Abstract Algebra

: Lecture 13

Leo

2024.11.7

Example 1. Consider the ring $\mathbb{Z}_n = \{1, 2, ..., n-1\}$. If $n = m_1 m_2 ... m_r$, where $gcd(m_i, m_j) = 1$ for $i \neq j$, then \mathbb{Z}_n is isomorphic to $\mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_r}$. This is called the Chinese Remainder Theorem.

Theorem 2. Let m_1, m_2, \ldots, m_r be integers which pairwise coprime. Let a_1, \ldots, a_r be integers s.t. $1 \le a_i < m_i$. Then there exists an integer x s.t.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

证明. For $1 \leqslant j \leqslant r$, let $n_j = \prod_{i \neq j} m_i$. Then $\gcd(m_j, n_j) = 1$, so there exists $s_j, t_j \in \mathbb{Z}$ s.t. $m_j s_j + n_j t_j = 1$. Further, $t_j n_j \equiv t_j n_j + s_j m_j = 1 \pmod{m_j}$. Let $x = a_1 t_1 n_1 + a_2 t_2 n_2 + \dots + a_r t_r n_r$. Then $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, ..., $x \equiv a_r \pmod{m_r}$.

Example 3. Let $(m_1, m_2) = (5, 7)$ and $(a_1, a_2) = (2, 3)$, find x s.t. $x \equiv 2 \pmod{5}$ and $x \equiv 3 \pmod{7}$.

Example 4. Let $(m_1, m_2, m_3) = (5, 7, 8)$ and $(a_1, a_2, a_3) = (2, 3, 4)$, find x s.t. $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$ and $x \equiv 4 \pmod{8}$.

Now we prove the integer ring version:

证明. Define a map: $\phi: \mathbb{Z} \to \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_r\mathbb{Z}$ s.t. $a \mapsto (a + (m_1), \dots, a + (m_r))$. Then ϕ is a ring homomorphism with $\ker \phi = (n)$.

To complete the proof, we need to prove ϕ is surjective. In general, an element of $\mathbb{Z}/m_1\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}/m_r\mathbb{Z}$ is of the form $(a_1+(m_1),\ldots,a_r+(m_r))$.

Let $I_1 = (m_1) = m_1 \mathbb{Z}$, and $J = (m_2) \cap (m_3) \cap \cdots \cap (m_r) = (m_2 \dots m_r)$, then $(m_1, m_2 \dots m_r) = 1$, and there exists s, t such that $sm_1 + tm_2 \dots m_r = 1$, let $sm_1 = a_1$ and $tm_2 \dots m_r = b_1$, let $x_1 = 1 - a_1 = b_1$, then $\phi(x_1) = (1 + (m_1), (m_2), \dots, (m_r))$.

Similarly, there exists x_j s.t. $\phi(x_j) = ((m_1), \dots, 1 + (m_j), \dots, (m_r)).$

Let $x = a_1x_1 + \dots a_rx_r$, then $\phi(x) = (a_1 + (m_1), \dots, a_r + (m_r))$, so ϕ is surjective. And $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/m_r\mathbb{Z}$

Theorem 5. (General case) Let R be a ring with identity, and I_1, \ldots, I_r ideals which are pairwise coprime. Then $R/(I_1 \cap \cdots \cap I_r) \simeq R/I_1 \oplus \cdots \oplus R/I_r$.

Definition 6. Two ideals I, J of a ring R are said to be coprime if I + J = R.

Definition 7. Let R be a ring and I, J two ideals of R, and we have $I + J = \{a + b | a \in I, b \in J\}$, $IJ = \{\sum_{finite} a_i b_i | a_i \in I, b_i \in J\}$.

Lemma 8. Let I_1, I_2, J be ideals of a ring R (commutative with identity). If I_1, I_2 are coprime to J, then I_1I_2 is coprime to J.

证明. Since $I_1 + J = R = I_2 + J$, we have $a_1 + b_1 = 1$ and $a_2 + b_2 = 1$ where $a_1 \in I_1$ and $a_2 \in I_2$ and $b_1, b_2 \in J$. Then $a_1a_2 + b_1a_2 + b_2a_1 + b_1b_2 = 1 \in I_1I_2 + J$. Therefore $I_1I_2 + J = R$, so I_1I_2 is coprime to J.

Corollary 9. If I_1, \ldots, I_t are coprime to J, then $I_1 \ldots I_t$ is coprime to J.

延明. (For general case of Chinese Remainder Theorem) Let $\varphi: R \to R/I_1 \oplus \cdots \oplus R/I_r$ s.t. $a \mapsto (a+I_1,\ldots,a+I_r)$. Then φ is a ring homomorphism with $\ker \varphi = I_1 \cap \cdots \cap I_r$. We only need to prove φ is surjective.

Definition 10. Let J be an ideal of R, where R is commutative and has an identity.

- (1). J is a prime ideal if for any element $a, b \in R$, if $ab \in J$, then $a \in J$ or $b \in J$.
- (2). J is a maximal ideal if I is an ideal and $J \subset I$, then I = R.

Theorem 11. Let J be an ideal of R.

- (1). J is a prime ideal if and only if R/J is an integral domain.
- (2). J is a maximal ideal if and only if R/J is a field.

证明. (1). J is prime $\Leftrightarrow a, b \in J$ implies $a \in J$ or $b \in J \Leftrightarrow \bar{a}\bar{b} = \bar{0}$ implies $\bar{a} = \bar{0}$ or $\bar{b} = \bar{0} \Leftrightarrow R/J$ is an integral domain.

(2). J is maximal \Leftrightarrow $(a) + J = (1), \forall a \in R - J, \Leftrightarrow (\bar{a}) = (\bar{1}) = \bar{R}, \Leftrightarrow \bar{a}$ is a unit in $R/J \Leftrightarrow R/J$ is a field.

In particular, if R is a commutative ring with identity, a maximal ideal is a prime ideal.

Consider $\mathbb{Z} = \{0, \pm 1, \dots, \}$ we can define $\mathbb{Q} = \{\frac{m}{n} | m, n \in \mathbb{Z}, n \neq 0\}$ with $\frac{m_1}{n_1} \frac{m_2}{n_2} = \frac{m_1 m_2}{n_1 n_2}$ and $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ if and only if $m_1 n_2 = m_2 n_1$ and $\frac{m_1}{n_1} + \frac{m_2}{n_2} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}$.

Definition 12. Let R be an integral domain. Define $S = \{(a,b)|a,b \in R, b \neq 0\}$ and $(a_1,b_1)(a_2,b_2) = (a_1a_2,b_1b_2)$ and $(a_1,b_1)+(a_2,b_2)=(a_1b_2+a_2b_1,b_1b_2)$. If $(a_1,b_1)=(a_2r,b_2r)$ then identify (a_1,b_1) and (a_2,b_2) .

Then $(S, +, \times)$ is a ring (actually a field) called the fractional field of R.

Definition 13. Let R be a commutative ring with identity. Let T be a set $T \subset R$ s.t. none of the elements of T is the zero divisor of R.

Let $S = \{(a,b) | a \in R, b \in T\}$, and make the same definitions as above. Then $(S,+,\times)$ is a ring called the localization of R at T, denoted by $T^{-1}R$. And R is the subring of S.