Study Notes of Abtract Algebra

Pei Zhong

Update on January 4, 2024

Contents

Preface

The notes mainly refer to the following materials:

- Abstract Algebra by Sun Zhiwei
- lecture notes from berkeley
- algebra II notes from mit
- algebra I notes from mit
- lecture notes by feog
- lecture notes from estu
- lecture notes from queen mary
- lecture summary from queen mary
- THEORY OF FIELD EXTENSIONS
- Galois Theory notes from Edinburgh

Chapter 1

Preliminary Knowledge

1.1 Congruence and Congruence Classes

Definition 1.1

An equivalence relation ”$\sim$” on a set S is a rule such that
(1) $a \sim a, \forall a \in S$
(2) $a \sim b \Rightarrow b \sim a$
(3) $a \sim b$ and $b \sim c \Rightarrow a \sim c$.

You should think of an equivalence relation as a generalization of the notion of equality. Indeed, the usual notion of equality among the set of integers is an example of an equivalence relation. The next definition yields another example of an equivalence relation.

Definition 1.2

Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then a is congruent to b modulo n, denoted by,

$$a \equiv b \pmod{n}$$

if n divides $a - b$.

Example 1.1

$17 \equiv 5 \pmod{6}$.

$(17 - 5) = 2 \cdot 6$.

The following theorem tells us that the notion of congruence defined above is an equivalence relation on the set of integers.

Theorem 1.1

Let n be a positive integer. For all $a, b, c \in \mathbb{Z}$
(1) $a \equiv a \pmod{n}$
(2) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
(3) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Theorem 1.2

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
(1) $a + c \equiv b + d \pmod{n}$
(2) $ac \equiv bd \pmod{n}$.

Proof. By the definition of congruence, there are $s, t \in \mathbb{Z}$ such that

$$a - b = sn, c - d = tn.$$

(1) $a + c - (b + d) = sn - tn = (s - t)n$. Hence, $a + c \equiv b + d \pmod{n}$.
(2) Using the fact that $-bc + bc = 0$, we have

$$\begin{aligned} ac - bd &= ac + 0 - bd \\ &= ac + (-bc + bc) - bd \\ &= c(a - b) + b(c - d) \\ &= c(sn) + b(tn) \\ &= n(cs + bt). \end{aligned}$$

Hence, $ac \equiv bd \pmod{n}$. □

Definition 1.3

Let a and n be integers with $n > 0$. The congruence class of a modulo n, denoted $\overline{a}_n$, is the set of all integers that are congruent to a modulo n, i.e.

$$\overline{a}_n = \{z \in \mathbb{Z} : a - z = kn \text{ for some } k \in \mathbb{Z}\}.$$

Example 1.2

In congruence modulo 2 , we have

$$\begin{aligned} \overline{0}_2 &= \{0, \pm 2, \pm 4, \ldots\} \\ \overline{1}_2 &= \{\pm 1, \pm 3, \pm 5, \ldots\}. \end{aligned}$$

Theorem 1.3

$a \equiv c \pmod{n}$ iff $\overline{a}_n = \overline{c}_n$.

Proof. (⇒): Assume $a \equiv c \pmod{n}$. Let $b \in \overline{a}_n$, then by definition1.3, $b \equiv a \pmod{n}$. Then

$$\begin{aligned} & a \equiv b \pmod{n} \text{ and } a \equiv c \pmod{n} \\ & \Rightarrow b \equiv c \pmod{n} \\ & \Rightarrow c \equiv b \pmod{n}. \end{aligned}$$

So, $b \in \overline{c}_n$. Thus, $\overline{a}_n \subseteq \overline{c}_n$. Reversing the roles of a and c in the argument above we similarly conclude that $\overline{c}_n \subseteq \overline{a}_n$. Hence, $\overline{a}_n = \overline{c}_n$.

(⇐): Suppose $\overline{a} = \overline{c}$. Since $a \equiv a \pmod{n}$, we have $a \in \overline{a}$ and so, by hypothesis $\overline{a} = \overline{c}$, $a \in \overline{c}$. Hence, $a \equiv c \pmod{n}$. □

Corollary 1.1

Two congruence classes modulo n are either disjoint or identical.

Proof. If $\overline{a}_n$ and $\overline{b}_n$ are disjoint there is nothing to prove. Suppose that $\overline{a} \cap \overline{b} \neq \emptyset$. Then there is an integer c such that $c \in \overline{a}_n$ and $c \in \overline{b}_n$. So $c \equiv a \pmod{n}$ and $c \equiv b \pmod{n}$. Then we have $a \equiv b \pmod{n}$. Hence, $\overline{a}_n = \overline{b}_n$ by theorem1.3. □

Corollary 1.2

There are exactly n distinct congruence classes modulo n; namely, $\overline{0}_n, \overline{1}_n, \overline{2}_n, \ldots, \overline{n-1}_n$.

Proof. We first show that $\overline{0}_n, \overline{1}_n, \overline{2}_n, \ldots, \overline{n-1}_n$ are all distinct. it is sufficient to show that no two of $0, 1, 2, \ldots, n-1$ are congruent modulo n. To see this, suppose that $0 \leqslant s < t < n$. Then $t - s$ is a positive integer and $t - s < n$. Thus, $n \nmid (t - s)$ and so t is not congruent to s modulo n. Then by theorem1.3, the classes $\overline{0}_n, \overline{1}_n, \overline{2}_n, \ldots, \overline{n-1}_n$ are all distinct.

To complete the proof we need to show that every congruence class is one of these classes. Let $a \in \mathbb{Z}$, by the division algorithm,

$$a = nq + r, q \in \mathbb{Z}, 0 \leqslant r < n. \tag{1.1}$$

The condition on r implies $r \in \{0, 1, 2, \ldots, n-1\}$. If we write (1.1) as

$$a - r = nq,$$

it is clear that $a \equiv r \pmod{n}$. Thus, by theorem1.3, $\overline{a} = \overline{r}$ for some $r \in \{0, 1, 2, \ldots, n-1\}$. □

Definition 1.4

The set of all congruence classes modulo n is denoted $\mathbb{Z}_n$. Thus

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Proposition 1.1

$\forall \overline{a}, \overline{b} \in \mathbb{Z}_n, \overline{a} + \overline{b} = \overline{a+b}, \overline{a} \cdot \overline{b} = \overline{ab}.$

1.2 Chinese Remainder Theorem

The Chinese remainder theorem arises from the following congruence equations:

$$\begin{cases} x & \equiv a_1 \pmod{m_1} \\ \dots\dots & \\ x & \equiv a_n \pmod{m_n}, \end{cases}$$

where, $m_1, \ldots, m_n \in \mathbb{N}$ are pairwise coprime and $a_1, \ldots, a_n \in \mathbb{Z}$.

How to get the solution of these eqations? Let's think about it from the view of algebra. Let us concentrate on the case of $n = 3$. The case of $n \neq 3$ is similar. If we can find a map from $\mathbb{Z}_{abc} \to \mathbb{Z}_a \times \mathbb{Z}_b \times Z_c$ is bijective, and then if we can find the inverse of this map, we can get the solution of these equations by the inverse mapping.

Theorem 1.4

Let a, b, c be pairwise relatively prime positive integers. Then the map f

$$\mathbb{Z}_{abc} \to \mathbb{Z}_a \times \mathbb{Z}_b \times \mathbb{Z}_c.$$

defined by the rule $\overline{x}_{abc} \mapsto (\overline{x}_a, \overline{x}_b, \overline{x}_c)$ is a bijection. The inverse of f is given by the formula

$$f^{-1}(\overline{x}_a, \overline{y}_b, \overline{z}_c) = \overline{xe_1 + ye_2 + ze_3}_{abc}$$

where e_1, e_2

1.3 Phi Function

1.4 Reference

- leture notes from okstate
- Residue Class Rings
- THE CHINESE REMAINDER THEOREM AND THE PHI FUNCTION

Part I

Group Theory

Chapter 2

Semi-Group and Group

Definition 2.1

If G is a nonempty set, then a binary operation on G is a function from $G \times G$ to G. If the binary operation is denoted $\circ$, then we use the notation $a \circ b = c$ if $(a, b) \in G \times G$ is mapped to $c \in G$ under the binary operation.

Remark. We will consider both ”additive” and ”multiplicative” binary operations. The only difference between these operations is notational, really. When considering a binary operation, we denote the image of (a, b) as $a+b$. When using multiplicative notation, we denote the image of (a, b) as ab (called the product of a and b). Throughout the group theory we use multiplicative notation.

Definition 2.2

For a multiplicative binary operation on $G \times G$, we define the following properties:
(1) Multiplication is associative if $a(bc) = (ab)c$ for all $a, b, c \in G$.
(2) Element $e \in G$ is a identity if $ae = ea = a$ for all $a \in G$.
(3) Element $a \in G$ has a inversee b if for some $b \in G$ we have $ab = ba = e$.
A semigroup is a nonempty set G with an associative binary operation.
A monoid is a semigroup with an identity.
A group is a monoid such that each $a \in G$ has an inverse.
In a semigroup, we define the property:
(4) Semigroup G is abelian or commutative if $ab = ba$ for all $a, b \in G$.
The order of a semigroup/monoid/group is the cardinality of set G, denoted $|G|$. If $|G| < \infty$, then the semigroup/monoid/group is said to be finite.

Remark. If we define a binary algebraic structure as a set with a binary operation on it, then we have the following schematic:

$$\text{(Binary Algebraic Structures)} \supseteq \text{(Semigroups)} \supseteq \text{(Monoids)} \supseteq \text{(Groups)}.$$

Proposition 2.1: Generalized Associative Law

Let G be a semigroup. For any $a_1, \ldots, a_n \in G$, the value of $a_1 \cdots a_n$ is independent of how the expression is bracketed.

Proposition 2.2: Generalized Commutative Law

If G is a commutative semigroup and $a_1, a_2, \ldots, a_n \in G$ then for any permutation $i_1, i_2, \ldots, i_n$ of $i = 1, 2, \ldots, n$ we have the products $a_1 a_2 \cdots a_n = a_{i_1} a_{i_2} \cdots a_{i_n}$.

Definition 2.3

Let G be a (multiplicative) semigroup, $a \in G$, and $n \in \mathbb{N}$. The element a^n is defined as the standard n product $a^n = \prod_{i=1}^{n} a_i$ where $a = a_i$ for $1 \leqslant i \leqslant n$. If G is a monoid, a^0 is defined to be the identity element of G, $a^0 = e$. If G is a group, then for each $n \in \mathbb{N}$, a^{-n} is defined to be $a^{-n} = (a^{-1})^n \in G$. If G is an additive group we replace a^n, a^0, a^{-n}, and e with $na, 0a, -na$, and 0, respectively.

Proposition 2.3

If G is a group (respectively, semigroup, monoid) and $a \in G$, then for all $m, n \in \mathbb{Z}$ (respectively, $\mathbb{N}$, $\mathbb{N} \cup \{0\}$): (1) $a^m a^n = a^{m+n}$ (or $ma + na = (m+n)a$ in additive notation);
(2) $(a^m)^n = a^{mn}$(or $n(ma) = (mn)a$ in additive notation).

Proposition 2.4

If G is a monoid, then the identity element e is unique. If G is a group then:
(1) If $c \in G$ and $cc = c$ then $c = e$.
(2) For all $a, b \in G$, if $ab = ac$ then $b = c$, and if $ba = ca$ then $b = c$ (these properties of a group is called left cancellation and right cancellation, respectively).
(3) For $a \in G$, the inverse of a is unique.
(4) For all $a \in G$, we have $(a^{-1})^{-1} = a$.
(5) For all $a, b \in G$, we have $(ab)^{-1} = b^{-1}a^{-1}$.
(6) For all $a, b \in G$, the equations $ax = b$ and $ya = b$ have unique solutions in G, namely $x = a^{-1}b$ and $y = ba^{-1}$, respectively.

Remark. We can weaken the two-sided identity and inverse properties used in Definition 2.2 of group. It turns out that if we simply assume right inverses and a right identity (or just left inverses and a left identity) then this implies the existence of left inverses and a left identity (and conversely), as shown in the following theorem.

Proposition 2.5

Let G be a semigroup. Then G is a group if and only if the following conditions hold.
(1) There exists an element $e \in G$ such that $ea = a$ for all $a \in G$ (called a left identity in G).
(ii) For each $a \in G$, there exists an element $a^{-1} \in G$ such that $a^{-1}a = e$ (a^{-1} is called a left inverse of a).

The following proposition gives another condition by which a semigroup is a group.

Proposition 2.6

(1) Let G be a semigroup. Then G is a group if and only if for all $a, b \in G$ the equations $ax = b$ and $ya = b$ have solutions in G.
(2) Let G be a finite semigroup, if G satisfys cancellation law, then G is a group.

2.1 Reference

- Semigroups, Monoids, and Groups

Chapter 3

Examples of Group

Chapter 4

Subgroup and Coset

4.1 Subgroups

Definition 4.1

Let G be a semigroup and H a nonempty subset of G. If for every $a, b \in H$ we have $ab \in H$ then H is closed under the binary operation of G. Let G be a group and H a nonempty subset of G that is closed under the binary operation of G. If H itself is a group under the binary operation then H is a subgroup of G. This is denote $H \leqslant G$. For group G, the trivial subgroup is $\{e_G\}$. Subgroup $H \leqslant G$ is a proper subgroup if $H \neq G$ and $H \neq \{e_G\}$.

Proposition 4.1

Let H be a nonempty subset of a group G. Then H is a subgroup of G if and only if $ab^{-1} \in H$ for all $a, b \in H$.

Example 4.1

$\mathbb{Q}^* \leqslant \mathbb{R}^* \leqslant \mathbb{C}^*$

Example 4.2

$\mathrm{SL}_n(\mathbb{R}) \leqslant \mathrm{GL}_n(\mathbb{R})$.

Corollary 4.1

If G is a group and $\{H_i : i \in I\}$ is a nonempty set of subgroup of G, then $\cap_{i \in I} H_i$ is a subgroup of G.

Remark. Notice that index set I may not be finite and it may not even be countable!

Definition 4.2

Let G be a group and $X, Y \subseteq G$. X^{-1} is defined as $X^{-1} = \{x^{-1} : x \in X\}$. And XY is defined as $XY = \{xy : x \in X \text{ and } y \in Y\}$.

Proposition 4.2

Let G be a group and $X, Y, Z \subseteq G$, then $(X^{-1})^{-1} = X$ and $(XY)Z = X(YZ)$.

Proposition 4.3

Let G be a group and $H \leqslant G$, then $H^{-1} = H$ and $HH = H$.

Proposition 4.4

Let G is a group and $H, K \leqslant G$, then

$$HK \leqslant G \Leftrightarrow HK = KH.$$

4.2 Cosets

In this section, we generalize the idea of congruence modulo m on $\mathbb{Z}$ (Chapter1) to a more general setting.

Definition 4.3

Let H be a subgroup of group G and $a, b \in G$. a is right congruent to b modulo H, denoted $a \equiv_r b \pmod{H}$, if $ab^{-1} \in H$. a is left congruent to b modulo H, denoted by $a \equiv_l b \pmod{H}$, if $a^{-1}b \in H$.

We use left and right congruent to define left and right cosets.

Theorem 4.1

Let H be a subgroup of a group G.
(1) Right and left congruence modulo H are each equivalence relations on G.
(2) The equivalence class of $a \in G$ under right (and left) congruence modulo H is the set $Ha = \{ha : h \in H\}$ (and $aH = ah : h \in H$ for left congruence).
(3) $|Ha| = |H| = |aH|$ for all $a \in G$.
The set Ha is a right coset of H in G and aH is a left coset of H in G.

Corollary 4.2

Let H be a subgroup of group G.
(1) G is the union of the right (and left) cosets of H in G.
(2) Two right (or two left) cosets of H in G are either disjoint or equal.
(3) For $a, b \in G$, we have $Ha = Hb$ if and only if $ab^{-1} \in H$, and $aH = bH$ if and only if $a^{-1}b \in H$.
(4) If $\mathcal{R}$ is the set of distinct right cosets of H in G and $\mathcal{L}$ is the set of distinct left cosets of H in G, then $|\mathcal{R}| = |\mathcal{L}|$.

Remark. (1)(2) imply that the right (and left) cosets of H in G partition G.

Definition 4.4

Let H be a subgroup of a group G. The index of H in G, denoted $[G : H]$, is the cardinal number of the set of distinct right (or left) cosets of H in G.

Theorem 4.2

Let G be a finite group and $H \leqslant G$, then $|H|$ divides $|G|$ and $|G| = [G : H]|H|$.

Remark. The converse of the Lagrange's Theorem does not hold. For example, the alternating group A_4 of order 12 does not have a subgroup of order 6. So it is natural to ask: ”For a given divisor d of the order of a finite group G, under what conditions does G have a subgroup of order d?” This is partially addressed by The Sylow Theorems (see chapter10).

4.3 Reference

- Subgroup
- Cosets

Chapter 5

Normal Subgroup and Qutient Subgroup

Proposition 5.1

If N is a subgroup of group G, then the following conditions are equivalent.
(1) $aN = Na$ for all $a \in G$.
(2) For all $a \in G$, $n \in N$, $ana^{-1} \in N$.
(3) For all $a \in G$, $aNa^{-1} = N$.

Definition 5.1

A subgroup N of a group G which satisfies the equivalent conditions of proposition 5.1 is said to be normal in G (or a normal subgroup of G), denoted $N \trianglelefteq G$.

Proposition 5.2

Every subgroup of an abelian group is normal.

Proposition 5.3

Any subgroup N of index 2 in group G is a normal subgroup.

Proposition 5.4

The intersection of any collection of normal subgroups of group G is itself a normal subgroup.

Proposition 5.5

Let G be a group and $H \leqslant K \leqslant M$. If $H \trianglelefteq G$, then $H \trianglelefteq K$.

Remark. It may be the case that for group G, we have subgroups of G satisfying $H \trianglelefteq K$ and $K \trianglelefteq G$ but H is not a normal subgroup of G.

The following result is a big one! It says that if N is a normal subgroup of G, then we can form a group out of the cosets of N by defining a binary operation on the cosets using representatives of the cosets. In fact, this can be done only when N is a normal subgroup, the group of cosets is called a ”factor group” or ”quotient group.” Quotient groups are at the backbone of modern algebra!

Theorem 5.1

If N is a normal subgroup of a group G and G/N is the set of all left cosets of N in G, then G/N is a group of order $[G : N]$ under the binary operation given by $(aN)(bN) = (ab)N$.

Remark. By the definition of the binary operation in G/N, we see that the identity element is $eN = N$, and the inverse of aN is $a^{-1}N$.

Definition 5.2

If N is a normal subgroup of G, then the group G/N of theorem5.1 is the quotient group of G by N.

Remark. The relationship between quotient groups and normal subgroups is a little deeper than Theorem 5.1 implies. From Fraleigh, we have: Let H be a subgroup of a group G. Then left coset multiplication is well defined by $(aH)(bH) = (ab)H$ if and only if H is a normal subgroup of G. This result gives the real importance of normal subgroups.

5.1 Reference

- Normality, Quotient Groups

Chapter 6

Group Homomorphism and Isomorphism

Definition 6.1

Let G and H be semigroups. A function $f : G \to H$ is a homomorphism if $f(ab) = f(a)f(b)$ for all $a, b \in G$. A one to one (injective) homomorphism is a monomorphism. An onto (surjective) homomorphism is an epimorphism. A one to one and onto (bijective) homomorphism is an isomorphism. If there is an isomorphism from G to H, we say that G and H are isomorphic, denoted $G \cong H$. A homomorphism $f : G \to G$ is an endomorphism of G. An isomorphism $f : G \to G$ is an automorphism of G.

Proposition 6.1

If $f : G \to H$ and $g : H \to K$ are homomorphisms on semigroups G, H, K, then the composition $g \circ f = gf : G \to K$ is a homomorphism. Similarly, compositions of monomorphisms, epimorphisms, isomorphisms, and automorphisms are respectively monomorphisms, epimorphisms, isomorphisms, and automorphisms.

Proposition 6.2

a group homomorphism maps identities to identities and inverses to inverses.

Definition 6.2

Let $f : G \to H$ be a homomorphism of groups. The kernel of f is $\text{Ker}(f) = \{g \in G : f(g) = e_H \in H\}$. If $A \subset G$, then the image of A is $f(A) = \{h \in H : h = f(a) \text{ for some } a \in A\}$. The set $f(G)$ is called the image of homomorphism f, denoted $\text{Im}(f)$.

Proposition 6.3

Let $f : G \to H$ be a homomorphism of groups. Then:
(1) f is a monomorphism if and only if $\text{Ker}(f) = \{e_G\}$;
(2) f is an isomorphism if and only if there is a homomorphism $f^{-1} : H \to G$ such that $ff^{-1} = 1_H$ and $f^{-1}f = 1_G$.

Theorem 6.1

If $f : G \to H$ is a homomorphism of groups, then the kernel of f is a normal subgroup of G. Conversely, if N is a normal subgroup of G, then the map $\pi : G \to G/N$ given by $\pi(a) = aN$ is an epimorphism (that is, an onto homomorphism) with kernel N.

Definition 6.3

The map $\pi : G \to G/N$ of theorem 6.1 defined as $\pi(a) = aN$ is the canonical epimorphism.

Theorem 6.2

If $f : G \to H$ is a homomorphism of groups, then f induces an isomorphism of $G/\text{Ker}(f)$ with $\text{Im}(f)$.

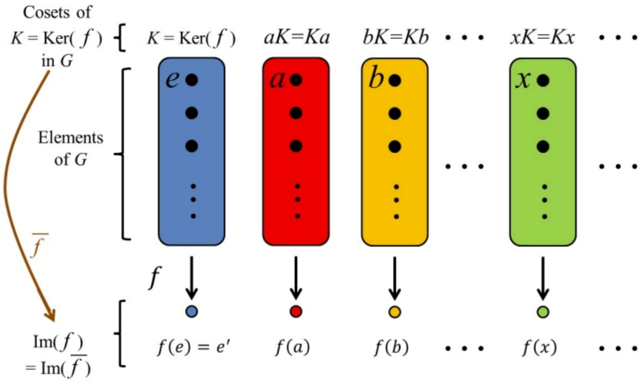

Figure 6.1

6.1 Reference

- Homomorphisms
- Homomorphisms

Chapter 7

Properties and Application of Index

Proposition 7.1

If K, H, G are groups with $K \leqslant H \leqslant G$ and $[G : H]$, $[H : K]$ are finite, then $[G : K] = [G : H][H : K]$.

Chapter 8

Order of Element and Cyclic Group

8.1 Order of element and cyclic group

Definition 8.1

Let G be a group and X a subset of G. Let $\{H_i : i \in I\}$ be the set of all subgroups of G which contain X. Then $\cap_{i\in I} H_i$ is the subgroup of G generated by the set X, denoted $\langle X \rangle$.

Definition 8.2

For group G. the elements of $X \subset G$ are called generators of subgroup $\langle X \rangle$. If $G = \langle a_1, a_2, ..., a_n \rangle$ (notice the set brackets are dropped by convention) then G is finitely generated.

Theorem 8.1

If G is group and X is a nonempty subset of G, then

$$\langle X \rangle = \{x_1^{m_1} x_2^{m_2} \cdots x_k^{m_k} : k \in \mathbb{N}_+, x_1, ..., x_k \in X \text{ and } m_1, ..., m_k \in \mathbb{Z}\}.$$

In particular, for every $a \in G$, $\langle a \rangle = \{a^m : m \in \mathbb{Z}\}$.

Definition 8.3

Let G be a group. Then G is cyclic if $\exists a \in G$ such that $G = \langle a \rangle = \{a^m : m \in \mathbb{Z}\}$.

Definition 8.4

Let G be a group and $a \in G$. The order of a is the least positive integer such that $a^n = e$, denoted $o(a)$. If such positive integer does not exist, $o(a) = \infty$.

Proposition 8.1

$o(a) = |\langle a \rangle|$.

We now explore the properties of elements of finite and infinite order.

Proposition 8.2

Let G be a group and $a \in G$. If a has infinite order then
(1) $a^k = e$ if and only if $k = 0$.
(2) the elements a^k are all distinct as the values of k range over $\mathbb{Z}$.
If a has finite order $m > 0$ then
(3) $a^k = e$ if and only if $m|k$.
(4) $a^r = a^s$ if and only if $r \equiv s \pmod{m}$.
(5) $\langle a \rangle$ consists of the distinct elements $a, a^2, \ldots, a^{m-1}, a^m = e$.
(6) for each $k \in \mathbb{Z}$, $o(a^k) = \frac{m}{(m,k)}$, where $(m,k) = \text{gcd}(m,k)$.

Proposition 8.3

Let $G = \langle a \rangle$ be a cyclic group. If G is infinite, then a and a^{-1} are the only generators of G. If G is finite of order m, then a^k is a generator of G if and only if $(k, m) = 1$ (i.e. k and m are coprime).

Proposition 8.4

The subgroup of cyclic group is cyclic.

Proposition 8.5

Subgroup of infinite cyclic group is infinite cyclic group.

Proposition 8.6

A finite cyclic group of order n contains a subgroup of order m for each positive integer m which divides n.

Proposition 8.7

Every infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ and every finite cyclic group of order m is isomorphic to the additive group $\mathbb{Z}_m$.

Proposition 8.8

If a group G has order p^n where p is a prime, then G has a element of order p.

Corollary 8.1

A group of order p where p is a prime number is cyclic.

8.2 Application

Proposition 8.9

Let G be a group of order n, then for $a \in G$, $a^n = e$.

Definition 8.5

Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n. It is written using $\varphi(n)$.

Proposition 8.10

For $m \in \mathbb{N}_+$, $U_m := \{\bar{a} = a + m\mathbb{Z} : a \in \mathbb{Z} \text{ and } \gcd(a, m) = 1\}$, then U_m is a commutative semigroup with respect to multiplication and $|U_m| = \varphi(m)$. If U_m is finite, then U_m is a abelian group.

Theorem 8.2

If m is a positive integer and a is an integer such that $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

8.3 Reference

- cyclic group
- cyclic group

Chapter 9

Group Action

Definition 9.1

An action of a group G on a set S is a function mapping $G \times S \to S$ (denoted $(g, x) \mapsto g \circ x$) such that for all $x \in S$ and $g_1, g_2 \in G$, we have

$$e \circ x = x \text{ and } (g_1 g_2) \circ x = g_1 \circ (g_2 \circ x).$$

When this occurs, we say that G acts on set S.

- Group Action

Chapter 10

Sylow Theorem

Theorem 10.1: Cauchy Theorem

If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.

Chapter 11

The Direct Product of Group

Definition 11.1

Let $(G, \circ)$ and $(H, \diamond)$ be groups. Put

$$G \times H = \{(g, h) : g \in G, h \in H\}$$

with the operation $(g_1, h_1) \times (g_2, h_2) = (g_1 \circ g_2, h_1 \diamond h_2)$. Then $G \times H$ is a group, with identity $(1_G, 1_H)$ and $(g, h)^{-1} = (g^{-1}, h^{-1})$. It is called the outer direct product of G and H.

Similarly, there is a general case.

Definition 11.2

Let $G_1, ..., G_n$ be groups. Put

$$G = G_1 \times ... \times G_n = \{(x_1, ..., x_n) : x_i \in G_i\}$$

with the operation $(x_1, ..., x_n) \times (y_1, ..., y_n) = (x_1 y_1, ..., x_n y_n)$. Then G is a group, with identity $e = (e_1, ..., e_n)$ and $(x_1, ..., x_n)^{-1} = (x_1^{-1}, ..., x_n^{-1})$. It is called the outer direct product of $G_1, ..., G_n$.

Let's review the product of subgroups:

Proposition 11.1

Let $(G, \cdot)$ be a group and $X, Y \leqslant G$, then

$$XY = x \cdot y : x \in X, y \in Y.$$

If $X < Y \trianglelefteq G$, then XY is a normal subgroup of G.

Theorem 11.1

Put

$$G^* = \{(g, 1_H) : g \in G\}.H^* \qquad = \{(1_G, h) : h \in H\}$$

and define $\sigma_1 : G \times H \to H$ by $\sigma_1(g, h) = h$. Then
(1) σ_1 is a homomorphism, $\operatorname{Im}\sigma_1 = H$ and $\operatorname{Ker}\sigma_1 = G^*$
(2) $G^* \trianglelefteq G \times H$ and $(G \times H)/G^* \cong H$.
Similarly, define $\sigma_2 : G \times H \to G$ by $\sigma_2(g, h) = g$. Then
(3) σ_2 is a homomorphism, $\operatorname{Im}\sigma_2 = G$ and $\operatorname{Ker}\sigma_2 = H^*$
(4) $H^* \trianglelefteq G \times H$ and $(G \times H)/H^* \cong G$.
And more,
(5) $G \cong G^*$ and $H \cong H^*$
(6) $G^*H^* = G \times H$
(7) $G^* \cap H^* = \{(1_G, 1_H)\}$.

Similarly, there is general case.

Theorem 11.2

$G = G_1 \times ... \times G_n$. Put

$$G_i^* = \{(x_1, ..., x_n) \in G : x_i \in G_i \text{ and } x_j = e_j, \forall j \neq i\}$$

and define $\sigma_i : G \to G_i$ by $\sigma_i(x_1, ..., x_n) = x_i$. Then
(1) σ_i is a homomorphism, $\operatorname{Im}\sigma_i = G_i$ and $\operatorname{Ker}\sigma_i = G_i^*$
(2) $G_i^* \trianglelefteq G$.
And more,
(3) $\forall i, G_i \cong G_i^*$
(4) $G_1^* \cdots G_n^* = G$
(5) $\forall i, G_i^* \cap \prod_{j\neq i} G_j^* = \{e\}$.

Proposition 11.2

Let $N_1, ..., N_m$ be normal groups of G, then the following statements are equivalent:
(1) $\forall i = 1, ..., n$, $N_i \cap \prod_{j\neq i} N_j = \{e\}$.
(2) $x_i, y_i \in N_i, i = 1, ..., m$. Then $x_1 \cdots x_m = y_1 \cdots y_m$ iff $x_i = y_i, \forall i$.
(3) $e = x_1 \cdots x_m(x_i \in N_i)$, then $x_1 = x_2 = ... = x_m = \{e\}$.

If $N_1, ..., N_m$ are subgroups of G and $\forall x \in G, \exists! x_i \in N_i$, s.t. $x = x_1 \cdots x_m$, then G is called the inner direct product of $N_1, ..., N_m$. If $N_1, ..., N_m$ are normal, by proposition11.2, we can get a concise proposition.

Proposition 11.3

If $N_1, \ldots, N_m$ are normal subgroups of G, G is called the inner direct produt of $N_1, .., N_m$ if
(1) $N_1 \cdots N_m = G$, and
(2) $\forall i, N_i \cap \prod_{j \neq i} N_j = \{e\}$

Proposition 11.4

Let $G_1, \ldots, G_n$ be groups. Then $G = G_1 \times \ldots \times G_n$ is the inner direct sum of $G_1^*, \ldots, G_n^*$.

Theorem 11.3

Let G be a group and let $N_1, \ldots, N_m$ be normal subgroups of G. If G is the inner direct sum of $N_1, \ldots, N_m$, then $G \cong N_1 \times \ldots \times N_m$.

Example 11.1

Let p be a prime

Haven't done!

11.1 Reference

- lecture notes from queen mary
- lecture notes from uou

Chapter 12

Exercise About Group

Exercise 12.1

Let G be a group and for all $a \in G$, $a^2 = e$, then G is Abelian group.

Exercise 12.2

$H, K \leqslant G$, then $HK = G$ iff $\forall x, y \in G$, $xH \cap yK \neq \emptyset$.

Exercise 12.3

For $x \in G$, $C_G(x) = \{g \in G : gx = xg\}$, then $C_G(x) \leqslant G$.

Exercise 12.4

Let G be a finite group. There exist $x \in G$ such that $o(x) = 2$ iff $|G|$ is even.

Proof. ($\Rightarrow$): By Largrange theorem, $2 = o(x) | |G|$.
($\Leftarrow$): Suppose there is not such element $x \in G$, then for $a \in G$, $aa \neq e$, then $a^{-1} \neq a$. Define $S = \{a \in G : a \neq e\}$ and $U = \cup_{a \in G}\{a, a^{-1}\}$. Then $|S| = |G| - 1 = 2n - 1$ and $|U| = 2s$, but $|S| = |U|$, contradiction. □

Part II

Ring Theory

Chapter 13

The Concept and Basic Properties of Rings

Definition 13.1

A ring is a set R endowed with addition and multiplication, usually denote " $+$ " and " $\cdot$ ", satisfying (1)-(3) :
(1) R is an abelian group with respect to addition : addition is associative and commutative, there is an additive identity 0_R such that $0_R + a = a + 0_R = a$ for all $a \in R$, and every element has an additive inverse.
(2) R is an semigroup with respect to multiplication : Multiplication is associative.
(3) Addition and multiplication satisfy distributivity: for all $a, b, c \in R$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c, \ (b + c) \cdot a = b \cdot a + c \cdot a.$$

Most often we will also impose some additional conditions on our rings, as follows:

(4) There exists an element, denoted 1, which has the property that $a \cdot 1 = 1 \cdot a = a$ for all a in R, 1 is called the unity of R.
A ring satisfying (4) is called a ring with unity (or sometimes a unital ring).

(5) multiplication is commutative : $a \cdot b = b \cdot a$ for all $a, b \in R$.
A ring satisfying (5) is called a commutative ring.

Remark. We always denote $a \cdot b$ by ab.

Remark. As usual we use exponents to denote compounded multiplication; associativity guarantees that the usual rules for exponents apply. However, with rings (as opposed to multiplicative groups), we must use a little caution, since a^k may not make sense for $k < 0$, as a is not guaranteed to have a multiplicative inverse.

Definition 13.2

Let R be a ring. The additive identity in R is called the zero in R.

Proposition 13.1

For any element a in a ring R, one has $a0 = 0 = 0a$ (zero is an absorbing element with respect to multiplication).

Proposition 13.2

For elements $a_1, ..., a_m, b_1, ..., b_n$, one has

$$(a_1 + ... + a_m)(b_1 + ... + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j .$$

Definition 13.3

For any element a in a ring R and $n \in \mathbb{N}$.

$$na := \underbrace{a + ... + a}_{n \text{ elements}},$$

$$(-n)a = n(-a) := \underbrace{-a - ... - a}_{n \text{ elements}}.$$

Proposition 13.3

For a, b in a ring R and $m \in \mathbb{Z}$, one has

$$(ma)b = a(mb) = m(ab).$$

Definition 13.4

Let a, b be in a ring R. If $a \neq 0$ and $b \neq 0$ but $ab = 0$, then we say that a and b are zero divisors. A commutative ring with unity but without zero divisors is called integral domain.

A natural question: under what conditions, the ring has no zero divisors. THe answer in the next proposition.

Proposition 13.4

Let R be a ring, then R have no zero divisors iff R satisfy cancellation law:

$$\text{if } a, b, c \in R \text{ and } a \neq 0, \text{ then } ab = ac \text{ implies } b = c \text{ and } ba = ca \text{ implies } b = c.$$

Proof. ($\Leftarrow$): Suppose R satisfys cancellation law. Assume R has zero divisors i.e. there exists $a, b \in R \setminus \{0\}$ such that $ab = 0$. Since $a0 = 0 = ab$, we have $b = 0$ by the cancellation law. This is a contradiction as $b \neq 0$. Hence, R has no zero divisors and so is a integer domain. ($\Rightarrow$): Suppose R is a integral domain. Then for $a, b, c \in R$ and $a \neq 0$, we have

$$ab = ac \Rightarrow a(b - c) = ab - ac = 0 \Rightarrow b - c = 0 \Rightarrow b = c.$$

Similarly, $ba = ca \Rightarrow (b-c)a = 0 \Rightarrow b = c$. □

Theorem 13.1

Let R be a commutative ring, then for any $a, b \in R$ and $n \in \mathbb{N}$, one has

$$(a+b)^n = a^n + \sum_{0<k<n} \frac{n!}{k!(n-k)!} a^k b^{n-k} + b^n.$$

There are many familiar examples of rings:

Example 13.1: The ring of integers

$\mathbb{Z}$: the integers ..., $-2, -1, 0, 1, 2$, ..., with usual addition and multiplication, form a ring.

Example 13.2: The ring of residue classes modulo n

$\mathbb{Z}/m\mathbb{Z}$: The integers mod m. These are equivalence classes of the integers under the equivalence relation "congruence mod m". If we just think about addition, this is exactly the cyclic group of order m. However, when we call it a ring, it means we are also using the operation of multiplication.

$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mZ \to \mathbb{Z}/mZ$ is given by $\overline{a} + \overline{b} = \overline{a+b}$. $\cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mZ \to \mathbb{Z}/mZ$ is given by $\overline{a}\overline{b} = \overline{ab}$.

Example 13.3: The ring of integer polynomials

$\mathbb{Z}[x]$: this is the set of polynomials whose coefficients are integers. It is an "extension" of $\mathbb{Z}$ in the sense that we allow all the integers, plus an "extra symbol" x, which we are allowed to multiply and add, giving rise to x^2, x^3, etc., as well as $2x, 3x$, etc. Adding up various combinations of these gives all the possible integer polynomials.

Example 13.4: The ring of matrices

$M_n(\mathbb{R})$ (non-commutative): the set of $n \times n$ matrices with entries in $\mathbb{R}$. These form a ring, since we can add, subtract, and multiply square matrices. This is the first example we've seen where the order of multiplication matters: AB is not always equal to BA (usually it's not).

Remark. Similar with example13.3 and example13.4, for ring R, we can define $R[x]$ as the set of polynomials whose coefficients are in the field of R and $M_n(R)$ the set of $n \times n$ matrices with entries in the field of R. Since, $R[x]$ an "extension" of R, they have many similar properties:

- If R is unital ring, then $R[x]$ is unital ring.
- If R is commutative ring, then $R[x]$ is commutative ring.
- If R is integer domain, then $R[x]$ is integer domain.

However, there are many difference between R and $M_n(R)$.

- If R is unital ring, then $M_n(R)$ is unital ring.

- If R is a commutative ring, $M_n(R)$ may be not a commutative ring.
- If R is an integer domain, $M_n(R)$ may be not an integer domain.

Definition 13.5

If R is a ring, and S is a non-empty subset of R, we will say that S is a subring of R if
(1) S is a subgroup of R under $+$. (closed under addition and subtraction)
(2) S is closed under multiplication.

Remark. The minimum subring in R is zero ring $O = \{0\}$, the maximum subring in R is R, which is similar to the minimum subgroup e in group G and the maximum subgroup G in G.

Example 13.5

$\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ is a ring with respect to the addition and multiplication in $\mathbb{C}$, which is called Gaussian integers. Integer ring is a subring of Gaussian integers.

Definition 13.6

Let a be an element of a unital R. We say that a is a unit if a has a multiplicative inverse, i.e. if there exists an element b in R such that $ab = ba = 1_R$. b is denoted by a^{-1}. The set of units in R is a group with respect to multiplication, which is called the unit group of R and denoted by $U(R)$.

Remark. R must have unity.
Remark. If u, v are units in R, then uv is a unit in R as $(uv)(v^{-1}u^{-1}) = 1_R$.

Example 13.6

$U(\mathbb{Z}) = \{1, -1\}$.

$1 \cdot 1 = 1, (-1) \cdot (-1) = 1$

Example 13.7

$U(\mathbb{Z}/mZ) = \{\overline{a} = a + m\mathbb{Z} : a \in \mathbb{Z}, gcd(a, m) = 1\}$

$\overline{a}\overline{b} = \overline{ab} = 1 \Leftrightarrow ab \equiv 1 \pmod{m} \Leftrightarrow ab + my = 1 \Leftrightarrow \gcd(a, m) = 1$.
We also can prove that $U(\mathbb{Z}/mZ)$ (some textbooks denote it by U_m or $\mathbb{Z}_m^*$) is a group with multiplication.

Proposition 13.5

Let R be a ring, then $R = \{0\}$ iff $0_R = 1_R$.

Proof. ($\Rightarrow$): $0 \cdot 0 = 0 \cdot 0 = 0$, then $1_R = 0_R$.
($\Leftarrow$): If $0_R = 1_R$, then $\forall a \in R$, $a = a \cdot 1_R = a \cdot 0_R = 0$. Hence, $R = \{0\}$. □

By proposition13.5, we know that zero is not equal to identity for a general ring. Hence, zero always has no inverse. So if every non-zero element in a ring has inverse, we can get more.

Definition 13.7

Let R be a unital ring. R is called skew field if $U(R) = R \setminus \{0\}$.

Definition 13.8

Let R be a skew field. R is called a field if $R \setminus \{0\}$ is abelian group with respect ro multiplication.

Proposition 13.6

Let R be a field, then R is a integer domain.

Proof. Suppose R is not a integer domain, i.e. there exists $0 \neq a, b \in R, ab = 0$. But

$$ab = 0 \Rightarrow a^{-1}ab = 0 \Rightarrow b = 0.$$

This is a contradiction as $b \neq 0$. Hence, R is a integral domain. □

Example 13.8

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are field.

Example 13.9

Let p be a prime, then $\mathbb{Z}/p\mathbb{Z}$ is a field.

For $a, b, c \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$, $\overline{a} \cdot \overline{b} = \overline{a} \cdot \overline{c} \Rightarrow ab - ac = np \Rightarrow a(b-c) = np \Rightarrow p|a(b-c) \xRightarrow{\text{gcd(a,p)=1}} p|b-c \Rightarrow \overline{b} = \overline{c}$, then $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ satisfys cancellation law. Hence, $\mathbb{Z}/p\mathbb{Z}$ is a group and commutative is clear.

Let us construct the smallest and also most famous example of skew field. Take $1, i, j, k$ to be basis vectors for a 4-dimensional vector space over $\mathbb{R}$, and define multiplication by

$$i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j, ji = -ij, kj = -jk, ik = -ki.$$

Then

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

forms a skew field, called the Hamilton's quaternions. So far, we have only seen the ring structure. Let us now discuss the fact that every nonzero element is invertible. Define the conjugate of an element $h = a + bi + cj + dk \in \mathbb{H}$ to be $\overline{h} = a - bi - cj - dk$(yes, exactly the same way you did it for complex numbers). And define the norm of h to be $|h| = \sqrt{a^2 + b^2 + c^2 + d^2}$. Then

$$\begin{aligned} h\overline{h} = (a + bi + cj + dk)(a - bi - cj - dk) =& a^2 - abi - acj - adk \\ &+ bai - b^2i^2 - bcij - bdik \\ &+ caj - cbji - c^2j^2 + cdjk \\ &+ dak - dbki - dckj - d^2k^2 \\ =& a^2 + b^2 + c^2 + d^2 = |h|^2. \end{aligned}$$

If $h \neq 0$, then $h\overline{h} = \overline{h}h \neq 0$, take h^{-1} to be

$$h^{-1} = \frac{\overline{h}}{h\overline{h}}.$$

Clearly $hh^{-1} = h^{-1}h = 1$. Hence, $U(\mathbb{H}) = \mathbb{H} \setminus \{0\}$. Then $\mathbb{H}$ is a skew field.

13.1 Reference

- lecture notes by feog

Chapter 14

Homomorphism and Ideals

Just as with groups, when we study rings, we are only concerned with functions that "preserve the structure" of a ring, and these are called ring homomorphisms. Maybe you can guess what the definition should be, by analogy with the case of groups.

Definition 14.1

Let R and S be rings, and $\sigma : R \to S$ be a function. We say σ is a ring homomorphism if, for all $a, b \in R$,
(1) $\sigma(a+b) = \sigma(a) + \sigma(b)$,
(2) $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$.

Remark. $\sigma(0) = \sigma(0+0) = \sigma(0) + \sigma(0) \Rightarrow \sigma(0) = 0$.

Just as for groups, bijective homomorphisms are called isomorphisms, and they tell us when two rings ”have the same structure”.

Definition 14.2

An isomorphism from a ring R to another ring S is a bijective homomorphism. If an isomorphism between R and S exists, then we say R and S are isomorphic and we write $R \cong S$.

There is an alternative way to characterize isomorphisms, using inverse functions.

Proposition 14.1

Let $f : R \to S$ be a homomorphism. Then f is an isomorphism iff there exists a homomorphism $g : S \to R$ such that $g \circ f$ is the identity map on R and $f \circ g$ is the identity map on S.

Definition 14.3

Let $\sigma : R \to S$ be a homomorphism of rings. The kernel of σ, denoted $\mathrm{Ker}(\sigma)$, is the subset $\{r \in R : \sigma(r) = 0\}$ of R. In other words, it's the pre-image of 0 under σ. The image of σ is the set $\mathrm{Im}(\sigma) = \{s \in S : s = \sigma(r) \text{ for some } r \in R\}$.

Example 14.1

The kernel of $\sigma : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ sengding a to $\bar{a}$ is $\{km : k \in \mathbb{Z}\}$.

Just as for groups, the kernel and image detect injectivity and surjectivity: to be injective means to have a trivial kernel, so maps with a large kernel can be thought of as "very un-injective".

Proposition 14.2

Let $\sigma : R \to S$ be a homomorphism of rings. Then σ is injective iff $\mathrm{Ker}\sigma = \{0_R\}$; σ is surjective iff $\mathrm{Im}\sigma = S$.

Let's look back at example14.1. What properties does $\mathrm{Ker}\sigma$ have? For $am, bm \in \mathrm{Ker}\sigma$, $am + bm = (a+b)m \in \mathrm{Ker}\sigma$, $-am \in \mathrm{Ker}\sigma$, $am \cdot bm = (abm)m \in \mathrm{Ker}\sigma$. Hence, $\mathrm{Ker}\sigma$ is a subring of $\mathbb{Z}$. But we find more: if we take one integer which is in $\mathrm{Ker}\sigma$, and another one which might not even be in $\mathrm{Ker}\sigma$, and multiply, we still stay in $\mathrm{Ker}\sigma$ as $a \cdot bm = ab \cdot m$. So the kernel is closed even under multiplication when one of the factors need not lie in the kernel. This is stronger than the usual closure under multiplication, and this movtivate the definition of ideals.

Definition 14.4

Let R be a ring. A non-empty subset I of R is called an ideal if it satisfies the following conditions:
(1) I is an additive subgroup of R under $+$. (closed under addition and subtraction)
(2) For any $a \in I$ and $r \in R$, $ra, ar \in I$. (closed under scaling)
If I is an ideal of a ring R, we write $I \trianglelefteq R$.

Remark. $\forall a, b \in I \subset R$, $ab, ba \in I$, then I is a subring of R.

Example 14.2

Every ring has at least one ideal: the subset consisting of only 0. It's an additive subgroup, and closed under scaling because anything times zero is zero.

Example 14.3

In any ring R, the entire ring R is itself ideal, called the "unit ideal" . The reason for this name is: if an ideal I contains 1, then it is equal to the entire ring, because if 1 is in I, then for any $r \in R$, $r = r \cdot 1$ is also in I by closure under scaling. This is the largest ideal in R.

Example 14.4

Let $I_1, I_2, \ldots, I_n$ be ideals of R, then the sum of $I_1, \ldots, I_n$

$$I_1 + \ldots + I_2 := \{a_1 + \ldots + a_n : a_1 \in I_1, \ldots, a_n \in I_n\}$$

is a ideal of R.

$(a_1 + \ldots + a_n) + (b_1 + \ldots + b_n) = (a_1 + b_1) + \ldots + (a_n + b_n) \in I_1 + \ldots + I_n$.
$(a_1 - \ldots - a_n) + (b_1 - \ldots - b_n) = (a_1 - b_1) + \ldots + (a_n - b_n) \in I_1 + \ldots + I_n$.

$(a_1 + ... + a_n) \cdot r = a_1 \cdot r + ... + a_n \cdot r \in I_1 + ... + I_n$

Example 14.5

Let $I_1, I_2, ..., I_n$ be ideals of R, then $\cap_i^n I_i$ is an ideal of R.

$a + b \in I_i, \forall I_i$
$a - b \in I_i, \forall I_i$
$a \cdot r \in I_i, \forall I_i$.

Proposition 14.3

Let R be an unital ring and I be an ideal in R. I contains a unit if and only if $I = R$.

Proof. ($\Rightarrow$): If I has a unit, then $1_R \in I$, then $\forall r \in R, r \cdot 1 = r \in I$ and so $R \subseteq I$. Hence, $R = I$ as $\emptyset \neq I \subseteq R$.
($\Leftarrow$): If $I = R$, then $1_R \in I$ and so I have a unit 1_R. □

Proposition 14.4

Let R be a ring and I is an ideal in R. Then $(I, +)$ is a normal subgroup of $(R, +)$.

Proof. By the definitino of ideals, $\emptyset \neq I \leqslant R$. Since R is abelian group with addition, $(I, +)$ is abelian group and so normal. □

Definition 14.5

Let X be any subset of a ring R. The ideal generated by X is the intersection of all ideals containing X. Hence, this ideal is the smallest ideal containing X, and is denoted $\langle X \rangle$. If X is a finite set, say $X = \{a_1, a_2, ..., a_n\}$, we will write $\langle X \rangle$ as $(a_1, ..., a_n)$. An ideal generated by a single element a is called a principal ideal, denoted by (a).

Remark. Generalizing the example14.5 to infinite, we can know $\cap_i^\infty I_i$ is a ideal. Then the definition is well-defined.

Proposition 14.5

If R is an unital ring and $\emptyset \neq X \subseteq R$. Then

$$\langle X \rangle = \{\sum_{i=1}^{n} r_i x_i s_i : x_i \in X \text{ and } r_i, s_i \in R\}.$$

Proof. hard! □

Proposition 14.6

If R is a commutative ring with unity and $\emptyset \neq X \subseteq R$. Then

$$\langle X\rangle = \{\sum_{i=1}^{n} r_i x_i : x_i \in X \text{ and } r_i \in R\}.$$

Particularly,

$$(a) = \{ra : r \in R\}.$$

If $X = \{a_1, ..., a_n\}$, then

$$(a_1, ..., a_n) = (a_1) + ... + (a_n).$$

Remark. zero ideal can be denoted (0) and unit ideal can be denote (1).

Let I be a ideal of R. Since I is an additive subgroup of R by definition, it makes sense to speak of cosets $r + I$ of I, $r \in R$. Furthermore, a ring has a structure of abelian group of addition, so I satisfies the definition of a normal subgroup. From group theory, we thus know that it makes sense to speak of the quotient group

$$R/I = \{\overline{r} = r + I : r \in R\}.$$

Since R is abelian group , $r \in R$ and $I \subset R$, R/I is an abelian group for addition.

We now endow R/I with a multiplication operation as follows. Define

$$(r + I)(s + I) = rs + I.$$

Let us make sure that this is well-defined, namely that it does not depend on the choice of the repersentative in each coset. Suppose that

$$r + I = r' + I, s + I = s' + I.$$

Then, $a = r' - r \in I$ and $b = s' - s \in I$. Now

$$r's' = (a + r)(b + s) = ab + as + rb + rs \in rs + I$$

This tells us $r's'$ is also in the coset $rs + I$ and thus multiplication does not depend on the choice of repersentatives. The multiplication association and distributivity are easily to prove. Hence, R/I is a ring and is called quotient ring.

Theorem 14.1

Let σ be a homomorphism from ring R to ring S, then

$$\text{Ker}\sigma \trianglelefteq R, \text{Im}\sigma \leqslant R \text{ and } R/\text{Ker}\sigma \cong \text{Im}\sigma$$

Proof. Firstly, we prove Ker$\sigma \trianglelefteq R$. Since $\sigma(0_R) = \sigma(0_R + 0_R)$, $\sigma(0_R) = 0_S$. Then, $0_R \in$ Kerσ. Then

$\emptyset \neq$ Kerσ. For $a, b \in$ Kerσ,

$$\sigma(a \pm b) = \sigma(a) \pm \sigma(b) = 0_S + 0_S = 0_S.$$

Hence, Kerσ is a addition subgroup of R. If $a \in$ Kerσ and $r \in R$, then

$$\sigma(ra) = \sigma(r) \cdot \sigma(a) = \sigma(r) \cdot 0_S = 0_S,$$
$$\sigma(ar) = \sigma(a) \cdot \sigma(r) = 0_S \cdot \sigma(r) = 0_S.$$

Hence, $ra, ar \in$ Kerσ and so Kerσ is a ideal of R.

Next, we prove Im$\sigma \leqslant R$. Since $0_S = \sigma(0_R) \in$ Imσ, Imσ is non-empty. For $a, b \in R$,

$$\sigma(a) \pm \sigma(b) = \sigma(a \pm b) \in \operatorname{Im}\sigma,$$
$$\sigma(a)\sigma(b) = \sigma(ab) \in \operatorname{Im}\sigma.$$

Hence, $\operatorname{Im}\sigma$ is a subring of R.

Finally, we prove that $R/$Ker $\sigma \cong \operatorname{Im}\sigma$. Let $I =$ Ker σ. Define $\overline{\sigma} : R/I \cong \operatorname{Im}\sigma$ given by $\overline{r} = \sigma(r)$. Since we're dealing with cosets, there may be many different representatives for the same coset, which means we have to check it's well-defined.

Havn't done! □

14.1 Reference

- lecture notes from berkeley
- lecture notes by feog

Chapter 15

The Direct Sum of Ring and Chinese Remainder Theorem

Definition 15.1: G

ven rings $R_1, ..., R_n$, the outer direct sum of $R_1, ..., R_n$ (denoted by $R_1 \oplus \cdots \oplus R_n$) is

$$\{(r_1, ..., r_n) : r_i \in R_i\},$$

with addtion and multiplication defined by

$$(r_1, ..., r_n) + (s_1, ..., s_n) = (r_1 + s_1, ..., r_n + s_n)$$

and

$$(r_1, ..., r_n) \times (s_1, ..., s_n) = (r_1 s_1, ..., r_n s_n),$$

where the operation in the i-th coordinate position is the relevant operation in R_i.

It can be check that $R_1 \oplus \cdots \oplus R_n$ is a ring.

Theorem 15.1

$R = R_1 \oplus ... \oplus R_n$. Put

$$R_i^* = \{(x_1, ..., x_n) \in R : x_i \in R_i \text{ and } x_j = e_j, \forall j \neq i\}$$

and define $\sigma_i : R \to R_i$ by $\sigma_i(x_1, ..., x_n) = x_i$. Then
(1) σ_i is a homomorphism, $\operatorname{Im} \sigma_i = R_i$ and $\operatorname{Ker} \sigma_i = R_i^*$
(2) $R_i^* \trianglelefteq R$.
And more,
(3) $\forall i, R_i \cong R_i^*$
(4) $R_1^* \cdots R_n^* = G$
(5) $\forall i, R_i^* \cap \prod_{j \neq i} R_j^* = \{0\}$.

Proposition 15.1

If $I_1, ..., I_m$ are ideals of R, R is called the inner direct sum of $I_1, .., I_m$ if
(1) $I_1 + .. + I_m = R$, and
(2) $\forall i, I_i \cap \sum_{j \neq i} I_j = \{0\}$

Remark. Since $(I, +)$ is a normal subgroup of $(R, +)$, the definition makes sense.

Theorem 15.2

Let R be a ring and let $I_1, ..., I_m$ be ideals of R. If R is the inner direct sum of $I_1, ..., I_m$, then $R \cong I_1 \oplus ... \oplus I_m$.

Definition 15.2

Let R be a ring and $I, J \subseteq R$ be ideals. The sum and product of I and J are the ideals

$$\begin{aligned} I + J &= \langle I \cap J \rangle, \\ IJ &= \langle I \cdot J \rangle, \end{aligned}$$

where $I \cdot J = \{ab : a \in I, b \in J\}$.

Lemma 15.1

Let R be a ring with ideals I and J. Then

$$\begin{aligned} I + J &= \{a + b : a \in I, b \in J\}, \\ IJ &= \{\sum_{i=1}^{n} a_i b_i : a_i \in I, b_i \in J, n \in \mathbb{N}\}. \end{aligned}$$

The distributive law holds for ideals I, J, K,

- $I(J + K) = IJ + IK$
- $(I + J)K = IK + JK$.

If a product is replaced by an intersection, a partial distributive law holds: $I \cap (J + K) \supset I \cap J + I \cap K$.

Proposition 15.2

Let I, J be ideals in a ring R. Then $IJ \subseteq R$ and $IJ \subseteq I$.

Proof. Because I and J are ideals, the elements of $I \cdot J$ all belong to both I and J. Thus, $I \cdot J \subseteq I \cap J$, which implies $IJ \subseteq I \cap J$. □

In number theory, two integers a and b are coprime iff there exists $m, n \in Z$, such that $ma + nb = 1$. This identity is called Bézout's identity. By this identity, we can define coprime about ideals.

Definition 15.3

Two ideals I and J in a ring R are called coprime if $A + B = R$.

Proposition 15.3

Let R be an unital ring. Then two ideals I and J in R are coprime iff $1 \in I + J$.

Proposition 15.4

Let R be a ring with unity and I, J are ideals in R. Then

$$(I \cap J)(I + J) \subseteq IJ + JI.$$

Proof.

$$\begin{aligned} (I \cap J)(I + J) &= (I \cap J)I + (I \cap J)J && (I \cap J \subseteq J, I \cap J \subseteq I) \\ &\subseteq JI + IJ \end{aligned}$$

□

Lemma 15.2

Let R be an unital ring. Two ideals I and J in R are coprime, then

$$IJ + JI = I \cap J.$$

In particular, if R is commutative, $IJ = I \cap J$.

Proof. Since $IJ, JI \subseteq I \cap J$ and $I \cap J$ is a ring, $IJ + JI \subseteq I \cap J$. Also, $I + J = R$ and $(I \cap J)R = I \cap J$, then $(I \cap J) \subset IJ + JI$. □

Lemma 15.3

Let R be an unital ring and I, J, K are ideals in R. If $I + J = R$ and $I + K = R$, then I and JK are coprime.

Proof. It suffices to show that $1 \in I + JK$. Since $I + J = R$, there exists $i \in I$ and $j \in J$ such that $i + j = 1$. Since $I + K = R$, there exists $i' \in I, k \in K$ such that $i' + k = 1$. Hence in R,

$$1 = 1 \cdot 1 = (i + j)(i' + k) = ii' + ik + ji' + jk = (ii' + ik + ji') + jk \in I + JK.$$

□

15.1 Reference

- lecture notes from queen mary

- Product of two ideals
- The Multiplicative Arithmetic of Ideals
- THE CHINESE REMAINDER THEOREM AND THE PHI FUNCTION

Chapter 16

Characteristic of a Ring and Factorization in Commutative Rings

16.1 Characteristic of a Ring

16.2 Factorization in Commutative Rings

16.3 Reference

- Factorization in Commutative Rings
- Characteristic of a Ring

Chapter 17

Maximal Ideals and Prime Ideals

Today we discuss two very important types of ideals, and learn how to use them to check whether certain quotients are fields or integral domains.

17.1 Prime Ideals

Proposition 17.1

Let $f, g \in \mathbb{Z}$. $f|g$ iff $g \in (f)$.

Proof. $\exists h \in \mathbb{Z}$ s.t. $g = fh$ □

Proposition 17.2

Let $p, a, b \in \mathbb{Z}$. p is prime iff $p|ab \Rightarrow p|a$ or $p|b$.

Proof. ($\Rightarrow$): Suppose $p \nmid a$. Since p is prime, $\gcd(p, a) = 1$. Then there exists $m, n \in \mathbb{Z}$ such that $mp + na = 1$ and then $(mb)p + (n)ab = b$. Since $p|ab$, $\exists t \in \mathbb{Z}$, $tp = ab$. Then $(mb + tn)p = b$. Hence, $p|b$.
($\Leftarrow$): Suppose p is not prime, then $\exists k, s \in \mathbb{Z}$ ($k, s \neq 1, p$ and $k, s \leq p$) s.t. $ks = p$. Since $p|ks$, by the condition, $p|k$ or $p|s$. This is a contradiction as $p > k, s$. Hence, p is prime. □

By proposition17.1, $p|ab$ means $ab \in (p)$, and similarly $p|a$ means $a \in (p)$. So in terms of ideals, p is prime number means that if $ab \in (p)$, then a or b (or both) must be in (p). So for an ideal in $\mathbb{Z}$ generated by a prime number, we have the following slogn: if a product is in it, one of the factors must be, also. This is basically the definition of a prime ideal, and it makes sense in any ring.

Definition 17.1

Let I be a proper ideal in a commutative ring with unity. We say I is a prime ideal if whenever $ab (a, b \in R)$ in I, either a or b (or both) is in I.

Example 17.1

In $\mathbb{Z}$, an ideal (n) is prime iff the integer $|n|$ is prime (being absolute value since primes are positive, but the generator may not be), or $n = 0$.

If $|n|$ is not prime

Example 17.2

In the ring $\mathbb{Z}$, the zero ideal is prime, but in the ring $\mathbb{Z}/6\mathbb{Z}$, the zero ideal is not prime, since $\overline{2} \cdot \overline{3} \in (0)$ but $\overline{2} \notin (0)$ and $\overline{3} \notin (0)$

17.2 Maximal Ideals

A maximal ideal is what the name suggests: the biggest possible ideal. But that would be the entire ring, and there would be only one. So we require maximal ideals to be proper, and then it turns out that there can be many of them.

Definition 17.2

An ideal I in a commutative ring with unity is called maximal if it is not the unit ideal and there are no other ideals J such that $I \subset J \subset R$.

Proposition 17.3

Every nonzero subgroup of $(\mathbb{Z}, +)$ has the form $n\mathbb{Z}$, then every nonzero ideals of $\mathbb{Z}$ has the form (n).

Proof. proof referring to proof from subwiki □

Proposition 17.4

In $\mathbb{Z}$, if $n > 1$ is prime, then (n) is maximal.

Proof. If (n) is not maximal, then there exists (d) such that $(n) \subset (d)$. Then $n = md$ for some $m \in \mathbb{Z}$. Since n is prime, by example 17.1, (n) is prime. Since $n = md \in (n)$, $m \in (n)$ or $d \in (n)$. The latter would imply $(d) \subseteq (n)$, a contradiction. Hence, $m \in (n)$. Then $m = tn$ for some $t \in \mathbb{Z}$, hence $n = tnd$, implying that $td = 1$. Thus $1 \in (d)$ so $(d) = R$. Hence, (n) is maximal. □

The relationship between prime and maximal ideals is as follows:

Proposition 17.5

Any maximal ideal in a commutative ring with unity is prime.

Proof. Let I be a maximal ideal. To show it's prime, assume $a, b \in R$, with $ab \in I$ and $a \notin I$. We must show that $b \in I$. Since $a \notin I$, the ideal sum $(a) + I$ is strictly larger than I, and since I is maximal, $(a) + I = R$. So $1 \in (a) + I$, which means we can write $1 = x + ra$ for some $x \in I$ and

$r \in R$. Then $b = b \cdot 1 = b(x + ra) = bx + bra$, and since both x and ab are in I, this shows that $b \in I$. □

17.3 Relations between these ideals and their quotients

Proposition 17.6

Let R be a commutative ring with unity. Then

$$I \text{ is prime } \Leftrightarrow R/I \text{ is an integral domain }.$$

Proof. Since R is a commutative ring with unity, $R/I = \{\overline{a} = a + I : a \in R\}$ is a commutative unital ring. And for $a, b \in R$, $\overline{ab} = ab + I$. Then $\overline{ab} = \overline{0} \Leftrightarrow ab + I = I \Leftrightarrow ab \in I$. Similarly, $\overline{a} = \overline{0} \Leftrightarrow a \in I, \overline{b} = \overline{0} \Leftrightarrow b \in I$. Hence,

$$\begin{aligned} I \text{ is prime} &\Leftrightarrow ab \in I \text{ implies } a \in I \text{ or } b \in I \\ &\Leftrightarrow \overline{ab} = \overline{0} \text{ implies } \overline{a} = \overline{0} \text{ or } \overline{b} = \overline{0} \\ &\Leftrightarrow R/I \text{ is a integer domain.} \end{aligned}$$

□

Proposition 17.7

Let R be a commutative ring with unity. Then

$$R \text{ is a field} \Leftrightarrow \text{ the only ideals of } R \text{ are } R \text{ and } (0).$$

Proof. ($\Rightarrow$): Let I be a ideal of R. Since R is field, R is a skew field and every non-zero element in R is a unit. If $I \neq (0)$, then for $0 \neq a \in I$, $\exists r \in R$ s.t. $ar = 1 \in I$. Then $I = (1) = R$. And $I = (0)$ is a ideal for every ring. Hence, the only ideals of R are (0) and R.
($\Leftarrow$): Let $a \in R \backslash \{0\}$, then $(a) \neq (0)$. Since the only ideals of R are (0) and R, $(a) = R$. Thus $1 \in (a)$. Then by proposition14.6, $\exists r \in R, ra = ar = 1$. Therefore, a is a unit of R. Then $U(R) = R \setminus \{0\}$ and $R \setminus \{0\}$ is abelian group with respect to multiplication as R is commutative. Hence, R is a field. □

Proposition 17.8

Let R be a commutative ring with unity and $I \neq R$ be a ideal of R. Then

$$I \text{ is maximal } \Leftrightarrow R/I \text{ is a field.}$$

Proof. R is a commutative ring with unity, then R/I is a commutative ring with unity. Then
($\Rightarrow$): Let $\overline{a} \neq \overline{0}$. Then $a \notin I$. Since $I \subseteq I + (a)$ and I is maximal, $I + (a) = R$. Since $1 \notin I, 1 \in (a)$. Then $\exists r \in R$ such that $ra = ar = 1 \in I$. Thus, $\overline{ar} = ar + I = \overline{1}$. Hence, every non-zero elements in R/I has inverse. Then, $U(R/I) = R/I \setminus \{\overline{0}\}$ and R/I is commutative. So, R/I is a field.
($\Leftarrow$): Suppose $\exists$ ideal J s.t. $I \subset J \subset R$. Let $a \in J \setminus I$, then $a \notin I$ and so $\overline{a} \neq \overline{0}$. Since R/I is a field,

$\exists \bar{b} \in R/I$ s.t. $\bar{a}\bar{b} = \bar{1}$. Then $ab - 1 \in I \subset I'$. Since $1 = ab - (ab - 1)$ and $ab \in J$ (J is ideal, $a \in J$ and $b \in R$, then $ab \in J$), $1 \in J$ and so $J = R$. Hence, I is maximal. □

17.4 Zorn's Lemma and the existence of maximal ideals

17.5 Reference

- lecture notes from berkeley
- lecture notes from upr
- Let R be a PID. Then every nonzero prime ideal is maximal.

Chapter 18

Exercise About Ring

Exercise 18.1

Let R be a ring with unity and a be nilpotent in R(i.e. $\exists n \in \mathbb{N}$ s.t. $a^n = 0$). Then $1 - a$ is a unit in R.

Proof. It suffices to show there exists $b \in R$ such that $(1-a)b = b(1-a) = 1$. Since

$$(1-a)(a^{n-1} + a^{n-2} + \ldots + a + 1) = 1 - a^n = 1,$$
$$(a^{n-1} + a^{n-2} + \ldots + a + 1)(1-a) = 1 - a^n = 1.$$

Hence, $1 - a$ has a multiplication inverse in R and so is a unit in R. □

Exercise 18.2

Prove

$$\mathcal{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z} \text{ or } a, b, c, d \in \frac{1}{2} + \mathbb{Z}\}$$

is a subring of Hamilton's quaternions $\mathbb{H}$.

Proof. It suffices to show $\mathcal{H}$ is a subgroup of $\mathbb{H}$ under addition and is closed under multiplication. For $x = a_1 + b_1 i + c_1 j + d_1 k_1, y = a_2 + b_2 i + c_2 j + d_2 k_2 \in \mathcal{H}$,

$$x \pm y = (a_1 \pm a_2) + (b_1 \pm b_2)i + (c_1 \pm c_2)j + (d_1 \pm d_2)k$$

If $a_1, a_2 \in \mathbb{Z}$, then $a_1 \pm a_2 \in \mathbb{Z}$ as $\mathbb{Z}$ is a ring. If $a_1, a_2 \in \frac{1}{2} + \mathbb{Z}$, then $a_1 \pm a_2 \in \mathbb{Z}$. If $a_1 \in \mathbb{Z}$ and $a_2 \in \frac{1}{2} + \mathbb{Z}$, then $a_1 \pm a_2 \in \frac{1}{2} + \mathbb{Z}$. Similarly, $b_1 \pm b_2, c_1 \pm c_2, d_1 \pm d_2 \in \mathbb{Z}$ or $\frac{1}{2} + \mathbb{Z}$. Hence, $\mathcal{H}$ is a subgroup of $\mathbb{H}$ under addition.

$$\begin{aligned}
xy = (a_1 + b_1 i + c_1 j + d_1 k)(a_2 + b_2 i + c_2 j + d_2 k) &= a_1a_2 + a_1b_2 i + a_1c_2 j + a_1d_2 k \\
&\quad b_1a_2 i + b_1b_2 i^2 + b_1c_2 ij + b_1d_2 ik \\
&\quad c_1a_2 j + c_1b_2 ji + c_1c_2 j^2 + c_1d_2 jk \\
&\quad d_1a_2 k + d_1b_2 ki + d_1c_2 kj + d_1d_2 k^2 \\
= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)i& \\
+ (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)k&
\end{aligned}$$

If $a_1, a_2 \in \mathbb{Z}$, then $a_1a_2 \in \mathbb{Z}$ as $\mathbb{Z}$ is a ring. Similarly, $b_1b_2, c_1c_2, d_1d_2 \in \mathbb{Z}$, then, $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \in \mathbb{Z}$. If $a_1, a_2 \in \frac{1}{2} + \mathbb{Z}$, $a_1a_2 = (\frac{1}{2} + t)(\frac{1}{2} + s) = \frac{1}{4} + \frac{1}{2}(s + t + 2st) \in \frac{1}{4} + \frac{1}{2}\mathbb{Z}$, then $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \in \frac{1}{2} + \mathbb{Z}$. If $a_1 \in \mathbb{Z}, a_2 \in \frac{1}{2} + \mathbb{Z}$, $a_1a_2 = s(\frac{1}{2} + t) = \frac{1}{2}s + st \in \frac{1}{2}\mathbb{Z} + \mathbb{Z}$, then $a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 \in \mathbb{Z}$. Similar results are found for other coefficient terms. Hence, $\mathcal{H}$ is closed under multiplication. □

Exercise 18.3

Let R be a ring and S be a collection of all ideals in R. Is S a abelian group with respect to the addition of ideal?

Proof. For $I, J, K \in S$, if
(0) $I + J \in S$
(1) $(I + J) + K = I + (J + K)$
(2) $(0) \in S$
(3) If $I + J = (0)$, then any $a \in I, b \in J, a + b = 0$, then $I = J = (0)$. Hence, every non-zero ideal has no inverse in S and so S is not group with respect to the addition of ideal. □

Exercise 18.4

Let R be a commutative ring with unity and I be a ideal in R, then

$$\sqrt{I} = \{a \in R : \exists n > 0 \text{ s.t. } a^n \in I\}$$

is a ideal in R.

Proof. It suffices to show $\sqrt{I}$ is a addition subgroup of R and for any $a \in \sqrt{I}$ and $r \in R$, $ra, ar \in I$. For any $a, b \in \sqrt{I}$ with some powers $a^n, b^m \in I$. To show that $(a + b) \in \sqrt{I}$, we use the binomial theorem (which holds for any commutative ring):

$$(a + b)^{n+m-1} = \sum_{i=0}^{n+m-1} \binom{n + m - 1}{i} a^i b^{n+m-1-i}.$$

When $i < n$, $n + m - 1 - i \geqslant m$, the corresponding item has the form $rb^m (r \in R)$ and is in I. When $i \geqslant n$, the corresponding item has the form $ra^n (r \in R)$ and is in I. Then, $(a + b)^{n+m-1} \in I$. Similarly, $(a - b)^{n+m-1} \in I$. Then, $a \pm b \in \sqrt{I}$. Hence, $\sqrt{I}$ is a addition subgroup of R. For any $r \in R$,

$$(ra)^n = r^n a^n$$

Since $r^n \in R, a^n \in I, r^n a^n \in I$. Then $ra \in \sqrt{I}$. Hence, $\sqrt{I}$ is an ideal in R. □

Remark. $\sqrt{I}$ is called The radical of I.

Exercise 18.5

Put $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = \frac{-1+\sqrt{-3}}{2}$. What is $|U(\mathbb{Z}[\omega])|$ equal to?

Proof. Suppose $a, b, c, d \in \mathbb{Z}$ and $(a + b\omega)(c + d\omega) = 1$. Take the conjugate of both sides:

$$(a + b\overline{\omega})(c + d\overline{\omega}) = 1.$$

Since $\omega = \frac{-1+\sqrt{-3}}{2} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\overline{\omega} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ and $\omega\overline{\omega} = 1$. Then

$$1 = (a + b\omega)(a + b\overline{\omega})(c + d\omega)(c + d\overline{\omega}) = (a^2 - ab + b^2)(c^2 - cd + d^2).$$

Since $a, b, c, d \in \mathbb{Z}$, $a^2 - ab + b^2 = 1$ and $c^2 - cd + d^2 = 1$. Then $(a - \frac{b}{2})^2 + \frac{3}{4}b^2 = 1$. Clearly, if $|b| \geqslant 2$, then the left hand side is at least 3, so it must be the case that $|b| \leqslant 1$. Thus we need to check if integer solutions exist for $b = -1, b = 0$ or $b = 1$. In fact, to each of those b's correspond two values of a. The complete list of solutions is: $(a, b) = (-1, -1), (-1, 0), (0, -1), (0, 1), (1, 0), (1, 1)$ Hence, $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, 1 + \omega, -1 - \omega\}$. Since $\omega^3 = 1$, $\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1) = 0$ and so $\omega^2 = -1 - \omega$. Hence, $U(\mathbb{Z}[\omega]) = \{\pm 1, \pm\omega, \pm\omega^2\}$ and $|U(\mathbb{Z}[\omega])| = 6$. □

Remark. $\mathbb{Z}[\omega]$ is called Eisenstein Integers.

Exercise 18.6

Let R be a ring with unity and I, J, K be ideals in R, then

$$I \text{ and } JK \text{ are coprime } \Leftrightarrow I, J \text{ are coprime and } I, K \text{ are coprime.}$$

Proof. ($\Rightarrow$): It suffices to show that $1 \in I + J$ and $1 \in I + K$. Since $I + JK = 1$, there exists $i \in I, j \in J, k \in K$ such that $i + jk = 1$. Then in R,

$$\begin{aligned} 1 = 1 \cdot 1 = (i + jk)(i + jk) = i^2 + ijk + jki + (jk)^2 &= (i^2 + ijk + jki) + (jk)^2 \in I + J \\ &= i^2 + (ijk + jki + (jk)^2) \in I + K. \end{aligned}$$

Hence, $I + J = R$ and $I + K = R$ and so be coprime respectively.
($\Leftarrow$): It suffices to show that $1 \in I + JK$. Since $I + J = R$, there exists $i \in I$ and $j \in J$ such that $i + j = 1$. Since $I + K = R$, there exists $i' \in I, k \in K$ such that $i' + k = 1$. Hence in R,

$$1 = 1 \cdot 1 = (i + j)(i' + k) = ii' + ik + ji' + jk = (ii' + ik + ji') + jk \in I + JK.$$

□

Exercise 18.7

Let R be a ring with unity and $R_1, \ldots, R_n$ be ideals in R. If R is inner direct sum of $R_1, \ldots, R_n$, then for any ideal I in R, I is inner direct sum of $I \cap R_1, \ldots, I \cap R_n$.

Proof. Any ideal in a ring is a ring, then I is a ring. Firstly, we should show that $I \cap R_i$ is a ideal in I. (1) $\emptyset \neq I \cap R_i \subseteq I$.
(2) $I \cap R_i$ is a abelian group with respect to addition as I and R_i are abelian group with respect to addition.
(3) for $x \in I$, $y \in I \cap R_i$, $xy, yx \in I \cap R_i$ as I and R_i are ideals.
Secondly, we should show that $I = (I \cap R_1) + ... + (I \cap R_n)$ and $\forall i, (I \cap R_i) \cap \sum_{j \neq i} (I \cap R_j) = \{0\}$. We have known that $R = R_1 + ... + R_n$ and $\forall i, R_i \cap \sum_{j \neq i} R_j = \{0\}$. Since $I = IR = IR_1 + ... + IR_n \subset (I \cap R_1) + ... + (I \cap R_n)$ and $(I \cap R) + ... + (I \cap R_n) \subset I \cap (R_1 + ... + R_n) = I \cap R = I$, $I = (I \cap R_1) + ... + (I \cap R_n)$. And $\forall i, (I \cap R_i) \cap \sum_{j \neq i} (I \cap R_j) \subset I \cap (R_i \cap \sum_{j \neq i} R_j) = \{0\}$ and $0 \subset (I \cap R_i) \cap \sum_{j \neq i} (I \cap R_j)$. Then, $(I \cap R_i) \cap \sum_{j \neq i} (I \cap R_j) = 0$. Hence, I is inner direct sum of $I \cap R_1, ..., I \cap R_n$. □

Exercise 18.8

Let R be a commutative ring with unity. If for any $a \in R$, there exists $n \in \mathbb{Z}$ and $n > 1$ such that $a^n = a$, then any prime ideal in R is maximal.

Proof. Suppose I is a ideal in R. To prove I is maximal, it suffices to show that the quotient R/I is a field. Let $\overline{a} = a + I$ be a nonzero element of R/I, where $a \in R$. Since there exists an integer $n > 1$ such that $a^n = a$. Then we have

$$(\overline{a})^n = a^n + I = a + I = \overline{a}.$$

Thus we have

$$\overline{a}(\overline{a}^{n-1} - 1) = 0$$

in R/I. Note that R/I is an integral domain since I is prime. Since $\overline{a} \neq \overline{0}$, the above equality yields that $\overline{a}^{n-1} - 1 = \overline{0}$, and hence

$$\overline{a} \cdot \overline{a}^{n-2} = 1.$$

Thus, $\overline{a}$ has multiplicative inverse $\overline{a}^{n-2}$. This prove that each nonzero element of R/I is invertible. Since R is commutative, R/I is commutative. Hence, R/I is a field. □

Exercise 18.9

In $\mathbb{Z}[x]$, (3) is prime but not maximal.

Proof. Assume P and Q are polynomials. Suppose $PQ \in (3)$ but neither P or Q is in (3), then each has at least one coefficient which is not a multiple of 3. Suppose p_i and q_j are the lowest degree term of P and Q such that the coefficient is not a multiple of 3. Consider the coefficient of x^{i+j} in PQ, it is given by

$$(p_0 q_{i+j} + ... + p_{i-1} q_{j+1}) + (p_i q_j) + (p_{i+1} q_{j-1} + ... + p_{i+j} q_0)$$

As each of $p_0, ..., p_{i-1}$ is divisible by 3 by assumption, the first piece is divisible by 3, and likewise each of $q_0, ..., q_{j-1}$ is divisible by 3 so the third piece is also divisible by 3. But the middle term is not divisible by 3 since neither p_i nor q_j is divisible by 3, so the coefficient of x^{i+j} in PQ is not divisible by 3, so PQ does not lie in (3). Thus (3) is prime. Since $(3) \subset < 3, x > \subset R$, (3) is not maximal. □

Exercise 18.10

Let R be a commutative finite ring with unity, then any prime ideal in R is maximal.

Proof. Suppose I is prime ideal in R, then R/I is a finite integral domain with unity $\overline{1}$. Let $\overline{a}$ is nonzero element in R/I. Since R/I is finite, there exists $i > j$ such that $\overline{a}^i = \overline{a}^j$. Since R is integral domain, by the cancellation, we have $\overline{a}(\overline{a}^{i-j-1}) = 1$ and so $\overline{a}$ is invertible. Hence, R/I is a field as R/I is commutative and so I is maximal. □

18.1 Reference

- Radical of an ideal
- Eisenstein Integers
- Prove that (3) and (x) are prime ideals in $\mathbb{Z}[x]$.
- Every finite integral domain is a field

Part III

Field Theory

Chapter 19

Basic Properties of Field

19.1 Rings and fields

Definition 19.1

A ring $(R, +, *)$ is a set R, together with two binary operations, denoted by $+$ and $*$, such that
(1) R is an abelian group with respect to $+$;
(2) R is closed under $*$.
(3) $*$ is associative, that is $(a * b) * c = a * (b * c)$ for all $a, b, c \in R$;
(4) the distributive laws hold, that is, for all $a, b, c \in R$ we have $a * (b + c) = (a * b) + (a * c)$ and $(b + c) * a = (b * a) + (c * a)$.
Typically, we use 0 to denote the identity element of the abelian group R with respect to addition, and $-a$ to denote the additive inverse of $a \in R$.

Definition 19.2

(1) A ring is called a ring with identity if the ring has a multiplicative identity (usually denoted e or 1).
(2) A ring is called commutative if $*$ is commutative.
(3) A ring is called an integral domain if it is a commutative ring with identity $e \neq 0$ in which $ab = 0$ implies $a = 0$ or $b = 0$ (i.e. no zero divisors).
(3) A ring is called a division ring (or skew field) if the non-zero elements form a group under $*$.
(4) A commutative division ring is called a field.

So, in summary: a field is a set F on which two binary operations, called addition and multiplication, are defined, and which contains two distinguished elements e and 0 with $0 \neq e$. Moreover, F is an abelian group with respect to addition, having 0 as the identity element, and the non-zero elements of F (often written F^*) form an abelian group with respect to multiplication having e as the identity element. The two operations are linked by the distributive laws.

Proposition 19.1

Every finite integral domain is a field.

Definition 19.3

(1) A subset S of a ring R is called a subring of R if S is a subgroup of R under $+$ (closed under addition and subtraction) and is closed under multiplication.
(2) A subset S of a ring R is called an ideal if I is a subring of R and for all $a \in I$ and $r \in R$ we have $ar \in I$ and $ra \in I$.
(3) Let R be a commutative ring with an identity. Then the smallest ideal containing an element $a \in R$ is $(a) := ra : r \in R$. We call (a) the principal ideal generated by a.

Definition 19.4

An integral domain in which every ideal is principal is called a principal ideal domain (PID).

An ideal I of R defines a partition of R into disjoint cosets (with respect to $+$), these form a ring with respect to the following operations:

$$\begin{aligned}(a+I)+(b+I) &= (a+b)+J,\\ (a+I)(b+I) &= ab+J.\end{aligned}$$

This ring is called the quotient ring and is denoted by R/I.

Proposition 19.2

$\mathbb{Z}/(p)$, the ring of residue classes of the integers modulo the principal ideal generated by a prime p, is a field.

Proof. proof of example13.9. □

These are our first examples of finite fields!

Theorem 19.1

Let σ be a homomorphism from ring R to ring S, then the quotient ring $R/\mathrm{ker}\sigma$ and the ring $Im\sigma$ are isomorphic by the map $r + \mathrm{ker}\sigma \mapsto \sigma(r)$.

We can use mappings to transfer a structure from an algebraic system to a set without structure. Given a ring R, a set S and a bijective map $\sigma : R \to S$, we can use σ to define a ring structure on S that converts σ into an isomorphism. Sepcifically, for $s_1 = \sigma(r_1)$ and $s_2 = \sigma(r_2)$, define

$$s_1 + s_2 \text{ to be } \sigma(r_1 + r_2) \text{ and } s_1 s_2 \text{ to be } \sigma(r_1)\sigma(r_2).$$

This is called the ring structure induced by σ; any extra properties of R are inherited by S.

This idea allows us to obtain a more convenient representation for the finite fields $\mathbb{Z}/(p)$.

Definition 19.5

For a prime p, let $\mathbb{F}_p$ be the set $\{0, 1, ..., p-1\}$ of integers, and let $\sigma : \mathbb{Z}/(p) \to \mathbb{F}_p$ be the mapping defined by $\sigma(\bar{a}) = a$ for $a = 0, 1, ..., p-1$. Then $\mathbb{F}_p$ endowed with the field structure induced by σ is a finite field, called the Galois field of order p.

From above, the mapping σ becomes an isomorphism, so $\sigma(\bar{a}+\bar{b}) = \sigma(\bar{a}) + \sigma(\bar{b})$ and $\sigma(\bar{a}\bar{b}) = \sigma(\bar{a})\sigma(\bar{b})$. The finite field $\mathbb{F}_p$ has zero element 0, identity element 1 and its structure is that of $\mathbb{Z}/(p)$. So, computing with element of $\mathbb{F}_p$ now means ordinary arithmetic of integers with reduction modulo p.

Definition 19.6

If R is an arbitrary ring and there exists a positive integer n such that $nr = 0$ for every $r \in R$ (i.e. r added to itself n times is the zero element) then the least such positive integer n is called the characteristic of R, and R is said to have positive characteristic. If no such positive integer n exists, R is said to have characteristic 0.

Proposition 19.3

A ring $R \neq \{0\}$ of positive characteristic with an identity and no zero divisors must have prime characteristic.

Proof. Since R contains non-zero elements, it follows that R has characteristic $n \geqslant 2$. If n were not prime, we could wirte $n = km$ with $k, m \in \mathbb{Z}$, $1 < k, m < n$. Then $0 = ne = (km)e = (ke)(me)$, so either $ke = 0$ or $me = 0$, since R has no zero divisors. Hence either $kr = (ke)r = 0$ for all $r \in R$ or $mr = (me)r = 0$ for all $r \in R$, contradicting the definition of n as the characteristic. □

Corollary 19.1

A finite field has prime characteristic.

Proof. From proposition19.3, we need only show that a finite field F has a positive characteristic. Consider the multiples $e, 2e, 3e, ...$ of the identity. Since F contains only finitely many elements, there must exist integers k and m with $1 \leqslant k < m$ such that $ke = me$, i.e. $(k-m)e = 0$, and thus $(k-m)f = (k-m)ef = 0f = 0$ for all $f \in F$ so F has a positive characteristic. □

Example 19.1

The field $\mathbb{Z}/(p)$ (equivalently, $\mathbb{F}_p$) has characteristic p.

Definition 19.7

A field containing no proper subfields is called a prime field.

For example, $\mathbb{F}_p$ is a prime field, since any subfield must contain the elements 0 and 1, and since it is closed under addition it must contain all other elements, i.e. it must be the whole field.

Proposition 19.4

The intersection of all subfields of a field F is a prime field, called the prime subfield of F.

Proposition 19.5

The prime subfield of a field F is isomorphic to $\mathbb{Q}$ if F has characteristic 0 and is isomorphic to $\mathbb{F}_p$ if F has characteristic p.

19.2 Polynomials

Definition 19.8

Let $f = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n$ be a Polynomial over R which is not the zero polynomial, so we can suppose $a_n \neq 0$. Then n is called the degree of f. By convention, $deg(0) = -\infty$. Polynomials of degree 0 are called constant polynomials. If the leading coefficient of f is 1 (the identity of R) then f is called a monic polynomial.

Theorem 19.2

The set of polynomials over a ring R forms a ring. It is called the polynomial ring over R and denoted by $R[x]$. Its zero element is the zero polynomial, all of whose coefficients are zero.

Let F denote a (not necessarily finite) field. From now on, we consider polynomials over fields. We say that the polynomial $g \in F[x]$ divides $f \in F[x]$ if there exists a polynomial $h \in F[x]$ such that $f = gh$.

Theorem 19.3: Division Algorithm

Let $g \neq 0$ be a polynomial in $F[x]$. Then for any $f \in F[x]$, there exists polynomial $q, r \in F[x]$ such that

$$f = qg + r, \text{ where } \deg(r) < \deg(g).$$

Using the division algorithm, we can show that every ideal of $F[x]$ is principal.

Proposition 19.6

$F[x]$ is a principal ideal domain. In fact, for every $I \neq (0)$ of $F[x]$ there is a uniquely determined monic polynomial $g \in F[x]$ such that $I = (g)$.

Proof. Let I be an ideal in $F[x]$. If $I = \{0\}$, then $I = (0)$. If $I \neq \{0\}$, choose a non-zero polynomial $k \in I$ of smallest degree. Let b be the leading coefficient of k, and set $m = b^{-1}k$. Then $m \in I$ and m is monic. We will show: $I = (m)$. Clearly, $(m) \subset I$. Now take $f \in I$; by the division algorithm there are polynomial q, r with $f = qm + r$ where either $r = 0$ or deg(r)¡deg(m). Now, $r = f - qm \in I$. If $r \neq 0$, we contradict the minimality of m; so we must have $r = 0$, i.e. f is a multiple of m and

$I = (m)$.

We now show uniqueness: if $m_1 \in F[x]$ is another monic polynomial with $I = (m_1)$, then $m = c_1m_1$ and $m_1 = c_2m$ with $c_1, c_2 \in F[x]$. Then $m = c_1c_2m$, i.e. $c_1c_2 = 1$, and so c_1, c_2 are constant polynomials. Since both m and m_1 are monic, we must have $m = m_1$. □

We next introduce an important type of polynomial.

Definition 19.9

A polynomial $p \in F[x]$ is said to be irreducible over F if p has positive degree and $p = bc$ with $b, c \in F[x]$ implies that either b or c is a constant polynomial. A polynomial which does allow a non-trivial factorization over F is called reducible over F.

Remark. Note that the field F under consideration is all-important here, e.g. the polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but reducible in $\mathbb{C}[x]$, where it factors as $(x + i)(x - i)$.

Theorem 19.4

Any polynomial $f \in F[x]$ of positive degreee an be written in the form

$$f = ap_1^{e_1} \cdots p_k^{e_k}$$

where $a \in F$, $p_1, \ldots, p_k$ are distinct monic irreducible in $F[x]$ and $e_1, \ldots, e_k$ are positive integers. This factorization is unique and is called the canonical factorization of f in $F[x]$.

Example 19.2

Find all irreducible polynomials over $\mathbb{F}_2$ of degree 3.

Proof. The operation tables of $\mathbb{F}_2$ are:

+	0	1
0	0	1
1	1	0

,

*	0	1
0	0	0
1	0	1

Figure 19.1

Since $\mathbb{F}_2 = \{0, 1\}$, it follows that a non-zero polynomial in $\mathbb{F}_2[x]$ must be monic. The degree 3 polynomials are of the form $x^3 + ax^2 + bx + c$, where each coefficient is 0 or 1, i.e. there are $2^3 = 8$ of them.
If $c = 0$, such a polynomial is reducible over $\mathbb{F}_2$ since it has x as divisor.
If $a = b = 0, c = 1$, assume $x^3 + 1 = (x + a_0)(x^2 + b_1x + b_0) = x^3 + (b_1 + a_0)x^2 + (a_0b_1 + b_0)x + a_0b_0$, then $a_0 = b_0 = b_1 = 1$ and so be reducible.
If $a = b = c = 1$, assume $x^3 + x^2 + x + 1 = (x + a_0)(x^2 + b_1x + b_0) = x^3 + (b_1 + a_0)x^2 + (a_0b_1 + b_0)x + a_0b_0$, then $a_0 = b_0 = 1, b_1 = 0$ and so be reducible.
If $a = c = 1, b = 0$, assume $x^3 + x^2 + 1 = (x + a_0)(x^2 + b_1x + b_0) = x^3 + (b_1 + a_0)x^2 + (a_0b_1 + b_0)x + a_0b_0$, then $a_0 = b_0 = 1, b_1 = 0$ and so $a_0b_1 + b_0 = 1 \neq 0$. This is a contradiction and so be irreducible.

If $b = c = 1$, $a = 0$, assume $x^3+x+1 = (x+a_0)(x^2+b_1x+b_0) = x^3+(b_1+a_0)x^2+(a_0b_1+b_0)x+a_0b_0$, then $a_0 = b_0 = 1$,$b_1 = 1$ and so $a_0b_1 + b_0 = 0$. This is a contradiction and so be irreducible.
Hence, $x^3 + x^2 + 1$ and $x^3 + x + 1$ are irreducible. □

Proposition 19.7

For $f \in F[x]$, the quotient ring $F[x]/(f)$ is a field if and only if f is irreducible over F.

19.3 Reference

- lecture note by anskor
- Introduction
- prime field

Chapter 20

The Degree of Field Extension

20.1 Field extensions

Definition 20.1

Let R be a ring with unity. A (Left) R-module is an additive abelian group V together with a function mapping $R \times V \to V$(the image of (a, x) being denoted ax) such that for all $a, b \in R$ and $x, y \in V$:
(1) $1_R x = x$
(2) $(ab)x = a(bx)$
(3) $(a + b)x = ax + bx$
(4) $a(x + y) = ax + ay$

Remark. If R is a field, then R-module is called a (left) vector space.

Definition 20.2

A field L is an extension field of field K if K is a subfield of L. And we denote the corresponding field extension by L/K.

Remark. with $R = K$ (the field of ”scalars”) and $V = L$ (the additive abelian group of ”vectors”), we see that L is a vector space over K. It then makes sense to speak of the dimension of L over K.

Definition 20.3

Let L/K be a field extension. The dimension of L as a vector space over L is called the degree of the extension, written $[L : K]$. If $[L : K] < \infty$, we say that L is a finite extension of K, or that the extension L/K is finite.

Proposition 20.1

Let L/M and M/K be finite field extension, then

$$[L:K]=[L:M][M:K].$$

Definition 20.4

For field L and $\emptyset \neq X \subset L$, the subfield (respectively, subring) generated by X is the intersection of all subfields (respectively, subrings) of L that contain X. i.e., the smallest subfield (resp. subring) of F containing X.

Definition 20.5

Let L/K be a field extension and $\emptyset \neq X \subset L$. Then the subfield (respectively, subring) generated by $K \cup X$ is the subfield(respectively, subring) generated by X over K and is denoted $K(X)$ (or, respectively, in the case of rings, $K[X]$). i.e., the smallest subfield (resp. subring) of F containing $K \cup X$.

Definition 20.6

If $X = \{\alpha_1, \alpha_2, ..., \alpha_n\}$, then the subfield $K(X)$ (respectively, subring $K[X]$) of F is denoted $K(\alpha_1, \alpha_2, ..., \alpha_n)$ (respectively, $K[\alpha_1, ..., \alpha_n]$). The field $K(\alpha_1, ..., \alpha_n)$ is a finitely generated extension of K. If $X = \{\alpha\}$ then $K(\alpha)$ is a simple extension of K.

Remark. The field $K(\alpha_1, ..., \alpha_n)$ is a finitely generated extension of K but it may not be a finite dimensional extension over K.

Theorem 20.1

Let L/K be a field extension and $X \subseteq L$ and $\alpha, \alpha_i \in L$. Then
(1) the subring $K[\alpha]$ consists of all elements of the form $f(\alpha)$ where f is a polynomial with coefficients in K (that is, $f \in K[x]$), i.e. $K[\alpha] = \{f(\alpha) : f(x) \in K[x]\}$.
(2) the subring $K[\alpha_1, \alpha_2, ..., \alpha_n]$ consists of all elements of the form $f(\alpha_1, \alpha_2, ..., \alpha_n)$, where f is a polynomial in n indeterminates with coefficients in K (that is, $f \in K[x_1, x_2, ..., x_n]$); i.e. $K[\alpha_1, ...\alpha_n] = \{f(\alpha_1, ..., \alpha_n) : f(x_1, ..., x_n) \in K[x_1, ..., x_n]\}$.
(3) $K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in K[x]$ and $g(\alpha) \neq 0\}$.
(4) $K(\alpha_1, ..., \alpha_n) = \{\frac{f(\alpha_1,...,\alpha_n)}{g(\alpha_1,...,\alpha_n)} : f, g \in K[x_1, ..., x_n]$ and $g(\alpha_1, ..., \alpha_n) \neq 0\}$.

Proof. (2) Let $S = \{f(\alpha_1, ..., \alpha_n) : f(x_1, ..., x_n) \in K[x_1, ..., x_n]\}$ and $X = \{\alpha_1, ..., \alpha_n\}$. Then $S \subset K[\alpha_1, ..., \alpha_n]$, as $K[\alpha_1, ..., \alpha_n]$ is a subring of L containing $K \cup X$ and S is the collection of linear combination of elements of $K \cup X$. Conversely, if $f_1 \in K[x_1, ..., x_m]$ and $f_2 \in K[x_1, ..., x_n]$, as $f_1 \pm f_2, f_1 \cdot f_2 \in K[x_1, ..., x_n]$, then for $\alpha_1, ..., \alpha_n$,

$$f_1(\alpha_1, ...\alpha_n) \pm f_2(\alpha_1, ...\alpha_n), f_1(\alpha_1, ...\alpha_n) \cdot f_2(\alpha_1, ...\alpha_n) \in S.$$

Therefore, S is an subring of L and so a ring. Since $X \subset S$ ($\forall i$, let $f(x_1, ..., x_n) = x_i$ then

$f(\alpha_1, ..., \alpha_n) = \alpha_i$) and $K \subset S$ ($\forall k \in K$, Let $f(x_1, ..., x_n) = k$ then $f(\alpha_1, ..., \alpha_n) = k$) and $K[\alpha_1, ..., \alpha_n]$ is the intersection of subring containing $K \cup X$, $K[\alpha_1, ..., \alpha_n] \subset S$. Hence, $K[\alpha_1, ..., \alpha_n] = S$. □

We now distinguish between two types of elements of an extension field. This is fundamental to all that follows.

Definition 20.7

Let L/K be a field extension. An element $\alpha \in L$ is algebraic over K if α is a root of some nonzero polynomial $f \in K[x]$. If α is not a root of any nonzero $f \in K[x]$ then α is transcendental over K. L is an algebraic extension of K if every element of L is algebraic over K. L is a transcendental extension if at least one element of L is transcendental over K.

Let L/K be a field extension and $\alpha \in L$ is algebraic over K. We claim that $I = \{g(x) \in K[x] : g(\alpha) = 0\}$ is a ideal in $K[x]$. In fact, for $f(x), g(x) \in I, h(x) \in K[x]$, $f(\alpha) \pm g(\alpha) = 0$ and $h(\alpha)f(\alpha) = 0$. Since $K[x]$ is principal ideal domain, there exists unique monic polynomial $f(x) \in K[x]$ such that $I = (f(x))$. If $g(x) \in I = (f(x))$, then $f(x)|g(x)$. Hence, the degree of $f(x)$ is smallest in I. Now we prove $f(x)$ is irreducible in K. Suppose $f = gh$. Since $f(\alpha) = g(\alpha)h(\alpha) = 0$ and K is a field(hence also an integer domain), either $g(\alpha) = 0$ or $h(\alpha) = 0$. But this is a contradiction with the minimal degree on f, so f must be irreducible. such monic $f(x)$ is called the minimal polynomial of algebraic α over K. The degree of α over K is deg(f).

Example 20.1

The element $\sqrt[3]{3} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ since it is a root of $x^3 - 3 \in \mathbb{Q}[x]$. Since $x^3 - 3$ is irreducible over $\mathbb{Q}$, it is the minimal polynomial of $\sqrt[3]{3}$ over $\mathbb{Q}$, and hence $\sqrt[3]{3}$ has degree 3 over $\mathbb{Q}$.

Example 20.2

Then element $i = \sqrt{-1} \in \mathbb{C}$ is algebraic over the subfield $\mathbb{R}$ of $\mathbb{C}$, since it is a root of the polynomial $x^2 + 1 \in \mathbb{R}[x]$. Since $x^2 + 1$ is irreducible over $\mathbb{R}$, it is the minimal polynomial of i over $\mathbb{R}$, and hence i has degree 2 over $\mathbb{R}$.

Proposition 20.2

Every finite extension of K is algebraic over K.

Proof. Let K be a finite extension of K and let $[L : K] = m$. For $\alpha \in L$, then $m + 1$ elements $1, \alpha, ..., \alpha^m$ must be linearly dependent over K, i.e. must satisfy $a_0 + a_1\alpha + \cdots + a_m\alpha^m = 0$ for some $a_i \in K$ (not all zero). Then α is algebraic over K. □

In the next two theorems, we classify simple extensions (first, extending by a transcendental and second extending by an algebraic).

Theorem 20.2

If L/K is a field extension and $\alpha \in L$ is transcendental over K, then there is an isomorphism of fields $K(\alpha) \cong K(x)$ which is the identity when restricted to K, where $K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} : f(x), g(x) \in K[x]$ and $g(\alpha) \neq 0\}$ and $K(x) = \{\frac{f(x)}{g(x)} : f(x), g(x) \in K[x]$ and $g(x) \neq 0\}$

Proof. Since α is transcendental then $f(\alpha) \neq 0, g(\alpha) \neq 0$ for all nonzero $f, g \in K[x]$. Define $\varphi : K(x) \to L$ as $\frac{f}{g} \mapsto \frac{f(u)}{g(u)}$. Since $\varphi(\frac{f_1}{g_1} + \frac{f_2}{g_2}) = (\frac{f_1}{g_1} + \frac{f_2}{g_2})(u) = \frac{f_1}{g_1}(u) + \frac{f_2}{g_2}(u) = \varphi(\frac{f_1}{g_1}) + \varphi(\frac{f_2}{g_2})$ and $\varphi(\frac{f_1}{g_1} \cdot \frac{f_2}{g_2}) = \frac{f_1}{g_1} \cdot \frac{f_2}{g_2}(u) = \frac{f_1}{g_1}(u) \cdot \frac{f_2}{g_2}(u) = \varphi(\frac{f_1}{g_1})\varphi(\frac{f_2}{g_2})$, φ is a homomorphism. Now for $\frac{f_1}{g_1} \neq \frac{f_2}{g_2}$, then $f_1g_2 \neq f_2g_1$ and $f_1g_2 - f_2g_1 \neq 0$ (not the 0 polynomial, that is). Now $f_1(\alpha)g_2(\alpha) - f_2(\alpha)g_1(\alpha) \neq 0$ (or else α is algebraic over K), and so $\varphi(\frac{f_1}{g_1}) = \frac{f_1(u)}{g_1(u)} \neq \frac{f_2(u)}{g_2(u)} = \varphi(\frac{f_2}{g_2})$. Therefore, φ is one to one. Also, φ is the identity on K (treating K as a subfield of $K(x)$; think of K as the constant rational functions in $L(x)$). So the image of φ is $K(\alpha)$. So φ is an isomorphism from $K(x)$ to $K(\alpha)$ which is the identity on K. □

Remark. Theorem 20.2 tells us what elements of the transcendental extension $K(\alpha)$ of K "look like":

$$\frac{f(\alpha)}{g(\alpha)}, \text{ where } f, g \in K[x] \text{ and } g(\alpha) \neq 0$$

Theorem 20.3

If L/K is a field extension and $\alpha \in L$ is algebraic over K, then
(1) $K(\alpha) = K[\alpha]$;
(2) $K(\alpha) \cong K[x]/f(x)$ where $f \in K[x]$ is the minimal polynomial of α with degree $n \geqslant 1$ over K;
(3) $[K(\alpha) : K] = n$;
(4) $\{1_K, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis of the vector space $K(\alpha)$ over K;
(5) every element of $K(\alpha)$ can be written uniquely in the form $a_0 + a_1\alpha + a_2\alpha^2 + ... + a_{n-1}\alpha^{n-1}$ where each $a_i \in K$.

Proof. (1) and (2): Define $\varphi : K[x] \to K[\alpha]$ as $g \mapsto g(\alpha)$. Then clearly φ is a ring homomorphism. By the form of elements of $K[x]$, φ is onto. Since K is a field, $K[x]$ is a principal ideal domain. So Ker $(\varphi) = (f)$ for some $f \in K[x]$ as Ker (φ) is an ideal. Since α is algebraic and $\varphi(f) = f(\alpha) = 0$, Ker $(f) \neq \{0\}$. □

Remark. Theorem 20.3 tells us what elements of the algebraic extension $K(\alpha)$ of K "look like". That is, there exists a fixed $n \in \mathbb{N}$ such that every element of $K(\alpha)$ is of the form $a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1}$ for some $a_i \in K$.

Example 20.3

Consider the simple extension $\mathbb{R}(i)$ of $\mathbb{R}$. We saw earlier that i has minimal polynomial x^2+1 over $\mathbb{R}$. So $\mathbb{R}(i) \cong \mathbb{R}[x]/(x^2+1)$, and $\{1, i\}$ is a basis for $\mathbb{R}(i)$ over $\mathbb{R}$. So $\mathbb{R}(i) = \{a + bi : a, b \in \mathbb{R}\} = \mathbb{C}$.

Example 20.4

Consider the simple extension $\mathbb{Q}(\sqrt[3]{3})$ of $\mathbb{Q}$. We saw earlier that $\sqrt[3]{3}$ has minimal polynomial $x^3 - 3$ over $\mathbb{Q}$. So $\mathbb{Q}(\sqrt[3]{3}) \cong \mathbb{Q}[x]/(x^3 - 3)$, and $\{1, \sqrt[3]{3}, (\sqrt[3]{3})^2\}$ is a basis for $\mathbb{Q}(\sqrt[3]{3})$ over $\mathbb{Q}$. So $\mathbb{Q}(\sqrt[3]{3}) = \{a + b\sqrt[3]{3} + c(\sqrt[3]{3})^2 : a, b, c \in \mathbb{Q}\}$.

Note that we have been assuming that both K and α are embedded in some larger field F. Next, we will consider constructing a simple algebraic extension without reference to a previously given larger field, i.e. “from the ground up”. The next result, due to Kronecker, is one of the most fundamental results in the theory of fields: it says that, given any non-constant polynomial over any field, there exists an extension field in which the polynomial has a root.

Theorem 20.4: Kronecker’s Theorem

If K is a field and $f \in K[x]$ a monic irreducible polynomial of degree n, then there exists a simple extension field $L = K(\alpha)$ of K such that $\alpha \in L$ and f is the minimal polynomial of α.

Theorem 20.5

If L is a finite dimensional extension field of K, then L is finitely generated and algebraic over K.

Theorem 20.6

Let L be an extension field of K. Then $[L : K] < \infty$ iff there exists finite algebraic $\alpha_1, ..., \alpha_n \in L$ over K such that $K(\alpha_1, ..., \alpha_n) = L$.

20.2 Splitting fields

Given a polynomial, we now want an extension field which contains all its roots.

Definition 20.8

Let $f \in K[x]$ be polynomial of positive degree and F an extension field of K. Then we say that f splits in F if f can be written as a product of linear factors in $F[x]$, i.e. if there exist elements $\alpha_1, \alpha_2, ..., \alpha_n \in F$ such that

$$f = a(x - a_1) \cdots (x - \alpha_n)$$

where a is the leading coefficient of f. The field F is called a splitting field of f over K if it splits in F and $F = K(\alpha_1, ..., \alpha_n)$.

Remark. a splitting field F of a polynomial f over K is an extension field containing all the roots of f, and is ”smallest possible” in the sense that no subfield of F contains all roots of f. The following result answers the questions: can we always find a splitting field, and how many are there?

Theorem 20.7: Existence and uniqueness of splitting field

(1) If K is a field and f any polynomial of positive degree in $K[x]$, then there exists a splitting field of f over K.
(2) Any two splitting fields of f over K are isomorphic under an isomorphism which keeps the elements of K fixed and maps roots of f into each other.

So, we may therefore talk of the splitting field of f over K. It is obtained by adjoining to K finitely many elements algebraic over K, and so it is a finite extension. of K.

Example 20.5

Find the splitting field of the polynomial $f = x^2 + 2 \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

Up to now we have been saying 'a' splitting field. Theorem20.7 give us the right to speak of the splitting field of a given polynomial f over a given field K. We write it as $\mathrm{SF}_K(f)$.

Splitting fields will be central to our characterization of finite fields, in the next chapter.

20.3 Reference

- Section V.1. Field Extensions
- THEORY OF FIELD EXTENSIONS
- Field Theory
- lecture notes by yanghs
- lecture notes by gardnerr
- Some field theory

Chapter 21

Algebraic Extension

Chapter 22

Finite Field

We have seen, in the previous chapters, some examples of finite fields. For example, the quotient ring $\mathbb{Z}/p\mathbb{Z}$ (when p is a prime) forms a field with p elements which may be identified with the Galois field $\mathbb{F}_p$ of order p.

The fields $\mathbb{F}_p$ are important in field theory. Since every finite field must have characteristic p, this helps us to classify finite fields.

Lemma 22.1

Let F be a finite field containing a subfield K with q elements. Then F has q^m elements, where $m = [F : K]$.

Proof. F is a vector space over K, finite-dimensional since F is finite. Denote this dimension by m, then F has a basis over K consisting of m elements, say $\alpha_1, ..., \alpha_m$. Every element of F can be uniquely represented in the form $k_1\alpha_1 + ... + k_m\alpha_m$ (where $k_1, ..., k_m \in K$). Since each $k_i \in K$ can take q values, F must have exactly q^m elements. □

We are now ready to answer the question: ”What are the possible cardinalities for finite fields?”

Proposition 22.1

Let F be a finite field. Then F has p^n elements, where the prime p is the characteristic of F and n is the degree of F over its prime subfield.

Proof. Since F is finite, it must have characteristic p for some prime p for some prime p.(by corollary19.1) Thus, the prime subfield K of F is isomorphic to $\mathbb{F}_p$ (by proposition19.5), and so contains p elements. By lemma22.1, F has p^n elements. □

So, all finite fields must have prime power order - there is no finite field with 6 elements, for example. We next ask: does there exist a finite field of order p^n for every prime power p^n? How can such fields be constructed? We can take the prime fields $\mathbb{F}_p$ and construct other finite fields from them by adjoining roots of polynomials. If $f \in \mathbb{F}_p[x]$ is irreducible of degree n over $\mathbb{F}_p$, by Kronecker's Theorem20.4, then adjoining a root of f to $\mathbb{F}_p$ yields a finite field of p^n elements. However, it is not clear whether we can find an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n, for every integer n.

The following two lemmas will help us to characterize fields using root adjunction.

22.1 Reference

- Finite fields

Chapter 23

Normal Extension and Separable Extension

23.1 Normality

Definition 23.1

An algebraic field extension L/K is normal if for all $\alpha \in L$, the minimal polynomial of α splits in L.

Lemma 23.1

Let L/K be an algebraic extension. Then L/K is normal if and only if every irreducible polynomial over K either has no roots in L or splits in L.

Proof. □

Example 23.1

$\mathbb{Q}(\sqrt[3]{2})$

Proposition 23.1

Let L/K be a field extension. Then

$$L = \mathrm{SF}_K(f) \text{ for some nonzero } f \in K[x] \Leftrightarrow L/k \text{ is finite and normal.}$$

23.2 Normality

Definition 23.2

An irreducible polynomial over a field is separable if it has no repeated roots in its splitting field.

Remark. Formally, for a polynomial $f(x) \in K[x]$ and a root α of f in some extension L of K, we say that α is a repeated root if $(x-\alpha)^2|f(x)$ in $L[x]$.

Remark. Equivalently, an irreducible polynomial $f \in K[x]$ is separable if it splits into distinct linear factors in $\mathrm{SF}_K(f)$:

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n)$$

for some $a \in K$ and distinct $\alpha_1, \ldots, \alpha_2 \in \mathrm{SF}_K(f)$. Put another way, an irreducible f is separable if and only it has $\deg(f)$ distinct roots in its splitting field.

Example 23.2

$x^3 - 2 \in \mathbb{Q}[x]$ is separable, since it has 3 distinct roots in $\mathbb{C}$, hence in its splitting field.

23.3 Reference

- Normality; P98
- Separability; P105

Chapter 24

Exercise about Field

Exercise 24.1

Every finite integral domain with at least two elements is a field.

Proof. Let R be an finite integral domain with at least two elements. Then R is commutative and satisfys cancellation law. Since $R \setminus \{0\}$ is finite and a multiplication semigroup, $R\{0\}$ is a group. Hence, R is a field. □

Exercise 24.2

Let L/M and M/K be field extension. If $[L:K]$ is prime, then either $M = K$ or $M = L$.

Proof. Since $[L:K] = [L:M][M:K]$ and $[L:K]$ is prime, either $[L:M] = 1$ or $[M:K] = 1$. If $[L:M] = 1$, there exists a basis of L over M consisting of a single element. In other words, there exists a $v \in L$ with the property that every element of L can be written as mv for some $m \in M$. In particular, $1_M \in L$, so $1_M = m_0 v$ for some $m_0 \in M$. Hence v is the inverse of $m_0 \in M$. Hence, $v \in M$. Now every element of L is a product of two elements of M, hence every element of L is in M. Also, $M \subseteq L$ and so $M = L$. Similarly, if $[M:K] = 1$, then $M = K$. □

Exercise 24.3

Let $\alpha, \beta \in \mathbb{Q}(i)$, then $\alpha = \beta = 0$ iff $\alpha^2 + 2\beta^2 = 0$.

Proof. $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$, so $\dim_{\mathbb{Q}}(\mathbb{Q}(i)) = 2$ and $\{1, i\}$ is a basis of $\mathbb{Q}(i)$. Suppose $\alpha = a_1 + b_1 i, \beta = a_2 + b_2 i$

(⇒): $\alpha = \beta = 0$, then $\alpha^2 + 2\beta^2 = 0^2 + 2 \cdot 0^2 = 0$.

(⇐): Suppose neither α or β equal 0, then $\sqrt{2}i = \sqrt{-2} = \frac{\alpha}{\beta} \in \mathbb{Q}(i)$. This is a contradiction as the coefficients of element in $\mathbb{Q}(i)$ under $\{1, i\}$ must be rational. Hence, $\alpha = \beta = 0$. □

Exercise 24.4

Let L/K be field extension. For $\alpha, \beta \in L$ algebraic over K with the same minimal polynomial then $K(\alpha) \cong K(\beta)$.

Proof. Suppose f is the minimal polynomial of $\alpha, \beta \in L$ over K, then $K(\alpha) \cong K[x]/f(x)$ and $K(\beta) \cong K[x]/f(x)$. Then there exist isomorphisms $\varphi : K(\alpha) \to K[x]/f(x)$ and $\mu : K(\beta) \to K[x]/f(x)$. Then $\psi = \mu^{-1}\varphi : K(\alpha) \to K(\beta)$ is a isomorphism and so $K(\alpha) \cong K(\beta)$. □

Exercise 24.5

Let L/K be field extension. For $\alpha \in L$ with a minimal polynomial of odd degree in K then $K(\alpha) = K(\alpha^2)$

Proof. For $s \in K(\alpha^2)$, there exist $f, g \in K[x]$ such that $g(\alpha^2) \neq 0$ and $s = \frac{f(\alpha^2)}{g(\alpha^2)} = \frac{a_0+a_1\alpha^2+\ldots+a_n(\alpha^2)^n}{b_0+b_1\alpha^2+\ldots+b_m(\alpha^2)^m}$ $= \frac{a_0+a_1\alpha^2+\ldots+a_n(\alpha)^{2n}}{b_0+b_1\alpha^2+\ldots+b_m(\alpha)^{2m}} = \frac{f_1(\alpha)}{g_1(\alpha)} \in K(\alpha)$. Hence, $K(\alpha^2) \subseteq K(\alpha)$. Now for $f(x) = x^2 - \alpha^2 \in K(\alpha^2)[x]$, $f(\alpha) = 0$. Thus, $[K(\alpha) : K(\alpha^2)] = 1$ or 2. If $[K(\alpha) : K(\alpha^2)] = 2$, $[K(\alpha) : K] = [K(\alpha) : K(\alpha^2)][K(\alpha^2) : K] = 2[K(\alpha^2) : K]$. This is a contradiction as $[K(\alpha) : K]$ is odd. Hence, $[K(\alpha) : K(\alpha^2)] = 1$ and so $K(\alpha) = K(\alpha^2)$. □

Exercise 24.6

Let K be a subfield of $\mathbb{C}$. If $a, b \in K$ and $\sqrt{a}, \sqrt{b}, \sqrt{ab}$ is not in K, then $[K(\sqrt{a}, \sqrt{b}) : K] = 4$.

Proof. Firstly, we claim that $K(\sqrt{a}, \sqrt{b}) = K(\sqrt{a})(\sqrt{b})$. In fact, for $s \in K(\sqrt{a}, \sqrt{b})$, there exists $f, g \in K[x_1, x_2]$ and $f_1, g_1 \in K(\sqrt{a})[x]$ such that $g(\sqrt{a}, \sqrt{b}) \neq 0$, $g_1(\sqrt{b}) \neq 0$ and $s = \frac{f(\sqrt{a},\sqrt{b})}{g(\sqrt{a},\sqrt{b})} = \frac{f_1(\sqrt{b})}{g_2(\sqrt{b})}$. Hence, $K(\sqrt{a}, \sqrt{b}) \subseteq K(\sqrt{a})(\sqrt{b})$. Similarly, $K(\sqrt{a}, \sqrt{b}) \supseteq K(\sqrt{a})(\sqrt{b})$ and so equality holds. Then, $[K(\sqrt{a}, \sqrt{b}) : K] = [K(\sqrt{a})(\sqrt{b}) : K] = [K(\sqrt{a})(\sqrt{b}) : K(\sqrt{a})][K(\sqrt{a}) : K] = [L(\sqrt{b}) : L][L : K]$, where $L = K(\sqrt{a})$. By $\sqrt{a} \notin K$, $[L : K] = 2$. So it suffices to show that $[L(\sqrt{b}) : L] = 2$. It holds only if $\sqrt{b} \notin L$. Suppose $\sqrt{b} \in L$, then $\sqrt{b} = r + s\sqrt{a}, r, s \in K$. But that is impossible since squaring yields $a = r^2 + bs^2 + 2rs\sqrt{b}$, which contradicts hypotheses as follows:
if $rs \neq 0$, then $\sqrt{b} = \frac{a-r^2-bs^2}{2rs} \in K$ as $a, b, r, s \in K$;
if $s = 0$, then $a = r^2$ and $\sqrt{a} = r \in K$;
if $r = 0$, then $a = bs^2 \Rightarrow \sqrt{ab} = bs \in K$.
Hence, $\sqrt{b} \notin L$ and so $[L(\sqrt{b}) : L] = 2$. Then, $[K(\sqrt{a}, \sqrt{b}) : K] = 4$. □

Exercise 24.7

Let $\mathbb{Q}$ be rational field and $p \in \mathbb{Z}$ is prime. Then $\mathbb{Q}(\sqrt{p}, \sqrt[3]{p}, \sqrt[4]{p}, \sqrt[5]{p}, \ldots)$ is a infinte algebraic extension of $\mathbb{Q}$.

Exercise 24.8

Let $\mathbb{F}_2 = \{0, 1\}$ is a finite field of two elements. Find out all the irreducible polynomial with two degree and three degree in $\mathbb{F}_2$.

Exercise 24.9

Let $p \in \mathbb{Z}$ is prime and $\mathbb{F}_p$ is a finite field with p elements. Then $\forall n \in \mathbb{N}$ and $n \geqslant 1$, $\mathbb{F}_{p^n}$ is the normal extension of $\mathbb{F}_p$

24.1 Reference

- Same minimal polynomial gives isomorphism
- Minimal polynomial of odd degree
- answer from mathexchage
- Infinite algebraic extension of Q
- Irreducible Polynomials in GF(2) of degree 1, 2 and 3.
- $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$.