Algebra-2 Note

lin150117

Contents

1 Ring

1.1 More on rings and ideals

Theorem 1.1.1 (Correspondence Theorem)**.** Ideals of R containing I have a bijection with ideals with R/I

Definition 1.1.1. $x \in R$, x is said to be

1. a **zerodivisor** if $x \neq 0$ and $\exists y \neq 0$ s.t. $xy = 0$
2. **nilpotent** if $\exists n > 0$ s.t. $x^n = 0$
3. an **idempotent** if $x^2 = x$

Definition 1.1.2. $\sqrt{0} := \{x \in R : nilpotentinR\} \subset R$, called nilpotent radical.

Example 1. For K a field, $K[x]/(x^2)$ has $\sqrt{0} = \overline{x}K[x]/(x^2)$
Call $K[\epsilon] = K[x]/(x^2)$ **ring of dual number**

Definition 1.1.3. A ring R is called **reduced** if $\sqrt{0} = 0$

Proposition 1.1.2. The followings are right.

1. $\sqrt{0} \subset R$ is an ideal
2. $R/\sqrt{0}$ is reduced
3. If R' is a reduced ring,then every ring homomorphism $\phi : R \to R'$,factors through uniquely s.t. $\phi = \overline{\phi} \circ \pi$, where $\pi : R \to R/\sqrt{0}$

1.2 product ring and idempotent

Definition 1.2.1. Let R_1, R_2 be rings, **product ring** $R_1 \times R_2$ is a ring with $(x_1, x_2) + / * (y_1, y_2) = (x_1 + / * y_1, x_2 + / * y_2)$

Remark 1.2.1. Note that

1. $(0,0)$ is 0 of $R_1 \times R_2$, $(1,1)$ is 1 of $R_1 \times R_2$
2. Set $R = R_1 \times R_2$, then

   the projection map p_1, p_2 are ring homomorphism.

   the inclusion map i_1, i_2 are not
3. $(1,0), (0,1)$ are idempotents.

From those properties, we can construct an isomorphism for an arbitrary idempotent.

Proposition 1.2.2. $e \in R$ idempotent i.e. $e^2 = e$

1. eR is a ring with e as mult identity and $p : R \to eR, x \mapsto ex$ is a ring homomorphism
2. $e' = 1 - e$ is also an idempotent and $R \to (eR) \times (e'R) : x \mapsto (ex, e'x)$ is an isomorphism of rings.

1.3 Prime ideals and maximal ideals

Observation 1. R ring

1. $x \in R$, $(x) = R \Leftrightarrow x \in R^\times$ unit.
2. R is a field $\Leftrightarrow$ R has exactly two ideals.

Definition 1.3.1. A ring is called an **integral domain** if it is not the zero ring and has no nonzero zerodivisor $\Leftrightarrow$ "$xy = 0 \Rightarrow x = 0$ or $y = 0$".

Definition 1.3.2. An ideal $P \subset R$ is called **prime** if $p \neq 0R$ and "$xy \in P$ implies $x \in P$ or $y \in P$". Equivalently, R/P is an integral domain.

Definition 1.3.3. An ideal $M \subset R$ is called **maximal** if $M \neq R$ and $\forall$ ideal $M \subset I \subset R$, $I = M$ or $I = R$
Equivalently, ideals of R/M are only 0 and R/M. $\Rightarrow$ R/M is a field.

In this subsection we will discuss R integral domain.

Definition 1.3.4. Let $f \in R$ be nonzero and nonunit.
Say f is **irreducible** if $f = gh \Rightarrow$ either g or h is a unit.
Say f is a **prime** prime element if $f|gh \Rightarrow f|g$ or $f|h$
Here, $a|b$ means $\exists c \in R$ such that $ac = b$

Proposition 1.3.1. $f \in R$

1. f is irreducible $\Leftrightarrow (f)$ is maximal among proper principal ideals.

2. f is prime if and only if (f) is a prime ideal.

Proposition 1.3.2.

1. A prime element is irreducible.

2. If R is a PID(i.e. every ideal is principal), then an irreducible element is prime.

Proposition 1.3.3. For $\varphi : R \to R'$ ring homomorphism.

1. $J \subset R'$ ideal $\to \varphi^{-1}J \subset R$ ideal.

2. $J \subset R'$ prime ideal $\to \varphi^{-1}J \subset R$ prime ideal.

3. Maximal ideal is not preserved between homomorphism.

Example 2. $\mathbb{Z}[i]/(3) \backsimeq \mathbb{Z}[x]/(x^2+1,3) \backsimeq \mathbb{F}_3[x]/(x^2+1)$.
Since x^2+1 have no root in $\mathbb{F}_3$, x^2+1 is irreducible, hence prime in $\mho_3[x]$. Therefore $\mathbb{Z}[i]/(3) \backsimeq \mathbb{F}_3[x]/(x^2+1)$ is an integral domain. Then 3 is prime in $\mathbb{Z}[i]$.

Example 3. $\mathbb{Z}\sqrt{-5}/(2) \backsimeq \mathbb{Z}[x]/(x^2+5,2) \backsimeq \mathbb{F}_2[x]/(x^2+5)$.
Since x^2+5 is not prime. Therefore 2 is not prime in $\mathbb{Z}\sqrt{-5}/(2)$.

Example 4. However 2 is irreducible.
Set $P = (2, 1+\sqrt{-5})$.

Claim 1.

1. P is a prime.

2. $P^2 = (2)$

Let $Q = (3, 1+\sqrt{-5})$. Then $Q, \overline{Q}$ are maximal.
$Q\overline{Q} = (3), PQ = (1+\sqrt{-5}), P\overline{Q} = (1-\sqrt{-5})$
$\Rightarrow (6) = P^2Q\overline{Q}$ called **prime ideal factorization**(i.e. $\mathbb{Z}[\sqrt{-5}]$ is a Dedekind domain)

Example 5. $R = \mathbb{C}[x,y]$.

Fact. $SpecR := \{0\} \cup \{(f(x,y)) : f \in R\, irreducible\} \cup \{(x-a, y-b), a, b \in \mathbb{C}\}$

Theorem 1.3.4 (Hilbert Nullstellensate)**.** Maximal ideals of $\mathbb{C}[x,y]$ are $(x-a, y-b)$.

1.4 Zorn's lemma

Theorem 1.4.1. If $I \subset R$ is a proper ideal, $\exists$ maximal ideal $\mathfrak{M}$ s.t. $\mathfrak{M} \supset I$.
In particular, if $R \neq 0$, then $SpecR \neq 0$

Definition 1.4.1. Say a partially ordered set S is inductive, if every totally ordered subset $s' \subset S$ has an upper bound.

Theorem 1.4.2 (Zorn's lemma)**.** Every nonempty inductive partially ordered set has a maximal element.

1.5 Fraction

Definition 1.5.1. Let R be an integral domain.

$$Frac\, R := \{(r,s) \in R^2 : s \neq 0\}/\sim$$

where $(a,s) \sim (b,t)$ iff $at = bs$
Define sum and product by

$$a/s + b/t = \frac{at+bs}{st}, a/s \cdot b/t = ab/st$$

$R \to FracR : a \mapsto a/1$ ring homomorphism.

Theorem 1.5.1.

1. $Frac\, R$ is a field, and $\varphi : R \to Frac\, R$ is injective.
2. (universality) $\forall K$ field and $\forall \psi : R \to K$ injective ring homomorphism, $\exists! \widehat{\psi} : Frac\, R \to L$ s.t. $\psi = \widehat{\psi} \circ \varphi$

1.6 Localization

From now on, R is any commutative ring.

Definition 1.6.1. A **multiplicative** set of R is a subset $S \subset R$ s.t. (1)$1 \in S$ (2)$s, t \in S \Rightarrow st \in S$.

Definition 1.6.2. $S^{-1}R := \{(a,s) : a \in R, s \in S\}/\sim$
where $(a,s) \sim (a', s')$ iff $\exists t \in S, tas' = ta's$.
Call $S^{-1}R$ the **Localization** of R by S.

Lemma 1.6.1.

1. $\sim$ is an equivalence relation.
2. $a/s + b/t = at + bs/st, a/s \cdot b/t = ab/st$ are well defined, and make it into a ring.
3. $\varphi : R \to S^{-1}R : a \mapsto a/1$ is a ring homomorphism with $Ker\, \varphi = \{b \in R : \exists s \in S, sb = 0\}$

Theorem 1.6.1 (universality)**.** $\forall R'$ and $\psi : R \to R'$ ring homomorphism s.t. $\psi(S) \subset R'^{\times}$. Then $\exists! \widehat{\psi} : S^{-1}R \to R'$ s.t. $\psi = \widehat{\psi} \circ \varphi$.

Example 6. R is an integral domain. Then

$$Frac\, R = S^{-1}R$$

where $S = R\backslash\{0\}$

Example 7. $R = \mathbb{Z}, S = \{2^n : n \geq 0\} \Rightarrow S^{-1}R = \mathbb{Z}[2^{-1}]$
$R = \mathbb{Z}/6, S = \{\overline{2}^n : n \geq 0\} \Rightarrow S^{-1}R = \mathbb{F}_3$
In general, $f \in R \Rightarrow S = \{f^n : n \geq 0\}, S^{-1}R$ is denoted by $R_f = R[x]/(fx-1)$ (adjoining f^{-1})

Example 8. $R = \mathbb{Z}, S = \{odd\} \subset \mathbb{Z} \Rightarrow S^{-1}R = \{a/s : a, s \in \mathbb{Z}, 2 \not| s\}$
In general, for $P \in Spec\, R$ (prime ideal), we have $S = R - P$ is multiplicative.
$\Rightarrow S^{-1}R$ is denoted by R_P, called **localization** of R at P.

Define $S^{-1}T = \{a/s \in S^{-1}R : a \in I\} = \varphi(I) \cdot S^{-1}R$

Proposition 1.6.2.

1. $S^{-1}I = S^{-1}R$ if and only if $S \cap I \neq \emptyset$
2. $S^{-1}/S^{-1}I \simeq \overline{S}^{-1}(R/I)$ where $\overline{S}$ image of S under $R \to R/I$.
3. If $P \in Spec\, R$ with $S \cap P = \emptyset$, then $S^{-1}P$ is prime in $S^{-1}R$, and $\varphi^{-1}(S^{-1}P) = P$.

Theorem 1.6.3. $Spec\, S^{-1}R \to SpecR$ induces a bijection

$$Spec\, S^{-1}R \to \{P \in SpecR : P \cap S = \emptyset\}, q \mapsto \varphi^{-1}(q)$$

Proof. Only need to prove $S^{-1}(\varphi^{-1}(q)) = q$. $\square$

1.7 localization

R ring , $S \subset R$ multiplicative set. $\Rightarrow S^{-1}R$ is a ring.

$$\begin{aligned} Spec\, S^{-1}R &\longrightarrow \{p \in Spec\, R : p \cap S = \emptyset\} \\ q &\mapsto \varphi^{-1}q \\ S^{-1}p &\leftarrow p \end{aligned}$$

is a bijection.
Recall that nilpotent radical $\sqrt{0} = \{x \in R : \text{nilpotent}\}$. $R_{red} = R/\sqrt{0}$ is reduced(i.e. no nonzero nilpotent.)

Theorem 1.7.1. $\sqrt{0} = \bigcap_{p \in Spec\, R} p$

Then we have $Spec\, R_{red} \to Spec\, R$ is a bijection, moreover a homomorphism.
Let $R_f = S^{-1}R$, $S = \{1, f, \cdots\}$. In particular, $R_f \neq 0$ and hence $R_f \neq \varnothing$. $\Rightarrow \exists p \in Spec\, R$ s.t. $f \notin p$ by correspondence theorem for localization.

1.8 Euclidean domains, PIDs, UFDs

$$\{\text{Euclidean domains}\} \subsetneq \{\text{PIDs}\} \subsetneq \{\text{UFDs}\} \subsetneq \{\text{integral domains}\}$$

Definition 1.8.1. R is a **Euclidean domain** if $\exists \sigma : R - \{0\} \to \mathbb{Z}_{\geq 0}$ s.t.

$$\forall a, b \in R \text{ with } a \neq 0, \exists q, r \in R \text{ s.t. } b = qa + r \text{ and } r = 0 \text{ or } \sigma(r) < \sigma(a)$$

Definition 1.8.2. A **principle ideal domain** is an integral domain where every ideal is principle.

Theorem 1.8.1. A Euclidean domain is a **PID**.

However, there are PIDs that are not Euclidean domain.

Proposition 1.8.2.

1. A prime element is irreducible.
2. In PID, irreducible element is prime.
3. In $\mathbb{Z}[\sqrt{-5}]$, 2 is irreducible but not prime.

Definition 1.8.3. An integral domain is a **unique factorization domain** if

1. (existence of factorization) every nonzero non unit is a product fo irreducible elements.
2. (uniqueness up to associates) if $p_1 \cdots p_m = q_1 \cdots q_n$ for p_i, q_j irreducible. Then $m = n$ and after reindexing, we have
3. $\forall i = 1, \cdots, m$, p_i and q_i are associates i.e.

$$q_i = c \cdot p_i \text{ where } c \text{ is a unit, or } (p_i) = (q_i).$$

Proposition 1.8.3. In a UFD, irreducible can imply prime.

Theorem 1.8.4. PID is a UFD.

Proof. Let R be a PID.
First prove (2)uniqueness.
Suppose $p_1 \cdots p_m = q_1 \cdots q_n$, p_i, q_j irreducible.
By induction on $\max\{m, n\}$, show that it is the same.
If $m = n = 1$, we are done.
By Prop 1.8.3 p_i is prime. Easy to prove it by induction.
Now we prove (1)existence
Take any nonzero nonunit $a \in R$.
Assume a doesn't factorize. In particular, a is not irreducible.
Write $a = a_0 = a_1 \cdot a_1'$, a_1, a_1' are not unit.
If a_1, a_1' factorize into irreducible elements, so does a.

WLOG, we assume a_1 doesn't factorize.

Repeat this gives

$$(a_0 \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots \subsetneq R)$$

Set $I = \bigcup_{n \geq 0} \subsetneq R$. Then I is an ideal $\Rightarrow I = (b)$ for some $b \in R$.

$\Rightarrow b \in (a_n) \subsetneq (a_{n+1})$ for some n, then $b = ca_n = ca_{n+1}a'_{n+1} = cc'b \cdot a'_{n+1}$

$\Rightarrow a'_{n+1}$ is a unit $\Rightarrow$ contradiction. □

1.9 Gauss' lemma

Theorem 1.9.1. If R is a UFD, so is $R[x]$.

Example 9. $K[x_1, \cdots, x_n]$ is a UFD.

For $a = u \cdot p_1^{e_1} \cdots p_n^{e_n}, a' = u' p_1^{e'_1} \cdots p_n^{e'_n}$ where u, u' are units, p_i are (nonassociate) irreducible, $e_i, e'_i \geq 0$

.

We define the great common divisor of a, a' as $gcd(a, a') = \cdot p_1^{min(e_1, e'_1)} \cdots p_n^{min(e_n, e'_n)} \in R$.

Definition 1.9.1. An element $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ is called **primitive** if $gcd(a_0, \cdots, a_n)$ is a unit.

Proposition 1.9.2. Every element $f \in R[x]$ can be expressed as $f = c \cdot f_0$ where $c \in R$, $f_0(x) \in R[x]$ is primitive.

Theorem 1.9.3 (Gauss' lemma)**.** If $f_0, g_0 \in R[x]$ are primitive, so is $f_0 g_0$.

Proof. Take any $p \in R$ irreducible. By assumption, $\overline{f_0}, \overline{g_0} \neq 0$ in $R/(p)[x]$

$\Rightarrow \overline{f_0 g_0} \neq 0$ since $R/(p)[x]$ is integral domain.

This means $f_0 g_0$ is primitive in $R[x]$. □

Next step we will classify irreducible element of $R[x]$. We consider the fraction $K = Frac\, R$.

Lemma 1.9.1. For $f \in K[x]$, $\exists c \in K, f_0 \in R[x]$ primitive s.t. $f = cf_0$.

Proposition 1.9.4. $f(x) = c \cdot f_0(x) = c' f'_0(x)$ where $f \in K[x], c, c' \in K$ and f_0, f'_0 is primitive in $R[x]$. Then c and c' are differed by an element in $R^\times$.

Lemma 1.9.2. Let $f_0, g \in R[x]$ with f_0 primitive. If $f_0 | g$ in $K[x]$, then $f_0 | g$ in $R[x]$

Proof. If $g = hf_0 = c \cdot h_0 f_0$. where $c \in K, h_0, f_0 \in R[x]$ primitive.

Since $g \in R[x]$, $h_0 f_0$ is primitive by Gauss' lemma, we have $c \in R$ by Prop 1.9.4. □

Theorem 1.9.5. Irreducible elements of $R[x]$ are exactly

(a) $\pi \in R$ irreducible.

(b) $f_0(x) \in R[x]$ primitive s.t. f_0 irreducible as element in $K[x]$.

Moreover, irreducible can imply prime in $R[x]$.

Proof. First we prove that element satisfying (a) or (b) is prime by lemma 1.9.2, hence irreducible in $R[x]$.

Second we consider $f(x)$ is irreducible.

If $f(x)$ is a unit $\Rightarrow f(x) = c \in R$.

Otherwise, $f(x) = c \cdot f_0(x)$. Since f is irreducible, $c \in R[x]^\times = R^\times$. This means f is primitve. If $f(x) = g(x) \cdot h(x)$ in $K[x]$. Write $g(x) = d \cdot g_0(x), h(x) = e \cdot h_0(x)$, g_0, h_0 primitive in $R[x]$, $d, e \in K$. Then $f(x) = (d \cdot e) \cdot g_0(x) \cdot h_0(x)$ where $g_0(x)h_0(x)$ is primitive by Gauss' lemma. By Prop 1.9.4, $d \cdot e \in R$. Since f is irreducible in $R[x]$, g_0 or h_0 should be a unit $\Rightarrow f(x)$ is irreducible in $K[x]$. □

Then we can prove the first theorem in this section.

Theorem 1.9.6. If R UFD, so is $R[x]$ UFD.

Proof. In the proof of PID $\Rightarrow$ UFD, uniqueness follows if irreducible element= prime in rings.

For existence of facctorization, take $f(x) \in R[x]$ nonzero, nonunit.

Since $K[x]$ is a PID ($\Rightarrow$ UFD), write $f(x) = cg_1(x) \cdots g_r(x)$. By Prop 1.9.4 we can prove it. □

We have some method to check $f(x) \in \mathbb{Z}[x]$ monic polynomial is irreducible.

Proposition 1.9.7. If $\exists p$ prime s.t. $f(x)$ is irreducible in $\mathbb{F}_p[x]$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$

Proposition 1.9.8 (Eisenstein criterion)**.** If $f(x) = x^n + \cdots + a_0$ s.t. $\exists p$ prime, $p|a_i, \forall 0 \le i \le n-1$, $p^2 \nmid a_0$, then $f(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. If $f(x) = g(x)h(x)$ in $\mathbb{Z}[x] \Rightarrow \overline{g}(x)\overline{h}(x)\overline{x}^n$ in $\mathbb{F}_p[x]$. Since $\mathbb{F}_p[x]$ UFD, then $x|\overline{g}(x), \overline{h}(x) \Rightarrow a_0 = g(0)h(0) \equiv 0 \mod p^2$ □

1.10 primes in $\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2+1)$

We have proved that $\mathbb{Z}[i]$ is a Euclidean domain, hence PID,UFD.

Prime in $\mathbb{Z}[i]$ is called **Gauss prime**. The norm $N : \mathbb{Z}[i] \to \mathbb{Z}_{\ge 0}, z \mapsto z \cdots \overline{z} = |z|^2$.

Proposition 1.10.1.

(a) z is a unit in $\mathbb{Z}[i]$ if and only if $N(z) = 1$.

(b) $N(z) = p \in \mathbb{Z}$ is a prime, then z is a Gauss prime.

Theorem 1.10.2. Gauss prime are exactly

(a) $\pm p, \pm i$ for $p \in \mathbb{Z}$ prime s.t. $p \equiv 3 \mod 4$.

(b) $a + bi \in \mathbb{Z}[i]$ s.t. $a^2 + b^2 = p$ for $p \in \mathbb{Z}$ prime with

Moreover, if $p \equiv 1, 2 \mod 4$, then $\exists a, b \in \mathbb{Z}$ s.t. $a^2 + b^2 = p$.

Lemma 1.10.1. If z is a Gauss prime, the $N(z) = p$ or p^2 for a prime p in $\mathbb{Z}$.

Proof. This follows from $\mathbb{Z}[i]$ UFD. $\square$

Lemma 1.10.2. $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$.

proof of theorem **??**. Choose any $p \in \mathbb{Z}$ prime.
Consider $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[x]/(x^2+1)$. It is an integral domain is equivalent to x^2+1 has no solution in $\mathbb{F}_p$.
x^2+1 has a solution in $\mathbb{F} \Leftrightarrow \exists a \in \mathbb{F}_p^\times$ s.t. $a^2=-1, a^4=1$, i.e. $ord(a)=4$. By lemma 1.10.2 we have $4|p-1$.
Hence $p \neq 2$ is a Gauss prime $\Leftrightarrow p \not\equiv 1 \mod 4$ i.e. $4|p-3$.
Moreover, if $p \equiv 1 \mod 4$, p is not a Gauss prime. $p = z \cdot w$ where z Gauss prime.
$\Rightarrow p^2 = N(p) = N(z) \cdot N(w) \Rightarrow N(z) = p$ so we can write $z = a + bi$ a.t. $a^+b^2 = p$. $\square$

1.11 Algebraic numbers/integers

Definition 1.11.1. $\alpha \in \mathbb{C}$ is called an **algebraic number** if $\exists f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x]$, s.t. $f(\alpha) = 0$.
Moreover, if we can take $f(x) \in \mathbb{Z}[x]$, call α an algebraic integer.

Example 10. $\pi, e \in \mathbb{C}$ not algebraic numbers.

For $\alpha \in \mathbb{C}$, consider $\varphi_\alpha : \mathbb{Q}[x] \to \mathbb{C} : f(x) \mapsto f(\alpha)$. Then $\operatorname{Im} \varphi_\alpha = \mathbb{Q}[\alpha] \subset \mathbb{C}$
Note that $\mathbb{Q}[x]$ is PID $\Rightarrow \ker \varphi_\alpha = (F(x))$ principal.
i.e. we have two cases:

(a) $\ker \varphi_\alpha = 0$

(b) $F(x)$ is monic irreducible $\Leftrightarrow \alpha$ is an algebraic number.

In case (b),

$$\alpha \text{ is an algebraic integer} \Leftrightarrow F(x) \in \mathbb{Z}[x].$$

Definition 1.11.2. Monic generator $F(x)$ of $\ker \varphi_\alpha$ is called the **minimal polynomial for** α.

For $d \in \mathbb{Q}$, consider $\mathbb{Q}[\sqrt{d}]$.
We may assume $d \in \mathbb{Z}$ and square free.
Then $K = \mathbb{Q}[\sqrt{d}]$ is called a **quadratic field**.

$$\mathcal{O}_K := \{\text{algebraic integers in } K\ \} \subset K$$

Proposition 1.11.1.

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{d}\right] & \text{if } d \equiv 2, 3 \mod 4 \\ \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Proof. For $\alpha = a + b\sqrt{d}$ $(a, b \in \mathbb{Q})$, minimal polynomial for α is $x^2 - 2ax + (a^2 - b^2 d)$.
Then $\alpha \in \mathcal{O}_K$ if and only if $2a, a^2 - b^2 d \in \mathbb{Z}$. $\square$

Call $\mathcal{O}_K$ the ring of integers of K.
In general, $K \subset \mathbb{C}$, $\mathcal{O}_K = \{\text{algebraic integers}\} \subset K$ is a ring.
If we define $N : K \to \mathbb{Q}, a + b\sqrt{d} \mapsto a^2 - b^2 d$.
One can check $\alpha \in \mathcal{O}_K \Rightarrow N(\alpha) \in \mathbb{Z}$. Morover, α is a unit in $\mathcal{O}_K$ if and only if $N(\alpha) = \pm 1$. $d \geq 0$ then $N(\alpha \geq 0)$.
For $0 \geq d \geq -5$, $\mathcal{O}_K^\times = \{\pm 1\}$.

Theorem 1.11.2 (unit theorem)**.** For $d \geq 0$, $\exists u \in \mathcal{O}_L^\times$, $u \neq \pm 1$, s.t.

$$\mathcal{O}_K^\times = \{\pm u^n : n \in \mathbb{Z}\}$$

Theorem 1.11.3. For $d < 0$, $\mathcal{O}_K$ is a PID $\Leftrightarrow$ $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ called **Heegner number**

However, we don't know there are infinitely many $d > 0$ s.t. $\mathcal{O}_K$ is a PID.

Proposition 1.11.4. $\mathcal{O}_K$ is a **Dedekind domain**: an integral domain s.t. $\forall I \subset \mathcal{O}_K$ nonzero ideal, $\exists P_1, P_2, \cdots, P_r \subset \mathcal{O}_K$maximal ideal. $e_1, \cdots, e_r \in \mathbb{Z}_{>0}$ s.t.

$$I = P_1^{e_1} \cdots P_r^{e_r}$$

2 Modules

2.1 Introduction

Let R be a ring.(unital and commutative)

Definition 2.1.1. An R**-module** (or left R-module) is an abelian group $(V, +)$ together with

$$R \times V \to V,\ (a, v) \mapsto av \qquad \text{(Scalar multiplication)}$$

s.t. $\forall a, b \in R, v, w \in V$

$$\begin{aligned} &(1) \quad 1 \cdot v = v \\ &(2) \quad (ab)v = a(bv) \\ &(3) \quad a(v + w) = av + aw \\ &(4) \quad (a + b)v = av + bv \end{aligned}$$

A **submodule** of V is an abelian subgroup $W \subset V$ s.t. $\forall a \in R, \forall w \in W, a \cdot w \in W$.

Definition 2.1.2. A **homomorphism**(or R-linear map) is a group homomorphism $\varphi : V \to V'$ s.t. $\varphi(av) = a\varphi(v)$.

Definition 2.1.3 (Quotient module)**.** For $W \subset V$ submodule,

$$\pi : V \to V/W, v \mapsto [v + W]$$

3 submodule of a free module

Theorem 3.0.1. R is a PID.

1. Every submodule of a free R-module is free.

2. If V is a free R-module of finite rank n and if $W \subset V$ submodule. Then W is free of rank $m \leq n$, $\exists\, v_1, v_2, \cdots, v_n \in V$ R-basis and $b_1, \cdots, b_n \in R \neq 0$ s.t.

   (a) $\omega_i = b_i v_i$

   (b) $b_1 | b_2 \cdots | b_m$

   Moreover, $\{(b_1) \supset \cdots \supset (b_m)\}$ is unique.

Observation 2.

$$V/W \cong R/(b_1) \oplus \cdots \oplus R/(b_m) \oplus R^{\oplus n-m}$$

3.1 Finite generated modules/PID

Theorem 3.1.1. R is a PID. V is a finitely generated R-module.
Then

(a) $\exists\, b_1 \cdots b_m \in R$, $b_1 | \cdots | b_m$ s.t. $\exists\, n$ s.t.

$$V \cong R/(b_1) \oplus \cdots \oplus R/(b_m) \oplus R^{\oplus n-m}$$

(b) $\exists\, p_1, \cdots, p_m \in R$ irreducibles $(p_i) \neq (p_j)$, $i \neq j$. $1 \leq e_{i,1} \leq e_{i,l_i}$ and $\exists\, n \geq 0$

$$V \cong R/(p_1)^{e_{1,1}} \oplus \cdots \oplus R/(p_m)^{e_{m,l_m}} \oplus R^{\oplus n}$$

Corollary 3.1.2. For $A \in M_{m,n}(R)$ $m \times n$ matrix with entries in R PID. $\exists Q \in \mathrm{GL}_m(R), P \in \mathrm{GL}_n(R)$ s.t.

$$Q^{-1}AP = \begin{pmatrix} b_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & b_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_l & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

where $b_i \neq 0, b_1 | b_2 | cdots | b_l$

3.2 presentation

Given $f : R^n \to R^m$ R-linear map.
$M := R^m / \operatorname{Im} f$ is $R - module.$
In this case, f is called a **presentaion** of M and if M admits such a presentation, we say M is of finite presentation.
Usually, by change of basis, we get better presentation(for R Euclidean domain) through elementary row/column operation.

Note. Now, we may assume R is a PID.

Theorem 3.2.1. If V is a free R-module of rank n, and $W \subset V$ is a submodule, then $\exists m \leq n$, $\exists v_1, \cdots, v_n$ R-basis of V, $\exists b_1 | b_2 \cdots | b_m \in R \neq 0$ s.t. W is free of rank m with basis $b_1 v_1, \cdots, b_m v_m$. Moreover, $\{(b_1) \supset \cdots \supset (b_m)\}$ is unique.

Theorem 3.2.2. If V is finite generated over a PID R, then $V \cong R/(b_1) \oplus \cdots \oplus R/(b_l) \oplus R^k$ for $b_1 | \cdots | b_l$.

In particular, for $R = \mathbb{Z}$, R-module is exactly abelian group. Every finitely generated abelian group is isom to $\oplus \mathbb{Z}_{n_i} \oplus \mathbb{Z}^k$

3.3 Rational canonical form and Jordan canonical form

Theorem 3.3.1. For $T = A \in GL_n(K)$, $\exists P \in GL_n(K)$ s.t.

$$P^{-1}AP = \begin{pmatrix} C_1 & 0 & \cdots & 0 \\ 0 & C_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & C_n \end{pmatrix}$$

where C_i is comparion matrix of $f_i(x)$

3.4 Noetherian moudles

Definition 3.4.1. An R-module V is called a noetherian R-module if the following equivalent conditions holds:

1. every R-module of V is finitely generated.
2. (Ascending chain condition) For any $V_0 \subset V_1 \subset \cdots$ ascending chain of R-submodules of V, there exists n such that $V_n = V_{n+1} = \cdots$.
3. Every nonempty set of R-modules of V contains a maximal element.

Proposition 3.4.1. R is PID, then R is a noetherian ring.
If R is a noetherian ring, then every quotient ring R/I is a noetherian ring.(but not true for subrings)

Theorem 3.4.2. R noetherian ring.

1. Every finitely generated R-module is a noetherian R-module. Therefore, every finitely generated R-module is of finite presentation.
2. (Hilbert's basis theorem) $R[x]$ is also a noetherian ring.

3.5 integral elements

For α algebraic integer, if $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some $a_i \in \mathbb{Z}$.
Then $1, \alpha, \cdots, \alpha^{n-1}$ span $\mathbb{Z}[\alpha]$ as a $\mathbb{Z}$-module.

Lemma 3.5.1. Let $A \to B$ is a ring homomorphism, V a B-module. If B, as an A-module, is finite generated, and V is a finite generated B-module, then V is also a finite generated A-module.

Definition 3.5.1. A is a subring of B.
$b \in B$ is **integral over** A if $\exists n \in \mathbb{Z}_+, a_0, \cdots, a_{n-1} \in A$ s.t. $b^n + a_{n-1}b_1 + \cdots + a_1 b + a_0 = 0$.
Sat B is integral over A if every $b \in B$ is integral over A.

Proposition 3.5.1. For $b \in B$, TFAE

(1) b is integral over A

(2) subring $A[b] \subset B$ is a finitely generated A-module.

(3) $\exists C \subset B$ subring s.t. $A[b] \subset C$ and C is a finite generated A-module.

We need to prove a lemma.

Lemma 3.5.2. $X \in M_n(A)$, then $\exists\, Y \in M_n(A)$ (which is called cofacter matrix) s.t.

$$YX = (\det X)I_n$$

Lemma 3.5.3. If $b_1, \cdots, b_r \in B$ are integral over A, then the subring $A[b_1, \cdots, b_r]$ is finitely generated as A-module.

Corollary 3.5.2. $b, b' \in B$ are integral over A, then $b \pm b', bb'$ are integral over A.

Hint. Using the lemma 3.5.1

Corollary 3.5.3. $A \subset B \subset C$. If B is integral over A, $c \in C$ is integral over B, then $c \in C$ is integral over A.

Definition 3.5.2. $\{b \in B : \text{integral over } A\}$ is a subring of B by Cor 3.5.2. Call this **integral closure** of A in B.

Definition 3.5.3. An integral domain A is called **integrally closed** if integral closure of A in $\operatorname{Frac} A$ is A

Example 11. $K = \mathbb{Q}[\sqrt{d}]$.

$$\mathcal{O}_k = \{\text{algebraic integers in } K\}$$

is integrally closed by Cor 3.5.3 ($A = \mathbb{Z} \subset B = \mathcal{O}_k \subset C = K$)

More generally, K is a number field. Then $\mathcal{O}_k = \{\text{algebraic integers in } K\ \}$ is the integral closure of $\mathbb{Z}$ in K and integrally closed integral domain.

Definition 3.5.4. A is called a **Dedekind domain** if A is an integrally closed integral domain *s.t.* A is noetherian and every nonzero prime ideal is maximal.

Fact. (1) $\mathcal{O}_K$ above is a Dedekind domain.

(2) In Dedeking domain, every nonzero ideal= $p_1^{e_1} \cdots p_r^{e_r}$ where p_i maximal ideals.

3.6 Homological and exact sequence

Definition 3.6.1. Let R be a ring , V, W R-module.

$$\mathrm{Hom}_R(V, W) = \{f : V \to W : f \text{ is } R\text{-linear}\}$$

which is an R-module.

Definition 3.6.2. Consider a chain of R-linear maps

$$\cdots \to V_{i-1} \xrightarrow{f_{i-1}} V_i \xrightarrow{f_i} V_{i+1} \to \cdots$$

Say this is **exact** at V_i if $\mathrm{Im}\, f_{i-1} = \ker f_i$.
Exact if exact at every V_i.

3.7 Tensor product

3.8 Introduction

Proposition 3.8.1.

(1) $0 \to W' \to W \to W''$ is exact if and only if
$\forall V$ R-module, $0 \to \mathrm{Hom}(V, W') \to \mathrm{Hom}(V, W) \to \mathrm{Hom}(V, W'')$ is exact.

(2) $V' \to V \to V'' \to 0$ is exact if and only if
$\forall W$ R-module, $0 \to \mathrm{Hom}(V'', W) \to \mathrm{Hom}(V, W) \to \mathrm{Hom}(V', W)$ is exact

Proposition 3.8.2. $V \xrightarrow{f} W \to U \to 0$ is exact means $U = \mathrm{Coker}\, f := W/\,\mathrm{Im}\, f$

3.9 Tensor Product

Definition 3.9.1. $\forall U, V$ R-module, $\exists$ R-module X and $U \times V \xrightarrow{F} X$ R-bilinear map *s.t.* $\forall$ $U \times V \xrightarrow{G} W$ R-bilinear map, there exists a unique R-linear map $g : X \to W$ with $g \circ F = G$.
Moreover, pair (X, F) is unique up to unique isomorphism.
Write $(U \otimes_R V, U \times V \to U \otimes V)$

Remark 3.9.1. The existence of X is proved through quotient space $R^{\oplus U \times V}/V$ for some equivalent submodule V.

Proposition 3.9.2 (Proper A)**.**

(1) $R \otimes_R V \cong V$

(2) $V \otimes W \cong W \otimes V$

(3) $(V \oplus U) \otimes W \cong (U \otimes W) \oplus (V \otimes W)$

(4) $(U \otimes V) \otimes W = U \otimes (V \otimes W)$

Example 12. $R^m \otimes R^n = R^{mn}$, $R^m \otimes V \cong V^m$

Proposition 3.9.3 (Proper B)**.**

$$\mathrm{Hom}(U \otimes V, W) \cong \mathrm{Hom}(U, \mathrm{Hom}(V, W))$$

Remark 3.9.4. It is up to the commutative diagram in the definition.

Proposition 3.9.5 (Proper C)**.** If $W' \to W \to W'' \to 0$ is exact, then $V \otimes W' \to V \otimes W \to V \otimes W'' \to 0$ is exact for all V R-module.

Remark 3.9.6. It is directly from Proper B and Prop 3.8.1

Example 13. $\mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/5 \to 0$ is exact

So $\mathbb{Z}/4 \otimes \mathbb{Z} \to \mathbb{Z}/4 \otimes \mathbb{Z} \to \mathbb{Z}/4 \otimes \mathbb{Z}/5 \to 0$ is exact.

By Prop 3.8.2, $\mathbb{Z}/4 \otimes \mathbb{Z}/5 = \mathbb{Z}/\mathbb{Z} = 0$

Similarly, $\mathbb{Z}/4 \otimes \mathbb{Z}/6 = \mathbb{Z}/2$

There is a proposition to describe it.

Proposition 3.9.7.

$$R/I \otimes V \cong V/_{IV}$$
$$R/I \otimes R/J \cong R/_{(I+J)}$$

Proposition 3.9.8.

$$R/I \otimes_R R' \cong R'/_{IR'}$$
$$R[x] \otimes_R R' \cong R'[x]$$

Therefore, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}[x]/(x^2+1) \otimes \mathbb{C} = \mathbb{C}[x]/(x^2+1) \cong \mathbb{C} \times \mathbb{C}$

3.10 Complement on Tensor Product

Proposition 3.10.1 (Universality of $R' \otimes_R V$)**.**

$$\mathrm{Hom}_{R-linear}(V, W') = \mathrm{Hom}_{R'-linear}(R' \otimes_R V, W')$$

for every W' R'-module.

$$\begin{tikzcd} V \arrow[r, "\forall R-linear"] \arrow[d, "inclusion"'] & W' \\ R' \otimes_R V \arrow[ur, "\exists! R'-linear"'] & \end{tikzcd}$$

Proposition 3.10.2 (Universality of $R' \otimes R''$)**.**

$$\begin{tikzcd} & R' \arrow[d] \arrow[dr, "\forall g'"] & \\ R \arrow[ur, "f'"] \arrow[dr, "f''"'] & R' \otimes_R R'' \arrow[r, "\exists! h"] & T \\ & R'' \arrow[u] \arrow[ur, "g''"'] & \end{tikzcd}$$

where f', f'' inclusion map and $f' \circ g' = f'' \circ g''$. h is a ring homomorphism.

4 Field and Galois Theory

4.1 Field extension

Definition 4.1.1. A **Field extension** K/F means $F \xrightarrow[\text{ring homo}]{\textit{injective}} K$ which K is a field.
Note that K is a F-vector space, we can define the dimension of K where $\dim_F K = [K : F]$.
If $[K : F] < +\infty$ say K/F is of **finite** extension.
If $F \hookrightarrow M \hookrightarrow K$, then M is called the **intermediate field** of K/F.

Now we consider the adjoining elements $\alpha_1, \cdots, \alpha_n \in K$.
$F(\alpha_1, \cdots, \alpha_n) \subset K$ is the smallest subfield of K containing F and $\alpha_1, \cdots, \alpha_n$.
$F(\alpha)/F$ is called a **simple extension**
Say α is a **primitive element** of $F(\alpha)/F$ There is a unique $\varphi_\alpha : F[x] \to K$ *s.t.* $\varphi_\alpha(x) = \alpha$.
For $\ker \varphi_\alpha = 0$, call α **transcendental**
For $\ker \varphi_\alpha = (f_\alpha(x)) \neq 0$, call f_α the **minimal polynomial** for α over F.Call α **algebraic**

4.2 algebraic extension

Lemma 4.2.1. If $\alpha, \beta \in K$ algebraic over $F \Rightarrow \alpha \pm \beta, \alpha\beta$ are algebraic over F.

It is proved by proposition of integral over rings.

Definition 4.2.1. Say K/F is **algebraic** if every element in K is algebraic

Proposition 4.2.1. $[K : F] < +\infty \Rightarrow K/F$ is algebraic.

4.3 algebraic extension and simple algebraic extention

Example 14. If $\mathbb{C}/K/\mathbb{Q}$ and $[K : Q] = 2$, then $K = \mathbb{Q}[\sqrt{d}]$ for some square-free d

From this example, we can know that if K is an nontrivial intermediate field of $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, it should be $\mathbb{Q}(\sqrt{d})$, $d = 2, 3, 6$.
Thus $\mathbb{Q}[\sqrt{2} + \sqrt{3}]$ should be $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. The way to prove it can be that find its minimal polynomial or check it can't be nontrivial intermediate field.
So $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a simple extension with $\sqrt{2}, \sqrt{3}$ a primitive element.

Proposition 4.3.1. K/F is finite extension. Then K/F is a simple extension if and only if there are only finitely many intermediate extensions.

Proof. If K/F is simple. Write $K = F(\alpha)$. Let $f(x) \in F[x]$ be the minimal polynomial for α. Take any $K/M/F$, then $M(\alpha) = K$. Let $g(x) \in M[x]$ be the minimal polynomial for α over M. Then $g|f$ in $M[x]$. Set $F_g := F(\text{coefficient of } g(x))$. Then $F_g = M$. Each intermediate extension is of the form F_g with $g(x) \in K[x]$ s.t. $g|f$ in $K[x]$.
$F_g = M$ is because degree of minimal polynomial for α over $F_g = [k : F_g]$ is less then degree of $g = [K : M]$. Since $F_g \subset M$, it should be true.

Conversely, we may assume F is infinite. Let M_i be the nontrivial intermediate extension of K/F. Let $\alpha \in K - (M_1 \cup \cdots \cup M_n)$ (α exists by the result of linear algebra) Then $K = F(\alpha)$ □

Remark 4.3.2. We can understand how degree and minimal polynomial plays role in this proof. And we can get a lemma.

Lemma 4.3.1. If $K = F(\alpha)/F$, $g(x)$ be the minimal polynomial for α over F. Then $F_g = \{\text{coefficient of } g(x)\} = F$

4.4 Complete splitting and algebraic closure

Proposition 4.4.1.

(1) If K/F finite, $\exists K_0 = F \subset K_1 \subset \cdots \subset K_m = K$ *s.t.* K_{i+1}/K_i is simple.

(2) $\forall f(x) \in F[x]$, $\exists K/F$ finite *s.t.* $f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$ in $K[x]$.

Proof. (1) Just repeat choosing adjoining element.

(2) We may assume $f(x)$ is monic. Take a monic irreducible divisor $f_1(x)$ of $f(x)$. Let $K_1 := F[x]/(f_1(x))$, $\alpha_1 \in K_1$ be the image of $\overline{x}$. Then $f(\alpha) = 0$, $f = (x-\alpha_1)g_1(x)$ for some $g_1 \in K_1[x]$. Repeating this process.

□

Remark 4.4.2. The extension can be abstract. The key is to construct a proper operation. (2) is a more abstract but essential way to understand root.

Definition 4.4.1.

(1) A field K is called **algebraically closed** if every polynomial in $K[x]$ splits completely in $K[x]$. Equivalenly, if L/K is an algebraic extension, then $L = K$.

(2) An **algebraic closure** of a field F is an algebraic extension K/F *s.t.* every polynomial in $F[x]$ splits completely in K, denoted by $\overline{F}$.

Fact.

(1) An algebraic closure of F exists and is unique up to K-isomorphic.

(2) $\overline{F}$ is algebraically closed.

4.5 Separable extension

Definition 4.5.1. A polynomial $f(x) \in F[x]$ is called **separable** if f has no double root in $\overline{F}$

We can check it by defining the derivative of f.

Proposition 4.5.1. f is separable if and only if $(f(x), f'(x)) = F[x]$,*i.e.* coprime.

Example 15.

(1) If $\operatorname{char} F = 0$, then every irreducible polynomial is separable.

(2) $\operatorname{char} F = p$, there is a counter example for $F = \mathbb{F}_p(t)$

Meanwhile, if $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $\overline{F}[x]$, then

$$\frac{F[x]}{(f(x))} \otimes_F \overline{F} \cong \frac{\overline{F}[x]}{(f(x))} \tag{1}$$

α_i distinct then $(x - \alpha_i)$ coprime. By Chinese remainder theorem,

$$(1) \cong \frac{\overline{F}[x]}{(x - \alpha_1)} \cdots \frac{\overline{F}[x]}{(x - \alpha_1)} \cong \overline{F}^n$$

as $\overline{F}$-algebra. If not, then $(*)$ is not reduced.
So $f(x)$ separable if and only if $\overline{F}[x]/(f(x))$ is reduced.

Definition 4.5.2. K/F algebraic extension.

(1) $\alpha \in K$ is called **separable over** F if the minimal polynomial for α over F is separable.

(2) K/F is separable if every element is separable over F

Proposition 4.5.2 (Property D)**.** $R \to R' \to R''$ ring homomoephism, V R-module.
Then $R'' \otimes_{R'} (R' \otimes_R V) \cong R'' \otimes_R V$ as R''-module.

Proposition 4.5.3 (Property E)**.** K/F field extension, V F-vector space, $W, W' \subset V$ subspace.
Then the inclusion map $W \hookrightarrow V$ induces $K \otimes_F W \hookrightarrow K \otimes_F V$ is injective.
Moreover, if $W \neq W'$ as subspace of V, $K \otimes_F W \neq K \otimes_F W'$ as subspace of $K \otimes_F V$

4.6 separable extension

Theorem 4.6.1. K/F is finite extension. TFAE:

(a) K/F is separable.

(b) $K = F(\alpha_1, \cdots, \alpha_n)$ for α_i separable over F

(c) $K \otimes_F \overline{F} \cong \overline{F}^{[K:F]}$ as $\overline{F}$-algebra.

Proof. $(a) \Rightarrow (b)$ is obvious.
$(b) \Rightarrow (c)$ we set $K_i = F(\alpha_1, \cdots, \alpha_i)$.

Note. $f_2(x) :=$ minimal polynomial of $\alpha_2 \in K_2$ over $K_1 \Rightarrow f_2(x)$ divides minimal polynomial of α_2 over F, which has no double root.
So $f_2(x)$ has no double root, hence $K_2 = K_1(\alpha_2) = K_1[x]/(f_2(x))$.
Therefore $K_2 \otimes_{K_1} \overline{K_1} = \overline{K_1}^{[K_2:K_1]}$ by 1.

Since $\overline{F} = \overline{K_1}$, by the note we know (c) is true.
$(c) \Rightarrow (a)$ If α is not separable over F.
Let $f(x)$ be the minimal polynomial of α over F. By (1) we know

$$F(\alpha) \otimes_F \overline{F} = \frac{F[x]}{(f(x))} \otimes_F \overline{F} = \frac{\overline{F}[x]}{(f(x))}$$

Moreover, $F(\alpha) \subset K \Rightarrow F(\alpha) \otimes_F \overline{F} \subset K \otimes_F \overline{F} = \overline{F}^{[K:F]}$ which is reduced. Contradiction!

$\square$

Theorem 4.6.2 (primitive element theorem)**.** Every separable extension of finite degree K/F is simple.

Proof. By Prop 4.3.1, it suffices to prove $\overline{K}$ has finitely many intermediate extension M_α, which is true since

$$\overline{F}^{[M:F]} = M \otimes_F \overline{F} \subset K \otimes_F \overline{F} = \overline{F}^{[\overline{F}:F]}$$

$\square$

Remark 4.6.3. It focus on the intermediate field of K and the uniqueness of $M \otimes_F \overline{F}$

Corollary 4.6.4. $K/M/F$ finite extension.
K/F separable $\Leftrightarrow$ K/M, M/F separable.

4.7 Splitting field, extension of K-homomorphism

Definition 4.7.1. The (minimal) **splitting field** of $f(x)$ is a field extension K/F *s.t.*

(1) $f(x)$ splits completely in K

(2) $K = F(\alpha_1, \cdots, \alpha_n)$, α_i roots of $f(x)$ in K

Note. Splitting field exists and has degree less then $(\deg f)!$

We set these notations.
$K'/K/F$, L/F field extension.
$\sigma : K \to L$ is an F-homomorphism.
An F-homomorphism $K' \xrightarrow{\sigma'} L$ is an **extension** of σ if $\sigma'|_K = \sigma$.

Proposition 4.7.1 (extension lemma)**.** With the set-up as above, suppose K'/K is simple, where $K' = K(\beta)$, $g(x) \in K[x]$ minimal polynomial of β over K. Then

$$\{\sigma' : K' \to L : \text{extension of } \sigma\} \xleftrightarrow{bijective} \{\gamma \in L \; \sigma g(\gamma) = 0\}, \; \sigma' \mapsto \gamma = \sigma'(\beta)$$

i.e. roots of σg is bijective with the extension of σ.
In particular, numbers of extensions is less then $\deg g = [K' : K]$. Moreover, if the equality holds, then g separable and K'/K separable.

Proof.

$$\begin{tikzcd}
K[x] \arrow[r, "\tilde{\sigma}"] \arrow[d] & L \\
K[x]/(g(x)) \arrow[ur, "\exists"] &
\end{tikzcd}$$

□

Corollary 4.7.2. If L, M are splitting fields of $f(x) \in F[x]$. Then $L \cong M$. i.e. splitting field is unique up to F-isomorphism.

Proof. We can construct a homomorphism by mapping the root of $f(x)$ in M to roots in L □

4.8 Finite field

K is a finite field, then $|K| = p^n$.

Theorem 4.8.1. Let K be a finite field of order $q = p^n$

(1) K is the splitting field of $x^q - x \in \mathbb{F}_p[x]$.
In particular, any two such K, K' are $\mathbb{F}_p$-isomorphic. Hence we can write $K = \mathbb{F}_q$

(2) $K^\times$ is a cyclic group of order $q-1$

(3) $\mathbb{F}_{p^m}$ is a subfield of $\mathbb{F}_{p^n} \Leftrightarrow m|n$. In particular, every extension of finite fields is simple and separable.

Proof. (1) $(f(x), f'(x)) = 1 \Rightarrow f(x) = x^q - x$ is separable. Since $\alpha^q = \alpha$ in K, K is splitting field of $x^q - x$ □

4.9 Normal extensions

Definition 4.9.1. A field extension K/F is normal if $\forall f(x) \in F[x]$ irreducible, having a root in K splits completely in K.

Theorem 4.9.1 (characterization of normal extensions)**.** K/F is finite extension. TFAE

(1) K/F is normal

(2) K is the splitting field of some $f(x) \in F[x]$

(3) $\forall L/K$, $\forall K \xrightarrow{\sigma} L$ F-homomorphism, $\sigma(K) = K$.

Proof. (2) $\Rightarrow$ (3). WLOG, $f(x)$ is monic.
Write $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $K[x]$ and $K = F(\alpha_1, \cdots, \alpha_n)$.
Take any L/K and $\sigma : K \to L$. It suffices to show $\sigma(\alpha_i) \in K, \forall\, i$.
Write $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, a_i \in F$.
Then $f(\sigma(\alpha_i)) = \sigma(\alpha_i^n + \cdots + a_1\alpha_i + a_0) = \sigma(f(\alpha_i)) = 0$.
SO $\sigma(\alpha_i)$ is one of $\alpha_1, \cdots, \alpha_n \in K$.
(3) $\Rightarrow$ (1). Take any $f(x) \in F[x]$ monic and irreducible. Assume $f(x)$ has a root $\alpha \in K$. Set $\alpha_1 =$

$\alpha, f_1 = f$ and write $K = F(\alpha_1, \cdots, \alpha_n)$. $f_i(x) \in F[x]$ minimial polynomial of α_i.
Let $L \supset K$ be the splitting field of $f_1 \cdots f_n$.
Take any $\alpha' \in L$ s.t. $f(\alpha') = 0$. Suffices to prove $\alpha' \in K$.
For this, we will construct $\sigma : K \to L$ F-homomorphism with $\sigma(\alpha) = \alpha'$.
By extension lemma, there is a F-homomorphism $\sigma : K_1 = F(\alpha_1) \to L$ s.t. $\sigma(\alpha) = \alpha'$.
By extension lemma, there is an extension of σ. So we end the proof.
(1) $\Rightarrow$ (2) □

Corollary 4.9.2. $K/M/F$ field extension.
If K/M, M/F normal $\Rightarrow K/F$ is normal. K/F normal $\Rightarrow K/M$ is normal, but M/F may not be normal.
See the example $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}(\sqrt[3]{2})/Q$

4.10 Galois extensions

For K/F field extension, $\operatorname{Aut}(K/F) := \{\sigma : K \to K : F\text{-isomorphism}\}$

Lemma 4.10.1. K/F is finite, $|\operatorname{Aut}(K/F)| \leq [K : F]$. If equality holds, K/F is separable.

Proof. Since we can define a chain of extension $\sigma_i : K_i = K_{i-1}(\alpha_i) \to K$. And by extension lemma

$$\sharp\{\text{extension of } \sigma_i : K_i \to K to K_{i+1} \to K\} \leq [K_{i+1} : K_i]$$

□

Definition 4.10.1. K/F is **Galois** if it is separable and normal.

Note. Every algebraic extension K/F in char 0 is separable. In this case Galois=normal.

Theorem 4.10.1 (characterization of finite Galois extension)**.** K/F is finite.

(1) K/F Galois.

(2) K/F is the splitting field of a separable polynomial in $F[x]$.

(3) $|\operatorname{Aut}(K/F)| = [K : F]$

in this case $\operatorname{Gal}(K/F) := \operatorname{Aut}(K/F)$

Proof. (1) $\Leftrightarrow$ (2) combine previous results.
(1) $\Rightarrow$ (3). Since K/F separable, $K = F(\alpha) = \frac{F[x]}{(f(x))}$ by primitive element theorem.
K/F normal $\Rightarrow f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ in $K[x]$ with α_i.
By extension lemma $|\operatorname{Aut}(K/F)| = \{\text{roots of } f(x) \in K\ \} = n = [K : F]$.
(3) $\Rightarrow$ (1), by the lemma 4.10.1 K/F is separable.
By primitive element theorem, $K = F(\alpha) = F[x]/(f(x))$.
Let $\operatorname{Aut}(K/F) = \{\sigma_1, \cdots, \sigma_n\}$. As we know, $\alpha = \sigma_1(\alpha), \cdots, \sigma_n(\alpha)$ are roots of $f(x)$ in K.
Since $K = F(\alpha)$, so $\sigma_i(\alpha)$ are distinct. Hence, $f(x) = (x - \sigma_1(\alpha)) \cdots (x - \sigma_n(\alpha))$.
So K/F is the splitting field of $f \in F[x]$ □

Definition 4.10.2. $H < \mathrm{Aut}(K/F)$ subgroup. Define

$$K^H := \{x \in K : \forall \sigma \in H, \sigma(x) = x\}$$

called **fixed field** by H (on intermediate field of K/F)

Theorem 4.10.2 (Fixed field theorem)**.** Let $H < \mathrm{Aut}(K/F)$ be a finite subgroup. Then K/K^H is a finite Galois extension with $H \xrightarrow{\cong} \mathrm{Aut}(K/K^H) = \mathrm{Gal}(K/K^H)$.

In this proof of the theorem, we need an important lemma which describes polynomial whose root is $\alpha \in K^H$

Lemma 4.10.2. Take any $\alpha \in K$. Let $\alpha = \alpha_1, \cdots, \alpha_m$ be the distinct elements in the orbit of α over H.
Consider $f_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_m)$. Then $f_\alpha(x) \in K^H[x]$

This means we can get an irreducible polymomial in $K^H[x]$ easily, and it implies that K/K^H is separable too.

Theorem 4.10.3 (characterization of finite Galois extension 2)**.** K/F finite. TFAE

(1) K/F is Galois

(2) K/F is the splitting field of a separable polynomial over M.

(3) $|\mathrm{Aut}(K/F)| = [K : F]$

(4) $K^{\mathrm{Aut}(K/F)} = F$

(5) $K \otimes_F K \cong K^{[K:F]}$

Proof. $K \supset K^{\mathrm{Aut}(K/F)} \supset F$. In theorem 4.10.2, we know $[K : K^{\mathrm{Aut}(K/F)}] = |\mathrm{Aut}(K/F)|$, so (3) $\Leftrightarrow$ (4) ☐

Corollary 4.10.4. $K = F(\alpha)/F$ is Galois. Then the minimial polynomial over F is $\prod_{\sigma \in \mathrm{Gal}(K/F)} (x - \sigma(\alpha))$.

Corollary 4.10.5. K/F Galois $\Rightarrow$ K/M Galois for M intermediate field.

Theorem 4.10.6 (fundamental theorem in Galois theory)**.** Let K/F be a finite Galois extension. Then

$$\{M \text{ intermediate of } K/F\} \xleftrightarrow{bij} \{K < \mathrm{Gal}(K/F)\} \tag{2}$$
$$M \mapsto H := \mathrm{Gal}(K/M) < \mathrm{Gal}(K/F) \tag{3}$$
$$M = K^H \leftarrow H \tag{4}$$

Moreover, foe $M, M' \leftrightarrow H, H'$.

(1) $M \subset M' \Leftrightarrow H > H'$

(2) $\forall \sigma \in \mathrm{Gal}(K/F)$, $\sigma(M)$ intermediate $\leftrightarrow \sigma H \sigma^{-1} < \mathrm{Gal}(K/F)$ *i.e.* $\sigma H \sigma^{-1} = \mathrm{Gal}(K/\sigma(M))$

(3) M/F Galois $\Leftrightarrow H \triangleleft \mathrm{Gal}(K/F)$

In this case, $\mathrm{Gal}(K/F) \to \mathrm{Gal}(M/F)$ induces

$$\mathrm{Gal}(K/F)/_{\mathrm{Gal}(K/M)} \xrightarrow{\cong} \mathrm{Gal}(M/F)$$

Proof. The first part only need to check

(1) is trivial

(2) First to prove $\sigma H \sigma^{-1} < \mathrm{Gal}(K/\sigma(M))$ (show they are fixed point). Then check the order of them.

(3) M/F Galois $\Leftrightarrow M/F$ normal $\Leftrightarrow \forall \sigma \in \mathrm{Gal}(K/F)$, $\sigma(M) = M \Leftrightarrow \forall \sigma, \sigma H \sigma^{-1} = H$.

Now consider the restriction $\sigma \mapsto \sigma|_M \in \mathrm{Gal}(M/F)$ we get the whole proof. □

Example 16. $q = p^m$, $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois extension(splitting field of $x^{q^n} - x$)

Let $F_{rq} : x \mapsto x^q$.

Then $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) =< F_{rq} >$ be a cyclic group(check the order).

Subgroups are $H =< F_{rq}^a >$, $a|n$

Fixed field are $\mathbb{F}_{q^n}^H = \mathbb{F}_{q^a}$.

So $\mathbb{F}_{q^n} \supset \mathbb{F}_{q^a} \Rightarrow a|n$.

By this example, if we can describe the Galois group, then it is easy to check whether the intermediate field is Galois by checking if the corresponding subgroup is normal.

Example 17. Consider K splitting field of $x^4 - 2$ over $\mathbb{Q}$.

Then the Galois group $G = \{1, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\} =< \rho, \tau : \rho^4 = 1, \tau^2 = 1, \tau\rho = \rho^3\tau >= D_8$.

where $\rho : \sqrt[4]{2} \mapsto \sqrt[4]{2}i$ $\tau : i \mapsto -i$

4.11 polynomials and discriminant

Definition 4.11.1.

$$\Delta(f) := \prod_{i<j} (\alpha_i - \alpha_j)^2 \in \overline{F}$$

called the **discriminant** of f.

Note.

(1) $\Delta(f)$ is independent of order of $\alpha_1, \cdots, \alpha_n$

(2) $\Delta(f) \neq 0 \Leftrightarrow f$ is separable.

Proposition 4.11.1. $\Delta(f) \in F$

Proof. $\Delta(f)$ is a symmetric function in α_i. So it can be written in terms of elementary symmetric function in $\alpha_i \in F$. □

Definition 4.11.2. Call $G := \mathrm{Gal}(K/F)$ the Galois group of f for K splitting field of a separable f.

Noticed that $\sigma(\Delta(f)) = \prod_{i<j}(\sigma(\alpha_i - \alpha_j))^2 = \Delta(f)$.

So $\Delta(f) \in K^G = F$.

Proposition 4.11.2. $G = \mathrm{Gal}(K/F) \hookrightarrow Perm(\{\alpha_1, \cdots, \alpha_n\}) = S_n$.

Moreover, if f is irreducible, $K \supset F(\alpha_1) \supset F$, $n|\,|G|$

Set $\delta := \prod_{i<j}(\alpha_i - \alpha_j) \in K$. Then $\sigma(\delta) = \mathrm{sign}(\sigma)\cdot\delta$. So $G = A_n \Leftrightarrow \forall\sigma \in G, \mathrm{sign}(\sigma) = 1 \Leftrightarrow \delta \in K^G = F$ in the case that $n = 3$.

i.e. $G = A_3$ if and only if $\sqrt{\Delta(f)}$ exists in F.

$G = S_3$ if and only if $\Delta(f)$ doesn't exists.

For $n = 4$ there is some similar result.

Now we consider $K := F(u_1, \cdots, u_n)$, and the induced injection $S_n \hookrightarrow \mathrm{Aut}(K/F)$.

Let Λ_i be the elementary symmetric function in $u_i \in K$ of degree i. ($\Lambda_1 = u_1 + \cdots, u_n$)

Theorem 4.11.3. $K/F(\Lambda_1, \cdots, \Lambda_n)$ is a Galois extension with Galois group S_n

Proof. $K \supset K^{S_n} \supset F(\Lambda_1, \cdots, \Lambda_i)$.

By fixed field theorem, the Galois group is of order $n!$. So it has degree of $n!$

However, $f(x) = x^n - \Lambda_1 x^{n-1} + \cdots + (-1)^n\Lambda_n \in F(\Lambda_1, \cdots, \Lambda_n)[x]$ and $f(x) = (x-u_1)\cdots(x-u_n) \in K[x]$.

So K is the splitting field of f.

$[K : F(\Lambda_1, \cdots, \Lambda_n)] \leq (\deg f)! = n!$. ☐

4.12 Cyclotomic fields

Definition 4.12.1. Call $\psi \in F$ is an n^{th} **root of unity** if $\psi^n = 1$.

If $\forall d|n, d < n, \psi^d \neq 1$. Call ψ is **primitive**

For $\mathrm{char}\, F = p$, there is no n^{th} primitive root of unity for $p|n$.

Now assume $n \in F^\times$.

Let K be the splitting field of $x^n - 1$ over F, which is separable be $n \in F^\times$.

Then $K = F(\psi)$ is simple, and ψ is a primitive n^{th} root of unity.

Now it induces a map

$$\begin{aligned} \mathrm{Gal}(K/F) &\xrightarrow{\chi} (\mathbb{Z}/n)^\times \\ \sigma &\mapsto \chi(\sigma) s.t.\ \psi^{\chi(\sigma)} = \sigma(\psi) \end{aligned}$$

Now we get these proposition:

Proposition 4.12.1.

(1) $\psi' = \psi^a$ is another primitive n^{th} root of unity and $\sigma(\psi') = (\psi')^{\chi(\sigma)}$

(2) χ is group homomorphism.

(3) $\chi(\sigma) = 1$ is and only if $\sigma(\psi) = \psi \Leftrightarrow \sigma = id$ *i.e.* χ is injective.

So there is a injective homomorphism so-called **cyclotomic character** for $n \in F^\times$

$$\mathrm{Gal}(F(\psi_n)/F) \overset{\chi}{\hookrightarrow} (\mathbb{Z}/n)^\times$$

$$\Phi_n(x) := \prod_{a \in (\mathbb{Z}/n)^\times} (x - \psi_n^a) \in F[x]$$

is called the **cyclotomic polynomial**.

Proposition 4.12.2.

(1) $\deg \Phi_n = |(\mathbb{Z}/\ltimes)^\times| = \varphi(n)$

(2) $x^n - 1 = \prod_{d|n} \Phi_d(x)$

(3) χ is isomorphism if and only if $\Phi_n(x)$ is irreducible over F.

Theorem 4.12.3. $\Phi_n(x) \in \mathbb{Q}[x]$ is irreducible.
In particular, $\chi : \mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}) \to (\mathbb{Z}/n)^\times$ is isomorphism.

Proof. ψ_n is an algebra integer so $\Phi_n \in \mathbb{Z}[x]$.
By Gauss' lemma, it suffices to prove $\Phi_n(x)$ is irreducible over $\mathbb{Z}$.
However, every polymomial that has one root should have all the roots. $\square$

Theorem 4.12.4 (Kronecher-Weber)**.** If K/Q is abelian, then $\exists n s.t.\ K \subset \mathbb{Q}(\psi_n)$.
In other words, abelian extensions of $\mathbb{Q}$ are governed by cyclotomic extensions.

4.13 Composite field

Definition 4.13.1. A **composite field** of K_1 and K_2 (over F) is a field L/F together with F-homomorphism $u_1 : K_1 \hookrightarrow L, u_2 : K_2 \hookrightarrow L$ s.t. L is generated by $u_1(K_1), u_2(K_2)$.
Often write $L = K_1K_2$.

Theorem 4.13.1. A composition field exists and is unique up to F-isomorphism.

Proof. Let $R := K_1 \otimes_F K_2$. M be its maximal ideal. Then $L := R/M$ is a field. $\square$

Theorem 4.13.2 (Galois theory for composite fields)**.**

(1) K/F finite Galois and F'/F any field extension. Set $K' = KF'$. Then K'/F' is finite Galois and

$$\mathrm{Gal}(K'/F') \xrightarrow{\cong} \mathrm{Gal}(K/_{K \cap F'}), \sigma \mapsto \sigma|_K$$

is an isomorphism. In particular, $[K' : F'] = [K : K \cap F']$

(2) $K_1, K_2/F$ is finite Galois. Then $K_1K_2, K_1 \cap K_2$ are Galois over F and

$$\mathrm{Gal}(K_1K_2/_{K_1 \cap K_2}) \to \mathrm{Gal}(K_1/_{K_1 \cap K_2}) \times \mathrm{Gal}(K_2/_{K_1 \cap K_2}), \sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

is an isomorphism.

Proof. (1)If $f(x) \in F[x]$ separable*s.t.* K is the splitting field of F. Then $K' = KF'$ is the splitting field of $f(x) \in F'[x]$. i.e. K'/F' is finite Galois.
Now take $\sigma \in \mathrm{Gal}(K'/F')$. K/F is normal $\Rightarrow \sigma|_K : K \to K'$ has image in K.
So $\mathrm{Gal}(K'/F') \to \mathrm{Gal}(K/_{K\cap F})$ is well-defined.
If $\sigma|_K$ is identity, then $\sigma = id$ on K' $\Rightarrow$ the map is injective,
Now since $K^{\mathrm{Gal}(K'/F')} = K \cap F'$(if not, then it is a simple extension and there is a contradiction from extension lemma) $\Rightarrow \mathrm{Gal}(K'/F') = \mathrm{Gal}(K/_{K\cap F'})$.
(2) Take $f_i \in F[x]$ separable *s.t.* K_i is the splitting field.
Let $f_i = g_i h$, $(g_1, g_2) = 1$.
Then K_1K_2 is the splitting field of separable polynomial $g_1g_2h \in F[x]$. So K_1K_2 is finite Galois extension.
The map is easy to check that it is well-defined and injective.
$|\mathrm{Gal}(K_1K_2/_{K_1\cap K_2})| = [K_1K_2 : K_1 \cap K_2] = [K_1K_2 : K_2][K_2 : K_1 \cap K_2] = [K_1 : K_1 \cap K_2][K_2 : K_1 \cap K_2]$ by (1). So it is isomorphism. $\square$

4.14 traces and norms

Definition 4.14.1. Let K/F be a finite extension. For $\alpha \in K$, write $m_\alpha : K \to K, x \mapsto \alpha x$

$$\mathrm{Tr}_{K/F}(\alpha) := \mathrm{Tr}(m_\alpha) \in F$$

$$\mathrm{N}_{K/F}(\alpha) := \det(m_\alpha) \in F$$

Call them trace and norm of α respectively.

Proposition 4.14.1.

(1) Tr is F-linear, $N(\alpha\beta) = N(\alpha)N(\beta), N(a\alpha) = a^{[K:F]}N(\alpha)$

(2) (transitivity) For $L/K/F$, $\mathrm{Tr}_{L/F} = \mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{L/K}$, $N_{L/F} = N_{K/F} \circ N_{L/K}$

(3) Assume K/F is separable and write $\mathrm{Hom}_F(K, \overline{F}) = \{\sigma_1, \cdots, \sigma_n\}$, $n = [K : F]$.
Then $\mathrm{Tr}_{K/F}(\alpha) = \sum \sigma_i(\alpha)$, $N_{K/F}(\alpha) = \sigma_1(\alpha)\cdots\sigma_n(\alpha)$(Note that if K/F is Galois, $\mathrm{Gal}(K/F) = \{\sigma_1, \cdots, \sigma_n\}$)

(4) (non-degeneracy of trace pairing) Assume K/F separable. The F-bilinear map $K\times K \to F, (\alpha, \beta) \mapsto \mathrm{Tr}_{K/F}(\alpha\beta)$ is non-degenerate, *i.e.* $\forall \alpha \neq 0 \in K$, $\exists \beta \in K$ *s.t.* $\mathrm{Tr}(\alpha\beta) \neq 0$

Proof. (1)(2) is easy to check
(3) Write $K = F(\beta)$, $f(x) \in F[x]$ minimal polynomial of β.
Write $f(x) = (x - \beta_1)\cdots(x - \beta_n)$ in $\overline{F}[x]$.
By extension lemma, $\mathrm{Hom}_F(K, \overline{F}) = \{\sigma_1, \cdots, \sigma_n\}$ *s.t.* $\sigma_i(\beta) = \beta_i$.
We know that $\overline{F} \otimes_F K \cong \overline{F} \otimes_F \frac{F[x]}{(f(x))} \cong \frac{\overline{F}[x]}{(f(x))}$.
And we can conclude that $\gamma \otimes \delta \mapsto (\gamma\sigma_1(\delta), \cdots, \gamma\sigma_n(\delta))$.
Now $id \otimes m_\alpha : \overline{F} \otimes_F K \to \overline{F} \otimes_F K, \gamma \otimes \delta \mapsto \gamma \otimes \alpha\delta$.

$\mathrm{Tr}(m_\alpha) = \mathrm{Tr}(id \otimes m_\alpha), \det(m_\alpha) = \det(id \otimes m_\alpha)$.

So in $\overline{F} \otimes K \cong \overline{F}^n$ we can easily find the answer.

(4)In char 0 case, take $\beta = \frac{1}{\alpha}$. In □

4.15 Advanced theorem in Galois theory

Theorem 4.15.1 (linear independence of F-homomorphism)**.** *K, L F field extension. Let $\sigma_1, \cdots, \sigma_n : K \to L$ be distinct F-homomorphism. $a_1, \cdots, a_n \in L$.*

If $\forall x \in K$, $a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0$, then $a_1 = \cdots = a_n = 0$

Theorem 4.15.2 (Hilbert 90)**.** *Let K/F be finite Galois extension with $G = \mathrm{Gal}(K/F)$.*

Let $A : G \to K^\times$ be a set map s.t. $\forall \sigma\tau \in G$, $A(\sigma\tau) = A(\sigma)\sigma(A(\tau))$.

Then $\exists \alpha \in K^\times$ s.t. $A(\sigma) = \frac{\sigma(\alpha)}{\alpha}, \forall \sigma \in G$.

Proof. Apply linear independence of F-homomorphism, $\exists \beta \in K^\times$ *s.t.* $\sum_{\tau \in G} A(\tau)\tau(\beta) \neq 0$ □

Remark 4.15.3. If we consider group cohomology $H^0(G, M) = M^G$, $H^1(G, M) = \{$1-cocycle $A : G \to M\}$. Then Hilbert 90 tells us if K/F finite Galois, $H^1(\mathrm{Gal}(K/F), K^\times) = \{1\}$

Corollary 4.15.4. Assume K/F is finite cyclic Galois *i.e.* $G = \mathrm{Gal}(K/F) = \langle\sigma\rangle$ cyclic.

If $\alpha \in K^\times$ satisfies $N_{K/F}(\alpha) = 1$, then $\exists \beta \in K^\times$ *s.t.* $\alpha = \frac{\sigma(\beta)}{\beta}$.

Proof. Set $A(\sigma^m) = \alpha\sigma(\alpha) \cdots \sigma^{m-1}(\alpha) \in K^\times$.

Then A defines a 1-cocycle $G = \langle\sigma\rangle \to K^\times$.(By using $N(\alpha) = 1$)

By Hilbert 90, $\exists \beta \in K^\times$ *s.t.* $A(\sigma) = \frac{\sigma(\beta)}{\beta}$. □

4.16 Kummer theory

Theorem 4.16.1 (Kummer's theorem)**.** *Assume $n \in F^\times$ and $\psi_n \in F$.*

(1) *For $a \in F^\times$, write $\sqrt[n]{a} \in \overline{F}$ for a root of $x^n - a$.*
 Then $F(\sqrt[n]{a})/F$ is finite cyclic Galois.
 Moreover, $d := [F(\sqrt[n]{a}) : F]$.
 Then $d|n$, $(\sqrt[n]{a})^i \notin F$ for $i < d$ and $(\sqrt[n]{a})^d \in F$.

(2) *Let K/F be a finite cyclic Galois extension of degree of $d|n$. Then $\exists a \in F^\times$ s.t. order of $\overline{a} \in F^\times/_{F^{\times n}}$ is d and $K = F(\sqrt[n]{a})$*
 or $\exists b \in F^\times$ s.t. order of $\overline{b} \in F^\times/_{(F^\times)^d}$ is d and $K = F(\sqrt[n]{b})$

Proof. (1)From $\psi_n \in F$ we know that K/F is the splitting field of separable polynomial $x^n - a$.

So $K = F(\sqrt[n]{a})$ is finite Galois.

Consider $\iota : G \to \mathbb{Z}/n, \sigma \mapsto m s.t.$ $\sigma(\sqrt[n]{a}) = \sqrt[n]{a}\psi_n^m$.

Then ι is a group isomorphism.

We can check that $\sigma((\sqrt[n]{a})^l) = (\sqrt[n]{a})^l$ is and only if $d|l$. So we end the proof of (1)

(2)Let $\psi_d = \psi_n^{n/d} \in F$, so WLOG we can assume $d = n$.

Then K/F is finite cyclic of degree n.

$N_{K/F}(\psi_n) = \prod_{\tau} \in G\tau(\psi_n) = \psi^{[K:F]} = 1$.

By the corollary to Hilbert 90, $\exists \alpha \in K^\times$ *s.t.* $\psi_n = \frac{\sigma(\alpha)}{\alpha}$, $\sigma \in G$ generator.

So $\sigma(\alpha) = \alpha \cdot \psi_n$ so $\sigma(\alpha^n) = \alpha^n$ *i.e.* $\alpha^n \in F^\times$.

Set $a = \alpha^n \in F^\times$ and we get the answer. □

4.17 Solvability by radicals

Assume $\mathrm{char}(F) = 0$. M is the splitting field of a polynomial $f(x) \in F[x]$

Definition 4.17.1. Say f is **solvable by radicals** if $\exists F = K_0 \subset K_1 \subset \cdots \subset K_m = K$ *s.t.* $K_{i+1} = K_i(\sqrt[n_i]{\alpha_i})$, $\alpha_i \in K_i^\times$, $M \subset K$

Recall that G is solvable if $G \triangleright D(G) \triangleright \cdots \triangleright D^m(G) = \{1\}$, where $D(G) = [G, G] =< ghg^{-1}h^{-1} >$

Proposition 4.17.1.

(1) G is solvable if and only if $\exists G \triangleright G_1 \triangleright \cdots \triangleright G_m = 1$ *s.t.* G_i/G_{i+1} is abelian. $\Leftrightarrow \exists G \triangleright G_1 \triangleright \cdots \triangleright G_m = 1$ *s.t.* $G_i/G_{i+1} \cong \mathbb{Z}/p_i$ cyclic group of prime order.

(2) Every subgroup or quotient group of solvable group is solvable.

(3) $N \triangleleft G$ if $N, G/N$ is solvable, then G is solvable.

Theorem 4.17.2. f is solvable by radicals if and only if the Galois group is a solvable group

Example 18. $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)(x - \alpha_5)$ for $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$, $\alpha_4, \alpha_5 \notin \mathbb{R}$.
Then Galois group is f is S_5 which is non-solvable $\Rightarrow$ f is not solvable by radicals.

4.18 Algebraic closure

Theorem 4.18.1 (Steinitz)**.** An algebraic closure exists and is unique up to isomorphism.

Index