MATH3030 Tutorial 9

J. SHEN

16 November, 2023

9 Product rings and the Chinese Remainder theorem

9.1 Definition and characterization of product rings

9.1.1 Product rings

Let R, R' be rings. Then $R \times R' := \{(r, r') : r \in R, r' \in R'\}$ is a ring with component-wise addition and multiplication. The unity is $(1_R, 1_{R'})$.

We have two projections: $\pi_1 : R \times R' \to R$ by $\pi_1(r, r') = r$, and $\pi_2 : R \times R' \to R'$ by $\pi_2(r, r') = r'$. The two maps preserves identity, addition, and multiplication. The kernels are $0 \times R'$ and $R \times 0$ respectively.

In other word, we have two short exact sequences:

$$0 \longrightarrow 0 \times R' \longrightarrow R \times R' \xrightarrow{\pi_1} R \longrightarrow 0.$$

$$0 \longrightarrow R \times 0 \longrightarrow R \times R' \xrightarrow{\pi_2} R' \longrightarrow 0.$$

Note that $R \times 0$ is a ring with unity $e_1 = (1, 0)$, and it is isomorphic to R. But it is not a subring of $R \times R'$ because the unity of the two rings are not the same. Similar things hold for $0 \times R'$, which has unity $e_2 = (0, 1)$.

Note that $e_1^2 = e_1$. We say that an element with this property as e_1 is **idempotent**.

9.1.2 A characterization of product rings

In fact, in the commutative case, product rings are characterized by idempotent elements:

Proposition 9.1. *Let S be a commutative ring. Let $e \in S$ be an idempotent element, that is, $e^2 = e$.*

1. *The element $e' = 1 - e$ is also idempotent, and $ee' = e'e = 0$.*

2. *eS and $e'S$ are rings with identity elements e and e'. Moreover, $m_e : S \to eS$ and $m_{e'} : S \to e'S$ are ring homomorphisms, where $m_a(s) = as$ for $a, s \in S$.*

3. *$S \simeq eS \times e'S$.*

Proof.

1. In the commutative ring R, since $e^2 = e$, $ee' = e'e = (1-e)e = e - e^2 = 0$ and $(e')^2 = e'(1-e) = e' - e'e = e'$.

2. Note that $m_e : S \to S$ is additive: $m_e(s + s') = e(s + s') = es + es' = m_e(s) + m_e(s')$ for any $s, s' \in S$, so its image eS is an additive subgroup of S. Let $es, es' \in eS$ with $s, s' \in S$. Then $eses' = e(ses') \in eS$. Therefore, eS is closed under multiplication. Moreover, for any $s \in S$, $e(es) = e^2 s = es$. Then e is an identity element in eS. It follows that eS is a ring with identity element e.

   Note that $m_e(1) = e$, and for any $s, s' \in S$, $m_e(s + s') = m_e(s) + m_e(s')$ and $m_e(s)m_e(s') = eses' = e^2 ss' = ess' = m_e(ss')$. Therefore, m_e is a ring homomorphism.

   The statements for e' are analogous.

3. Define $\phi : S \to eS \times e'S$ by $\phi(s) = (es, e's) = (m_e(s), m_{e'}(s))$. By 2, ϕ is a ring homomorphism. Let $s \in \ker(\phi)$, then $es = e's = 0$. Then $s = (e + e')s = 0$. Therefore ϕ is injective. Let $(a, b) \in eS \times e'S$. Write $(a, b) = (es_1, e's_2)$, where $s_1, s_2 \in S$. Then $\phi(a + b) = (ea + eb, e'a + e'b) = (ees_1 + ee's_2, ee's_1 + e'e's_2) = (es_1, e's_2) = (a, b)$. Therefore, ϕ is bijective. Thus, $\phi : S \simeq eS \times e'S$.

9.2 The Chinese remainder theorem

Theorem 9.2. *Let $I, J \subseteq R$ be ideals, such that $I + J = R$. Then*

1. *$I \cap J = IJ$.*

2. *$R/IJ \simeq R/I \times R/J$.*

Proof.

1. Clearly, $IJ \subseteq I$ and $IJ \subseteq J$. Then $IJ \subseteq I \cap J$. Conversely, let $x \in I \cap J$. Since $I + J = R$, there exists some $a \in I$, $b \in J$ such that $a + b = 1$. Then $x = x(a + b) = xa + xb$. Now, $x \in J$ and $a \in I$ imply that $xa \in IJ$; $x \in I$ and $b \in J$ imply that $xb \in IJ$. Therefore, $x = xa + xb \in IJ$. It follows that $IJ = I \cap J$.

2. Define $\phi : R \to R/I \times R/J$ by $\phi(r) = (r + I, r + J)$. Then ϕ is a ring homomorphism. The kernel is $\ker(\phi) = I \cap J = IJ$.

   Let $a \in I, b \in J$ be such that $a+b = 1$. Then $\phi(a) = (a+I, a+J) = (0+I, a+b+J) = (0+I, 1+J)$, and $\phi(b) = (b+I, b+J) = (a+b+I, 0+J) = (1+I, 0+J)$. Then for any $u, v \in R$, $\phi(ub+va) = (u+I, v+J)$. Therefore, ϕ is surjective. By the first isomorphism theorem, ϕ induces an isomorphism $R/IJ \simeq R/I \times R/J$.

Example. 1. $\mathbb{Z}/(105) \simeq \mathbb{Z}/(3) \times \mathbb{Z}/(5) \times \mathbb{Z}/(7)$.
2. $\mathbb{Z}[i]/(5) \simeq \mathbb{F}_5[x]/(x^2 + 1) \simeq \mathbb{F}_5[x]/(x - 2) \times \mathbb{F}_5[x]/(x + 2) \simeq \mathbb{F}_5 \times \mathbb{F}_5$.
3. $\mathbb{Z}[i]/(13) \simeq \mathbb{F}_{13}[x]/(x^2 + 1) \simeq \mathbb{F}_{13}[x]/(x - 5) \times \mathbb{F}_{13}[x]/(x + 5) \simeq \mathbb{F}_{13} \times \mathbb{F}_{13}$.