}(E/-)$ is injective if E/F is normal and separable.

(d) If E/F is finite and Galois, then the map $\text{Aut}(E/-)$ is bijective.

Part III

Galois groups

Chapter 7

Generators of Galois groups

reducible polynomials semidirect product

7.1 (Transitive subgroups of symmetric groups).

7.2 (Double quadratic equations).

7.3 (Reciprocal equations). palindromic

7.4 (Imaginary roots). number of imaginary roots= $2n$: composition of n transpositions

Chapter 8

Invariants of Galois groups

8.1 Resultants

8.2 Resolvent polynomials

8.1 (Discriminant of a polynomial).

8.2 (Irreducible cubic).

8.3 (Irreducible quartic).

8.4 (Irreducible quintic).

Let E be the splitting of a separable irreducible f over a field F and $G := \text{Gal}(E/F)$.

Theorem 8.2.1. *There are only five isomorphic types of transitive subgroups of the symmetric group S_4 .*

Corollary 8.2.2. $G \cong S_4, A_4, D_4, V_4, \text{ or } C_4$.

Proposition 8.2.3. *Two groups A_4 and V_4 are only transitive normal subgroups of S_4 .*

Now we define our resolvent polynomial.

Proposition 8.2.4. *Let $H := G \cap V_4$ and $K := \text{Fix}_E(H)$. Then,*

$$K = F(\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3).$$

Definition 8.2.1. Let K be the fixed field of H . A *resolvent cubic* is a cubic R_3 that has K as the splitting field over F .

Theorem 8.2.5. *We have*

- (a) $G \cong S_4$ if R_3 is irreducible and ,
- (b) $G \cong A_4$ if R_3 is irreducible and ,
- (c) $G \cong D_4$ if R_3 has only one root in K and f is irreducible over K ,
- (d) $G \cong C_4$ if R_3 has only one root in K and f is reducible over K ,
- (e) $G \cong V_4$ if R_3 splits in K .

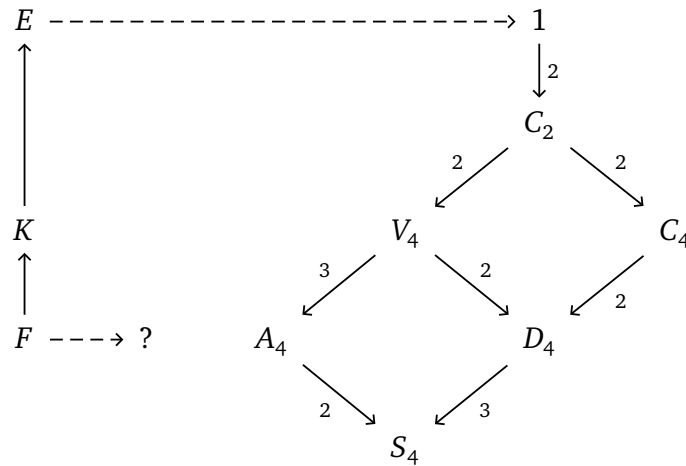
Proof. There are five possible cases:

$$(G, H) = (S_4, V_4), (A_4, V_4), (D_4, V_4), (V_4, V_4), (C_4, C_2).$$

We have

$$[K : F] = |G/H|, \quad [E : K] = |H|.$$

If f is reducible over K , then $\text{Gal}(E/K)$ is no more a transitive subgroup of S_4 so that $H \neq V_4$ and $G \cong C_4$. □



Chapter 9

Reduction of Galois groups

9.1 Finite fields

9.1 (Finite field as a splitting field). Let E be a finite field of characteristic p . Clearly $p > 0$ so that E has a subfield F of size p generated by $1 \in E$. Since E/F is finite, E is isomorphic to a subfield of $\overline{\mathbb{F}_p}$ by the isomorphism extension theorem. There we assume E is a subfield of a fixed algebraic closure $\overline{\mathbb{F}_p}$. Let $\alpha \in \overline{\mathbb{F}_p}$ and n the degree of E/F .

- (a) If $\alpha \in E$, then $\alpha^{p^n} - \alpha = 0$.
- (b) If $\alpha^{p^n} - \alpha = 0$, then $\alpha \in E$.
- (c) For each $m \in \mathbb{N}$, in $\overline{\mathbb{F}_p}$ is a unique field E of size p^m .

9.2 (Irreducibles over \mathbb{F}_p). the number of irreducibles, finite extension over a finite field is simple.

9.3 (Degree of an element in finite fields). Let $\alpha \in \overline{\mathbb{F}_p}$. The degree of α is computed by the order of p in $(\mathbb{Z}/\text{ord}(\alpha)\mathbb{Z})^\times$

9.4 (Cyclic groups in finite fields). (a) The number of elements of order d in a cyclic group of order n is $\phi(d)$ when $d \mid n$.

- (b) The group of units $(\mathbb{F}_{p^n})^\times$ is cyclic.
- (c) The Galois group $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic.

Proof. (b) We partition the elements of $G := (\mathbb{F}_{p^n})^\times$ by their orders. Let

$$A_d := \{ \alpha \in G : \text{ord}(\alpha) = d \}$$

for $d \mid p^n - 1$. It is contained in the subgroup $H := \{x \in \mathbb{F}_{p^n} : x^d = 1\}$, of which the order is $|H| = d$ because $x^d - 1$ is separable.

If $|A_d| \neq 0$, then any element of A_d is a generator of H , so H is cyclic. Since the number of elements of order d in a cyclic group is given by the Euler totient function $\phi(d)$, as a result we have $|A_d| \in \{0, \phi(d)\}$. Then,

$$|G| = \sum_{d \mid p^n - 1} |A_d| \leq \sum_{d \mid p^n - 1} \phi(d) = p^n - 1$$

implies $|A_{p^n - 1}| \neq 0$, G is hence cyclic. □

9.2 Ramification theory

9.3 The Dedekind theorem

Part IV

Insolvability of the quintic

Chapter 10

Cyclic extensions

Chapter 11

Cyclotomic extensions

11.1 Cyclotomic polynomials

11.1 (Cyclotomic polynomials). Let ζ be a primitive n th root of unity. The n th cyclotomic polynomial is defined by

$$\Phi_n(x) = \prod_{\substack{1 \leq i \leq n \\ (i,n)=1}} (x - \zeta^i).$$

- (a) $x^n = \prod_{d|n} \Phi_d(x)$.
- (b) $\Phi_n(x) \in \mathbb{Z}[x]$.
- (c) $\Phi_n(x)$ is irreducible over \mathbb{Q} .

Proof. (b) Induction, division algorithm implies $\Phi_n(x) \in \mathbb{Q}[x]$. Gauss' lemma implies $\Phi_n(x) \in \mathbb{Z}[x]$.

- (c) We first prove ζ^p are all conjugates for any prime p not dividing n . \square

11.2 (Computation of cyclotomic polynomials).

11.2 Kummer theory

Chapter 12

Radical extensions