Galois Theory

Ikhan Choi

April 15, 2025

Contents

Part I

Finite group theory

Chapter 1

Extension theory

1.1 Semidirect product

1.1 (Semidirect product)**.** Let N, H be groups, and let $\varphi : H \to \mathrm{Aut}(N)$ be a group homomorphism. The homomorphism φ can be considered as the permutation representation of a group action $H \times N \to N$ by automorphism. The *semidirect product*, written as $N \rtimes_\varphi H$ or just simply $N \rtimes H$ if no confusion, is a group defined on the set $N \times H$ by

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

(a) The semidirect product $N \rtimes H$ is really a group.

(b) If N, H are subgroups of another group G such that

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

then $G \cong N \rtimes_\varphi H$, where $\varphi(h) : n \mapsto hnh^{-1}$. In this case, we sometimes call G the *internal semidirect product*.

1.2 (Classification of semidirect products)**.** Let N and H be groups. On the set $\mathrm{Hom}(H, \mathrm{Aut}(N))$ of all group homomorphisms $H \to \mathrm{Aut}(N)$, we can establish an action by the group $\mathrm{Aut}(H) \times \mathrm{Aut}(N)$ with the following two operations: the *twisting* by $\eta \in \mathrm{Aut}(H)$ such that $\varphi \mapsto \varphi \circ \eta$, and the *intertwining* by $\nu \in \mathrm{Aut}(N)$ such that $\varphi \mapsto \nu\varphi\nu^{-1}$. Consider the following map from the orbit space, constructed by the definition of semidirect products:

$$\begin{array}{ccc} \dfrac{\mathrm{Hom}(H,\mathrm{Aut}(N))}{\mathrm{Aut}(H)\times\mathrm{Aut}(N)} & \to & \left\{ \begin{array}{c} \text{isomorphism classes of} \\ \text{semidirect products } N \rtimes H \end{array} \right\} \\ \varphi & \mapsto & N \rtimes_\varphi H. \end{array}$$

Also, we can define a map which takes images:

$$\begin{array}{ccc} \dfrac{\mathrm{Hom}(H,\mathrm{Aut}(N))}{\mathrm{Aut}(H)\times\mathrm{Aut}(N)} & \to & \left\{ \begin{array}{c} \text{conjugacy classes of} \\ \text{subgroups of } \mathrm{Aut}(N) \end{array} \right\} \\ \varphi & \mapsto & \mathrm{im}\,\varphi. \end{array}$$

(a) The first map is well-defined and surjective.

(b) The first map is injective if $|N|$ and $|H|$ are finite and relatively prime.

(c) The second map is injective if

Proof. (a)

(b)

(c) Assuming $\varphi_1(H) = \varphi_2(H)$, we claim $\varphi_2 = \varphi_1 \circ \eta$ for some $\eta \in \mathrm{Aut}(H)$.

Since $\varphi_1(H)$ is cyclic, □

1.2 Group extensions

1.3. Let N and H be groups. The following objects have one-to-one correspondences among each other.

(a) Isomorphic types of groups G such that a sequence $0 \to N \to G \to H \to 0$ 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 homomorphisms $H \to \mathrm{Aut}(N)$...?

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

$0 \to F \to E \to G \to 0$ Four data $G, F, \varphi : G \to \mathrm{Aut}(F), c : G \times G \to F$ completely determine the extension E.

Suppose we have an extension $F \to E \to G$. There is a *set-theoretic section* $s : G \to E$. 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* $\varphi : G \to \mathrm{Aut}(F)$ independently on sections.

Definition of *2-cocycle* c: It is a *set-theoretic function* $c : G \times G \to F$ 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 $G \times G \to F$ 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.

1.4 (Central extension)**.** For an abelian normal subgroup A of G, a homomorphism $G/C_G(A) \to \mathrm{Aut}(A)$ factors though G/A. If it has trivial image, then A is central.

Group cohomology

The category of G-modules can be identified with the category of $\mathbb{Z}[G]$-modules, which is abelian.

Let M be a G-module. The *invariant submodule* of M is denoted by M^G. Sending M to M^G yields a functor Grp $\to$ Ab, which is left exact but not right exact in general. Then we can consider the right derived functor to define cohomology groups. Let us do this concretely.

Let M be a G-module. Define $C^n(G,M)$ be the abelian group of all functions $G^n \to M$. The coboundary homomorphism $d : C^n(G,M) \to C^{n+1}(G,M)$ is defined such that

$$d\varphi(g_1, \cdots, g_{n+1}) := g_1\varphi(g_2, \cdots, g_{n+1}) + \sum_{i=1}^{n}(-1)^i\varphi(g_1, \cdots, g_{i-1}, g_ig_{i+1}, g_{i+2}, \cdots, g_{n+1}) + (-1)^{n+1}\varphi(g_1, \cdots, g_n).$$

$$H^0(G,M) = M^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M).$$

For $x \in C^0(G,M) = M$, $dx(g) = gx - x$. For $\varphi \in C^1(G,M)$, $d\varphi(g,h) = g\varphi(h) - \varphi(gh) + \varphi(g)$.

1.3 Subnormal series

Holder program solvable group nilpotent group central series abelianization

Exercises

1.5 (Wreath product).

Problems

Chapter 2

Sylow theory

2.1 Sylow subgroups

2.1 (Existence of Sylow subgroups). Two proofs:

Proof. (a) Suppose $\mathrm{Syl}_p(G) \neq \varnothing$ 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 $Q \in \mathrm{Syl}_p(G/P_p)$, the inverse image of Q under the projection $G \to G/P_p$ 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 $\mathrm{Syl}_p(C_G(g)) \subset \mathrm{Syl}_p(G)$. Then, we are done by induction.

(Wielandt) We use the lemma $\binom{p^a m}{p^a} \equiv m \pmod p$..? Let $|G| = p^{a+b}m$. Let $\mathcal{S}$ be the set of all subsets of G with size p^a. Give $G \to \mathrm{Sym}(\mathcal{S})$ by left multiplication. Since

$$\nu_p(|S|) = \nu_p(\binom{p^a(p^b m)}{p^a}) = b,$$

there is an orbit $\mathcal{O} \subset \mathcal{S}$ such that $\nu_p(|\mathcal{O}|) \leq b$. We have transitive action $G \to \mathrm{Sym}(\mathcal{O})$ and the stabilizer H satisfies $p^a \mid \frac{|G|}{|\mathcal{O}|} = |H|$. Since $H \to \mathrm{Sym}(\mathcal{O})$ trivially, $H \to \mathrm{Sym}(A)$ for $A \in \mathcal{O} \subset \mathcal{S}$. It is only possible when $H \subset A$, hence $|H| = p^a$. $\square$

2.2 (Number of Sylow subgroups). 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 by $\mathrm{Syl}_p(G)$ the set of Sylow p-subgroups and by $n_p(G)$ its cardinality.

(a) If P normalizes P', then $P = P'$.

(b) $n_p \equiv 1 \pmod p$.

(c) $n_p \mid m$.

Proof. (a) $P \leq N_G(P')$ implies

$$\frac{P}{P \cap P'} \cong \frac{PP'}{P'} \leq \frac{N_G(P')}{P'}.$$

(b) For $P \in \mathrm{Syl}_p(G)$, the class equation for the action of P on $\mathrm{Syl}_p(G)$ 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. 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 $P, P' \in \mathrm{Syl}_p(G)$ that are not conjugate. The class equations for actions of P and P' on $\mathrm{Orb}_G(P) \subset \mathrm{Syl}_p(G)$ are

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

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

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

for all $P \in \mathrm{Syl}_p(G)$. □

(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 paricular 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 p-groups

2.3 (p-groups)**.** (a) A nontrivial normalizer of a p-group meets its center out of identity.

(b) A proper subgroup of a finite p-group is a proper subgroup of its normalizer. In particular, every finite p-group is nilpotent.

2.3 Small groups

2.4 (Classification of groups of order pq)**.**

2.5 (Classification of groups of order p^2)**.**

2.6 (Classification of groups of order pqr)**.**

2.7 (Classification of groups of order p^2q). Let G be a finite group of order p^2q, where p and q are distinct primes. If we let P and Q be Sylow p and q-subgroup of G, then $P \cong Z_{p^2}$ or Z_p^2, and $Q \cong Z_q$. By the Sylow theorem, we consider three cases:

(a) If $p + 2 \le q$, then $G \cong Q \rtimes P$, and there are

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

non-isomorphic groups of order p^2q.

(b) If $p > q$, then $G \cong P \rtimes Q$, and there are

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

non-isomorphic groups of order p^2q

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

Proof. (a) $G \cong Z_q \rtimes Z_{p^2}$.

$$\varphi : Z_{p^2} \to Z_{q-1}.$$

There are $1 + \min\{v_p(q-1), 2\}$ (conjugacy classes of) subgroups of order dividing p^2 in Z_{q-1}.

(b) $G \cong Z_q \rtimes Z_p^2$.

$$\varphi : Z_p^2 \to Z_{q-1}.$$

Since $\mathrm{Aut}(Z_p^2) \cong \mathrm{GL}(2, \mathbb{F}_p)$ transitively acts on the set of surjective homomorphisms $Z_p^2 \to Z_p$ by twist, there are $1 + \min\{v_p(q-1), 1\}$ cases.

(c) $G \cong Z_{p^2} \rtimes Z_q$.

$$\varphi : Z_q \to Z_{p(p-1)}.$$

There are $1 + \min\{v_q(p-1), 1\}$ (conjugacy classes of) subgroups of order dividing q in $Z_{p(p-1)}$.

(d) $G \cong Z_p^2 \rtimes Z_q$.

$$\varphi : Z_q \to \mathrm{GL}(2, \mathbb{F}_p).$$

To compute the number of non-trivial semidirect products, we will find all the conjugacy classes of subgroups of $\mathrm{GL}(2, \mathbb{F}_p)$ with order q. Note that $|\mathrm{GL}(2, \mathbb{F}_p)| = (p^2 - 1)(p^2 - p) = (p-1)^2 p(p+1)$ so that we must have $q \mid p - 1$ or $q \mid p + 1$.

Let $q = 2$. Then

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

up to conjugation, and they generate distinct subgroups of $\mathrm{GL}(2, \mathbb{F}_p)$ up to conjugation.

Let $q \ne 2$ and $q \mid p + 1$. We claim that there is a unique subgroup of order q in $\mathrm{GL}_2(\mathbb{F}_p)$ up to conjugation. Let $A \in \mathrm{GL}(2, \mathbb{F}_p)$ be of order q, and $\lambda^{\pm 1} \in \overline{\mathbb{F}}_p$ 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 $0 \le i < q$. 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, Let $q \neq 2$ 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 $\mathrm{GL}_2(\mathbb{F}_p)$. (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)

$\square$

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

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

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

$\lvert G\rvert = pqr$	30	42
# of groups	4	6

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

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

2.4 Finite simple groups

Exercises

2.9 (Hall subgroups).

Problems

1. Show that if p is the smallest prime factor of the order of a finite group G, and if G has a cyclic normal Sylow p-subgroup P, then $P \leq Z(G)$.
2. Show that the number of Sylow p-subgroups of $\mathrm{SL}_3(\mathbb{F}_p)$ is $(p^2+p+1)(p+1)$.

Chapter 3

Group presentations

3.1 Free groups

3.2 Coset enumeration

3.1 (Todd-Coxeter algorithm).

3.2 (Knuth-Bendixon algorithm).

3.3 (Computing order from its group presentation).

3.3 Coxeter groups

Part II

Field theory

Chapter 4

Field extensions

4.1 Algebraic extensions

4.1 (Field extensions)**.** Vector space structures and degree, Finite extensions, Simple extensions, straightedge and compass construction

4.2 (Algebraic elements)**.** Let E/F be a field extension and let $\alpha \in E$. Let $I(\alpha)$ be the set of all $f \in F[x]$ such that $f(\alpha) = 0$. It is equal to the kernel of the evaluation homomorphism $\mathrm{ev}_\alpha : F[x] \to F[\alpha] : f \mapsto f(\alpha)$, which is surjective. We say α is *algebraic* over F if $I(\alpha)$ contains a non-zero polynomial, and call it *transcendental* over F if it is not.

If α is algebraic over F, then since the quotient $F[x]/I(\alpha) \cong F[\alpha]$ is an integral domain and $F[x]$ is a principal ideal domain, the non-zero prime ideal $I(\alpha)$ is maximal so that it has a unique monic irreducible generator $\mu_{\alpha,F} \in F[x]$, called the *minimal polynomial* of α over F.

Two algebraic elements $\alpha, \beta \in E$ over F are said to be *conjugate* over F if they share the common minimal polynomial.

(a) α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite, and moreover we have the degree formula $[F(\alpha) : F] = \deg \mu_{\alpha,F}$.

(b) $\alpha, \beta \in E$ are conjugate over F if and only if there is a (unique) field isomorphism $\phi : F(\alpha) \to F(\beta)$ such that $\phi(\alpha) = \beta$ and ϕ fixes F.

Proof. (a) If α is algebraic over F, then since $I(\alpha)$ is maximal in $F[x]$, the quotient $F[\alpha]$ is a field, and hence $F[\alpha] = F(\alpha)$. Fix any non-zero $f \in I(\alpha)$. If we take an arbitrary element $g(\alpha) \in F(\alpha) = F[\alpha]$ for some $g \in F[x]$, then by the Euclidean algorithm in $F[x]$, there exist $q, r \in F[x]$ such that $g = qf + r$ and $\deg r < \deg f$, so $g(\alpha) = q(\alpha)f(\alpha) + r(\alpha) = r(\alpha)$ is a linear combination of $\{1, \alpha, \cdots, \alpha^{\deg f - 1}\}$ over F. Thus we have $[F(\alpha) : F] \leq \deg f$.

Conversely, if $[F(\alpha) : F] < \infty$, then there is a linearly dependent finite subset over F of an infinite set $\{1, \alpha, \alpha^2, \cdots\} \subset F(\alpha)$. The coefficients on the linear dependency relation construct a non-zero polynomial in $I(\alpha)$.

For the degrees, since $F[x]/(\mu_{\alpha,F}) \cong F(\alpha)$, the claim follows from that $\{1, x, \cdots, x^{\deg \mu_{\alpha,F} - 1}\}$ is a basis, which can be checked with the Euclidean algorithm.

(b) Let $\mu \in F[x]$ be the common minimal polynomial of α and β over F and consider a field isomorphism

$$\phi : F(\alpha) \to F[x]/(\mu) \to F(\beta) : \alpha \mapsto x + (\mu) \mapsto \beta.$$

It is easy to check that $\phi(\alpha) = \beta$ and ϕ fixes F. The uniqueness is clear.

Conversely, suppose $\phi : F(\alpha) \to F(\beta) : \alpha \mapsto \beta$ is a field isomomorphism 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 $\mu_{\alpha,F} = \mu_{\beta,F}$. □

4.3 (Algebraic extensions)**.** A field extension E/F is called *algebraic* if every element of E is algebraic over F.

(a) A finite extension is algebraic.

(b) A simple algebraic extension is finite.

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

Proposition 4.1.2. *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 $F(\alpha) \leq E$.

□

4.4 (Algebraically closed field)**.** An *algebraically closed* field is a field that has no proper algebraic extension. For a field F, the following statements are all equivalent, and in particular, a field isomorphic to an algebraically closed field is algebraiclly closed:

(a) F is algebraically closed if and only if every polynomial in $F[x]$ has a root in F, or equivalently, every polynomial in $F[x]$ is linearly factorized in F. In other words, every root is in F.

Proof. (a) ⇒ (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) ⇒ (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) ⇒ (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. □

4.5 (Algebraic closure)**.** A field $\overline{F}$ is called an *algebraic closure* of a field F if $\overline{F}$ is algebraically closed field and $\overline{F}/F$ is algebraic. Let E/F be a field extension with E algebraically closed. Denote by $\overline{F}$ the set of all algebraic elements in E over F

(a) $\overline{F}$ is a field.

(b) $\overline{F}$ is an algebraic closure of F.

Proof. (a) Let $\alpha, \beta \in \overline{F}$. Since $\alpha + \beta$, $\alpha\beta$, and α^{-1} are all in $F(\alpha, \beta)$, which is a finite extension of F with degree $\deg_F(\alpha)\deg_F(\beta)$, we are done.

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

4.6 (Relations of algebraic extensions)**.** Let E/F be a field extension.

(a) $F \leq E$ implies $\overline{F} \leq \overline{E}$,

(b) $\overline{\overline{F}} = \overline{F}$.

(c) Fix any $L \geq E$. Then, E/F is algebraic iff $\overline{E} = \overline{F}$.

(d) Let $F \leq K \leq E$. Then, E/F is algebraic iff E/K and K/F are algebraic.

(e) The compositum E_1E_2/F is algebriac if E_1/F and E_2/F are algebraic.

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 $E = F(a_0, \cdots, a_n)$ 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.

(c) 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.

(d) 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 $\overline{K} = \overline{F}$.

(d') 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 $F(a_1, \cdots, a_n, \alpha)/F$ is finite, so α is algebriac over F.

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

4.7 (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 $\widetilde{\phi} : E \to \overline{F}'$ which extends ϕ.

$$\begin{tikzcd}
 & \overline{F}' \arrow[dd] \\
E \arrow[r, "\widetilde{\phi}"] \arrow[d, dashed] & {} \\
F \arrow[r, "\phi"] & F'
\end{tikzcd}$$

Proof. Let S be the set of all pairs (K, ψ) of a subfield $K \leq E$ and a field homomorphism $\psi : K \to \overline{F}'$ 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 $\widetilde{\phi} : K \to \overline{F}'$. 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 $K(\alpha) \to \overline{F}' : \alpha \mapsto \alpha'$. It leads a contradiction to the maximality of $\widetilde{\phi}$. Therefore, $K = E$. $\square$

4.8 (Algebraic closures). (a) An algebraic closure is unique up to isomorphism.

(b) Every field has an algebraic closure.

Proof. (a) 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 $\phi : \overline{F}_1 \to \overline{F}_2$ which extends the identitiy map on F. Since the image $\phi(F_1)$ is also algebraically closed and the field extension $F_2/\phi(F_1)$ is algebraic, we must have $\phi(F_1) = F_2$ by the definition of algebraically closedness. Thus, ϕ is surjective so that it is an isomorphism.

(b) Let F be a field.

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 $K := \lim_{\to} K_n$ 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.

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.

As a remark, in fact, this K_1 is already algebraically closed. Since it is difficult to prove directly, so we constructed an algebraically closed field K in another way. $\square$

4.2 Finite fields

4.9 (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.

4.10 (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 $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic.*

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

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

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. $\square$

4.11 (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 $(\mathbb{Z}/\operatorname{ord}(\alpha)\mathbb{Z})^\times$

4.3 Separable extensions

4.12 (Separable polynomials). 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 base 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.

4.13 (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 has a common factor, and let $\alpha \in \overline{F}$ be a root of the common factor. If we write

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

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

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

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 $F[x]$. $\square$

4.14 (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. $\square$

4.15. 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 4.3.1. 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 $\mathbb{F}_p(t) \to \mathbb{F}_p(t) : x \mapsto x^p$. 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 $\overline{\mathbb{F}_p(t)}[x]$.

4.16 (Separable extensions)**.** A field extension E/F is called *separable* if all elements in E is separable over F.

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

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

(a) The separable degree of a field extension E/F is the number of field embeddings $E \hookrightarrow \overline{F}$ fixing F.

(b) All roots of an irreducible polynomial has same multiplicity.

(c) Let K be an intermediate field of a finite extension E/F. Then,

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

(d) A finite field extension E/F is separable if and only if

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

multiplcation formula

4.4 Normal extensions

4.19 (Splitting fields)**.**

4.20 (Automorphism groups)**.** (a) $|\mathrm{Aut}(E/F)| \leq [E : F]$.

4.21 (Fixed fields)**.** Galois descent..?

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

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

$$\begin{array}{ccc} \{\text{subextensions of } E/F\} & \to & \{\text{subgroups of } G\} \\ K & \mapsto & \mathrm{Aut}(E/K) \end{array}$$

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

(b) The map is surjective onto finite subgroups of G.

(c) The map is injective if E/F is normal and separable.

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

reducible polynomials semidirect product

4.23 (Galois groups of binomials)**.**

$$f(x) = x^n - a$$

4.24 (Galois groups of biquadratics)**.** Let $f \in K[x]$ be

$$f(x) = x^4 + ax^2 + b$$

with $a \neq 0$,..? Let

$$\alpha := \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \quad \beta := \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

where $\sqrt{b^2 - 4ac}$ denotes a root of the polynomial $x^2 - (b^2 - 4ac)$. Then, they satisfies $\alpha + \beta = -b/a \in K$ and $\alpha\beta = c/a \in K$. So the splitting field L is $L = K(\alpha)$.

4.25 (Galois groups of palindromics)**.** If α is a root, then $\alpha^{\pm 1}$ are conjugate. palindromic

4.26 (Imaginary roots)**.** number of imaginary roots=2n: composition of n transpositions

Exercises

Example 4.4.1. 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 4.4.2. Finite extensions are not only the algebraic extensions. For examples,

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

are infinite algebraic extensions.

Example 4.4.3. $\pm\sqrt{2}$ are conjugate over $\mathbb{Q}$, but not over $\mathbb{C}$.

There are two, one, two field automorphisms of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, respectively.

4.27 (Straightedge and compass construction)**.** Regular n-gon Gauss-Wantzel theorem

(a) The regular heptagon is not constructible.

Proof. Let $\zeta = \zeta_7$. Then, $\zeta + \zeta^{-1}$ has the minimal polynomial $x^3 + x^2 - 2x - 1$. □

4.28 (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,

4.29. $\mathbb{Q}[x]/(x^2 - 2) \cong \mathbb{Q}[x]/(x^2 - 2x - 1)$.

4.30 (Dimension argument)**.** 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.

4.31 (Algebraic closure of $\mathbb{Q}$)**.** It is well-known fact that the set of all complex numbers $\mathbb{C}$ is an algebraically closed field; it is the fundamental theorem of algebra. The set of all algebraic numbers over $\mathbb{Q}$ is an algebraically closed subfield of $\mathbb{C}$.

(a) $\overline{\mathbb{Q}}$ is countable.

$x^6 + x^3 + 1$,

Problems

1. If $K/\mathbb{Q}$ be a Galois extension of Galois group isomorphic to S_5, then K is the splitting field of a quintic over $\mathbb{Q}$.

Chapter 5

Galois groups

5.1 Galois descent

5.2 Invariants of Galois groups

Resultants

Resolvent polynomials

5.1 (Transitive subgroups of symmetric groups).

5.2 (Discriminant of a polynomial).

5.3 (Irreducible cubic).

5.4 (Irreducible quartic).

5.5 (Irreducible quintic).

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

Theorem 5.2.1. *There are only five isomorphic types of transitive subgroups of the symmetric group S_4.*

Corollary 5.2.2. *$G \cong S_4,\ A_4,\ D_4,\ V_4,$ or C_4.*

Proposition 5.2.3. *Two groups A_4 and V_4 are only transitive normal subgroups of S_4.*

Now we define our resolvent polynomial.

Proposition 5.2.4. *Let $H := G \cap V_4$ and $K := \mathrm{Fix}_E(H)$. 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 5.2.5. 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 5.2.6. *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

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

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

$$\begin{tikzcd}
E \arrow[rrrr, dashed] & & & & 1 \arrow[d, "2"] & \\
& & & & C_2 \arrow[dl, "2"'] \arrow[dr, "2"] & \\
K \arrow[uu] & & & V_4 \arrow[dl, "3"'] \arrow[dr, "2"] & & C_4 \arrow[dl, "2"] \\
F \arrow[u] \arrow[r, dashed] & ? & A_4 \arrow[dr, "2"'] & & D_4 \arrow[dl, "3"] & \\
& & & S_4 & &
\end{tikzcd}$$

5.3 Reduction of Galois groups

Integral extensions

5.6 (Algebraic integers)**.** A (algebraic) *number field* is a finite extension K of $\mathbb{Q}$. We say an element $\alpha \in K$ is *integral* if there is a monic polynomial $f \in \mathbb{Z}[x]$ such that $f(\alpha) = 0$.

5.7 (Integral extensions)**.** Let A be a subring of a ring B. An element $b \in B$ is called *integral* over A if there is a monic polynomial $f \in A[x]$ such that $f(b) = 0$. The ring B is called an *integral* extension over A if every element is integral over A. The *integral closure* of A in B is the set of all integral elements over A in B.

(a) $b \in B$ is integral over A if and only if $A[b]$ is a finitely generated module.

(b) The integral closure of A in B is a subring of B.

(c) An integral extension over an integral extension is integral.

Proof. (a) ($\Rightarrow$) Let $g \in A[x]$ be a monic polynomial such that $g(b) = 0$. For every element $f(b) \in A[b]$, since g is monic, we have

$$f(x) = g(x)q(x) + r(x)$$

for $q, r \in A[x]$. $\square$

5.8 (Traces and norms)**.** Let L/K be a field extension. For each $\alpha \in L$ we can define a K-linear endomorphism $M_\alpha : L \to L$ by $M_\alpha(\beta) := \alpha\beta$. Then, the *trace* is a K-linear functional $\mathrm{Tr}_{L/K} : L \to K$ defined by

$$\mathrm{Tr}_{L/K}(\alpha) := \mathrm{Tr}(M_\alpha),$$

and the *norm* is a multiplicative group homomorphism $N_{L/K} : L^\times \to K^\times$ defined by

$$N_{L/K}(\alpha) := \det(M_\alpha)$$

for $\alpha \in L$.

(a) If L/K is separable, then the characteristic polynomial $\chi_\alpha \in K[x]$ of M_α is given by

$$\chi_\alpha(x) = \prod_{\sigma \in \mathrm{Hom}_K(L,\overline{K})} (x - \sigma(\alpha)).$$

(b) Let M/L be another field extension. Then,

$$\mathrm{Tr}_{L/K} \circ \mathrm{Tr}_{M/L} = \mathrm{Tr}_{M/K}, \qquad N_{L/K} \circ N_{M/L} = N_{M/K}.$$

(c) A K-bilinear form $L \times L \to K : (\alpha, \beta) \mapsto \mathrm{Tr}_{L/K}(\alpha\beta)$ is nondegenerate.

(d) For $\alpha \in L$, $Tr_{L/K}(\alpha) \in \mathcal{O}_K$ if $\alpha \in \mathcal{O}_L$.

(e) For $\alpha \in L$, $N_{L/K}(\alpha) \in \mathcal{O}_K$ if and only if $\alpha \in \mathcal{O}_L$.

5.9 (Integral bases)**.** An *integral basis* of a number field K is a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. Let $\{\omega_1, \cdots, \omega_n\}$ be a basis of K over $\mathbb{Q}$.

If $\Delta(\omega_1, \cdots, \omega_n)$ is square-free, then $\{\omega_1, \cdots, \omega_n\}$ is an integral basis. Let $\{\omega_1, \cdots, \omega_n\}$ be a basis of K over $\mathbb{Q}$ consisting of algebraic integers.

If $p^2 \mid \Delta$ and it is not an integral basis, then there is a nonzero algebraic integer of the form

$$\frac{1}{p}\sum_{i=1}^{n} \lambda_i \omega_i.$$

5.10 (Dedekind domains)**.**

Consider a $AKLB$-setting and let $\alpha \in L$.

(a) $\alpha \in B$ if and only if $\mu_\alpha \in A[x]$.

(b) $\alpha \in B^\times$ if and only if $N_{L/K}(\alpha) \in A^\times$, if L/K is separable and A integrally closed.

Ramification theory

The Dedekind theorem

Exercises

5.11 (Number of irreducibles over finite fields)**.** The minimal polynomial map

$$\mathbb{F}_{p^2} \setminus \mathbb{F}_p \to \{ \text{ quadratic irreducible monic polynomials } \}$$

is surjective and every preimage of singletons are of size two.

(a) The number of monic irreducibles over $\mathbb{F}_p$ of degree 6 is $(p^6 - p^3 - p^2 + p)/6$.

5.12. Computation of a generator of $\mathbb{F}_{p^n}^\times$.

5.13 (Berlekamp algorithm)**.**

5.14 (Quadratic integers)**.** Every quadratic field is of the form $\mathbb{Q}(\sqrt{d})$ for a square-free $d \in \mathbb{Z}$. Let d be a square-free.

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & , d \equiv 2,3 \pmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & , d \equiv 1 \pmod 4 \end{cases}$$

$$\Delta_{\mathbb{Q}(\sqrt{d})} = \begin{cases} 4d & , d \equiv 2,3 \pmod 4 \\ d & , d \equiv 1 \pmod 4 \end{cases}$$

5.15 (Cubic integers). (a) Let $\theta^3 = hk^2$ for h, k square-free's.

$$\mathcal{O}_{\mathbb{Q}(\theta)} = \begin{cases} \mathbb{Z} + \theta\mathbb{Z} + \frac{\theta^2}{k}\mathbb{Z} & , m \not\equiv \pm 1 \pmod 9 \\ \mathbb{Z} + \theta\mathbb{Z} + \frac{\theta^2 \pm \theta k + k^2}{3k}\mathbb{Z} & , m \equiv \pm 1 \pmod 9 \end{cases}$$

(b) If θ^3 is a square free integer, then

$$\mathcal{O}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta].$$

Problems

1. Let f be a quintic irreducible polynomial over a field F such that its splitting field has degree sixty over F. Show that if α is a root of f, then there is no proper intermediate field of $F(\alpha)/F$.

1. Find the number of $a \in \mathrm{SL}(2, \mathbb{F}_p)$ such that $a^{p-1} = 1$.

Chapter 6

Insolvability of the quintic

6.1 Cyclic extensions

6.1 (Kummer theory). A field extension L/K is called a *Kummer extension* if $\zeta_n \in K$ and $\mathrm{Gal}(L/K)$ is abelian group of exponent n..??

(a) If $\zeta_n \in K$,

Let $\sigma \in \mathrm{Gal}(L/K) \cong Z_n$ be a generator. If $f : \mathrm{Gal}(L/K) \to L^\times : g \mapsto \zeta_n$, then $f \in H^1(\mathrm{Gal}(L/K), L^\times)$. Hilbert 90 states that $H^1(\mathrm{Gal}(L/K), L^\times) = 0$, so we have $\alpha \in L$ such that $g(\alpha)/\alpha = f(g)$ for all $g \in \mathrm{Gal}(K/L)$. Then,

$$g(\alpha^n)/\alpha^n = \sigma^r(\alpha^n)/\alpha^n = f(\sigma^r)^n = (\zeta_n^r)^n = 1.$$

It means that α^n is fixed by all elements of $\mathrm{Gal}(L/K)$.

6.2 Cyclotomic extensions

6.2 (Cyclotomic polynomials). Let ζ be a primitive nth root of unity. The nth *cyclotomic polynomial* is defined by

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

(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. □

6.3 (Computation of cyclotomic polynomials).

6.3 Radical extensions