Notes on CS7343 – Applied Algebraic

Zhidan Li

Fall 2023

Contents

1 Groups, Rings, and Fields

Firstly we introduce some basic definitions.

Definition 1.1 (groups)**.** A *group* $(G, \cdot)$ is a tuple consist of a non-empty set G and an operator $\cdot : G \times G \to G$ satisfying:

1. **Associativity:** For all $\alpha, \beta, \gamma \in G$, $(\alpha\beta)\gamma = \alpha(\beta\gamma)$.
2. **Identity:** There exists an element $\varepsilon \in G$ with $\varepsilon\alpha = \alpha\varepsilon = \alpha$ for all $\alpha \in G$.
3. **Inverses:** For all $\alpha \in G$, there exists an element $\alpha^{-1} \in G$ such that $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \varepsilon$.

Moreover, if $\alpha\beta = \beta\alpha$ for all $\alpha, \beta \in G$, we call $(G, \cdot)$ to be *abelian* or *commutative*.

Remark 1.2. We often use '1' to denote the identity. And when we use '+' to denote the operator, we usually use '0' to denote the identity and '$-\alpha$' to denote the inverse.

Example 1.3. *$(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are groups (actually they are all abelian groups).*

$(M_n(\mathbb{R}), +)$ and $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ are groups where $M_n(\mathbb{R}) = \mathbb{R}^{n\times n}$ and $\mathrm{GL}_n(\mathbb{R}) := \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\}$.

Let $Z_n := \{0, 1, \ldots, n-1\}$ for all $n \in \mathbb{N}_{>0}$. For modular operators $+$ and $\cdot$, $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_p \setminus \{0\}, \cdot)$ are groups for all $n \in \mathbb{N}_{>0}$ and prime number p.

For the sake of simplicity, we define some notations here. For $x \in G$, we define $x^0 = 1$, and for all $n \geq 1$, let $x^n := x^{n-1} \cdot x = x \cdot x^{n-1}$. For $n < 0$, we define $x^{-n} := (x^n)^{-1} = (x^{-1})^n$. It's not hard to see for all $n, m \in \mathbb{N}$, $(x^n)^m = (x^m)^n = x^{nm}$.

Order of a group and an element

For a finite group $(G, \cdot)$, we define its *order* $o(G)$ as $o(G) := |G|$. With some abuse, for an element $\alpha \in G$, we define its *order* $o(\alpha)$ as: if there exists $n \in \mathbb{N}_{>0}$, $\alpha^n = 1$, then $o(\alpha) = \min\{n \in \mathbb{N}_{>0} : \alpha^n = 1\}$; otherwise $o(\alpha) = \infty$.

It is not hard to see, if $|G| < \infty$, then for all $\alpha \in G$, $o(\alpha) < \infty$.

Subgroups

Definition 1.4 (subgroups)**.** Given a group $(G, \cdot)$, for $S \subset G$, we call $(S, \cdot)$ is a *subgroup* of $(G, \cdot)$ if $(S, \cdot)$ is a group. We write it as $S < G$.

Remark 1.5. Note that the class of subgroups is not closed under the *set product*, e.g., for two subgroups H, K, the set product

$$HK := \{hk : \forall h \in H, k \in K\}$$

is not necessarily a subgroup of G.

We introduce a kind of subgroups named *cyclic subgroups*.

Definition 1.6 (cyclic subgroups)**.** Given a group $(G, \cdot)$ and $\alpha \in G$, the *cyclic subgroup* (α) is defined as

$$(\alpha) := \{\alpha^n : n \in \mathbb{N}\}.$$

We call this group as *the cyclic subgroup of G generated by α*. When G is (α), we say G is *cyclic*.

Corollary 1.7. *If $o(G)$ is a prime, then G is cyclic.*

For $G = (a)$ with $o(a) = n$, it holds that for every $k \in \mathbb{N}_{>0}$,

$$o(a^k) = \frac{n}{(n, k)}.$$

1.1 Cosets and Lagrange's Theorem

Given a group G and $H < G$, we define a relation $\sim$ on G by: for all $\alpha, \beta \in G$, we say $\alpha \sim \beta$ if and only if $\alpha^{-1}\beta \in H$. It's not hard to verify $\sim$ is an equivalence relation.

Based on $\sim$, we introduce the definition of cosets.

Definition 1.8 (left cosets)**.** For $\alpha \in G$, the *left coset* αH is defined as

$$\alpha H := \{\alpha h : h \in H\}.$$

Definition 1.9 (right cosets)**.** For $\alpha \in G$, the *right coset* $H\alpha$ is defined as

$$H\alpha := \{h\alpha : h \in H\}.$$

Under $\sim$, it is obvious to see the equivalence class of α is αH ($\alpha \sim \beta \iff \alpha^{-1}\beta \in H \iff \beta \in \alpha H$), thus leading to the statement that $\alpha \sim \beta \iff \alpha H = \beta H$. Then we can partition G as

$$G = \bigcup_{\alpha \in G} \alpha H.$$

Consider the mapping $\varphi : H \to \alpha H, h \mapsto \alpha h$. It can be verified that φ is a bijection. Then it holds that, if G is finite, $|H| = |\alpha H|$.

Theorem 1.10 (Lagrange's Theorem)**.** *For a finite group G and $H < G$, it holds that $|H| \mid |G|$.*

Then it is safe to introduce the index of H.

Definition 1.11 (index)**.** For a finite group G and $H < G$, we define the *index* of H as

$$(G : H) := |G|/|H|.$$

Moreover, we use G/H to denote the collection of all distinct left cosets of H.

Normal subgroups

Consider the set G/H, we want to define a proper operator $*$ on it such that $(G/H, *)$ is a new group. The goal is:

$$\alpha H * \beta H = \alpha\beta H.$$

A natural idea is to let $*$ to be the set product,

Note that, if for all $\beta \in H$, $H\beta = \beta H$

$$\alpha H \beta H = \alpha\beta H H = \alpha\beta H.$$

Then $(G/H, *)$ is a proper group. Then it motivates us to investigate such subgroups.

Definition 1.12 (normal subgroups)**.** We say a subgroup $H < G$ is normal if and only if for all $\alpha \in H$, $\alpha H = H\alpha$. We write it as $H \rhd G$.

Corollary 1.13. *If G is an abelian group and $H < G$, then $H \rhd G$.*

1.2 Euler's ϕ function

Now we show a typical application of groups. For $n \in \mathbb{N}_{>0}$, define the *Euler's ϕ function* as

$$\phi(n) := |\{i \in [n] : i \perp n\}|.$$

It is not hard to show that

$$\phi(m_1 m_2) = \phi(m_1)\phi(m_2), \forall (m_1, m_2) = 1.$$

By definition, $\phi(p^n) = p^{n-1}(p-1)$ for all prime p and $n \geq 1$.

Now we consider the group $(\mathbb{Z}_n^*, \cdot)$ where $\mathbb{Z}_n^* := \{\alpha \in \mathbb{Z}_n : (\alpha, n) = 1\}$.

Theorem 1.14 (Euler's Theorem)**.** *For all $\alpha \in \mathbb{Z}_n^*$, it holds that*

$$\alpha^{\phi(n)} = 1.$$

Proof. Since $\mathbb{Z}_n^*$ is finite, $o(\alpha)$ is finite. Then the cyclic subgroup (α) is a finite subgroup with cardinality $o(\alpha)$. By Theorem 1.10, it holds that $o(\alpha) \mid |G| = \phi(n)$ Then $\alpha^{\phi(n)} = 1$. ◻

Corollary 1.15 (Fermat's Little Theorem)**.** *For all $\alpha \in \mathbb{Z}_p^*$ with prime p, it holds that*

$$\alpha^p = \alpha.$$

1.3 Group homomorphism

Now we introduce a very important definition for groups.

Definition 1.16 (group homomorphism)**.** Given two groups G, H, we say a mapping $\varphi : G \to H$ is a *group homomorphism* if for all $\alpha, \beta \in G$, $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.

Moreover, when φ is bijective, we say φ is an *isomorphism.*

There are some trivial properties for group homomorphism.

- It holds that $\varphi(1) = 1$.
- For all $\alpha \in G$, it holds that $\varphi(\alpha^{-1}) = \varphi(\alpha)^{-1}$.

For a group homomorphism φ, define its *kernel* as

$$\ker(\varphi) := \{\alpha \in G \mid \varphi(\alpha) = 1\}.$$

Corollary 1.17. *It holds that* $\ker(\varphi) \rhd G$.

Proof. Firstly, it is not hard to see $\ker(\varphi) < G$. Now we show the kernel is normal.

For all $\alpha \in G$, $\beta \in \ker(\varphi)$, since φ is a group homomorphism,

$$\begin{aligned}\varphi(\alpha^{-1}\beta\alpha) &= \varphi(\alpha^{-1})\varphi(\beta)\varphi(\alpha) \\ &= \varphi(\alpha^{-1})\varphi(\alpha) = 1.\end{aligned}$$

Then it holds that $\alpha^{-1}\beta\alpha \in \ker(\varphi)$, which means $\bigcup_\alpha \alpha^{-1}\ker(\varphi)\alpha \subseteq \ker(\varphi)$.

On the other hand, it holds that $\ker(\varphi) \subseteq \bigcup_\alpha \alpha^{-1}\ker(\varphi)\alpha$. Then we can show $\ker(\varphi)$ is normal. ◻

Since the kernel is a normal group, we can show $(G/\ker(\varphi), \cdot)$ is a proper group.

Theorem 1.18 (First Isomorphism Theorem)**.** *Given a group homomorphism $\varphi : G \to H$ (without loss of generality assume that φ is surjective), the mapping $\varphi' : G/\ker(\varphi) \to H$, $\alpha\ker(\varphi) \mapsto \varphi(\alpha)$ is a group isomorphism.*

Proof. Firstly we prove the mapping φ' is well-defined. For $\alpha \sim \beta$ ($\alpha^{-1}\beta \in \ker(\varphi)$), it holds that $\varphi(\alpha^{-1}\beta) = 1$, thus leading to $\varphi(\alpha) = \varphi(\beta)$. Then it holds that $\varphi'(\alpha\ker(\varphi)) = \varphi'(\beta\ker(\varphi))$, which means φ' is well-defined.

Since φ is a group homomorphism, by direct calculation, for all $\alpha, \beta \in G$,

$$\begin{aligned}\varphi'(\alpha\ker(\varphi) \cdot \beta\ker(\varphi)) &= \varphi(\alpha\beta\ker(\varphi)) \\ &= \varphi(\alpha\beta) \\ &= \varphi(\alpha)\varphi(\beta) \\ &= \varphi'(\alpha\ker(\varphi))\varphi'(\beta\ker(\varphi)).\end{aligned}$$

Then we can show φ' is a group homomorphism. Since φ is surjective, it holds that φ' is surjective. And for $\alpha, \beta \in G$, if $\varphi'(\alpha\ker(\varphi)) = \varphi'(\beta\ker(\varphi))$, it holds that $\varphi(\alpha) = \varphi(\beta)$, which means $\alpha \sim \beta$. Then we can show that φ' is injective. Combining all above, we conclude φ' is a group isomorphism. ◻

Example 1.19. *The mapping $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $z \mapsto z \bmod n$ induces a group isomorphism $\varphi' : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}_n$.*

1.4 Rings

Now we introduce rings beyond the groups.

Definition 1.20 (rings)**.** A *ring* $(R, +, \cdot)$ is a tuple consist of a non-empty set R and two operators $+ : R \times R \to R$ (addition), $\cdot : R \times R \to R$ satisfying

- $(R, +)$ is an abelian group.
- **Associativity:** $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ for all $\alpha, \beta, \gamma \in R$.
- **Distributivity:** For all $\alpha, \beta, \gamma \in R$,

$$(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma \quad \text{and} \quad \alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

There are some special families of rings.

- If there exists $1 \in R$ such that, for all $r \in R$, $r \cdot 1 = 1 \cdot r = r$, then 1 is the identity and R is a *ring with identity.*
- If for all $\alpha, \beta \in R$, $\alpha\beta = \beta\alpha$, then R is *commutative.*
- For $\alpha \in R$, if there exists $\beta \in R$ such that $\alpha\beta = \beta\alpha = 1$, then we say α is a *unit.* All units of R form the *unit group* of R.
- For $\alpha \in R$, if there exists $\beta \in R$, $\beta \neq 0$ such that $\alpha\beta = 0$, then we call α a *zero-divisor.* If a commutative ring R with identity has no non-zero zero-divisor, then we say R is an *integral domain.*

We see a field as a special kind of ring.

Definition 1.21 (fields)**.** A ring $(F, +, \cdot)$ with identity is called a *field* if $(F \setminus \{0\}, \cdot)$ is an abelian group.

Example 1.22. *Two typical fields are* $(\mathbb{Q}, +, \cdot)$ *and* $(\mathbb{Z}_p, +, \cdot)$.

Example 1.23. *Given a field (or a ring) F, define the* polynomial ring over F *as*

$$F[x] := \left\{ \sum_{i=0}^{n} a_i x^i \;\middle|\; n \in \mathbb{N}_{\geq 0}, a_i \in F \right\}.$$

It's not hard to verify $(F[x], +, \cdot)$ *is a ring.*

Sub-rings and sub-fields

Definition 1.24 (sub-rings)**.** Given a ring R and $S \subseteq R$, $S \neq \emptyset$, we say S is a *sub-ring* if $(S, +, \cdot)$ is a ring.

Remark 1.25. In some references, if R is a ring with identity, S must contain the identity ($p\mathbb{Z} < \mathbb{Z}$ in our sense).

Definition 1.26 (sub-fields)**.** Given a field E and $F \subseteq E$, if F is a field then we say F is a *sub-field* of E. In this case, we call E is an extended field of F.

Example 1.27. *A typical example is* $(\mathbb{Q}, +, \cdot) < (\mathbb{R}, +, \cdot) < (\mathbb{C}, +, \cdot)$.

1.5 Ring homomorphism

Similar to the group homomorphism, we can introduce the *ring homomorphism.*

Definition 1.28 (ring homomorphism)**.** Given two rings R, S, we say a mapping $\varphi : R \to S$ is a *ring homomorphism* if for all $\alpha, \beta \in R$

$$\varphi(\alpha) + \varphi(\beta) = \varphi(\alpha + \beta) \quad \text{and} \quad \varphi(\alpha)\varphi(\beta) = \varphi(\alpha\beta).$$

Analogously we can define the kernel as

$$\ker(\varphi) := \{\alpha \in R \mid \varphi(\alpha) = 0\}.$$

And also, we introduce the *ideal* which corresponds to normal groups.

Definition 1.29 (ideals)**.** We say I is an *ideal* of ring R if I is a sub-ring of R and for all $r \in R$, $a \in I$, $ar, ra \in I$.

Consider $(R/I, +, \cdot)$ where the operators are defined as for all $\alpha, \beta \in R$,

$$(\alpha + I) + (\beta + I) := (\alpha + \beta) + I \quad \text{and} \quad (\alpha + I) \cdot (\beta + I) := (\alpha\beta) + I.$$

For the sake of simplicity, we use $\overline{\alpha}$ to denote the coset $\alpha + I$. The following lemma shows us the motivation to define the ideal.

Lemma 1.30. *$(R/I, +, \cdot)$ is a ring if and only if I is an ideal of R.*

Proof. When $(R/I, +, \cdot)$ is a ring, it holds that for all $r \in R$ and $a \in I$,

$$\overline{0} = \overline{0 \cdot r} = \overline{0} \cdot \overline{r} = \overline{a} \cdot \overline{r} = \overline{ar},$$

which means $ar \in I$. Similarly we can show $ra \in I$. Thus we conclude I is an ideal.

When I is an ideal, it holds that for all $r \in R$, $a \in I$, $ra, ar \in I$. Then for all $\alpha, \beta \in R$, $\alpha' \sim \alpha$, $\beta' \sim \beta$ ($\alpha - \alpha' \in I$, $\beta - \beta' \in I$), it holds that

$$\alpha\beta - \alpha'\beta' = (\alpha - \alpha')\beta + \alpha'(\beta - \beta') \in I,$$

which means $\overline{\alpha\beta} = \overline{\alpha'\beta'}$. Then we can show the operators are well-defined. What remains to do is to show the associativity and distributivity of $\cdot$, and it is not hard to verify them. □

Given $X \subseteq R$, we say the minimal ideal containing X is the *ideal generated by* X, denoted by (X). It might be not easy to construct (X) for general case. We only consider the case when R is a commutative ring with identity $1 \in R$. Then by definition,

$$(X) := \left\{ \sum_{i=1}^{n} r_i x_i \;\middle|\; n \in \mathbb{N}, x_i \in X, r_i \in R \right\}.$$

Example 1.31. *For $(\mathbb{Z}, +, \cdot)$ and any prime number p, it holds that $(p) = p\mathbb{Z}$. For $(F[x], +, \cdot)$ and $f(x) \in F[x]$, we have $(f(x)) = f \cdot F[x] = \{f \cdot g \mid g \in F[x]\}$.*

For every single element $x \in R$, it is not hard to show $(x) = Rx$. We call (x) a *principal ideal of* R. If R is an integral domain and all ideas of R are principal, we say R is a *principal ideal domain.* $(\mathbb{Z}, +, \cdot)$ and $(F[x], +, \cdot)$ are two typical principal ideal domains.

For a ring homomorphism $\varphi : R \longrightarrow S$, it is easy to verify that $\ker(\varphi)$ is an ideal of R. Then, analogous to Theorem 1.18, we have the following theorem.

Theorem 1.32 (First Isomorphism Theorem)**.** *Given a ring homomorphism $\varphi : R \longrightarrow S$ (without loss of generality assume that φ is surjective), the mapping $\varphi' : R/\ker(\varphi) \longrightarrow S$, $\alpha \ker(\varphi) \mapsto \varphi(\alpha)$ is a ring isomorphism.*

The proof of Theorem 1.32 is quite trivial directly from the definition.

For a ring R and an ideal I of R, if for all ideals J of R, $I \subseteq J \subseteq R$ implies $J = I$ or $J = R$, then we call I a *maximal ideal.* In this case, R/I is a field.

For all $a, b \in R$, if $ab \in I \implies a \in I$ or $b \in I$, then we call I a *prime ideal.* It holds that in the ring $(\mathbb{Z}, +, \cdot)$, (p) is prime and maximal.

1.6 Integral domain

Now we introduce some definitions in integral domain R.

- For $\alpha, \beta \in R$, if there exists $\gamma \in R$ such that $\beta = \alpha\gamma$, then we say α *divides* β ($\alpha \mid \beta$). If α and γ are not units, we say α *properly divides* β.
- For $\alpha, \beta \in R$, if there exists some unit u such that $\beta = \alpha u$, then we say α and β are *associated* ($\alpha \sim \beta$).
- For $\alpha \in R$, $\alpha \neq 0$ and $\alpha \notin$ unit, if α has no proper divisor, then we say α is *irreducible*.
- For $\pi \in R$, $\pi \neq 0$ and $\pi \notin$ unit, if $\pi \mid \alpha\beta \implies \pi \mid \alpha \text{ or } \pi \mid \beta$, then we say π is *prime*. Note that, every prime element is irreducible.
- Let $\alpha, \beta \in R$. An element $d \in R$ is called a *greatest common divisor (gcd)* of α and β if (i) $d \mid \alpha$ and $d \mid \beta$; (ii) for all $e \mid \alpha$ and $e \mid \beta$, $e \mid d$.

  If d is unit, we say α and β are relatively prime.

1.6.1 Unique factorization domain

Now we introduce a kind of integral domains.

Definition 1.33 (unique factorization domain)**.** An *unique factorization domain (UFD) R* is an integral domain satisfying that, for all $\alpha \in R$:

- We can write $\alpha = p_1 \dots p_n$ where p_i is irreducible.
- If $\alpha = p_1 \dots p_n = q_1 \dots q_m$, then $n = m$ and $p_1 \dots p_n$ is some permutation of $q_1 \dots q_n$.

Corollary 1.34. *For an UFD R, every irreducible element is prime.*

1.7 Characteristic of a ring

Let R be a ring and $r \in R$, we define

$$nr = (n-1)r + r, \forall n \geq 1$$

and $(-n)r = -nr$.

For a ring R, we define the $\mathrm{char}(R)$ as the smallest positive integer n such that $n1 = 0$ if exists and 0 otherwise. It holds that for all $r \in R$, $nr = 0$.

If $\mathrm{char}(R) = 0$, consider the mapping $\varphi : \mathbb{Z} \to R$, $n \mapsto n \cdot 1$. It is easy to verify φ is a ring homomorphism and it is injective. Then we say R *contains* $\mathbb{Z}$.

If $\mathrm{char}(R) = p$ where p is prime, consider the mapping $\varphi : \mathbb{Z} \to R$, $n \mapsto n \cdot 1$ and $\ker(\varphi) = (p)$. Then we show that R contains $\mathbb{Z}/(p) = \mathbb{Z}_p$.

Theorem 1.35. *For an integral domain R,* $\mathrm{char}(R) = 0$ *or* $\mathrm{char}(R) = p$ *for some prime number p.*

Proof. We prove the case $\mathrm{char}(R) \neq 0$. Let $r = \mathrm{char}(R)$ and assume that $r = st$. Then it holds that

$$r \cdot 1 = st \cdot 1 = (s1)(t1) = 0.$$

Since R is an integral domain, we have $s1 = 0$ or $t1 = 0$. This means $r = s$ or $r = t$. Then we conclude p is prime. ◻

For a field F, if $\mathrm{char}(F) = p > 0$, it holds that $\mathbb{Z}_p \subseteq F$. Then we say $\mathbb{Z}_p$ is a prime sub-field of F. If $\mathsf{F} = 0$, consider the mapping $\varphi : Q \to F$, $a/b \mapsto (a1)/(b1)$. Since $\ker\varphi = \{0\}$, it holds that φ is a homomorphism and injection. This means F contains Q. Then we say Q is a prime sub-field of F.

There are some useful properties for a commutative ring R with 1 and $\mathrm{char}(R) = p$.

- For all $\alpha, \beta \in R$, $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n}$.

1.8 Euclidean domain

For every $a, b \in \mathbb{Z}$, $b \neq 0$, there exists $q, r \in \mathbb{Z}$ such that

$$a = qb + r, \quad r = 0 \text{ or } |r| < |b|.$$

And it is easy to verify $(a, b) = (b, r)$. Now we extend the definition to rings.

Definition 1.36 (Euclidean domain)**.** We say a ring R is an *Euclidean domain* if there exists $v : R \setminus \{0\} \to \mathbb{R}$ satisfying

- For $a \in R \setminus \{0\}$, $v(a) \geq 0$.
- For $a \in R$, $b \in R \setminus \{0\}$, there exists $q, r \in R$ such that

$$a = qb + r, \quad r = 0 \text{ or } v(r) < v(b).$$

Example 1.37. *For a field F, $(F[x], +, \cdot)$ is an Euclidean domain if we define $v(f) := \deg(f)$. Note that in some reference we define* $\deg(0) = -\infty$.

Theorem 1.38. *Every Euclidean domain is a principal ideal domain.*

Proof. For an Euclidean domain R and an ideal I of R, we pick the element $a \in I$ such that $v(a)$ is smallest in I. Then for all $b \in I$, there exists $q, r \in R$ such that

$$b = qa + r, \quad r = 0 \text{ or } v(r) < v(a).$$

Since $a, b \in I$, it holds that $r \in I$. Since $v(a)$ is minimal in I, we obtain $r = 0$. Then we can show $I = (a)$. □

2 Polynomials over Fields

For a field F, consider $(F[x], +, \cdot)$. For all ideal $I \subseteq F[x]$, since $F[x]$ is an Euclidean domain, it holds that $I = (p(x))$ for some $p(x) \in F[x]$. It is trivial that the units are $F \setminus \{0\}$. For all $f, g \in F[x]$, it holds that

$$(f, g) = f \cdot F[x] + g \cdot F[x] = \{af + bg \mid a, b \in F[x]\}.$$

Then there exists $p \in F[x]$ such that $(f, g) = (p)$. Then it holds that $p \mid f$ and $p \mid g$. On the other hand, for all $r \mid f$ and $r \mid g$, it holds that $r \mid p$ (since $p = af + bg$ for some $a, b \in F[x]$). Then we can show p is the *greatest common divisor* of f, g.

Without loss of generality, assume that p is monic (so the greatest common divisor is unique).

As an extension, for $f_1, \ldots, f_n \in F[x]$. If $(f_1, \ldots, f_n) = p$, then there exist $a_1, \ldots, a_n \in F[x]$ such that

$$\sum_{i \in [n]} a_i f_i = p.$$

2.1 The field independence of the greatest common divisor

For fields $F < K$, and for two polynomials $f, g \in F[x]$ (also $f, g \in K[x]$), we denote *the greatest common divisor of f and g in F* by $r_F(x) = (f, g) \in F[x]$, and similarly denote the one in K by $r_K(x) = (f, g) \in K[x]$. Then,

$$r_F \mid f, r_F \mid g \implies r_F \mid r_K.$$

Then it holds that $r_F = af + bg \in K[x]$, which means $r_K \mid r_F$. Then it holds that $r_F = r_K$.

Corollary 2.1. *$f, g \in F[x]$ have a non-constant divisor in $F[x]$ if and only if f, g have a non-constant divisor in $K[x]$.*

2.2 Roots and common roots

Now we consider the roots of a polynomial.

Theorem 2.2. *For a field F and $f \in F[x]$ with $\deg(f) \geq 1$, there exists an extension E of F ($F < E$) such that for some $a \in E$, $f(a) = 0$.*

Proof. Without loss of generality we assume that f is irreducible. Firstly we prove the ideal (f) is maximal. In fact, assume that $J = (g)$ for some $g \in F[x]$ such that $(f) \subseteq (g) \subseteq F[x]$. It holds that $f \in (g)$, which means $g \mid f$. This means g is unit or $g \sim f$. Then we know $J = F[x]$ or $J = (f)$. Thus we know (f) is maximal.

Now, we let $E := F[x]/(f)$. Consider the mapping $\varphi : F \to E$, $a \mapsto a + (f)$. Since $\ker \varphi = 0$, it holds that φ is injective, which means $F < E$. Assume that

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad \forall 0 \leq i \leq n, a_i \in F.$$

Then we know

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

where $\overline{a_i} = a_i + (f)$. Now we consider $f(x + (f))$. This means

$$\begin{aligned} f(x + (f)) &= \sum_{i=0}^{n} \overline{a_i} (x + (f))^i \\ &= \sum_{i=0}^{n} (a_i + (f))(x + (f))^i \\ &= f(x) + (f) = 0. \end{aligned}$$

□

Corollary 2.3. *For $f \in F[x]$ with $\deg(f) = n$, there exists $E > F$ such that f has n roots on E.*

Now we show the common root of two polynomials is strongly related with the common divisor. For two polynomials f, g, if $f(a) = 0$ and $g(a) = 0$, then we say a is the *common root of f, g.*

Corollary 2.4. *f, g have a non-constant common divisor d if and only f and g have a common root on some extended field.*

If $f(x) \in F[x]$ can be written as $f(x) = C(x - a_1) \dots (x - a_n)$, then we say f splits in F.

2.3 Minimal polynomials

Let $F < E$. For $a \in E$, we say a is *algebraic over F* if a is the root of some $p(x) \in F[x]$. Otherwise we say a is *transcendental over F*.

Definition 2.5 (minimal polynomials)**.** For an algebraic element a over F, we say a monic polynomial $p \in F[x]$ is the *minimal polynomial of a* if $p(a) = 0$ and $\deg(p)$ is the smallest. We write it as $p = \min(F, a)$.

The following definitions are the equivalent.

- The monic irreducible $p \in F[x]$ with $p(a) = 0$.
- The monic $p \in F[x]$ satisfying for all $f \in F[x]$, $f(a) = 0$, $p \mid f$.

The ideal generated by p is $I = \{f \mid f(a) = 0\}$.

Definition 2.6. We say $\alpha, \beta \in E$ are *conjugates over F* if they share the same minimal polynomial.

2.4 Extend a field

Now we discuss more about how to extend a field. Given a field F, for $f \in F[x]$, we have already known that (f) is a maximal ideal if and only if f is irreducible. When f is irreducible, $E := F[x]/(f)$ is a field and $E < F$. Now we consider $|E|$.

Assume that $|F| < \infty$ and $\deg(f) = n$. Then it holds that

$$E = \{p(x) + (f) \mid p(x) \in F[x]\}.$$

Since $F[x]$ is an Euclidean domain, we know

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

which means $p(x) - r(x) = q(x)f(x) \in (f)$. Then we obtain $p(x) + (f) = r(x) + f(x)$ where $\deg(r) < \deg(f)$. When $r_1 \neq r_2$, it holds that $r_1 + (f) \neq r_2 + (f)$. Thus we can show that

$$|E| = |F|^n.$$

Example 2.7. *Let $F = F_2 = \{0, 1\}$. Consider $f(x) = x^2 + x + 1$. Then we can construct a new field $F_{2^2} = F_2[x]/(f)$.*

2.5 Multiple roots

In this part, we discuss the multiple roots of a polynomial. Given $f(x) \in F[x]$, α is a root of f (α might be in an extended field of F not necessarily in F). The *multiplicity of α* is the largest natural number n such that $(x - \alpha)^n \mid f(x)$. If $n > 1$, we say α is a multiple root. Otherwise we say α is a *simple root* of f.

Definition 2.8. Given an irreducible polynomial $f(x) \in F[x]$, we say $f(x)$ is *separable* if it has no multiple roots. Otherwise we say $f(x)$ is *inseparable.*

It's necessary to introduce the derivative of polynomial. For $f(x) = \sum_{i=0}^{n} a_i x^i$, define its *derivative* $f'(x)$ as

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

It's not hard to verify

$$(af)' = af', (f \pm g)' = f' \pm g', (fg)' = f'g + fg', (g^n)' = ng^{n-1}g'.$$

Assume that (without loss of generality suppose that f is monic),

$$f(x) = (x - a_1)^{e_1} \dots (x - a_n)^{e_n}$$

and $a_1, \dots, a_n$ are different.

Theorem 2.9. *$f(x), f'(x)$ share a common root if and only if there exists $e_i > 1$.*

Proof. When $f(x), f'(x)$ share a common root. Assume that $f(a_i) = f'(a_i) = 0$ and $e_i = 1$. Then there exists $p(x) \in F[x]$ such that

$$f(x) = (x - a_i)p(x), f'(x) = p(x) + (x - a_i)p'(x).$$

Then we know $0 = f'(a_i) = p(a_i) \neq 0$, which leads to a contradiction. Then $e_i > 1$.

If there exists $e_i > 1$, assume that $f(x) = (x - a_i)^{e_i} p(x)$. Then

$$f'(x) = e_i (x - a_i)^{e_i - 1} p(x) + (x - a_i)^{e_i} p'(x).$$

It is obvious that $f'(a_i) = 0$. Then we know f, f' share a common root. □

By the above theorem, we know that f, f' share no common roots if and only if f is separable. Based on Theorem 2.9, we have the following results.

Corollary 2.10. *For an irreducible polynomial $f(x) \in F[x]$, f is separable if and only if $f'(x) \neq 0$.*

Proof. When f is separable, by Theorem 2.9, we know f and f' share no common root. This means $(f, f') = 1$. Since $\deg(f') < \deg(f)$, it holds that $f'(x) \neq 0$.

When $f'(x) \neq 0$, we assume that f and f' share a common root. Then it holds that $(f, f') = p(x)$ where $\deg(p) \geq 1$. This means $p \mid f$, which leads to a contradiction to f is irreducible. □

Then we have the following two conclusions:

- For a field F with $\text{char}(f) = 0$, it holds that every irreducible $f \in F[x]$ is separable.
- For a finite field F, it holds that every irreducible $f \in F[x]$ is separable.

Remark 2.11. The conclusions above do not hold for every field F. In fact, the quotient field of $F_2[x]$ is a counterexample.

2.6 Testing for irreducibility

Now we test whether a polynomial is irreducible.

Definition 2.12. Given an UFD R and its quotient field F, let $f(x)$ be a polynomial in $R[x]$. We write $f(x)$ as

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

We say $(a_0, \dots, a_n)$ is the *content* of f, denoted by $c(f)$.

If $c(f) \sim 1$, we say f is *primitive*. Note that, for all $d \in R$, $c(df) \sim dc(f)$. Then for all $f \in R[x]$, it holds that

$$f = c(f) f_1, \quad f_1 \text{ is primitive.}$$

Lemma 2.13 (Gauss's Lemma)**.** *For two polynomials $f, g \in R[x]$, it holds that $c(fg) \sim c(f)c(g)$.*

Proof. Assume that $f = c(f)f_1$ and $g = c(g)g_1$ where $f_1, g_1 \in R[x]$ are primitive polynomials. Then we know that

$$fg = c(f)c(g)f_1g_1 \implies c(fg) = c(f)c(g)c(f_1g_1).$$

What remains to do is to prove f_1g_1 is a primitive polynomial. We write f_1, g_1 as

$$f_1 = \sum_{i=0}^{n} a_i x^i, g_1 = \sum_{j=0}^{m} b_j x^j$$

and write f_1g_1 as

$$f_1g_1 = \sum_{k=0}^{m+n} c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j \ \forall 0 \le k \le m+n.$$

Suppose that f_1g_1 is not primitive, which means there exists a prime p such that $p \mid c_k$ for all $0 \le k \le n+m$. Since $c(f_1) = c(g_1) = 1$, we choose a_s as the very element $p \nmid a_s$ with smallest s and b_t as the element $p \nmid b_t$ with largest t. We consider the coefficient c_{s+t}:

$$\begin{aligned} c_{s+t} &= \sum_{i+j=s+t} a_i b_j \\ &= \sum_{\substack{i+j=s+t \\ i<s}} a_i b_j + a_s b_t. \end{aligned}$$

Since $p \mid c_{s+t}$, we know $p \mid a_s b_t$, which means $p \mid a_s$ or $p \mid b_t$. This leads to a contradiction. So we conclude that f_1g_1 is primitive. □

Corollary 2.14. *Given an UFD R, its quotient field F and a primitive polynomial $f \in R[x]$ with $\deg(f) \ge 1$, f is irreducible in $R[x]$ if and only if f is irreducible in $F[x]$.*

Proof. When f is irreducible in $F[x]$, assume that $f = gh$ in $R[x]$. Since F is the quotient field of R, we know $f = gh$ is also a decomposition in $F[x]$. Since f is irreducible in $F[x]$, assume that g is the unit. Then $g \in F \setminus \{0\}$. Moreover, since $g \in R[x]$, it holds that $g \in R \setminus \{0\}$. Additionally, by Lemma 2.13,

$$1 \sim c(f) \sim g \cdot c(h).$$

Then we know g is unit in R, which means f is irreducible in $R[x]$.

When f is irreducible in $R[x]$, assume that $f = gh$ in $F[x]$ with $\deg(g) \ge 1$ and $\deg(h) \ge 1$. We can write g, h as

$$g(x) = \frac{a}{b} g_1(x), h(x) = \frac{c}{d} h_1(x)$$

where $g_1, h_1 \in R[x]$ are primitive polynomials. This means

$$f = \frac{ac}{bd} g_1 h_1 \text{ or } bdf = acg_1h_1.$$

By Lemma 2.13, it holds that

$$bd \sim bdc(f) \sim acc(g_1)c(h_1).$$

This means $bd \sim ac$ and $f = ug_1h_1$ where u is a unit. Then we conclude f is reducible, leading to a contradiction. □

Based on above, we introduce *Eisenstein's criterion* to test the irreducibility.

Theorem 2.15 (Eisenstein's criterion)**.** *Given an UFD R and primitive $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ with $\deg(f) \ge 1$, if there exists an irreducible element $p \in R$ satisfying $p \mid a_0, \ldots, a_{n-1}$ and $p \nmid a_n$, $p^2 \nmid a_0$, then f is irreducible in $R[x]$.*

Proof. Assume $f = gh$ in $R[x]$ with $\deg(g) \geq 1$ and $\deg(h) \geq 1$. We write g, h as

$$g(x) = b_r x^r + \ldots + b_1 x + b_0,$$
$$h(x) = c_s x^x + \ldots + c_1 x + c_0.$$

Since $p \mid a_0 = b_0 c_0$ and $p^2 \nmid a_0 = b_0 c_0$, we assume $p \mid b_0$ and $p \nmid c_0$.

Since f is primitive, it holds that g and h are primitive. Then we can pick b_k as the element $p \nmid b_k$ with the smallest k. It holds that $1 \leq k \leq r < n$. Consider the coefficient a_k. It holds that

$$a_k = \sum_{i+j=k} b_i c_j = \sum_{\substack{i+j=k \\ i<k}} b_i c_j + b_k c_0.$$

Since $k < n$, we know $p \mid a_k$, which means $p \mid b_k c_0$. Then $p \mid b_k$ or $p \mid c_0$. This leads to a contradiction. Thus we conclude f is irreducible. □

Remark 2.16. Note that the most important thing is p is prime. So when R is an integral domain and p is prime, the same argument holds.

3 Field Extensions

Now we come to the kernel in this course. Firstly we give a view of field extensions from linear spaces.

Definition 3.1 (vector space over a field)**.** A *vector space* over a field F is a non-empty set V with two operators $+ : V \times V \to V$ and $\cdot : F \times V \to V$ satisfying:

- $(V, +)$ is an abelian group.
- For all $r, s \in F$, $u, v \in V$, it holds that

$$\begin{aligned} r(u+v) &= ru + rv, \\ (r+s)u &= ru + su, \\ rs \cdot u &= r \cdot (su), \\ 1 \cdot u &= u. \end{aligned}$$

For two fields $F < E$, if we view E as V, it is not hard to see E is a vector space over F. The dimension of E over F is called the *degree* of E over F denoted by $[E : F]$.

Example 3.2. *For $\mathbb{R} < \mathbb{C}$, it holds that $[\mathbb{C} : \mathbb{Q}] = 2$ since the basis can be picked as $\{1, i\}$.*
For $\mathbb{Q} < \mathbb{R}$, we will prove later that $[\mathbb{R} : \mathbb{Q}] = \infty$.

Theorem 3.3. *Let $F < K < E$ be finite fields. Then it holds that*

$$[E : F] = [E : K] \cdot [K : F].$$

Proof. Let $A = \{\alpha_i \mid i \in I\}$ be a basis for E over K and $B = \left\{\beta_j \;\middle|\; j \in J\right\}$ be a basis for E over F. Now we prove that

$$C = \left\{\alpha_i \beta_j \;\middle|\; i \in I, j \in J\right\}$$

is a basis for E over F. Firstly we show C is linearly independent. Assume that

$$\sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j = 0.$$

This means

$$0 = \sum_{i \in I} \left(\sum_{j \in J} a_{ij} \beta_j \right) \alpha_i = 0.$$

Since A, B are both linearly independent, we know $a_{ij} = 0$ for all $i \in I, j \in J$. Then C is linearly independent. Next, for $\gamma \in E$, there exist $a_i \in K$ such that $\gamma = \sum_{i \in J} a_i \alpha_i$. Since all $a_i = \sum_{j \in J} b_{ij} \beta_j$, we know

$$\gamma = \sum_{i \in I, j \in J} b_{ij} \alpha_i \beta_j.$$

This means C is a basis for E over F. Then we obtain what we desire. □

3.1 Generated extensions

Now we introduce the definition of generated extensions.

Definition 3.4. Let $F < E$ and $X \subseteq E$. We say the minimal field containing F and X is the *generated extension* of F by X, denoted by $F(X)$.

If $X = \{\alpha_1, \ldots, \alpha_n\}$, we say $F(X) = F(\alpha_1, \ldots, \alpha_n)$ is *finitely generated by* X. If $X = \{\alpha\}$, we say $F(X) = F(\alpha)$ is a *simple extension*, and α is called a *primitive element* of $F(\alpha)$.

- When $X = \{\alpha\}$, we consider the minimal ring containing F and α
$$F[x] := \{f(\alpha) \mid f(x) \in F[x]\} \subseteq F(\alpha).$$
Then we can show that
$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \,\middle|\, f, g \in F[x], g(\alpha) \neq 0 \right\}.$$
- When $X = \{\alpha_1, \ldots, \alpha_n\}$, the minimal ring containing F and X is
$$F[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in F[x_1, \ldots, x_n]\}.$$
Then we know
$$F(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \,\middle|\, f, g \in F[x_1, \ldots, x_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$
- When X is infinite, now we prove that
$$F(X) = \bigcup_{\alpha_1, \ldots, \alpha_n} F(\alpha_1, \ldots, \alpha_n)$$
Where $\{\alpha_1, \ldots, \alpha_n\}$ range over all finite subsets of X. It's trivial to see $F(X) \subseteq \bigcup_{\alpha_1, \ldots, \alpha_n} F(\alpha_1, \ldots, \alpha_n)$. On the other hand, for every $\{\alpha_1, \ldots, \alpha_n\}$, it holds that $F(\alpha_1, \ldots, \alpha_n) \subseteq F(X)$, meaning that $F(X) = \bigcup_{\alpha_1, \ldots, \alpha_n} F(\alpha_1, \ldots, \alpha_n)$.

3.2 Algebraic extensions

An important definition in field extensions is the algebraic extensions.

Definition 3.5. We say $F < E$ is *algebraic* if for all $\alpha \in E$, α is algebraic over F.

3.2.1 Simple algebraic extensions

Let $F < E$ and $\alpha \in E$ be an algebraic element over F. We say $F(\alpha)$ is a simple algebraic extension. Now we investigate $F(\alpha)$. Let $p(x) := \min(F, \alpha)$ be the minimal polynomial of α over F. Consider $f(\alpha)/g(\alpha) \in F(\alpha)$. Since $g(\alpha) \neq 0$, it holds that $(p, g) = 1$, meaning that $\exists a, b \in F[x]$ such that $ap + bg = 1$. Then we know $b(\alpha)g(\alpha) = 1$, which means
$$\frac{f(\alpha)}{g(\alpha)} = f(\alpha)b(\alpha) \in F[\alpha].$$
Then we know $F(\alpha) = F[\alpha]$. Furthermore, for all $f \in F[x]$, it holds that $\exists q, r \in F[x]$,
$$f(x) = q(x)p(x) + r(x)$$
where $r = 0$ or $\deg(r) < \deg(p)$. Then $f(\alpha) = r(\alpha)$. So,
$$F(\alpha) = \{r(\alpha) \mid r = 0 \vee \deg(r) < \deg(p)\}.$$
Let $n = \deg(p)$. If $|F| < \infty$, we obtain that $|F(\alpha)| = |F|^n$.

Since $p(x)$ is the minimal polynomial of α over F, it's not hard to show the basis of $F(\alpha)$ over F is
$$\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}.$$
Equivalently $[F(\alpha) : F] = n = \deg(p)$.

Example 3.6. *It holds that* $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. *For* $\omega = e^{2\pi i/3}$, *it holds that* $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$.

For $F < F(\alpha)$ where α is algebraic over F and $\beta \in F(\alpha)$, let $n = \deg(\min(F, \alpha))$. Since $[F(\alpha) : F] = n$, we know

$$1, \beta, \dots, \beta^n$$

are not linearly independent. Then we know β is algebraic over F. This means $F(\alpha)$ is algebraic over F.

Theorem 3.7. *Let $F < E$ and $\alpha_1, \dots, \alpha_n \in E$ be algebraic elements over F. Then*

$$[F(\alpha_1, \dots, \alpha_n) : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

Proof. We prove it by induction. For $n = 1$ it holds trivially. Assume that the inequality holds when $k = n - 1$. Let $L := F(\alpha_1, \dots, \alpha_{n-1})$. By Theorem 3.3, it holds that

$$[L(\alpha_n) : F] = [L(\alpha_n) : L] \cdot [L : F].$$

Consider the minimal polynomial $p(x) \in F[x]$ of α_n over F. It holds that $p(x) \in L[x]$. So we know

$$[L(\alpha_n) : L] \leq [F(\alpha_n) : F].$$

Then we know

$$[L(\alpha_n) : F] \leq [F(\alpha_n) : F] \cdot [L : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F].$$

□

To prove more properties, we need the following fact.

Fact 3.8. *The multiplication group of a finite field is cyclic.*

Together with Fact 3.8, we can establish the following lemma.

Lemma 3.9. *Let $F < E$ and $\alpha_1, \dots, \alpha_n \in E$ be algebraic elements over F. If $|F| < \infty$, then $F(\alpha_1, \dots, \alpha_n) = F(\alpha)$ for some α.*

Proof. By Theorem 3.7, it holds that

$$[F(\alpha_1, \dots, \alpha_n) : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F] < \infty.$$

Since $|F| < \infty$, it holds that $|F(\alpha_1, \dots, \alpha_n)| < \infty$. By Fact 3.8, its multiple group is cyclic. Denote by α the generator of such a group. Then we know that

$$F(\alpha) = \left\{0, 1, \alpha^1, \dots, \alpha^{|F(\alpha_1, \dots, \alpha_n)|-2}\right\} = F(\alpha_1, \dots, \alpha_n).$$

On the other hand, it is trivial that α is algebraic. □

Remark 3.10. It's not hard to see every finite extension of a finite field is a simple algebraic extension.

Example 3.11. *Consider the field extension $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18})$ over $\mathbb{Q}$. It holds that*

$$[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}] \leq 16.$$

However, it holds that $\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) = \mathbb{Q}(\sqrt[4]{2}, \sqrt{3})$. Then we know

$$[\mathbb{Q}(\sqrt[4]{2}, \sqrt[4]{18}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, \sqrt{3}) : \mathbb{Q}] \leq 8 < 16.$$

3.2.2 Finite extensions and algebraic extensions

Now we discuss the relationship between finite extensions and algebraic extensions.

Theorem 3.12. *Let $F < E$. If $[E : F] < \infty$, then E is algebraic over F.*

Proof. Let $n := [E : F] < \infty$. For all $\beta \in E$, it holds that

$$1, \beta, \ldots, \beta^n$$

are not linearly independent. Then we know β is algebraic over F. □

Based on Theorem 3.12, we have the following corollaries.

Corollary 3.13. *Let $F < E$ and $X \subseteq E$ such that every element $x \in X$ is algebraic over F. Then $F(X)$ is algebraic over F.*

Proof. For all $\{\alpha_1, \ldots, \alpha_n\} \subseteq X$, it holds that $F(\alpha_1, \ldots, \alpha_n)$ is algebraic over F ($[F(\alpha_1, \ldots, \alpha_n) : F] < \infty$ and by Theorem 3.12). Then for all $\alpha \in F(X)$, there exists $\alpha_1, \ldots, \alpha_n \subseteq X$ such that $\alpha \in F(\alpha_1, \ldots, \alpha_n)$. Then we know α is algebraic. Thus we know $F(X)$ is algebraic. □

Corollary 3.14. *Let $F < L < E$. If L is algebraic over F and E is algebraic over F, then E is algebraic over F.*

Proof. For $\alpha \in E$, since E is algebraic over L, then there exists

$$\min(L, \alpha) = \sum_{i=0}^{n} a_i x^i, \quad \forall 0 \leq i \leq n, a_i \in L.$$

Consider $L_0 = F(a_0, \ldots, a_n)$. It holds that $F < L_0 < L_0(\alpha) < E$. It holds that

$$[L_0(\alpha) : F] = [L_0(\alpha) : L] \cdot [L : F] < \infty.$$

Then we know $L_0(\alpha)$ is algebraic over F, thus we know α is algebraic. □

Definition 3.15. Let $F < E$. The set K of all algebraic elements in E over F is called the *algebraic closure* of F in E.

Lemma 3.16. *The algebraic closure K of F in E is a field. Thus it is the maximal algebraic extension of F in E.*

Proof. For all $\alpha, \beta \in K$, by Corollary 3.13, $F(\alpha, \beta)$ is algebraic over F, meaning that $\alpha \pm \beta$, $\alpha\beta$ and α/β are algebraic (they are both in K). Then we prove that K is a field. □

Note that, algebraic extensions are not necessarily finite. See the following counterexample: for $\mathbb{Q} < \mathbb{C}$, consider the algebraic closure A of $\mathbb{Q}$ in $\mathbb{C}$, for all $n \in \mathbb{N}$, $x^n - 2 = 0$ can be a minimal polynomial of some element in A, meaning that $[A : \mathbb{Q}] = \infty$.

3.3 Transcendental extensions

Now we discuss more types of extensions

3.3.1 Simple transcendental extensions

Let $F < E$ and a transcendental element $\alpha \in E$ over F. Then we show

$$F(\alpha) = \left\{ \frac{f(\alpha)}{g(\alpha)} \;\middle|\; f, g \in F[x], g(\alpha) \neq 0 \right\}.$$

For an arbitrary symbol t, let

$$F(t) = \left\{ \frac{f(t)}{g(t)} \;\middle|\; f, g \in F[x], g \neq 0 \right\}.$$

For any $f' \in F(t)$, we know

$$F(f') = \left\{ \frac{f(f')}{g(f')} \;\middle|\; f, g \in F[x], g(f') \neq 0 \right\}.$$

Let $f' = t^2$. It holds that $[F(t) : F(t^2)] = 2$.

3.4 Galois group

For fields K, L, consider a field homomorphism $\sigma : K \to L$. It is routine to investigate $\ker(\sigma)$. Since $\ker(\sigma)$ is an ideal, if there exists $\alpha \neq 0 \in \ker(\sigma)$, we know $1 = \alpha\alpha^{-1} \in \ker(\sigma)$, meaning that $\ker(\sigma) = K$. Then $\ker(\sigma) = (0)$ or K.

When $\ker(\sigma) = K$, we show $\sigma = 0$. When $\ker(\sigma) = (0)$, it holds that σ is an injection. And we say $\sigma : K \to L$ is embedded.

For $F < K$ and $F < L$ and $\sigma : K \to L$, we say σ is an F-*homomorphism* if $\sigma|_F = \mathrm{Id}$. If σ is a bijection, we say σ is an F-*isomorphism*. An F-isomorphism from a field K to itself is called an F-*automorphism*.

Note that, for an F-homomorphism $\sigma : K \to L$, it is a linear mapping from K to L. Additionally, if $[K : F] = [L : F] = n$, for an F-basis $\{\alpha_1, \ldots, \alpha_n\}$ of K, it's not hard to show $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ is an F-basis of L. Then we know σ is bijection. This means σ is F-isomorphism.

We denote by $\mathrm{Aut}(K)$ the collection of all automorphisms of K, and denote by $\mathrm{Aut}_F(K)$ the collection of F-automorphisms.

Definition 3.17 (Galois group)**.** Let $F < K$. We say $\mathrm{Aut}_F(K)$ is the Galois group of K/F, denoted by $\mathrm{Gal}(K/F)$.

Theorem 3.18. *Let $K = F(X)$ and $\sigma, \tau \in \mathrm{Gal}(K/F)$. If $\sigma|_X = \tau|_X$, then $\sigma = \tau$.*

Proof. For all $\alpha \in K$, there exist $f, g \in F[x_1, \ldots, x_n]$ and $\{\alpha_1, \ldots, \alpha_n\} \subseteq X$ such that

$$\alpha = \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)}.$$

Suppose that

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n} b_{i_1, \ldots, i_n} \prod_{j \in [n]} x_j^{i_j}.$$
$$g(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n} c_{i_1, \ldots, i_n} \prod_{j \in [n]} x_j^{i_j}.$$

Since $\sigma|_X = \tau|_X$, it holds that

$$\sigma(f(\alpha_1, \ldots, \alpha_n)) = \tau(f(\alpha_1, \ldots, \alpha_n)), \sigma(g(\alpha_1, \ldots, \alpha_n)) = \tau(g(\alpha_1, \ldots, \alpha_n)).$$

Then $\sigma(\alpha) = \tau(\alpha)$. Thus we conclude $\sigma = \tau$. □

The following result comes directly from the definition of homomorphism.

Theorem 3.19. *Let $\sigma : K \to L$ be an isomorphism. For $\alpha \in K$ and $p(x) := \min(F, \alpha)$, if $f(\alpha) = 0, f \in F[x]$, then $f(\sigma(\alpha)) = 0$. Also we know $\min(F, \sigma(\alpha)) = p$.*

On the other hand, we pick any arbitrary root β of $p(x)$. We construct a mapping $\sigma : F(\alpha) \to F(\alpha)$ such that $\alpha \mapsto \beta$. Then σ is an F-automorphism.

When $K = L$, $[K : F] = n < \infty$ and an F-automorphism $\sigma : K \to K$, by Theorem 3.19, for $\alpha \in K$, if $f(\alpha) = 0$ then $f(\sigma(\alpha)) = 0$. If $\alpha_1, \ldots, \alpha_m \in K$ are roots of f, then $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$ are roots of f (a permutation of $\alpha_1, \ldots, \alpha_n$).

With the discussion above, we can show that, if $[K : F] = n < \infty$, we know $K = F(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are algebraic. Then we know $\sigma(\alpha_i) \leq \deg \min(F, \alpha_i)$. This means $|\mathrm{Gal}(K/F)| < \infty$.

Example 3.20. *For $\mathbb{R} < \mathbb{C}$, since $\mathbb{C} = \mathbb{R}(i)$ and $\min(\mathbb{R}, i) = x^2 + 1$, we know $\sigma = \mathrm{Id}$ or $\sigma : z \mapsto \bar{z}$. Then $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$.*

Example 3.21. *For $\mathbb{Q} < \mathbb{Q}(\sqrt[3]{2})$, let $\omega = e^{2\pi i/3}$. We know*

$$\sigma(\sqrt[3]{2}) \in \left\{\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2\right\}.$$

However, since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, we know $\sigma = \mathrm{Id}$. Then $\left|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})\right| = 1$.

Example 3.22. *Let $F = F_2(t^2) < K = F_2(t)$. It's not hard to see $K = F(t)$. Since $\min(F, t) = x^2 - t^2 = (x - t)^2$. Then we know $\sigma = \mathrm{Id}$.*

Example 3.23. *Let $F = F_2 < K = F_{2^2}$. We know $K = \frac{F_2[x]}{(f)}$ where $f(x) = x^2 + x + 1$. We write K as*

$$K = \{a + bx + (f) \mid a, b \in F\} = \left\{\overline{a + bx} \;\middle|\; a, b \in F\right\}.$$

It's not hard to see the F-basis of K is $\{\overline{1}, \overline{x}\}$, which means $K = F(\overline{x})$.

It's not hard to verify $\min(F, \overline{x}) = f$ and $f(\overline{x}) = f(\overline{x+1}) = \overline{0}$. Then we know $\sigma = \mathrm{Id}$ or $\sigma(\overline{x}) = \overline{x+1}$. This means $|\mathrm{Gal}(K/F)| = 2$.

Definition 3.24. Let K be a finite extension of F. If $|\mathrm{Gal}(K/F)| = [K : F]$, then we say K is a *Galois extension* of F.

Now we study further on Galois theory. Let $F < L < K$. It's not hard to see $\mathrm{Gal}(K/L) \subseteq \mathrm{Gal}(K/F)$.

Definition 3.25 (fixed field)**.** For $S \subseteq \mathrm{Aut}(K)$, define its fixed field as

$$\mathcal{F}(S) = \{\alpha \in K \mid \forall \sigma \in S, \sigma(\alpha) = \alpha\}.$$

It's not hard to verify $\mathcal{F}(S)$ is a field.

Here are some basic properties.

(P1) If $L_1 < L_2 < K$, then $\mathrm{Gal}(K/L_2) \subseteq \mathrm{Gal}(K/L_1)$.

(P2) For $L < K$, $L \subseteq \mathcal{F}(\mathrm{Gal}(K/L))$.

(P3) For $S_1 \subseteq S_2 \subseteq \mathrm{Aut}(K)$, it holds that $\mathcal{F}(S_2) \subseteq \mathcal{F}(S_1)$.

(P4) For $S \subseteq \mathrm{Aut}(K)$, $S \subseteq \mathrm{Gal}(K/\mathcal{F}(S))$.

(P5) If $L = \mathcal{F}(S)$ for some $S \subseteq \mathrm{Aut}(K)$, then it holds that $L = \mathcal{F}(\mathrm{Gal}(K/L))$.

Proof. By (P4), we know $S \subseteq \mathrm{Gal}(K/L)$. By (P3), we show $\mathcal{F}(\mathrm{Gal}(K/L)) \subseteq \mathcal{F}(S) = L$. On the other hand, by (P2), $L \subseteq \mathcal{F}(\mathrm{Gal}(K/L))$. □

(P6) If $H = \mathrm{Gal}(K/L)$ for some $L < K$, then $H = \mathrm{Gal}(K/F(H))$.

Proof. By (P4), $H \subseteq \mathrm{Gal}(K/F(H))$. On the other hand, by (P2), we know $L \subseteq F(\mathrm{Gal}(K/L))$. By (P1), we know $\mathrm{Gal}(K/F(H)) \subseteq \mathrm{Gal}(K/L) = H$. □

We use $\mathcal{F}$ to denote the collection of all sub-fields L such that $F < L < K$ and $L = \mathcal{F}(S)$ for some $S \subseteq \mathrm{Gal}(K/F)$, and use $\mathcal{G}$ to denote all sub-groups $H \subseteq \mathrm{Gal}(K/F)$ such that $H = \mathrm{Gal}(K/L)$ for some $L < K$. By (P5) and (P6), it's not hard to see the mapping $\mathcal{F} \to \mathcal{G}$, $L \mapsto \mathrm{Gal}(K/L)$ is bijective, and its inverse is $\mathcal{G} \to \mathcal{F}$, $H \mapsto F(H)$.

Definition 3.26. Let G be a group and K be a field. A *character* is a group homomorphism from G to $K \setminus \{0\}$.

Note that, for all $\sigma \in \mathrm{Aut}(K)$, it can be a character from $K \setminus \{0\}$ to $K \setminus \{0\}$.

Lemma 3.27 (Dedekind's Lemma)**.** *Assume that $\tau_1, \ldots, \tau_n$ are distinct characters from G to $K \setminus \{0\}$. Then $\tau_1, \ldots, \tau_n$ are linearly independent. Precisely speaking, if there exist $c_1, \ldots, c_n \in K$ such that $\sum_{i=1}^n c_i \tau_i(g) = 0$ for all $g \in G$, then $c_i = 0$ for all $i \in [n]$.*

Proof. Assume that $\tau_1, \ldots, \tau_k$ are not linearly independent and k is the minimal. Since $\tau_1 \neq \tau_2$, there exists $h \in G$ such that $\tau_1(h) \neq \tau_2(h)$. Since $\tau_1, \ldots, \tau_k$ are not linear independent, there exist $c_1, \ldots, c_k \in K$ such that $c_1, \ldots, c_k$ are not all zero and for all $g \in G$,

$$\sum_{i=1}^{k} c_i \tau_i(g) = 0, \quad \sum_{i=1}^{k} c_i \tau_i(h \cdot g) = 0.$$

Since k is minimal, we know $c_i \neq 0$ for all $i \in [k]$. Thus we know

$$\sum_{i=1}^{k} c_i \tau_1(h)\tau_i(g) = 0 \qquad \sum_{i=1}^{k} c_i \tau_i(h)\tau_i(g) = 0.$$

Then it implies

$$\sum_{i=2}^{k} c_i(\tau_i(h) - \tau_1(h))\tau_i(g) = 0.$$

Then we see $\tau_2, \ldots, \tau_k$ are not linearly independent, leading to a contradiction to the choice k is minimal. □

It makes sense that we give a vector space interpretation of Dedekind's Lemma.

Proposition 3.28. *If K is a finite field extension of F, then $|\mathrm{Gal}(K/F)| \leq [K : F]$.*

Proof. Since $[K : F] < \infty$, we know $|\mathrm{Gal}(K/F)| < \infty$. Let $\mathrm{Gal}(K/F) = \{\tau_1, \ldots, \tau_n\}$, and let $\alpha_1, \ldots, \alpha_m$ be a basis for K as an F-vector space. Consider the matrix $\Gamma \in K^{n\times m}$ defined as

$$\Gamma_{ij} = \tau_i(\alpha_j), \quad \forall i \in [n], j \in [m].$$

Suppose that $m < n$. Then we know $\mathrm{rank}(\Gamma) = m < n$, which means $\Gamma_1, \ldots, \Gamma_n$ are not linearly independent. Thus there exist $c_1, \ldots, c_n \in K$ such that $c_1, \ldots, c_n$ are not all zero and

$$\sum_{i=1}^{n} c_i \tau_i(\alpha_j) = 0, \quad \forall j \in [m].$$

For all $g \in K \setminus \{0\}$, it holds that $g = \sum_{j=1}^{m} a_j \alpha_j$ for some $a_1, \ldots, a_m \in K$. Thus,

$$\begin{aligned}
\sum_{i=1}^{n} c_i \tau_i(g) &= \sum_{i=1}^{n} c_i \tau_i \left(\sum_{j=1}^{m} a_j \alpha_j \right) \\
&= \sum_{i=1}^{n} c_i \sum_{j=1}^{m} a_j \tau_i(\alpha_j) \\
&= \sum_{j=1}^{m} a_j \sum_{i=1}^{n} c_i \tau_i(\alpha_j) \\
&= 0.
\end{aligned}$$

By Lemma 3.27, we know $c_i = 0$ for all $i \in [n]$. This leads to a contradiction. □

It's very interesting to investigate when $|\mathrm{Gal}(K/F)| = [K : F]$.

Proposition 3.29. *Let $G \subseteq \mathrm{Aut}(K)$ be a finite subgroup and $F = \mathcal{F}(G)$. Then $|G| = [K : F]$ and $G = \mathrm{Gal}(K/F)$.*

Proof. Since $G \subseteq \mathrm{Gal}(K/F)$, we know $|G| \leq [K : F]$. Assume that $n := |G| < [K : F]$. We pick $\alpha_1, \ldots, \alpha_{n+1} \in K$ which are linearly independent over F. And assume that $G = \{\tau_1, \ldots, \tau_n\}$. Consider the matrix $\Gamma \in K^{n\times(n+1)}$ defined as $\Gamma_{ij} = \tau_i(\alpha_j)$ for all $i \in [n]$ and $j \in [n+1]$. Then we know $\Gamma_1^\top, \ldots, \Gamma_{n+1}^\top$ are linearly dependent. Choose k minimal so that, $\Gamma_1^\top, \ldots, \Gamma_k^\top$ are linearly dependent over K. That is to say, there are not all zero $c_1, \ldots, c_k \in K$ such that $\sum_{i=1}^{k} c_i \tau_j(\alpha_i) = 0$ for all $j \in [n]$. By the minimality of k, for all $i \in [k]$, $c_i \neq 0$. Without loss of generality, we assume that $c_1 = 1$. If all $c_i \in F$, it holds that $0 = \tau_j \left(\sum_{i=1}^{k} c_i \alpha_i \right)$ for all $j \in [n]$, which means

$$\sum_{i=1}^{k} c_i \alpha_i = 0,$$

leading to a contradiction to the choice of $\alpha_1, \ldots, \alpha_{n+1}$. Take $\sigma \in G$. Note that we can view σ as a permutation of K, meaning that $\sum_{i=1}^{k} \sigma(c_i)\tau_j(\alpha_i) = 0$ for all $j \in [n]$. Then, we know $\sum_{i=2}^{k} (c_i - \sigma(c_i))\tau_j(\alpha_i) = 0$ for all $j \in [n]$. From the minimality of k, we know $c_i = \sigma(c_i)$ for all $i \in [k]$. Then we know for all $\sigma \in G$, $\sigma \in \mathcal{F}(G) = F$. Thus we know $|G| = [K : F]$. Since $G \subseteq \mathrm{Gal}(K/F)$, then we know $G = \mathrm{Gal}(K/F)$. □

Now we are ready to introduce the formal definition of Galois extensions.

Definition 3.30 (formal definition of Galois extensions)**.** Let K be an algebraic extension of F. We say K is a *Galois extension* of F if and only if $F = \mathcal{F}(\mathrm{Gal}(K/F))$.

Remark 3.31. It's not hard to show when $[K : F] < \infty$, Definition 3.24 is equivalent to Definition 3.30. Also, another equivalent definition is that K/F is a Galois extension if and only if K/F is normal and splitting.

It's not an easy work to see whether an extension is Galois. To consider a simple/basic case, we consider a simple algebraic extension over a field.

Corollary 3.32. *Let K be a field extension of F and $\alpha \in K \setminus F$ be algebraic over F. Then $|\mathrm{Gal}(F(\alpha)/F)|$ is equal to the number of distinct roots of $\min(F, \alpha)$ in F. Therefore $F(\alpha)$ is a Galois extension over F if and only if $\min(F, \alpha)$ has n distinct roots in $F(\alpha)$, where $n = \deg(\min(F, \alpha))$.*

3.5 Normal extensions

Now let's see the normal extensions. Let F be a field. For $f(x) \in F[x]$ with $\deg(f) = n > 0$, we know that there exists a field extension K of F such that f has n roots in K, and $[K : F] \leq n!$. Conversely, for any field extension E of F, f has at most n roots in E.

Definition 3.33. Let $F < K$ and $f \in F[x]$. If $f(x) = \alpha(x - \alpha_1) \ldots (x - \alpha_n)$ where $\alpha_i \in K$ for all $i \in [n]$, then we say f *splits* over K.

Definition 3.34. Let $F < K$ and $f(x) \in F[x]$, and let S be a collection of non-constant polynomials over F.

1. If $f(x) = \alpha(x - \alpha_1) \ldots (x - \alpha_n)$ splits over K and $K = F(\alpha_1, \ldots, \alpha_n)$, then we say K is a *splitting field* of f over F.

2. We say K is a *splitting field* of S over F if for all $f \in S$, f splits over K and $K = F(X)$ where X is the collection of all roots of all $f \in S$.

Given F and S, it needs to show whether the splitting field exists. Firstly, when S is finite, assume that $S = \{f_1, \ldots, f_m\}$. Let $f = f_1 \ldots f_m$. Then there exists a field extension K of F such that K is the splitting field of S over F.

Theorem 3.35. *The followings are equivalent.*

1. *There are no algebraic extensions of K other than K itself.*

2. *There are no finite extensions of K other than K itself.*

3. *If L is a field extension of K, then $K = \{\alpha \in L \mid \alpha$ is algebraic over $K\}$.*

4. *Every $f(x) \in K[x]$ splits over K.*

5. *Every $f(x) \in K[x]$ has a root in K.*

6. *Every irreducible polynomial over K has degree* 1.

Proof. $1 \implies 2$: This is trivial.

$2 \implies 3$: Firstly it is clear that $K \subseteq \{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$. On the other hand, for all $\alpha \in L$ which is algebraic over K, $K(\alpha)$ is a finite extension of K, which means $K(\alpha) = K$. Then we know $\alpha \in K$.

$3 \implies 4$: Let L be the splitting field of f over K. Then we know L is algebraic over K, which means $L = K$.

$4 \implies 5$: This is clear.

$5 \implies 6$: Let $f \in K[x]$ be irreducible. By 5, f has a root in K, so f has a linear factor. Since f is irreducible, we know that f must be linear, meaning that $\deg(f) = 1$.

$6 \implies 1$: Let L be an algebraic extension of K. For $\alpha \in L$, consider $p(x) = \min(K, \alpha)$. By 6, it holds that $\deg(p(x)) = 1$, which means $[K(\alpha) : K] = 1$. Then $\alpha \in K$. ◻

Then we can give a formal definition of algebraic closures.

Definition 3.36 (formal definition of algebraic closures)**.** For a field K, if K satisfies one of $1-6$, then we say K is *algebraically closed.* If K is an algebraic extension of F and K is algebraically closed, we say K is an algebraic closure of F, written as $\overline{F}$.

Example 3.37. *$\mathbb{C}$ is algebraically closed. But $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$. Now consider*

$$A := \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

Then it's not hard to verify A is an algebraic closure of $\mathbb{Q}$.

The following theorem shows the algebraic closures always exist. For the sake of simplicity, we omit the proof.

Theorem 3.38. *Let F be a field. Then $\overline{F}$ exists.*

Based on Theorem 3.38, we know the splitting field exists.

Corollary 3.39. *For all $S \subseteq F[x]$, there exists a splitting field of S over F.*

Proof. For all $f \in S$, it is clear that f splits over $\overline{F}$. Then we know $X \subseteq \overline{F}$ where X is the collection of all roots of $f \in S$. Then we know $F(X) \subseteq \overline{F}$. Then we prove the corollary. □

Corollary 3.40. *The splitting field of $F[x]$ is $\overline{F}$.*

Proof. Let K be the splitting field of $F[x]$. It is clear that $K \subseteq K[x]$. For all $\alpha \in \overline{F}$, α is algebraic over F. Then we know the roots of $\min(F, \alpha)$ are in K, meaning that $\alpha \in K$. Then we know $K = \overline{F}$. □

The following theorem is **very significant**.

Theorem 3.41 (Isomorphism Extension Theorem)**.** *Let $\sigma : F \longrightarrow F'$ be a field isomorphism and $S = \{f_i\} \subseteq F[x]$. Let $S' = \{\sigma(f_i)\} \subseteq F'[x]$. Assume that K is the splitting field of S over F and K' is the splitting field of S' over F'. Then there exists a field isomorphism $\tau : K \longrightarrow K'$ with $\tau|_F = \sigma$.*

Corollary 3.42. *Let F be a field and $S \subseteq F[x]$. Then there exists a field isomorphism between two splitting fields of S. In particular, two algebraic closures of F are F-isomorphic.*

Now we introduce the normal extension.

Definition 3.43 (normal extension)**.** Let $F < K$. We say K is a *normal extension* of F if K is a splitting field of S over F for some $S \subseteq F[x]$.

Lemma 3.44. *Let K be an algebraic extension of F. The followings are equivalent.*

1. *K is a normal extension of F.*
2. *M is the algebraic closure of F and $\tau : K \longrightarrow M$ is an F-embedding. Then $\tau(K) = K$.*
3. *Let $F < L < K < M = \overline{F}$ and $\sigma : L \longrightarrow M$ be an F-embedding. Then $\sigma(L) < K$ and there exists $\tau \in \mathrm{Gal}(K/F)$ such that $\tau|_L = \sigma$.*
4. *For every irreducible polynomial $f(x) \in F[x]$, if f has a root in K, then f splits over K.*

Proof. $1 \Longrightarrow 2$: Assume that X is the collection of roots of S in M and then $K = F(X)$. Thus we know

$$K = \bigcup_{\{\alpha_1,\ldots,\alpha_n\}\subseteq X} F(\alpha_1, \ldots, \alpha_n).$$

Thus we know $\tau(K) = \tau(F(X)) = F(\tau(X))$. Since $\tau|_X$ is a permutation of X, then we know $F(\tau(X)) = F(X)$.

$2 \Longrightarrow 3$: Given an F-embedding $\sigma : L \longrightarrow M$, we know $\sigma : L \longrightarrow \sigma(L)$ is an F-homomorphism. Since $M = \overline{F}$, meaning that M is the splitting field of $F[x] \setminus F$, by Theorem 3.41, there exists an F-isomorphism $\sigma' : M \longrightarrow M$ such that $\sigma'|_L = \sigma$. Let $\tau := \sigma'|_K$. By 2, we know $\tau(K) = K$. Thus we have

$$\sigma(L) = \sigma'(L) \subseteq \sigma'(K) = \tau(K) = K.$$

Additionally, we know $\tau(F) = \sigma'(F) = \sigma(F) = F$. Then we show $\tau \in \mathrm{Gal}(K/F)$.

$3 \implies 4$: Assume that $\alpha \in K$ is a root of f, and suppose that $\beta \in M = \overline{F}$ is another root of f. Let $L = F(\alpha)$. Consider $\sigma : L \to M$ such that $\sigma : \alpha \mapsto \beta$. By 3, we know $\sigma(L) \subseteq K$. Since $\beta = \sigma(\alpha) \in \sigma(L)$, we know $\beta \in K$. By the arbitrary choice of β, we conclude f splits over K.

$4 \implies 1$: Let

$$S = \{\min(F, \alpha) \mid \alpha \in K\}$$

and X be the collection of all roots of $f \in S$. By 4, we know $X \subseteq K$, meaning that $F(X) \subseteq K$. On the other hand, by the construction of S, we know $K \subseteq X$, $K \subseteq F(X)$. Then we know $K = F(X)$. □

Example 3.45. *Consider $\mathbb{Q} < \mathbb{Q}(\sqrt[3]{2}, \omega)$, $\omega = e^{2\pi i/3}$. Using 2 in Lemma 3.44, we know $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is normal.*

3.6 Separable extensions

Now we focus on some results on separable extensions.

Theorem 3.46. *Let K be an algebraic extension of F. Then the followings are equivalent.*

1. *K/F is Galois.*
2. *K/F is normal and separable.*
3. *K is a splitting field of a family of separable polynomials on F.*

Proof. $1 \implies 2$: For all $\alpha \in K$, it holds that

$$\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(K/F)\} \subseteq K.$$

Let $\{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(K/F)\} = \{\alpha_1, \ldots, \alpha_n\}$. It holds that $\min(F, \alpha) = \min(F, \alpha_i)$, for all $i \in [n]$.

Consider $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$. Then we know

$$\sigma f = \prod_{i=1}^{n}(x - \sigma(\alpha_i)) = f.$$

This means σ keeps the coefficients of f stable, $\mathrm{coef}(f) \subseteq \mathcal{F}(\mathrm{Gal}(K \setminus F)) = F$. Then $f(x) \in F[x]$, meaning that $\min(F, \alpha) \mid f$. Obviously $f \mid \min(F, \alpha)$. Then $f(x) = \min(F, \alpha)$, meaning that f is separable on K.

$2 \implies 3$: Consider $S = \{\min(F, \alpha) \mid \alpha \in K\}$ and K is the splitting field of S on F.

$3 \implies 1$: Assume that $[K : F] < \infty$. Let $n = [K : F]$. If $n = 1$, $K = F$, then it is trivial $F = \mathcal{F}(\mathrm{Gal}(K/F))$. Assume that when $m < n$ the statement is true. Assume that K is the splitting field of $\{f_i\}$ on F where each f_i is separable. Pick a root α of f_i, $\alpha \notin F$. Let $L = F(\alpha)$. Then $[K : L] < n$. By hypothesis assumption, K/L is Galois. Let $H = \mathrm{Gal}(K/L)$. Then $|H| = [K : L]$. Let $G = \mathrm{Gal}(K/F)$. It is trivial that $H \subseteq L$. Consider G/H. Let $\alpha_1, \ldots, \alpha_r$ be different roots of $\min(F, \alpha)$ in K. Consider the homomorphism $\mathrm{id} : F \to F$. By Theorem 3.41, there exists an F-isomorphism $\tau : K \to K$. We can pick $\tau(\alpha) = \alpha_i$ for any arbitrary $i \in [n]$. We enumerate them as $\tau_1, \ldots, \tau_r$ and $\tau_i \in \mathrm{Gal}(K/F) = G$. Note that $\tau_1 H, \ldots, \tau_r H$ are different cosets, meaning that $|G/H| \geq r$.

$$|G| = |G/H| \cdot |H| \geq r|H| = [L : F][K : L] = [K : F].$$

Together with the fact $|G| \leq [K : F]$, we know $[K : F] = |G|$. Since $[K : F] < \infty$, we know K/F is Galois.

Now we consider any arbitrary algebraic $F < K$. Assume that K is the splitting field of S on F and any $f \in S$ is separable. Let X be the collection of all roots of $f \in S$. Then $K = F(X)$. Now we prove that for all $\alpha \in \mathcal{F}(\mathrm{Gal}(K/F))$, $\alpha \in F$. Since $K = F(X)$, there exists $\{\alpha_1, \ldots, \alpha_n\} \subseteq X$ such that

$$\alpha \in F(\alpha_1, \ldots, \alpha_n).$$

Consider the splitting field $L \subseteq K$ of $\{\min(F, \alpha_i) : \forall i \in [n]\}$. Then we know L/F is Galois. Note that $\alpha \in L$. By Theorem 3.41, we have

$$\mathrm{Gal}(L/F) = \{\sigma|_L \mid \sigma \in \mathrm{Gal}(K/F)\}.$$

Then we know $\alpha \in \mathcal{F}(\mathrm{Gal}(L/F)) = F$. Then we know $\mathcal{F}(\mathrm{Gal}(L/F)) = F$, meaning that K/F is Galois. □

3.7 Fundamental theorem of Galois theory

Now we introduce the most important theorem of Galois theory.

Theorem 3.47 (fundamental theorem of Galois theory)**.** *Let K/F be a finite Galois extension and $G = \mathrm{Gal}(K/F)$. Then,*

1. *There exists an one-to-one mappings between all intermediate fields of K/F and all subgroups of G. Precisely, for $F < L < K$, we map L to $\mathrm{Gal}(K/L)$ and for $H < G$, we map H to $\mathcal{F}(H)$.*
2. *For $L \leftrightarrow H$, it holds that $[K : L] = |H|$ and $[L : F] = [G : H]$.*
3. *For $L \leftrightarrow H$, H is a normal subgroup of G if and only if L/F is Galois. When it occurs, $\mathrm{Gal}(L/F) \cong G/H$.*

Proof.

1. We have already known that the maps $L \mapsto \mathrm{Gal}(K/L)$ and the map $H \mapsto \mathcal{F}(H)$ give an one-to-one correspondence from $\{F < L < K \mid \exists H \subseteq G, L = \mathcal{F}(H)\}$ and $\{H < G \mid \exists F < L < K, H = \mathrm{Gal}(K/L)\}$. What remains to do is to prove for all $F < L < K$, there exists $H < G$ such that $\mathcal{F}(H) = L$ and for all $H < G$, there exists $F < L < K$ such that $\mathrm{Gal}(K/L) = H$.

   Since K/F is Galois, we assume that K is the splitting field of $\{f_i\}$ on F and each f_i is separable. Then K is the splitting field of $\{f_i\}$ on L and each f_i is separable, meaning that K/L is Galois. Thus we know $L = \mathcal{F}(\mathrm{Gal}(K/L))$.

   For all $H < G$, since H is finite, we know $H = \mathrm{Gal}(K/\mathcal{F}(H))$.

2. Since K/L is a finite Galois extension, we know that

   $$[K : L] = |\mathrm{Gal}(K/L)| = |H|.$$

   On the other hand,

   $$|G : H| = |G|/|H| = [K : F]/[K : L] = [L : F].$$

3. Assume that H is the normal subgroup of G. For all $\alpha \in L$, we consider $\min(F, \alpha)$. Assume that β is another root of $\min(F, \alpha)$. For $\mathrm{id} : F \to F$, by Theorem 3.41, we can find an F-isomorphism $\sigma : K \to K$ such that $\sigma(\alpha) = \beta$. For $\tau \in H = \mathrm{Gal}(K/L)$, $\tau|_L = L$. Since H is normal, we know $\sigma^{-1}\tau\sigma \in H$ and $\tau(\beta) = \beta(\sigma(\alpha)) = \sigma\sigma^{-1}\tau(\sigma(\alpha)) = \sigma(\alpha) = \beta$. Thus $\beta \in \mathcal{F}(H)$. Then $\beta \in L$, meaning that $\min(F, \alpha)$ splits over L. That is to say, L/F is normal. Additionally, since K/F is separable, we know L/F is Galois.

   Now we assume that L/F is Galois. Define $\theta : G \to \mathrm{Gal}(L/F)$, $\sigma \mapsto \sigma|_L$. It's not hard to see θ is a homomorphism. Since L/F is normal, we know $\sigma|_L = L$. Thus we know

   $$\ker(\theta) = \{\sigma \in G \mid \sigma|_L = \mathrm{id}\} = \mathrm{Gal}(K/L) = H.$$

   This implies H is the normal subgroup. Moreover, we know θ is surjective, meaning that $G/\ker(\theta) \cong \mathrm{Gal}(L/F)$, $G/H \cong \mathrm{Gal}(L/F)$.

□

4 Finite Fields

Given a finite field F, we know $\text{char}(F) = p$ where p is a prime number, and $(F^* = F \setminus \{0\}, \times)$ is a cyclic group. Then, we know the extension of F of finite degree is simple.

For $F_p < F$, $[F : F_p] = n$, assume that $\alpha_1, \ldots, \alpha_n$ are F_p-basis of F. Then we know $|F| = p^n$.

Lemma 4.1. *Every finite field is a splitting field.*

Proof. Assume that $F_p < F_q$, where $q = p^n$. For all $\alpha \in F_q^*$, we know $\alpha^{q-1} = 1$. Then for all $\alpha \in F_q$, α is a zero of $x^q - x$. Since $x^q - x$ has at most q zeros and $(x^q - x)' = -1 \neq 0$, we know all zeros of $x^q - x$ are F_q. Then we know F_q is the splitting field of $x^q - x$ over F_p. □

Recall that, every irreducible polynomial has no repeated roots. Then we know $K < L$ is Galois of finite degree, for finite fields $K < L$.

Question: For all $n > 0$, does there exist F_q with $q = p^n$?

The answer is yes. For all n, p, q such that $q = p^n$, let $f_q(x) = x^q - x$. Then we know $f_q(x)$ splits on $\overline{F_p}$ and is separable. Let R be q distinct zeros of $f_q(x)$. For all $\alpha, \beta \in R$, it's not hard to show $\alpha - \beta \in R$, $\alpha\beta^{-1} \in R$. Then we know R is a field ($R = F_q$).

Note that, by Theorem 3.41, under the isomorphism we can say F_q is unique. Now for $F_q < F_{q^n}$, we conclude:

- $f_{q^n}(x) = x^{q^n} - x$ is the determining polynomial of F_{q^n}.
- F_{q^n} is the splitting field of f_{q^n} over F_q.
- For all $n > 0$, there exists F_{q^n}.
- Every extension of F_q must be F_{q^n} for some $n \in \mathbb{N}$.

Since $F_q < F_{q^n}$ is finitely Galois, we know

$$\left|\text{Gal}(F_{q^n}/F_q)\right| = [F_{q^n} : F_q] = n.$$

4.1 Subfields of a finite field

Let $F_q < K < L$ where $K = F_{q^d}$, $L = F_{q^n}$. Then we know

$$[F_{q^n} : F_q] = [F_{q^n} : F_{q^d}] \cdot [F_{q^d} : F_q],$$

meaning that $d \mid n$.

When $d \mid n$, for all $\alpha \in F_{q^d}$, we know $\alpha^{q^d} = \alpha$. Then we show that

$$\alpha^{q^n} = \alpha^{(q^d)^{n/d}} = \alpha.$$

Thus we know $\alpha \in F_{q^n}$. Then $F_{q^d} < F_{q^n}$. Combining all above, we conclude

$$F_{q^d} < F_{q^n} \iff d \mid n.$$

We consider $f_{q^d}(x)$ and $f_{q^n}(x)$. If $F_{q^d} < F_{q^n}$, we know

$$f_{q^d}(x) = \prod_{\alpha \in F_{q^d}} (x - \alpha) \,\Bigg|\, \prod_{\alpha \in F_{q^n}} (x - \alpha) = f_{q^n}(x).$$

Conversely, if $f_{q^d}(x) \mid f_{q^n}(x)$, it is trivial to see $F_{q^d} < F_{q^n}$. Then we know

$$F_{q^d} < F_{q^n} \iff d \mid n \iff f_{q^d} \mid f_{q^n}.$$

4.2 Galois group of finite extension of finite fields

Let $F_q < F_{q^n}$ and $G = \text{Gal}(F_{q^n}/F_q)$. Then $|G| = n$. We define an isomorphism $\sigma : F_{q^n} \to F_{q^n}, \alpha \mapsto \alpha^q$. For all $\alpha \in F_q$, we know $\sigma(\alpha) = \alpha^q = \alpha$. Then we know $\sigma \in \text{Gal}(F_{q^n}/F_q)$. Consider $\mathcal{F}(\sigma) = \left\{\alpha \in F_{q^n} \;\middle|\; \alpha^q = \alpha\right\}$. Then $F_q \subseteq \mathcal{F}(\sigma)$. Obviously $|\mathcal{F}(\sigma)| \le q$. Then we know $\mathcal{F}(\sigma) = F_q$. Actually we know

$$\mathcal{F}(\langle\sigma\rangle) = \mathcal{F}(\sigma) = F_q.$$

Then we know $\langle\sigma\rangle = \text{Gal}(F_{q^n}/F_q)$. We call σ the Frobenius mapping.

For an extension, if its Galois group is cyclic, we say this extension is cyclic. Also if its Galois group is abelian, we call this extension abelian.

4.3 Existence of irreducible polynomials

Now we answer the question: for all $d > 0$, is there any irreducible polynomial with degree d over F_q? The answer is yes. For $F_q < F_{q^d} = F_q(\alpha)$, it holds that $\deg(\min(F_q, \alpha)) = d$.

Assume that $p(x)$ is an irreducible polynomial over F_q with degree d, and $p(\alpha) = 0$. Then we know $F_q(\alpha) = F_{q^d}$. Since $F_q < F_{q^d}$ is normal, we know $p(x) \mid x^{q^d} - x$. And it's not hard to show

$$p(x) \mid x^{q^n} - x \iff F_{q^d} < F_{q^n} \iff d \mid n.$$

Assume that $F_q(\alpha) = F_{q^d}$, and $G = \text{Gal}(F_{q^d}/F_q) = \langle\sigma\rangle$, where $\sigma : \alpha \mapsto \alpha^q$. Then we know $\alpha, \sigma(\alpha), \ldots, \sigma^{d-1}(\alpha)$ are d distinct roots of $\min(F_q, \alpha)$. Then we know

$$\min(F_q, \alpha) = \prod_{i=0}^{d-1}(x - \alpha^{q^{d-1}}).$$

Then we know

$$f_{q^n}(x) = \prod_{\alpha \in F_{q^n}} (x - \alpha) = p_1(x) \ldots p_m(x)$$

where $\deg(p_i) \mid n$ for all $i \in [m]$.

Conversely, we know $f_{q^n}(x) = x^{q^n} - x$ can be decomposed into all monic minimal irreducible with degree $d \mid n$.

For $F_q < K < F_{q^d} = F_q(\alpha)$, we know for $\beta \in K$, its conjugate elements are $\sigma(\beta), \ldots, \sigma^d(\beta)$.

4.4 Order of irreducible polynomials

Given an irreducible polynomial $p(x)$ and its zero α, assume that $\deg(p) = d$. Then we know $\alpha^{q^d - 1} = 1$. Assume that $o(\alpha) = v$. Then it can be shown that $o(\sigma(\alpha)) = o(\alpha) = v$. Then we define $o(p(x)) = o(\alpha) = v$.

If $o(p) = q^d - 1$, we say p is a primitive polynomial.

4.4.1 Connection between degree and order

It's not hard to show

$$v \mid q^d - 1, q^d \equiv 1 (\operatorname{mod} v).$$

For all n, if $\alpha^{q^n} = \alpha$, then we know $q^n \equiv 1 (\operatorname{mod} v)$. Thus we know $d \le n$, meaning that it is the order of q in Z_v^*.

4.4.2 Calculate the order of a polynomial

Assume that $v = o(p)$. We know that

- $v \mid p^d - 1$.
- For all $n \in \mathbb{N}_{>0}$, $v \mid n \iff p(x) \mid x^n - 1$.

Then we calculate the factorization of $p^d - 1$ as $p_1^{e_1} \dots p_m^{e_m}$. Then we know

$$v = p_1^{f_1} \dots p_m^{f_m}, f_i \le e_i \forall i \in [m].$$

For $i \in [m]$, we run $a_i = 0, 1, \dots, e_i$ and test

$$p(x) \mid x^{p_1^{e_1} \dots p_i^{a_i} \dots p_m^{em}} - 1.$$

If the test succeeds, we set $f_i = a_i$. Finally we get the value of v.

4.5 Finite field arithmetic

For $F_p < F = F_p(\alpha)$ where $\alpha \in F$ is primitive, assume that $\deg(\min(F_p, \alpha)) = d$ and $F^* = \langle\alpha\rangle$. Then we know

$$F = \left\{0, 1, \alpha, \dots, \alpha^{|F|-2}\right\}.$$

On the other hand, we know

$$F_p(\alpha) = \left\{f(\alpha) \;\middle|\; f \in F_p[x], \deg(f) < d\right\}.$$

Then we know for every $0 \le k \le |F| - 2$, there exists $f \in F_p[x]$ such that $\alpha^k = f(\alpha)$.

Example 4.2. *Let $F_2 < F_{2^4} = F_{16}$. Consider the polynomial $p(x) = x^4 + x + 1 \in F_2[x]$. It's not hard to verify $p(x)$ is irreducible. Let $\alpha \in \overline{F_2}$ be a zero of $p(x)$. Then, we know the element in F_{16} can be represented as*

Constants:	$0, 1$
Linear:	$\alpha, \alpha + 1$
Quadratic:	$\alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1$
Cubic:	$\alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1.$

For $0 \le k \le 14$, assume that $\alpha^k = a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + \alpha_0$. For instance, we have $\alpha^4 = \alpha + 1$. By direct calculation, we have the following field table.

k	$a_3a_2a_1a_0$
0	0001
1	0010
2	0100
3	1000
4	0011
5	0110
6	1100
7	1011
8	0101
9	1010
10	0111
11	1110
12	1111
13	1101
14	1001

We can use the field table to simplify the calculations.

Also, the field table can be used to find the minimal polynomial of $\beta \in F_{16}$ over F_2. Firstly, for all $\beta \in F_2(\alpha)$ where $F_2 < F_2(\beta) < F_2(\alpha)$, assume that $\mathrm{Gal}(F_2(\beta)/F) = \langle\tau\rangle$. *Let $L = F_2(\beta)$. Then $F_2 < L < F_{16}$. For all $\tau^* \in \langle\tau\rangle$, we know $\tau^* : L \longrightarrow L$ is an F_2-isomorphism. Then we can find $\sigma^* : F_{16} \longrightarrow F_{16}$ is an F_2-isomorphism and $\sigma^*|_L = \tau^*$. Conversely, for any $\sigma^* \in \langle\sigma\rangle$, we know $\sigma^*|_L : L \longrightarrow F$ is an F_2-embedding. Since L/F_2 is normal, we know $\sigma^*|_L \in \langle\tau\rangle$.*

Then, to find the minimal polynomial of β, it suffices to find all conjugations of β.

$$\begin{aligned}
&\left\{\alpha, \alpha^2, \alpha^4, \alpha^8\right\}, \\
&\left\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\right\}, \\
&\left\{\alpha^5, \alpha^{10}\right\}, \\
&\left\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\right\}.
\end{aligned}$$

Then we know

$$\begin{aligned}
\min(F_2, \alpha) = x^4 + x + 1, \min(F_2, \alpha^3) = x^4 + x^3 + x^2 + 1, \\
\min(F_2, \alpha^5) = x^2 + x + 1, \min(F_2, \alpha^7) = x^4 + x^3 + 1.
\end{aligned}$$

Also we can show

$$x^{16} - x = x(x+1)(x^4+x+1)(x^4+x^3+x^2+1)(x^2+x+1)(x^4+x^3+1).$$

4.6 The number of irreducible polynomials of degree d

Now we want to know the number of irreducible polynomials of degree d in $F_p[x]$, denoted by $N_q(d)$. Since we know

$$x^{q^n} - x = p_1(x) \ldots p_m(x)$$

where $p_1, \ldots, p_m$ are all irreducible polynomials in $F_p[x]$, taking zeros into consideration, we obtain

$$q^n = \sum_{d \mid n} dN_q(d).$$

We employ the Möbius inversion. For any f, g satisfying

$$g(n) = \sum_{d \mid n} f(d),$$

it holds that

$$f(n) = \sum_{d \mid n} g(d) \mu\left(\frac{n}{d}\right)$$

where μ is the Möbius function satisfying

$$\sum_{d \mid n} \mu(d) = \mathbb{1}\left[n = 1\right].$$

Thus we know

$$N_q(n) = \frac{1}{n} \sum_{d \mid n} q^d \mu\left(\frac{n}{d}\right).$$

4.7 Factoring over $\mathbb{Z}_p$: Berlekamp's algorithm

For every $f \in F_p[x]$ with $\deg(f) = d$, we want to check whether it is irreducible. Our goal is to find $g(x) \in F_p[x]$ of degree $< d$ such that $f(x) \mid g(x)^p - g(x)$.

The correctness of the method: Since

$$x^p - x = \prod_{i=0}^{p-1} (x - i),$$

we know

$$g(x)^p - g(x) = \prod_{i=0}^{p-1} (g(x) - i).$$

In an UFD, if $a \mid b_1 \dots b_k$ and for all distinct i, j, b_i and b_j are relative prime, then (assume that $a = p_1^{e_1} \dots p_m^{e_m}$) for all $i \in [m]$, there exists b_j such that $p_i^{e_i} \mid b_j$. Thus we know

$$a = p_1^{e_1} \dots p_m^{e_m} \mid \prod_{j=1}^{k} \gcd(a, b_j).$$

Conversely, we know

$$\prod_{j=1}^{k} \gcd(a, b_j) \mid a.$$

Then we know

$$a = \prod_{j=1}^{k} \gcd(a, b_j).$$

Then we know $f(x) = \prod_{j=0}^{p-1} \gcd(f, g - j)$.

The algorithm: Let $g(x) = \sum_{i=0}^{d-1} g_i x^i$. Then by direct calculation, it holds that

$$g(x)^p - g(x) = \sum_{i=0}^{d-1} g_i (x^{ip} - x^i).$$

Assume that $x^{ip} = a_i f(x) + r_i(x)$ where $\deg(r_i) < d$. Then

$$f \mid g^p - g \iff f \mid \sum_{i=0}^{d-1} g_i (r_i(x) - x^i) \iff \sum_{i=0}^{d-1} g_i (r_i(x) - x^i) = 0.$$

Let $r_i(x) = \sum_{\ell=0}^{d-1} r_{i\ell} x^\ell$. Then, let $M = (r_{ij})_{ij}$, $G^\top = (g_0, \dots, g_{d-1})$. Then we know

$$(M^\top - I)G = 0.$$

Solving this linear equations, we can obtain g or show f is irreducible.

5 Roots of Unity

Now we focus on the roots of x^n-1. We have already known the roots of x^n-1 over $\mathbb{C}$ is $\left\{e^{k\frac{2\pi i}{n}} \,\middle|\, k=0,1,\ldots,n-1\right\}$.

Definition 5.1. Given a field F, we say the roots of x^n-1 over F on $\overline{F}$ are *the n-th roots of the unity over F.*

Furthermore, for an n-th root ω, if $\operatorname{order}(\omega)=n$ on $\overline{F}$, we say ω is a primitive n-th root. Under this case, we say $F<F(\omega)$ is *a cyclotomic extension.*

Remark 5.2. If ω is a primitive n-th root, then we know $\operatorname{char}(F) \nmid n$. Assume that $n=mp$. Then we know

$$x^n-1=x^{mp}-1=(x^m-1)^p,$$

meaning that ω is an m-th root of the unity over F. Then we know $p \nmid n$.

If ω is the n-th root, it holds that $\operatorname{order}(\omega) \mid n$.

Let $U_n := \left\{\omega \in \overline{F} \,\middle|\, \omega^n-1=0\right\}$. It's not hard to see U_n is a group. Furthermore, U_n is a subgroup of $\overline{F}^*$. Recall that, a finite subgroup of the multiplication group F^* of a field F is cyclic. Then we have the following proposition.

Proposition 5.3. *U_n is cyclic. That is to say, there exists a generator $\omega \in U_n$ such that $U_n=\langle\omega\rangle$.*

Recall the Euler function $\varphi(n)$. Then we know the group

$$\mathbb{Z}_n^* := \{a \in \mathbb{Z}_n \mid (a,n)=1\}.$$

Then we know $\left|\mathbb{Z}_n^*\right|=\varphi(n)$.

Lemma 5.4. *Suppose that $\operatorname{char}(F) \nmid n$. Let K be the splitting field of x^n-1 over F. Then we know K/F is Galois, and $K=F(\omega)$ where ω is the primitive n-th root. Furthermore, there exists a subgroup S of $\mathbb{Z}_n^*$ such that $\operatorname{Gal}(K/F) \cong \mathbb{Z}_n^*$. Thus we know $\operatorname{Gal}(K/F)$ is abelian and $[K:F] \mid \varphi(n)$.*

Proof. Since $(x^n-1)'=nx^{n-1}\neq 0$ for all $x \neq 0 \in F$. Then we know x^n-1 has repetitive roots. Then we know K/F is separable. It is trivial that K/F is normal. Then we conclude K/F is Galois.

Let U_n be the collection of roots of x^n-1 and ω be a primitive n-th root. Then $K=F(U_n)=F(\omega)$. Consider a mapping $f: \operatorname{Gal}(K/F) \longrightarrow \mathbb{Z}_n^*$ where for all $\sigma \in \operatorname{Gal}(K/F)$, $\sigma(\omega)=\omega^i$ and $\operatorname{order}(\omega^i)=n=\frac{n}{(n,i)}$. Then we know $(i,n)=1$. We denote by σ_i this mapping. We let $f(\sigma_i)=i$ and $\ker(f)=\{\mathrm{id}\}$. Then we know there exists some $S<\mathbb{Z}_n^*$ such that $\operatorname{Gal}(K/F)\cong\mathbb{Z}_n^*$. □

Example 5.5. *We know i is the primitive 4-th root. Then we know $[\mathbb{Q}(i):\mathbb{Q}]=2$. Then we know*

$$\operatorname{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}_4^* = \{1,3\}.$$

Example 5.6. *For the field $\mathbb{F}_2$, ω is the primitive 3-rd root: $\omega^3-1=0$. Then we know*

$$\min(\mathbb{F}_2,\omega)=x^2+x+1.$$

And the roots of x^2+x+1 are $\{\omega,\omega+1\}$. Then we know $[\mathbb{F}_2:\mathbb{F}]=2$.

$$\operatorname{Gal}(\mathbb{F}_2(\omega)/\mathbb{F}_2) \cong \mathbb{Z}_3^* = \{1,2\}.$$

Example 5.7. *For the field $\mathbb{F}_2$, ρ is the primitive 7-th root of ρ^7-1. Then we know*

$$x^7-1=(x-1)(x^3+x+1)(x^3+x^2+1).$$

Then we know ρ is the root of x^3+x+1 or x^3+x^2+1. It holds that

$$[\mathbb{F}_2(\rho):\mathbb{F}_2]=3 \implies |\operatorname{Gal}(\mathbb{F}_2(\rho)/\mathbb{F}_2))|=3.$$

Then we know $\operatorname{Gal}(\mathbb{F}_2(\rho)/\mathbb{F}_2) \subsetneqq \mathbb{Z}_7^*$.

Definition 5.8. Given a field F, let $Q_n=\prod_\omega(x-\omega_i)$ where ω_i are all primitive n-th root be *the n-th cyclotomic polynomial.* It's not hard to see $\deg(Q_n)=\varphi(n)$.

It holds that for all $n \in \mathbb{N}$,

$$x^n = \prod_{d \mid n} Q_d(x).$$

Theorem 5.9. *$Q_d(x)$ is monic and all coefficients of F lie on the prime subfield of F.*

Proof. It's easy to show $Q_d(x)$ is monic. Now we prove the second statement by induction. For $n = 1$, it's not hard to see $Q_d(x) = 1$. For all prime number p,

$$Q_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1.$$

Consider $Q_n(x)$. Assume that for all $d \mid n$ with $d < n$, the coefficients of $Q_d(x)$ lie on the prime subfield of F.

$$x^n - 1 = \prod_{d \mid n} Q_d(x) = Q_n(x) \prod_{d \mid n, d<n} Q_d(x).$$

Assume that $R(x) = \prod_{d \mid n, d<n} Q_d(x)$. Then all coefficients of $R(x)$ lie on the prime subfield of F. Assume that

$$Q_n(x) = \sum_{i=0}^{m_1} a_i x^i, R(x) = \sum_{i=0}^{m_2} b_i x^i.$$

Assume that $a_{m'}$ does not lie on the prime subfield of F and m' is maximal. Consider the coefficient of $x^{m'+m_2}$. Thus we know

$$a'_m b_{m_2} + a_{m'+1} b_{m_2-1} + \ldots + a_{m_1} b_{m_2-m_1+m'}$$

lies on the prime subfield of F, meaning that $a'_m b_{m_2}$ lies on the prime subfield of F. □

Recall the Gaussian lemma: let R be an UFD and R' be the quotient field of R. For all $f(x) \in R[x]$, if $f(x) = p(x)h(x)$, $p \in R[x]$ primitive and $h(x) \in R'[x]$. Then we know $h \in R[x]$. Thus we know the following result.

Proposition 5.10. *All coefficients of $Q_n(x)$ lie on $\mathbb{Z}$.*

Also there exists another polynomial.

Proof. Let $x^n = Q_n(x)R(x)$ and $R \in \mathbb{Z}[x]$ (by induction). Assume that

$$x^n - 1 = q(x)R(x) + r(x) \quad p, r \in \mathbb{Z}[x], \deg(r) < deg(R).$$

Then we know $(Q_n(x) - q(x))R(x) = r(x)$, meaning that $Q_n(x) = q(x)$. □

For $\mathbb{F}_q < \mathbb{F}_{q^n}$, it holds that

$$x^{q^n-1} - 1 = \prod_{\alpha \in \mathbb{F}^*_{q^n}} (x - \alpha) = \prod_{d \mid q^n-1} p_{d,1}(x) \ldots p_{d,k_d}(x)$$

where for all $i \in [k_d]$, $\text{order}(p_{d,k_i}) = d$. Thus we can show

$$Q_d(x) = p_1(x) \ldots p_k(x)$$

where all $p_i(x)$ are of order d.

The following theorem is very interesting and of great significance.

Theorem 5.11. *For the field $\mathbb{Q}$, $Q_n(x)$ is irreducible.*

Then we know that $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}^*_n$ for any primitive n-th root ω.

6 Algebraic Coding Theory

Now we introduce an application of finite field: *algebraic coding theory.* Firstly we state some basic concepts and some informal introductions here.

Consider the field $\mathbb{F}_2$. For every 'legal' $0/1$-string, we call it *a codeword.* Let k be the number of bits of the information, r be the number of verification bits, and $n = k + r$ be the length of codewords. The collection of all 2^k codewords forms the *code.*

There exists another view for the codes. We can see all $0/1$-strings of length n as the vector space over $\mathbb{F}_2$ with dimension n, and the space of the codes is some sub-space of this vector space with dimension k.

To describe the efficiency of the codes, we define

$$\text{Rate} = \frac{k}{n}.$$

- **Repetition Code:** When $k = 1$, we repeat the bit for r times. The decoding process is quite simple: we only choose the majority. And Rate $= 1/n$, which is very low.
- **Single Parity-Check Code:** For a piece of information $c_1c_2 \dots c_k$, we let $r = 1$, and

  $$c_{k+1} := \sum_{i=1}^{k} c_i.$$

  If there exist odd number of errors, then the decode will fail. Otherwise the decode is wrong. And Rate $= \frac{n-1}{n} = 1 - \frac{1}{n}$.

Now we introduce the formal definition of the algebraic coding. We consider $\mathbb{F}_{q^n}$ as a vector space of dimension n over $\mathbb{F}_q$. Usually we denote it by $V_q[n]$. When the context is clear, we also use $V[n]$. Also we assume that $(n, q) = 1$.

Definition 6.1 (linear code)**.** For a vector sub-space C of $V_q[n]$, we say C is a *linear code.* Let k be the dimension of C. Then we denote C by $V_q[n, k]$ or $[n, k]$.

Definition 6.2 (weight and distance)**.** For every $c \in C$, we define the weight of c as the number of non-zero element in c. For $c_1, c_2 \in C$, we define the distance $d(c_1, c_2)$ between c_1 and c_2 as the weight of $c_1 - c_2$. Moreover, let

$$d = \min(C) := \min_{c_1 \neq c_2 \in C} d(c_1, c_2).$$

Also we denote $C = [n, k]$ by $[n, k, d]$.

6.1 Cyclic code

Now we focus a family of codes named *cyclic code.*

Definition 6.3 (cyclic code)**.** For a linear code $C \subseteq V_q[n]$, we say C is a *cyclic code* if for every $c_0c_1 \dots c_{n-1} \in C$, $c_{n-1}c_0c_1 \dots c_{n-2} \in C$.

Now we use the polynomials to express codes. For a codeword $c_0c_1 \dots c_{n-1}$, let

$$\varphi(c_0 \dots c_{n-1}) := c_0 + c_1x + \dots c_{n-1}x^{n-1}.$$

It is obvious to see $\varphi : C \longrightarrow \mathbb{F}_q^{\leq n-1}[x]$ is injective.

Consider $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Let $R_n = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then it's not hard to show, for all $p \in \varphi(C)$ and $r \in R_n$, $p(x)r(x) \in R_n$, meaning that $\varphi(C)$ is an ideal of R_n. Then we know

$$C \text{ is a cyclic code in } V_q[n] \iff \varphi(C) \text{ is an ideal of } R_n.$$

- Another fact is R_n is a principle integral domain. Let $g(x) \in C$ be the monic polynomial with minimal degree. Thus we know $\langle g(x)\rangle \subseteq C$. For every $f \in C$, assume that

  $$f(x) = q(x)g(x) + r(x), q(x) \in R_n, r = 0 \vee \deg(r) < \deg(g).$$

  Then we know $r(x) = 0$. Thus we know $C = \langle g\rangle$.

- Since $x^n - 1 = 0 \in C = \langle g \rangle$, we know $g \mid x^n - 1$.
- Let $\deg(g) = r$. We define $\dim(C) = n - r$. Since

  $$C = \{f(x)g(x) \mid f \in R_n\},$$

  we call $g(x)$ the generating polynomial of C. It's not hard to show $x^0 g(x), \ldots, x^{n-r-1}g(x)$ is a basis of C.
- For all $p(x) \mid x^n - 1$, we will show $p(x)$ could be a generating polynomial. Let $\langle p(x) \rangle = C = \langle g(x) \rangle$ and $\deg(g) < \deg(p)$. We pick $g(x)$ as the one of minimal degree. Since $g \in \langle p \rangle$, there exists $a \in R_n$ such that $g = pa$. Assume that $x^n - 1 = p(x)f(x)$. Then we know $g(x)f(x) = p(x)a(x)f(x) = 0$ over R_n. But this is impossible.

  To emphasize $g(x)$ is the monic polynomial of minimal degree, we use the notation $C = \langle\langle g(x) \rangle\rangle$. And if $x^n - 1 = g(x)h(x)$, we call $h(x)$ the parity-checking polynomial.
- It's not hard to show

  $$\langle g(x) \rangle = \{p(x) \in R_n \mid p(x)h(x) = 0\}.$$

6.1.1 Zeros of the cyclic code

Let $x^n - 1 = m_1(x) \ldots m_t(x)$ where for every i, $m_i(x)$ is irreducible over $\mathbb{F}_q$. Consider the zero $\alpha \in \overline{\mathbb{F}_q}$ of $m_i(x)$ ($m_i(\alpha) = 0$). For every $f \in \mathbb{F}_q[x]$, it holds that

$$f(\alpha) = 0 \iff f(x) = a(x)m_i(x)$$

meaning that

$$f(\alpha) = 0 \iff f \in \langle\langle m_i(x) \rangle\rangle.$$

For $m_1(x), \ldots, m_t(x)$ and $\alpha_1, \ldots, \alpha_t$ satisfying $\min(\mathbb{F}_q, \alpha_i)$, then we consider

$$g(x) = \operatorname{lcm}(m_1(x), \ldots, m_t(x))$$

and thus we know

$$\langle\langle g(x) \rangle\rangle = \{f \in R_n \mid \forall i \in [t], f(\alpha_i) = 0\}.$$

Let $f = \sum_{i=0}^{n-1} f_i x^i$. Thus we know

$$\begin{bmatrix} \alpha_1^0 & \alpha_1^1 & \ldots & \alpha_1^{n-1} \\ \vdots & & \ddots & \vdots \\ \alpha_t^0 & \alpha_t^1 & \ldots & \alpha_t^{n-1} \end{bmatrix} \begin{bmatrix} f_0 \\ \vdots \\ f_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}.$$

6.2 Hamming code

We set $n = 2^r - 1$ and assume that $\mathbb{F}_{2^r}^* = \langle \omega \rangle$. Then we know ω is the primitive $(2^r - 1)$-th root of unity. Thus we know $\mathbb{F}_{2^r} = \mathbb{F}_2(\omega)$ and the parity-check matrix

$$H = \begin{bmatrix} \omega^0 & \ldots & \omega^{n-2} \end{bmatrix}.$$

Then we know $C = \{f \in R_n \mid f(\omega) = 0\}$.

6.3 Bose-Chaudhuri-Hocquenghem code

Now we introduce *BCH codes*.

Definition 6.4 (BCH code)**.** For a field $\mathbb{F}_q$ and $R_n = \mathbb{F}_q[x]/\langle x^n - 1 \rangle$, let ω be the primitive n-th root of unity, and

$$g(x) := \operatorname{lcm}(\min(\mathbb{F}_q, \omega^b), \ldots, \min(\mathbb{F}_q, \omega^{b+\delta-2})), b \geq 0, \delta \geq 1.$$

Then we say $C = \langle\langle g(x) \rangle\rangle$ is the *BCH code* with parameters q, n, ω, b, δ, denoted by $B_q(n, \omega, b, \delta)$.

When $b = 1$, it is the typical BCH code. When $n = q^s - 1$, we call it the primitive BCH code.

Theorem 6.5. *Let* $C = B_q(n, \omega, b, \delta)$*. Then* $\min(C) \geq \delta$*.*

Remark 6.6. To correct m errors, we need to set $\delta = 2m + 1$.

6.3.1 Decoding for 2-ary BCH code

Consider the codeword $c_0, \dots, c_{n-1}$. Let $c(x) = \sum_{i=0}^{n-1} c_i x^i$. Assume that we receive $u(x)$ and the error polynomial is $e(x)$. Then $u(x) = c(x) + e(x)$.

For the parity-check matrix

$$H = \begin{bmatrix} 1 & \omega & \dots & \omega^{n-1} \\ 1 & \omega^2 & \dots & \omega^{2(n-1)} \\ \vdots & & \ddots & \vdots \\ 1 & \omega^{\delta-1} & \dots & \omega^{(\delta-1)(n-1)} \end{bmatrix},$$

we know that $c(\omega^j) = 0$. Assume that we need to correct w errors. Then $\delta = 2w + 1$. Let

$$u_1 = u(\omega) = e(\omega), u_3 = u(\omega^3) = e(\omega^3), \dots, u_{2w-1} = e(\omega^{2w-1}).$$

Assume that $e(x) = \sum_{j=1}^{w} x^{i_j}$. Then we know

$$u_1 = \sum_{j=1}^{w} \omega^{i_j}, \dots, u_{2w-1} = \sum_{j=1}^{w} \omega^{(2w-1)i_j}.$$

Let $X_j = \omega^{i_j}$. Then we know

$$u_1 = \sum_{j=1}^{w} X_j, \dots, u_{2w-1} = \sum_{j=1}^{w} X_{i_j}^{2w-1}.$$

Define $\ell(x) := \prod_{j=1}^{w}(1 - X_j x)$ and assume that $\ell(x) = \sum_{i=0}^{w} \sigma_i x^i$. Thus we know

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ u_2 & u_1 & 1 & 0 & 0 & 0 & \dots & 0 \\ u_4 & u_3 & u_2 & u_1 & 1 & 0 & \dots & 0 \\ \vdots & & & \ddots & & & & 0 \\ u_{2w-2} & u_{2w-3} & & & & & \dots & u_{w-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_w \end{bmatrix} = \begin{bmatrix} u_1 \\ u_3 \\ \vdots \\ u_{2w-1} \end{bmatrix}$$

To get $e(\omega^{2j})$, note that $e(\omega^{2j}) = (e(\omega^j))^2$ over $\mathbb{F}_2$.

6.4 Reed-Solomon code

For $B_q(n, \omega, b, \delta)$, let $n = q - 1$. Then we call this code *Reed-Solomon code (RS code).* Then we know the zeros of $x^n - 1$ is $\mathbb{F}_q^*$, and $\mathbb{F}_q^* = \langle \omega \rangle$. Then,

$$g(x) = (x - \omega) \dots (x - \omega^{\delta-1}),$$

meaning that $\deg(g) = \delta - 1$, $\dim(B_q(q - 1, 1, \omega, \delta)) = n - (\delta - 1) = q - \delta$.

To encode the message $a_0, \dots, a_{k-1}$, let $a(x) = \sum_{i=0}^{k-1} a_i x^i$. Then we know the codeword is $c(x) = a(x)g(x)$.

6.4.1 Original definition of RS code

For the sake of convenience, we introduce a simpler but equivalent definition for RS code. We focus on $B_q(n = q - 1, b = 0, \omega, d)$. For a message $a_0, \dots, a_{k-1} \in \mathbb{F}_q$, let $a(x) = \sum_{i=0}^{k-1} a_i x^i$. Then we let the codeword to be

$$c(x) := \sum_{j=0}^{n-1} a(\omega^j) x^j.$$

Consider the parity-check matrix

$$H = \begin{bmatrix} 1 & \omega^0 & \dots & \omega^0 \\ 1 & \omega & \dots & \omega^{n-1} \\ \vdots & & \ddots & \vdots \\ 1 & \omega^{d-2} & \dots & \omega^{(d-2)(n-1)} \end{bmatrix}.$$

We need to show $c(\omega^0) = c(\omega) = \ldots = c(\omega^{d-2}) = 0$. For convenience, we set $a(x) = \sum_{i=0}^{n-1} a_i x^i$ where $a_i = 0$ for $i \geq k$.

Lemma 6.7. *For $p(x) = p_0 + p_1 x + \ldots + p_{n-1} x^{n-1} \in \mathbb{F}_q[x]$ and ω is the primitive n-th root of unity. Then*

$$p_i = \frac{1}{n} \sum_{j=0}^{m-1} p(\omega^j) \omega^{-ij}.$$

Proof. By direct calculation, for every p_i,

$$\begin{aligned}
\frac{1}{n} \sum_{j=0}^{m-1} p(\omega^j) \omega^{-ij} &= \frac{1}{n} \sum_{j=0}^{n-1} \left(\sum_{k=0}^{n-1} p_k \omega^{jk} \right) \omega^{-ij} \\
&= \frac{1}{n} \sum_{k=0}^{n-1} p_k \sum_{j=0}^{n-1} \omega^{j(k-i)} \\
&= \frac{1}{n} p_i \sum_{j=0}^{n-1} \omega^0 + \frac{1}{n} \sum_{k \neq i} p_k \sum_{j=0}^{n-1} \omega^{j(k-i)} \\
&= p_i + \frac{1}{n} \sum_{k \neq i} p_k \frac{\omega^{n(k-i)} - 1}{\omega^{k-i} - 1} = p_i.
\end{aligned}$$

□

By Lemma 6.7, we know

$$\begin{aligned}
a_i &= \frac{1}{n} \sum_{j=0}^{n-1} a(\omega^j) \omega^{-ij} \\
&= \frac{1}{n} c(\omega^{-i})
\end{aligned}$$

meaning that $c(\omega^j) = n a_{n-j} = 0$, for all $0 \leq j \leq d - 2 = n - k$. For the decoding, we directly use $a_i = \frac{1}{n} c(\omega^{n-i})$.

7 Collection of All Homeworks

The followings are all homework of this course.

APPLIED ALGEBRAIC — HOMEWORK 1

ZHIDAN LI

Problem 1. *Prove that every Euclidean domain is a principal integral domain.*

Proof. Let $(R, +, \cdot)$ be a Euclidean domain with zero 0 and Euclidean function v. For all ideal I of R, we will show I is a principal ideal. Without loss of generality we assume $I \neq \{0\}$. Assume that $a \in I \setminus \{0\}$ with the smallest value, *i.e.*, $v(a)$ is the smallest in I.

For every $b \in I$, since R is an Euclidean domain, it holds that there exists $q, r \in R$ such that

$$b = qa + r, \quad r = 0 \vee v(r) < v(a).$$

When $r \neq 0$, it holds that $r = b - qa$. Since I is an ideal, it holds that $qa \in I$, which means $b - qa \in I$, or equivalently $r \in I$. However, since $v(r) < v(a)$ and $v(a)$ is the smallest in I, this leads to a contradiction. Thus $r = 0$. Then $b = qa$ for all $b \in I$. This means I is the principal ideal generated by a. Then we know $(R, +, \cdot)$ is a principal integral domain. □

Problem 2. *Prove that every principal integral domain is a unique factorization domain.*

Proof. For a principal integral domain $(R, +, \cdot)$, we prove it is an UFD by the following steps:

(1) Every element $a \in R \setminus \{0\}$ (not unit) can be expressed as $a = p_1 \dots p_n$ where p_i is irreducible for all $i \in [n]$.
(2) Every irreducible element in R is prime.
(3) $a = p_1 \dots p_n$ is "unique" (the definition in UFD).

We prove them step by step.

Proof of (1) To prove (1), assume that there exists an element $a \in R \setminus \{0\}$ such that a is not a unit and cannot be decomposed as product of finite irreducible elements. Then a is reducible, which means there exists $a_1, b_1 \in R$ such that $a = a_1 b_1$, and neither a_1 nor b_1 are unit. Since a cannot be decomposed as product of finite irreducible elements, either a_1 or b_1 cannot be a product of finite irreducible elements (otherwise, a can be decomposed). Without loss of generality, let a_1 be such an element. Since $a_1 \mid a$, it holds that $(a) \subset (a_1)$. Do the similar thing for a_1 and so on. Then we obtain $a_0 = a, a_1, a_2, \dots$ such that

$$(a_0) \subset (a_1) \subset (a_2) \subset \dots$$

Consider $I := \bigcup_{n \geq 0} (a_n)$, and we can show that, for all $b \in R$, $c \in I$, there exists some $m \geq 0$ such that $c \in (a_m)$ and $bc, cb \in (a_m) \subseteq I$, which means I is an ideal of R. Since R is a PID, we know $I = (a)$. Additionally, since $a \in I = \bigcup_{n \geq 0} (a_n)$, there exists $n \in \mathbb{N}_{\geq 0}$ such that $a \in (a_n)$. This show for every $j \geq n$, $(a_j) = (a)$, which leads to a contradiction. Then we know every element a can be decomposed as a product of finite irreducible elements.

Proof of (2) To show every irreducible element $p \in R$ is prime, it suffices to show that, in PID, a non-zero ideal is maximal if and only if it is prime. When I is a maximal ideal, suppose that I is not prime. Then there exists $a, b \in R \setminus I$ such that $ab = ba \in I$. Consider the minimal ideal I' containing $I \cup \{a\}$. Clearly $I \subset I'$, which means $I' = R$. On the other hand,

$$I' := \{x + ar \mid x \in I, r \in R\}.$$

This means $1 = x_1 + ar_1$ for some $x_1 \in I$ and $r_1 \in R$. Then

$$b = b1 = bx_1 + bar_1 \in I$$

which leads to a contradiction. Then we show I is prime.

When $I = (p)$ is prime, we need to show

$$(p) \subseteq (m) \subseteq R \implies (m) = (p) \vee (m) = R.$$

Since $(p) \subseteq (m)$, it holds that $m \mid p$. This means $p = mu$ for some $u \in R$. Since p is prime, p is irreducible. This means m or u is unit. Then $(m) = R$ or $(m) = R$.

Since for irreducible element $a \in R$, (a) is maximal, we know that (a) is prime. Then we know a is prime.

Proof of (3) For $a \in R$, assume that

$$a = p_1 \dots p_n = q_1 \dots q_m$$

where $p_1, \dots, p_n$ and $q_1, \dots, q_m$ are irreducible. Now we show there exists q_j such that $p_1 \mid q_j$. Since

$$p \mid q_1(q_2 \dots q_m)$$

and p is prime, it holds that

$$p \mid q_1 \vee p \mid q_2 \dots q_m.$$

By induction we know there exists q_j such that $p_1 \mid q_j$. Without loss of generality assume that $j = 1$ (reordering if necessary). Since they are both irreducible, we know $p_1 \sim q_1$. Since R is an integral domain, we know there exists some unit u

$$p_2 \dots p_n = uq_2 \dots q_m.$$

Continuing this process, we can match $p_i \sim q_i$ for any i (reordering if necessary) and $n = m$. Then we show this decomposition is unique.

Combining all above, we know R is an UFD. □

Problem 3. *Given an integral domain $(R, +, \cdot)$, construct a field of quotients of R. Prove that it is the smallest field containing R.*

Proof. Firstly we construct the quotient field of R. We define the collection of elements as

$$E := \{(a, b) \mid a, b \in R, b \neq 0\}.$$

Additionally, for $(a, b), (c, d) \in E$, we say (a, b) is equivalent to (c, d) if and only if $ad = bc$, denoted by $(a, b) \sim (c, d)$. It's not hard to show that, if $(a, b) \sim (c, d)$, $(c, d) \sim (e, f)$, then $(a, b) \sim (e, f)$. Then we define F as

$$F := \left\{\overline{(a, b)} \,\middle|\, (a, b) \in E\right\}$$

where we use $\overline{(a, b)}$ to denote the equivalent class of (a, b) in E.

Now we define the operators $+$ and $\cdot$ in F. For $\overline{(a, b)}, \overline{(c, d)} \in F$, we define

$$\overline{(a, b)} + \overline{(c, d)} := \overline{(ad + bc, bd)}.$$
$$\overline{(a, b)} \cdot \overline{(c, d)} := \overline{(ac, bd)}$$

Since R is an integral domain and $b, d \neq 0$, it holds that $bd \neq 0$. Then we know $+$ and $\cdot$ are closed in F. Now we prove $(F, +, \cdot)$ is a field.

- $(F, +)$ is an abelian group.
  - **Associativity:** For all $\overline{(a, b)}, \overline{(c, d)}, \overline{(e, f)} \in F$, it holds that

    $$\left(\overline{(a, b)} + \overline{(c, d)}\right) + \overline{(e, f)} = \overline{(ad + bc, bd)} + \overline{(e, f)} = \overline{(adf + bcf + bde, bdf)},$$
    $$\overline{(a, b)} + \left(\overline{(c, d)} + \overline{(e, f)}\right) = \overline{(a, b)} + \overline{(cf + de, df)} = \overline{(adf + bcf + bde, bdf)}.$$

    Then we know $\left(\overline{(a, b)} + \overline{(c, d)}\right) + \overline{(e, f)} = \overline{(a, b)} + \left(\overline{(c, d)} + \overline{(e, f)}\right)$.
  - **Identity:** Consider the element $\overline{(0, 1)}$. Then for all $\overline{(a, b)} \in F$, it holds that

    $$\overline{(a, b)} + \overline{(0, 1)} = \overline{(0, 1)} + \overline{(a, b)} = \overline{(a, b)}.$$
  - **Inverse:** For $\overline{(a, b)} \in F$, it holds that

    $$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b \cdot b)} = \overline{(0, 1)}.$$

- **Commutative:** For $\overline{(a,b)}, \overline{(c,d)} \in F$, by elementary calculation, since R is an integral domain,

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc, bd)} = \overline{(c,d)} + \overline{(a,b)}.$$

- $\left(F \setminus \left\{\overline{(0,1)}\right\}, \cdot\right)$ is an abelian group.
  - **Associativity:** For all $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in F \setminus \left\{\overline{(0,1)}\right\}$, by the fact R is an integral domain,

$$\left(\overline{(a,b)} \cdot \overline{(c,d)}\right) \cdot \overline{(e,f)} = \overline{(ac,bd)} \cdot \overline{(e,f)} = \overline{(ace,bdf)},$$
$$\overline{(a,b)} \cdot \left(\overline{(c,d)} \cdot \overline{(e,f)}\right) = \overline{(a,b)} \cdot \overline{(ce,df)} = \overline{(ace,bdf)}.$$

    Then we know $\left(\overline{(a,b)} \cdot \overline{(c,d)}\right) \cdot \overline{(e,f)} = \overline{(a,b)} \cdot \left(\overline{(c,d)} \cdot \overline{(e,f)}\right)$.
  - **Identity:** Consider the element $\overline{(1,1)}$. It holds that for all $(a,b) \in F \setminus \left\{\overline{(0,1)}\right\}$,

$$\overline{(1,1)} \cdot \overline{(a,b)} = \overline{(a,b)} \cdot \overline{(1,1)} = \overline{(a,b)}.$$

  - **Inverse:** For all $\overline{(a,b)} \in F \setminus \left\{\overline{(0,1)}\right\}$, since $\overline{(a,b)} \neq \overline{(0,1)}$, it holds that $a \neq 0$. Then we show that

$$\overline{(a,b)} \cdot \overline{(b,a)} = \overline{(b,a)} \cdot \overline{(a,b)} = \overline{(ab,ab)} = \overline{(1,1)}.$$

  - **Commutative:** For all $\overline{(a,b)}, \overline{(c,d)} \in F \setminus \left\{\overline{(0,1)}\right\}$, since R is an integral domain, it holds that $ac = ca$, $bd = db$. Then,

$$\overline{(a,b)} \cdot \overline{(c,d)} = \overline{(ac,bd)} = \overline{(ca,db)} = \overline{(c,d)} \cdot \overline{(a,b)}.$$

- **Distributivity:** For all $\overline{(a,b)}, \overline{(c,d)}, \overline{(e,f)} \in F$, by elementary calculation,

$$\left(\overline{(a,b)} + \overline{(c,d)}\right) \cdot \overline{(e,f)} = \overline{(ad+bc,bd)} \cdot \overline{(e,f)} = \overline{(ade+bce,bdf)},$$
$$\overline{(a,b)} \cdot \overline{(e,f)} + \overline{(c,d)} \cdot \overline{(e,f)} = \overline{(ae,bf)} + \overline{(ce,df)} = \overline{(adef+bcef, bdf \cdot f)}.$$

  Since $(ade+bce)bdf \cdot f = (adef+bcef) \cdot bdf$, it holds that

$$\left(\overline{(a,b)} + \overline{(c,d)}\right) \cdot \overline{(e,f)} = \overline{(a,b)} \cdot \overline{(e,f)} + \overline{(c,d)}.$$

  Similarly we can show that

$$\overline{(a,b)} \cdot \left(\overline{(c,d)} + \overline{(e,f)}\right) = \overline{(a,b)} \cdot \overline{(cf+de,df)} = \overline{(acf+ade,bdf)},$$
$$\overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)} = \overline{(ac,bd)} + \overline{(ae,bf)} = \overline{(abcf+abde, b \cdot bdf)} = \overline{(acf+ade,bdf)}.$$

  Then we know

$$\overline{(a,b)} \cdot \left(\overline{(c,d)} + \overline{(e,f)}\right) = \overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)}.$$

Combining all above, we show $(F,+,\cdot)$ is a field. Now we need to show R is a sub-integral domain of F. In fact, consider the mapping $\xi : R \to F$, $a \mapsto \overline{(a,1)}$. For $a,b \in R$, if $\xi(a) = \xi(b)$, it holds that $\overline{(a,1)} = \overline{(b,1)}$, then $(a,1) \sim (b,1)$, which means $a = b$. So ξ is injective. And by definition, $\xi(a) + \xi(b) = \overline{(a+b,1)} = \xi(a+b)$ and $\xi(a)\xi(b) = \overline{(ab,1)} = \xi(ab)$. Thus ξ is a ring isomorphism. Then we know F contains R.

Now we show every field E containing R must be an extension of F. Consider the mapping $\varphi : F \to E$, $\overline{(a,b)} \mapsto ab^{-1}$. It holds that $\varphi(\overline{(a,b)}) \cdot \varphi(\overline{(c,d)}) = (ac) \cdot (bd)^{-1} = \varphi(\overline{(ac,bd)})$ and $\varphi(\overline{(a,b)}) + \varphi(\overline{(c,d)}) = (ab^{-1} + cd^{-1}) = (adb^{-1}d^{-1} + bcb^{-1}d^{-1}) = (ad+bc)(bd)^{-1} = \varphi(\overline{(ad+bc,bd)})$. For $\overline{(a,b)}, \overline{(c,d)} \in F$, if $\varphi(\overline{(a,b)}) = \varphi(\overline{(c,d)})$, since R is an integral domain, it holds that

$$ab^{-1} = cd^{-1} \implies ad = bc$$

which means $(a,b) \sim (c,d)$, $\overline{(a,b)} = \overline{(c,d)}$. Then we know φ is injective. Thus we show F is isomorphism to a sub-field of E. Then we conclude that F is the minimal field containing R. □

Problem 4. *Is $2x+2$ irreducible in $\mathbb{Z}[x]$ or $\mathbb{Q}[x]$? Is x^2+1 irreducible in $\mathbb{R}[x]$ or $\mathbb{C}[x]$?*

Proof. For $f(x) := 2x+2$. Consider $\mathbb{Z}[x]$. Assume that $f = pq$ where $p, q \in \mathbb{Z}[x]$. It holds that $1 = \deg(f) = \deg(p) + \deg(q)$. Then it holds that $\deg(p) = 0$ or $\deg(q) = 0$, which means either p or q is unit. Then we know f is irreducible in $\mathbb{Z}[x]$. When we consider $\mathbb{Q}[x]$. The similar reason holds and we can show $f(x)$ is irreducible in $\mathbb{Q}[x]$.

For $f(x) := x^2+1$ in $\mathbb{R}[x]$, assume that $f = pq$ where $p, q \in \mathbb{R}[x]$. Without loss of generality assume that p, q are both monic. Assume that $\deg(p) > 0$ and $\deg(q) > 0$. Since $2 = \deg(f) = \deg(p) + \deg(q)$, it holds that $p = x + c_1$ and $q = x + c_2$ for some $c_1, c_2 \in \mathbb{R}$. Then we know that

$$\begin{cases} c_1 + c_2 = 0 \\ c_1 c_2 = 1 \end{cases}.$$

But there exist no $c_1, c_2 \in \mathbb{R}$ satisfying the above constraints. Then we know there exist no p, q with $\deg(p), \deg(q) > 0$ satisfying $f = pq$, which means either p or q is unit. Then we know $f(x) = x^2+1$ is irreducible.

For x^2+1 in $\mathbb{C}[x]$, it holds that $x^2+1 = (x+i)(x-i)$. Then we know x^2+1 is not irreducible in $\mathbb{C}[x]$. □

Problem 5. *Assume that α is an algebraic element over F. Define*

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

Prove that I_α is an ideal of $F[x]$. Define the minimal polynomial of α over F is the (unique) monic polynomial $p(x) \in I_\alpha$ with the lowest degree satisfying $p(\alpha) = 0$. Prove that $p(x)$ generates I_α.

Proof. Firstly we prove that I_α is an ideal. For every $f(x) \in F[x]$, $g(x) \in I_\alpha$, it holds that

$$(f \cdot g)(\alpha) = f(\alpha)g(\alpha) = 0,$$
$$(g \cdot f)(\alpha) = g(\alpha)f(\alpha) = 0.$$

Then we know $fg, gf \in I_\alpha$, which means I_α is an ideal.

Now we show the minimal polynomial $p(x)$ of α generates I_α. Since $p(\alpha) = 0$, it holds that $p \in I_\alpha$. Since $F[x]$ is an Euclidean domain, it holds that I_α is a principal ideal. Define $I_\alpha = (q)$. Then it holds that

$$p(x) = a(x)q(x) \quad \exists a(x) \in F[x], a(x) \neq 0.$$

This means $\deg(p) \geq \deg(q)$. Since the degree of p is the lowest, we know $\deg(q) \geq \deg(p)$, which means $\deg(a) = 0$. Then we conclude that $a(x)$ is unit in $F[x]$. This shows $p \sim q$. Thus we know p also generates $(q) = I_\alpha$. □

APPLIED ALGEBRAIC — HOMEWORK 2

ZHIDAN LI

Problem 1. Prove that $f(x) = x^2 + x + 2$ is irreducible on $\mathbb{Q}[x]$.

Proof. To show $f(x)$ is irreducible on $\mathbb{Q}$, it suffices to show f is irreducible on $\mathbb{Z}$. Note that $f(x+3) = x^2 + 7x + 14$. By Eisenstein's Criterion (with choice $p = 7$), $f(x+3)$ is irreducible on $\mathbb{Z}$, meaning that $f(x)$ is irreducible on $\mathbb{Z}$. Then we show f is irreducible on $\mathbb{Q}$. □

Problem 2. Let $F < E$. For $u \in E$ with odd $\deg(\min(F, u))$, prove that $F(u) = F(u^2)$.

Proof. It is not hard to see $F(u^2) \subseteq F(u)$. Now it suffices to prove $[F(u) : F(u^2)] = 1$. Let $f(x) = x^2 - u^2$. Since $f(u) = 0$, we know that $[F(u) : F(u^2)] \leq 2$. If $[F(u) : F(u^2)] = 2$, by the tower property, we know $[F(u) : F] = [F(u) : F(u^2)] \cdot [F(u^2) : F]$. Then we have $[F(u) : F]$ is even. However, since $\deg(\min(F, u))$ is odd, we can see $[F(u) : F] = \deg(\min(F, u))$ is odd, leading to a contradiction. Then we know $[F(u) : F(u^2)]$ must be 1, which means $F(u) = F(u^2)$. □

Problem 3.
a) Find all automorphisms of $\mathbb{Q}$.
b) Is there an isomorphism $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ over $\mathbb{Q}$ for which $\sigma(\sqrt{2}) = \sqrt{3}$?
c) Is there an isomorphism $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ other than identity?

Solution.
a) For an automorphism $\sigma : \mathbb{Q} \to \mathbb{Q}$, firstly, since σ is a ring homomorphism, we know $\sigma(0) = 0$ and $\sigma(1) = 1$. Then for all $m \in \mathbb{Z}$, it holds that

$$\sigma(m) = \sigma(m \cdot 1) = m\sigma(1) = m.$$

Then, for all $m/n \in \mathbb{Q}$, we have

$$\sigma(m) = \sigma(n \cdot m/n) = \sigma(n)\sigma(m/n).$$

Thus we have $\sigma(m/n) = m/n$. This means $\sigma : \mathbb{Q} \to \mathbb{Q}$ must be identity.

b) Suppose that σ is an isomorphism. Then we have $\sigma(0) = 0$. Consider $f(x) = x^2 - 2$. Since σ is an isomorphism, we know

$$f(\sigma(\sqrt{2})) = \sigma(f(\sqrt{2})) = \sigma(0) = 0.$$

However, $f(\sqrt{3}) = 3 - 2 = 1 \neq 0$. Then we conclude σ cannot be an isomorphism.

c) Let $p(x) = \min(\mathbb{Q}, \sqrt{2})$. It is not hard to see $p(x) = x^2 - 2$. The roots of $p(x)$ are $\pm\sqrt{2}$. Then, for an isomorphism $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, it holds that $\sigma(\sqrt{2}) = \sqrt{2}$ or $\sigma(\sqrt{2}) = -\sqrt{2}$. When $\sigma(\sqrt{2}) = \sqrt{2}$, by a), for all $\frac{a}{b} + \frac{m}{n}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have $\sigma\left(\frac{a}{b} + \frac{m}{n}\sqrt{2}\right) = \frac{a}{b} + \frac{m}{n}\sqrt{2}$, meaning that σ is identity. When $\sigma(\sqrt{2}) = -\sqrt{2}$, by a), for all $\frac{a}{b} + \frac{m}{n}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, we have $\sigma\left(\frac{a}{b} + \frac{m}{n}\sqrt{2}\right) = \frac{a}{b} - \frac{m}{n}\sqrt{2}$. Then, for all $x + y\sqrt{2}, \alpha + \beta\sqrt{2} \in \mathbb{Q}$, we have

$$\begin{aligned}
\sigma((x + y\sqrt{2}) + (\alpha + \beta\sqrt{2})) &= (x + \alpha) - (y + \beta)\sqrt{2} \\
&= \sigma(x + y\sqrt{2}) + \sigma(\alpha + \beta\sqrt{2}), \\
\sigma((x + y\sqrt{2})(\alpha + \beta\sqrt{2})) &= (x\alpha + 2y\beta) - (x\beta + y\alpha)\sqrt{2} \\
&= (x - y\sqrt{2})(\alpha - \beta\sqrt{2}) \\
&= \sigma(x + y\sqrt{2})\sigma(\alpha + \beta\sqrt{2}).
\end{aligned}$$

Thus we know σ is an isomorphism.

□

Problem 4. Prove that if $F < E$ is algebraic and has only finite intermediate fields, then $F < E$ is a finite extension.

Proof. Suppose that $F < K$ is not a finite extension. Then there exists a infinite sequence such that

$$F \subsetneq F(\alpha_1) \subsetneq F(\alpha_1, \alpha_2) \subsetneq \dots$$

and $F(\alpha_1, \dots, \alpha_n) \subsetneq K$ for all $n \in \mathbb{N}$. This leads to a contradiction with the statement $F < E$ only has finite intermediate fields. Then we conclude $K = F(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in K$ and all α_i are algebraic. Then we know

$$[K : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F] < \infty.$$

Thus we know $F < K$ is finite. □

Problem 5. Let $F = \mathbb{F}_2$ and $K = F(\alpha)$, where α is a root of $1+x+x^2$. Show that the function $\sigma : K \longrightarrow K$ given by $\sigma(a + b\alpha) = a + b + b\alpha$ for $a, b \in F$ is an F-automorphism of K.

Proof. Firstly we show σ is an automorphism. Since $K = F(\alpha)$ and α is algebraic over F (α is the root of $x^2 + x + 1$), it holds that

$$K = \{a + b\alpha \mid a, b \in F\}.$$

By definition, for $a = 1, b = 0$, we have $\sigma(1) = 1$. And for $a = b = 0$ we have $\sigma(0) = 0$. For $a + b\alpha, x + y\alpha \in K$, it holds that

$$\begin{aligned}
\sigma((a + b\alpha) + (x + y\alpha)) &= \sigma((a + x) + (b + y)\alpha) \\
&= (a + x) + (b + y) + (b + y)\alpha \\
&= (a + b + b\alpha) + (x + y + y\alpha) \\
&= \sigma(a + b\alpha) + \sigma(x + y\alpha), \\
\sigma((a + b\alpha)(x + y\alpha)) &= \sigma(ax + (ay + bx)\alpha + yb\alpha^2) \\
&= \sigma(ax + (ay + bx)\alpha + yb(-1 - \alpha)) \\
&= \sigma((ax + by) + (ay + bx + by)\alpha) \\
&= (ax + by) + (ay + bx + by) + (ay + bx + by)\alpha, \\
\sigma(a + b\alpha)\sigma(x + y\alpha) &= (a + b + b\alpha)(x + y + y\alpha) \\
&= ax + ay + ay\alpha + bx + by + by\alpha + bx\alpha + by\alpha + by\alpha^2 \\
&= (ax + by) + (ay + bx + by) + (ay + bx + by)\alpha + by(1 + \alpha + \alpha^2) \\
&= (ax + by) + (ay + bx + by) + (ay + bx + by)\alpha \\
&= \sigma((a + b\alpha)(x + y\alpha)).
\end{aligned}$$

Then we can show σ is an automorphism. For $b = 0$, we know $\sigma(a) = a$ for all $a \in F$. Then we conclude σ is an F-automorphism of K. □

Applied Algebraic — Homework 3

Zhidan Li

November 23, 2023

Problem 1. Prove that every finite separable extension is a simple extension. Find $a \in \mathbb{R}$ such that $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}) = \mathbb{Q}(a)$.

Proof. Firstly we prove the following more general lemma.

Lemma 1. *A finite field extension* E/F *is simple if and only if there exists only finitely many intermediate fields* L *with* $F < L < E$.

Proof. When E/F is a finite extension, we need to show there exists only finitely many intermediate fields. Assume that $E = F(\alpha)$. Let $p = \min(F, \alpha)$. If L is an intermediate field, then let $f = \min(L, \alpha)$. And let L' is the field generated by the coefficients of $f(x)$. Then we know, $\min(L', \alpha) = f(x)$ and $L' \subseteq L$. Since $K \subseteq L$, we know $f \mid p$. Then we know:

$$[E : L] = \deg(f) = [E : L'].$$

So that $L = L'$. This means, every intermediate field corresponds a factor of $\min(F, \alpha)$. Since $\min(F, \alpha)$ only has finite factors, we know there exists only finitely many intermediate subfields.

Now suppose conversely that there exists only finitely many subfields. When F is finite, E is finite and we have simply already known $E = F(\alpha)$ for some α. Suppose that F is infinite (and therefore E). Since $[E : F] < \infty$, assume that $E = F(\alpha_1, \ldots, \alpha_n)$. It suffices to show for the case $n = 2$ we can find α such that $F(\alpha) = F(\alpha_1, \alpha_2)$ and apply the hypothesis induction for the general case.

When $K = F(\alpha_1, \alpha_2)$, for every element $\{\alpha_1 + \beta\alpha_2\}$ for every $\beta \in F\backslash\{0\}$. By our assumption, this set is infinite but has only finitely many intermediate subfields. So there must be two values $\alpha_1 + \zeta\alpha_2, \alpha_1 + \chi\alpha_2$ generating a same intermediate subfield $L = F(\alpha_1 + \zeta\alpha_2) = F(\alpha_1 + \chi\alpha_2)$. L contains

$$\frac{(\alpha_1 + \zeta\alpha_2) - (\alpha_1 + \chi\alpha_2)}{\zeta - \chi} = \alpha_2$$

and

$$\frac{(\alpha_1 + \zeta\alpha_2)/\zeta - (\alpha_1 + \chi\alpha_2)/\chi}{1/\zeta - 1/\chi} = \alpha_1$$

meaning that $L = K$. Set $\alpha = \alpha_1 + \zeta\alpha_2$, and we know

$$F(\alpha) = L = K.$$

□

Suppose K/F is a finite separable extension. Then $K = F(\alpha_1, \dots, \alpha_n)$ for distinct α_i. Now we define E as the splitting field of $\{\min(F, \alpha_i) : \forall i \in [n]\}$ over F. Since K is a separable extension of F, we know $\min(F, \alpha_i)$ is separable over F for each $i \in [n]$. Then E is a finite Galois extension of F. Moreover, since all $\alpha_i \in E$, we know $F < K < E$. By the fundamental theorem of Galois theory, the intermediate subfields of E/F are in bijection with the subgroups of $\mathrm{Gal}(E/F)$. Since $\mathrm{Gal}(E/F)$ is finite, we know $|\{H < \mathrm{Gal}(E/F)\}| < \infty$ and $F < K < E$, there exists finitely many intermediate subfields of K/F. By Lemma 1, K/F is simple.

By the proof of Lemma 1, we set $a = \sqrt{3} + \sqrt{5} + \sqrt{7}$. It is obvious that $\mathbb{Q}(\sqrt{3} + \sqrt{5} + \sqrt{7}) \subseteq \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7})$. To show $\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{3} + \sqrt{5} + \sqrt{7})$, we compute $[\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}) : Q]$ and $[\mathbb{Q}(\sqrt{3} + \sqrt{5} + \sqrt{7}) : \mathbb{Q}]$.

$$[\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{5}, \sqrt{7})][\mathbb{Q}(\sqrt{5}, \sqrt{7}) : \mathbb{Q}(\sqrt{7})][\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2 \times 2 \times 2 = 8.$$

On the other hand, to compute $\min(\mathbb{Q}, \sqrt{3} + \sqrt{5} + \sqrt{7})$, it suffices to show

$$f(x) := \prod_{c_1, c_2, c_3 \in \{-1, +1\}} (x + c_1\sqrt{3} + c_2\sqrt{5} + c_3\sqrt{7}) \in \mathbb{Q}[x]$$

and we know all roots of $f(x)$ lies in $\mathbb{Q}(a)$, thus we obtain $\min(\mathbb{Q}, a) = f(x)$. And by direct calculation it can be shown that $f(x) = x^8 - 60x^6 + 782x^4 - 3180x^2 + 3481 \in \mathbb{Q}[x]$. Then we show $[\mathbb{Q}(a) : \mathbb{Q}] = 8 = [\mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7}) : \mathbb{Q}]$. Then we know $\mathbb{Q}(a) = \mathbb{Q}(\sqrt{3}, \sqrt{5}, \sqrt{7})$. □

Problem 2. Prove that $\sqrt{5}, \sqrt{7} \in \mathbb{Q}(\sqrt{5} + \sqrt{7})$.

Proof. For the sake of simplicity we let $a = \sqrt{5} + \sqrt{7}$. It holds that

$$\sqrt{7} - \sqrt{5} = \frac{2}{\sqrt{7} + \sqrt{5}} = \frac{2}{a}.$$

Then we know $\sqrt{5} = \frac{1}{2}(a - \frac{2}{a}) = \frac{a^2-2}{2a} \in \mathbb{Q}(a)$, $\sqrt{7} = \frac{1}{2}(a + \frac{2}{a}) = \frac{a^2+2}{2a} \in \mathbb{Q}(a)$. □

Problem 3. Prove that any extension of degree 2 is normal.

Proof. Let K be an extension of F of degree 2. For every $\alpha \in K \setminus F$, let $L = F(\alpha)$. Then we know $F < L < K$. Then it holds that

$$[K : F] = [K : L] \cdot [L : F].$$

If $[L : F] = 1$. In this case we know $F(\alpha) = F$, meaning that $\alpha \in F$. Then we know $[F(\alpha) : F] = 2$ and $K = F(\alpha)$. It holds that $\deg(\min(F, \alpha)) = 2$. That is to say, in K, we know $f(x) = (x - \alpha)g(x)$ and $\deg(g) = 1$. Since $f(x) \in F[x] \subseteq K[x]$, we know $g(x) \in K[x]$. That is to say $f(x) = (x - \alpha)(x - \beta)$ where $\alpha, \beta \in K$. Then we know f splits over K. Thus we conclude K/F is normal. □

Problem 4. Prove that $\mathbb{Q}(\sqrt[3]{5}, \omega)$ is a Galois extension of $\mathbb{Q}$ where $\omega = e^{2\pi i/3}$. Show the Galois group of this extension, all subgroups and their corresponding intermediate fields.

Proof. Now we show $\mathbb{Q}(\sqrt[3]{5}, \omega)$ is the splitting field of $S = \{x^3 - 1, x^3 - 5\}$ over $\mathbb{Q}$. Let X be the collection of all roots of $f \in S$. Then

$$X = \left\{1, \omega, \omega^2, \sqrt[3]{5}, \sqrt[3]{5}\omega, \sqrt[3]{5}\omega^2\right\}.$$

Then it is not hard to see $\mathbb{Q}(\sqrt[3]{5}, \omega) \subseteq \mathbb{Q}(X)$. On the other hand, we know $X \subseteq \mathbb{Q}(\sqrt[3]{5}, \omega)$, thus $\mathbb{Q}(X) \subseteq \mathbb{Q}(\sqrt[3]{5}, \omega)$. Then $\mathbb{Q}(\sqrt[3]{5}, \omega) = \mathbb{Q}(X)$. Equivalently speaking, $\mathbb{Q}(\sqrt[3]{5}, \omega)$ is the splitting field of S. Trivially all $f \in S$ are separable. Then we know $\mathbb{Q}(\sqrt[3]{5}, \omega)/\mathbb{Q}$ is Galois.

Let $G = \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{5}, \omega)/\mathbb{Q})$. By the fundamental theorem of Galois theory, we know $|G| = [\mathbb{Q}(\sqrt[3]{5}, \omega) : \mathbb{Q}] = 6$. Then we know G is made up of

$$\begin{aligned}
\mathrm{id} &: \sqrt[3]{5} \mapsto \sqrt[3]{5}, \omega \mapsto \omega, \\
\sigma &: \sqrt[3]{5} \mapsto \omega\sqrt[3]{5}, \omega \mapsto \omega, \\
\tau &: \sqrt[3]{5} \mapsto \sqrt[3]{5}, \omega \mapsto \omega^2, \\
\rho &: \sqrt[3]{5} \mapsto \omega\sqrt[3]{5}, \omega \mapsto \omega^2, \\
\mu &: \sqrt[3]{5} \mapsto \omega^2\sqrt[3]{5}, \omega \mapsto \omega, \\
\xi &: \sqrt[3]{5} \mapsto \omega^2\sqrt[3]{5}, \omega \mapsto \omega^2.
\end{aligned}$$

All subgroups of G and their corresponding intermediate fields are

$$\begin{aligned}
\langle \mathrm{id} \rangle &\mapsto \mathbb{Q}(\sqrt[3]{5}, \omega), \\
\langle \sigma \rangle = \{\mathrm{id}, \sigma, \mu\} &\mapsto \mathbb{Q}(\omega), \\
\langle \tau \rangle = \{\mathrm{id}, \tau\} &\mapsto \mathbb{Q}(\sqrt[3]{5}), \\
\langle \rho \rangle = \{\mathrm{id}, \rho\} &\mapsto \mathbb{Q}(\omega^2\sqrt[3]{5}), \\
\langle \xi \rangle = \{\mathrm{id}, \xi\} &\mapsto \mathbb{Q}(\omega\sqrt[3]{5}), \\
G &\mapsto \mathbb{Q}.
\end{aligned}$$

□

Applied Algebraic — Homework 4

Zhidan Li

November 24, 2023

Problem 1: Determine the number of subfields of $\mathbb{F}_{1024}$ and $\mathbb{F}_{729}$.

Proof. It holds that $\mathbb{F}_{1024} = \mathbb{F}_{2^{10}}$. Then for every $L = \mathbb{F}_{2^k}$ such that $L < \mathbb{F}_{1024} = \mathbb{F}_{2^{10}}$, L should satisfy

$$k \mid 10.$$

Then we can pick $k = 1, 2, 5, 10$, meaning that the subfields of $\mathbb{F}_{1024}$ are $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_{32}, \mathbb{F}_{1024}$.

It's not hard to see $\mathbb{F}_{729} = \mathbb{F}_{3^6}$. For every $L = \mathbb{F}_{3^k}$ such that $L < \mathbb{F}_{729} = \mathbb{F}_{3^6}$, L should satisfy

$$k \mid 6.$$

Then we can pick $k = 1, 2, 3, 6$, meaning that the subfields of $\mathbb{F}_{729}$ are $\mathbb{F}_3, \mathbb{F}_9, \mathbb{F}_{27}$ and $\mathbb{F}_{729}$. □

Problem 2: Find the order of the following irreducible polynomial: $x^4 + x + 1$ over $\mathbb{F}_2$.

Solution. Assume that the order of $x^4 + x + 1$ is v. Thus we know

$$v \mid q^d - 1 = 15.$$

Let $v = 3^a 5^b$. Then a is the smallest number such that

$$p(x) = x^4 + x + 1 \mid x^{3^a 5} - 1.$$

and b is the smallest number such that

$$p(x) = x^4 + x + 1 \mid x^{3 \cdot 5^b} - 1.$$

For $a = 0$, we know $p(x) \nmid x^5 - 1$. Then a must be 1. For $b = 0$, we know $p(x) \nmid x^3 - 1$ and b must be 1. Then we know $v = 15$. □

Problem 3: Construct two distinct field tables for $\mathbb{F}_8$ over $\mathbb{F}_2$.

Solution. Since $[\mathbb{F}_8 : \mathbb{F}_2] = 3$, the all polynomials over $\mathbb{F}_2$ of degree < 3 are

Constant	$0, 1;$
Linear	$x, x + 1;$
Square	$x^2, x^2 + 1, x^2 + x, x^2 + x + 1.$

By the hint, we know the polynomial $p(x) = x^3 + x + 1$ and $q(x) = x^3 + x^2 + 1$ are two irreducible polynomials.

- For $p(x) = x^3 + x + 1$, suppose that α is the root of p, *i.e.*, $\alpha^3 = \alpha + 1$. Then we calculate the field table as

k	$a_2a_1a_0$
0	001
1	010
2	100
3	011
4	110
5	111
6	101

- For $q(x) = x^3 + x^2 + 1$, suppose that β is the root of q, *i.e.*, $\beta^3 = \beta^2 + 1$. Then we calculate the field table as

k	$a_2a_1a_0$
0	001
1	010
2	100
3	101
4	111
5	011
6	110

□

Problem 4: Factor

$$f(x) = x^5 + x^4 + x^3 + x^2 + 1$$

over $\mathbb{Z}_2$.

Solution. We employ Berlekamp's algorithm. Firstly we get

$$\begin{aligned}
r_0(x) &= 1, \\
r_1(x) &= x^2, \\
r_2(x) &= x^4, \\
r_3(x) &= x^2 + x + 1, \\
r_4(x) &= x^4 + x^3 + x^2.
\end{aligned}$$

Then we know the matrix $M - I$ is

$$M - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Then we need to solve

$$\begin{cases} g_3 = 0 \\ g_1 + g_3 = 0 \\ g_1 + g_2 + g_3 + g_4 = 0 \\ g_3 + g_4 = 0 \\ g_2 = 0 \end{cases}$$

Then the solution is

$$g_0 \text{ is arbitrary}; g_1 = g_2 = g_3 = g_4 = 0.$$

Thus we know $g(x) = 0$ or $g(x) = 1$, meaning that f is irreducible over $\mathbb{Z}_2$. □

Problem 5: Calculate $N_q(20)$.

Solution. By Möbius inversion, it holds that

$$\begin{aligned} N_q(20) &= \frac{1}{20} \sum_{d \mid 20} q^d \mu\left(\frac{20}{d}\right) \\ &= \frac{1}{20}\left(q\mu(20) + q^2\mu(10) + q^4\mu(5) + q^5\mu(4) + q^{10}\mu(2) + q^{20}\mu(1)\right) \\ &= \frac{1}{20}\left(q^{20} - q^{10} - q^4 + q^2\right). \end{aligned}$$

□

Applied Algebraic — Homework 5

Zhidan Li

December 9, 2023

Problem 1: Assume $K = \mathbb{Q}(\omega_p)$ where ω_p is the p-th primitive root of unity, and p is a prime number. Prove that

1. $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$ (and then the order of this Galois group is $p-1$).
2. For every $d \mid p-1$, there exists a subfield $M \subseteq K$ such that $[M : \mathbb{Q}] = d$.

Proof.

1. Since we have already known $\mathrm{Gal}(K/\mathbb{Q}) \cong S$ for some $S \subseteq (\mathbb{Z}/p\mathbb{Z})^*$, to prove $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*$, it suffices to show $|\mathrm{Gal}(K/\mathbb{Q})| = \phi(p)$, equivalently $Q_p(x)$ is irreducible. Since p is a prime, we know that

$$Q_p(x) = x^{p-1} + \ldots + 1.$$

Consider the polynomial $Q_p(x+1)$. By the binomial theorem,

$$Q_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=0}^{p-1} \binom{p}{i+1} x^i.$$

Since $p \mid p = \binom{p}{1} = a_0$, $p^2 \nmid a_0$, $p \nmid \binom{p}{p} = a_{p-1}$, by Eisenstein's criterion, $Q_p(x+1)$ is irreducible, which means $Q_p(x)$ is irreducible.

2. By the fundamental theorem of Galois theory, it suffices to find a subgroup S of $\mathrm{Gal}(K/\mathbb{Q})$ such that $[\mathrm{Gal}(K/\mathbb{Q}) : S] = \frac{p-1}{d}$. Since $\mathrm{Gal}(K/\mathbb{Q})$ is a cyclic group with order $p-1$, we only need to find such a subgroup S with order d. Assume that $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma \rangle$. Consider $S = \left\langle \sigma^{\frac{p-1}{d}} \right\rangle$. Then we know

$$|S| = \mathrm{order}(\sigma^{(p-1)/d}) = d.$$

On the other hand, $[\mathrm{Gal}(K/\mathbb{Q}) : S] = |\mathrm{Gal}(K/\mathbb{Q})|/|S| = (p-1)/d$. Thus we can find $M = \mathcal{F}(\mathrm{Gal}(K/S))$ such that $[M : \mathbb{Q}] = d$.

$\square$

Problem 2: Factorize $x^{10} - 1$ over $\mathbb{F}_3$.

Solution. It holds that

$$\begin{aligned} x^{10} - 1 &= Q_1(x)Q_2(x)Q_5(x)Q_{10}(x) \\ &= (x-1)(x+1)(x^4 + x^3 + x^2 + x + 1)(x^4 + 2x^3 + x^2 + 2x + 1) \\ &= (x+1)(x+2)(x^4 + x^3 + x^2 + x + 1)(x^4 + 2x^3 + x^2 + 2x + 1). \end{aligned}$$

$\square$

Problem 3: Assume that the parity-check matrix is

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Decode the following words:

$$R = [1110000],$$
$$R = [1111000].$$

Solution. When $R = [1110000]$, its syndrome over $\mathbb{F}_2$ is

$$S = HR^\top = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Then we know $C = R$.

When $R = [1111000]$, its syndrome over $\mathbb{F}_2$ is

$$S = HR^\top = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Then we can find $E = [1000000]$. Thus we know $C = R + E = [0111000]$. □

Problem 4: Please state the BCH code and its method for correction over $\mathbb{F}_2$ with $n = 15$, $r = 8$.
Requirements: Firstly give the Hamming parity-check matrix H for $r = 4$. And then you can express each column of this matrix in $\mathbb{F}_{16}$. Extend H to correcting two errors, and describe the decode process.

Solution. Firstly we consider the Hamming parity-check matrix H_1 with $r = 4$, $n = 15$. Then we know

$$H_1 = \begin{bmatrix} 000000011111111 \\ 000111100001111 \\ 011001100110011 \\ 101010101010101 \end{bmatrix}.$$

Assume that $\mathbb{F}_{16} = \{0, \beta_1, \dots, \beta_{15}\}$. Then we can express H_2 as

$$H_1 = \begin{bmatrix} \beta_1 & \dots & \beta_{15} \end{bmatrix}.$$

For a permutation $f : \mathbb{F}_{16}^* \to \mathbb{F}_{16}^*$, we consider the parity-check matrix

$$H = \begin{bmatrix} \beta_1 & \dots & \beta_{15} \\ f(\beta_1) & \dots & f(\beta_{15}) \end{bmatrix} = \begin{bmatrix} H_1 \\ H_2 \end{bmatrix}.$$

Let $f(\beta) = \beta^3$. When receiving a code R, we compute

$$S_1 = H_1 R^\top = \sum \beta_i E_i,\ S_2 = H_2 R^\top = \sum \beta_i^3 E_i.$$

- $S_1 = 0$. Then there exists no error. We decode $C = R$.
- $S_1 \neq 0$, $S_2 = S_1^3$, we know that there exists exactly one error. Then we find E with least 1 such that $H_1 E^\top = S_1$ and decode $C = R + E$.

- $S_1 \neq 0$ and $S_2 \neq S_1^3$. We solve the equation

$$x^2 - S_1 x + \frac{S_2}{S_1} - S_1^2 = 0.$$

If we find two solution $x_1, x_2 \in \mathbb{F}_{16}^*$, we flip the values at position x_1 and x_2 in R as C. Otherwise we report the failure of decoding process.

□