Ring Theory

Guo Haoyang

March 2025

Contents

1 Basic ring concepts **2**
1.1 Chinese remainder theorem . . . 2
1.1.1 Basic form . . . 2
1.1.2 First abstract . . . 2
1.1.3 Second abstract . . . 2

2 EUD, PID, UFD **3**
2.1 UFD . . . 3

3 Polynomial rings **3**
3.1 Polynomial rings over PID . . . 3
3.2 Polynomial rings over UFD . . . 3

4 Group rings and group algebras **4**

1 Basic ring concepts

1.1 Chinese remainder theorem

1.1.1 Basic form

Theorem 1.1: Chinese remainder theorem in modulo

Let $m, n \in \mathbb{Z}$ with $\gcd(m, n) = 1$. $\forall a, b \in \mathbb{Z}$, the pair of congruence

$$x \equiv a \bmod m \quad x \equiv b \bmod n$$

has a solution, and this solution is **uniquely** determined modulo mn.

Theorem 1.2: Chinese remainder theorem in modulo

Let $m_i \in \mathbb{Z}$, $i = 1, \ldots, n$ with $\forall i, j$, $i \neq j$, $\gcd(m_i, m_j) = 1$. $\forall a_i \in \mathbb{Z}$, the n pairs of congruence

$$x \equiv a_i \bmod m_i$$

has a solution, and this solution is **uniquely** determined modulo $\prod_i m_i$.

1.1.2 First abstract

Now, let's consider the theorem 1.2. It gives a map $x \mapsto (x + m_i\mathbb{Z})_i = (a_i + m_i\mathbb{Z})_i$ elementwise. The whole picture is

$$\varphi : \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}$$

The existence of solutions for n pairs of congruence equations implies that this map is surjective, and since the solution is uniquely determined modulo $\prod_i m_i$. So, we can remove the redundancy of those elements that maps to the same element $(a_i + m_i\mathbb{Z})_i \in \prod_i (a_i\mathbb{Z})$ by modulo $(\prod_i m_i)\,\mathbb{Z}$ at $\mathbb{Z}$. In other words, φ can be made into injective by considering the quotient $\mathbb{Z}\Big/(\prod_i m_i)\,\mathbb{Z}$ and the map $\mathbb{Z}\Big/(\prod_i m_i)\,\mathbb{Z} \to \prod_i m_i\mathbb{Z}$.
Moreover, in theorem 1.2, those m_i are assumed to be pairwise coprime, so this leads to that for different i, j, $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$, i.e. for coprime m_i, m_j, the ideal generated by m_i, m_j actually generates the whole ring $\mathbb{Z}$.
So, we have our first extract of the theorem 1.2 as follows:

Theorem 1.3: Chinese remainder theorem in $\mathbb{Z}$

Let $m_i \in \mathbb{Z}$, $i = 1, \ldots, n$ with $\forall i, j$, $i \neq j$, $\gcd(m_i, m_j) = 1$. The map

$$\begin{aligned} \varphi : \mathbb{Z} &\to \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \\ x &\mapsto (x + m_1\mathbb{Z}, \ldots, x + m_n\mathbb{Z}) \end{aligned}$$

is a surjective homomorphism with $\ker\varphi = (\prod_i m_i)\,\mathbb{Z}$

1.1.3 Second abstract

In general, if $\mathbb{Z}$ is substituted into a general commutative ring R and each $m_i\mathbb{Z}$ is replaced by ideals $I_i \trianglelefteq R$. There is no coprime notion. To fit the general commutative rings, 'pairwise coprime' should be upgraded into 'comaximal'.

Definition 1.1: Comaximal ideals

Let R be a commutative ring and $I, J \trianglelefteq R$. I and J is **comaximal** $\Leftrightarrow I + J = R$.

Notice that $(\prod_i m_i)\,\mathbb{Z} = \bigcap_i m_i\mathbb{Z}$. Under comaximal condition, this intersection can re reformulated as well. We shall see this in the following theorem.
With all these notions, we have the most general form of Chinese remainder theorem:

Theorem 1.4: Chinese remainder theorem in general

Let R be a commutative ring and $I_j \trianglelefteq R$, $i = 1, \dots, n$. The map

$$\begin{aligned} \varphi : R &\to R/I_1 \times \cdots \times R/I_n \\ r &\mapsto (r + I_1, \dots, r + I_n) \end{aligned}$$

is a surjective ring homomorphism with $\ker \varphi = \bigcap_j I_j$.
Whenever $\forall i, j$, $i \neq j$, I_i and I_j are comaximal, $\bigcap_j I_j = \prod_j I_j$ and this map φ is surjective.

Remark Whenever I_i, I_j are comaximal for each two different i, j, we have the isomorphism

$$R\Big/\bigcap_j I_j \cong R\Big/\prod_j I_j \cong \prod_j R/I_j$$

The first product is the product of ideals while the second product is the Cartesian product.

2 EUD, PID, UFD

Definition 2.1: prime elements

Definition 2.2: Irreducible elements

2.1 UFD

Definition 2.3: Unique factorization domain

Example Rings that are not UFDs:
(1) $\mathbb{Z}[\sqrt{5}]$: One way is use the fact 'every UFD is not integrally closed'. Here we find $\phi = \frac{\sqrt{5}+1}{2} \in \mathrm{Frac}(\mathbb{Z}[\sqrt{5}])$ which is integral over $\mathbb{Z}[\sqrt{5}]$, but $\phi \notin \mathbb{Z}[\sqrt{5}]$. Hence, $\mathbb{Z}[\sqrt{5}]$ is not integrally closed.

3 Polynomial rings

3.1 Polynomial rings over PID

3.2 Polynomial rings over UFD

The first goal is to study the factorization of polynomial over a UFD. This encodes the $\mathbb{Z}$ and $\mathbb{Z}_p$ case. It would be useful everywhere.
Let R be a UFD, $K = \mathrm{Frac}(R)$ and p be a prime element in R. For $a \in R$, define $\mathrm{ord}_p(a) := r$ such that $p^r | a$ but $p^{r+1} \nmid a$. Further, for $f(x) = \sum_{0 \le i \le n} a_i x^i \in R[x]$, define $\mathrm{ord}_p(f) := \min_i \mathrm{ord}_p(a_i)$. The p-**content** of f is $up^{\mathrm{ord}_p(f)}$ for $u \in R^\times$ and the **content** of f, denoted (f), is defined to be the product of all p-contents ranging over all prime p:

$$(f) := \prod_p p^{\mathrm{ord}_p(f)}$$

primitive polynomial

Lemma 3.1: Gauss's lemma (general)

Let R be a UFD and $K = \mathrm{Frac}(R)$. Let $f, g \in K[x]$. Then,

$$(fg) = (f)(g)$$

Proof: If either one of f, g is 0, then both sides equal to ∞, true. Let's consider the case neither f nor g equals 0. Let $a = (f)$ and $b = (g)$. Then, set $f = af_1$ and $g = bg_1$. Then, $(fg) = (abf_1g_1) = ab(f_1g_1)$. It suffices to show that for polynomials f_1, g_1 of content 1, $(f_1g_1) = (f_1)(g_1)$, i.e. f_1g_1 has content 1. Again, it suffices to show that for such polynomials, $\forall$ prime p, $\mathrm{ord}_p(f_1g_1) = 0$.
Version 1: It suffices to show that p does not divide all coefficients of f_1g_1. Write

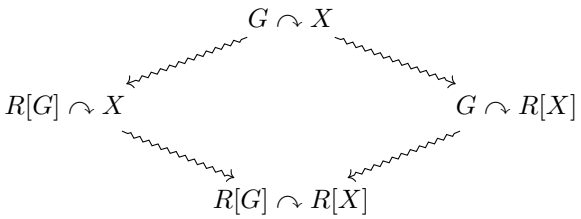
$$f_1(x) = \sum_{0 \le i \le n} a_i x^i \quad g_1(x) \sum_{0 \le i \le m} b_i x^i$$

Let $r := \max\{i : a_i \neq 0 \wedge p \nmid a_i\}$ and $s := \max\{i : b_i \neq 0 \wedge p \nmid b_i\}$. Such r and s exist because f_1, g_1 have content 1. Consider the coefficient of x^{r+s}, which is $\sum_{i+j=r+s} a_i b_j$. By setting of r and s, $p \nmid a_r b_s$. However, p divides any other term since for $i < r$, $p|a_i$ and for $i > r$ (meanwhile, $j < s$), $p|b_j$. Hence, p does not divide the whole sum.
Version 2: Consider the reduction mod p map: $\pi : R \to R/\langle p \rangle$, which induces a morphism $\tilde{\pi} : R[x] \to (R/\langle p \rangle)[x]$. f_1, g_1 are primitive $\Leftrightarrow \tilde{\pi}(f_1), \tilde{\pi}(g_1) \neq 0$. Also, $\tilde{\pi}(f_1g_1) = \tilde{\pi}(f_1)\tilde{\pi}(g_1)$. Since $R/\langle p \rangle$ is an integral domain, $\tilde{\pi}(f_1)\tilde{\pi}(g_1) \neq 0$. Hence, f_1g_1 is primitive □

4 Group rings and group algebras

Let R be a commutative rings. If X is a set, then there is a free R-module generated by X, denoted $R[X]$. Now, substituting X by a group G, the corresponding free R-module $R[G]$ has addition and ring action(scalar multiplication) on it as $R[X]$. In addition, $R[G]$ can be equipped with the third operation, multiplication as follows:

Hence, $R[G]$ becomes an R-algebra, called *group algebra*. If just looking at its addition and multiplication, then $R[G]$ is called a *group ring*.
If there is something else, say G has an action on X. Then, more interplay arises:



Through two paths, the action $G \curvearrowright X$ finally induces the action $R[G] \curvearrowright R[X]$. As a module, the ring action determines what kind of module $R[X]$ is. There is already an action R on X. But now, there is a new one: $R[G]$ acting on $R[X]$, making $R[X]$ a $R[G]$-module.