進階代數第四次作業

2008.10.27　2008.11.03

1. Solution:
$S = \{\ a \mid a$ is not a zero divisor $\}$, $S^{-1}R$ is the complete ring of quotient of R.

$$\begin{aligned} S &= \{x \in \mathbb{Z}_n \mid (x, n) = 1\} \\ S^{-1}\mathbb{Z}_n &= \{m/a \mid m \in \mathbb{Z}_n, a \in S\} \\ &= \{m \mid m \in \mathbb{Z}_n\} \\ &= \mathbb{Z}_n \end{aligned}$$

because $(a, n) = 1$ therefore $at + ns = 1$ for some $s, t \in \mathbb{Z}_n$. Hence $1/a = t$, because $m/a = mt \in \mathbb{Z}_n$.

2. Solution:
利用 universal theorem, 造一個函數 $\widehat{\phi} : S^{*^{-1}}S \to T^{*^{-1}}T$, 接著檢查 $\widehat{\phi}$ 是否爲一對一且映成。

- onto: If $(a/b)/(c/d) \in T^{*^{-1}}T$ then $\widehat{\phi}((ad)/(bc)) = (a/b)/(c/d)$.
- 1–1: $\ker(\widehat{\phi}) = \{0\}$.

3. SOLUTION:

a) In $S^{-1}R$, $\frac{b}{a}\frac{d}{c} = \frac{bd}{ac}$. (by definition)
Suppose $\frac{b}{a}\frac{d}{c} = 0$, then $\frac{b}{a}\frac{d}{c} = \frac{0}{1}$. Hence $(bd - 0 \cdot ac)s = 0$ for some $s \in S$. Hence $bd = 0$, $\because R$ is an integral domain. Thus $b = 0$ or $d = 0$. Then $\frac{b}{a} = 0$ or $\frac{d}{c} = 0$.

b) ★ $\frac{b}{a} = \frac{b_1 b_2 \cdots b_m}{a_1 a_2 \cdots a_n} = \frac{b_1}{1}\frac{b_2}{1} \cdots \frac{b_m}{1}\frac{1}{a_1}\frac{1}{a_2} \cdots \frac{1}{a_n}$
For example, $R = \mathbb{Z}, S = \{6^k \mid k = 0, 1, \ldots\}$. $S^{-1}R = \{n\ 6^k \mid n \in \mathbb{Z}, k \in \mathbb{N} \cup \{0\}\}$
$\Rightarrow\ S' = \{2^n, 3^n \mid n \in \mathbb{Z} \cup \{0\}\}$
$\Rightarrow\ S'^{-1}\mathbb{Z} = S^{-1}\mathbb{Z}$.
Proof. If $a \in S$, $b \mid a$ then b is a unit. It suffices to assume $a \in S$ and $b \mid a \Rightarrow b \in S$
Note:

- $U = \{\, c\,\frac{a}{b} \mid c$ is a unit in R, $a, b \in S\}$ is the set of units in $S^{-1}R$.
- $T = \{\, ra \mid a \in R - S$ is an irreducible element in R and $r \in S^{-1}R$ is a unit.$\}$

It is clear each nonzero nonunit element can be written as a product of finite elements in T. Suppose $cu_1u_2 \cdots u_t = dv_1v_2 \cdots v_s$ where $u_i, v_i \in R - S$ and $c, d \in U$. Suppose

$$c = r \cdot \frac{c_1c_2 \cdots c_p}{c_1^{'}c_2^{'} \cdots c_q^{'}}\ ,\ d = k \cdot \frac{d_1d_2 \cdots d_l}{d_1^{'}d_2^{'} \cdots d_m^{'}}$$

where $c_i, c_i^{'}, d_i, d_i^{'} \in S$ and $r, k \in R$ are units. Then

$$r \cdot \underbrace{c_1c_2 \cdots c_p}_{S} \cdot \underbrace{u_1u_2 \cdots u_t}_{\notin S} \cdot \underbrace{d_1^{'}d_2^{'} \cdots d_m^{'}}_{S} = k \cdot \underbrace{d_1d_2 \cdots d_l}_{S} \cdot \underbrace{v_1v_2 \cdots v_s}_{\notin S} \cdot \underbrace{c_1^{'}c_2^{'} \cdots c_q^{'}}_{S}$$

By the UFD of R, we hava $t = s$ and there exists a bijection on $\{1, 2, 3, \ldots, t\}$ such that $u_i, v_{\sigma(i)}$ are associates in R.

4. SOLUTION:

Let $V = \{P \mid P \text{ is a prime ideal in } S^{-1}R\}$. Given $P' \in V$, let $P = \{b \mid b/a \in P', a \in S, b \in R\}$.

1) Check P is a prime ideal.

   (i) $b_1, b_2 \in P$,
   $\Rightarrow \exists\, a_1, a_2 \in S$ such that $\frac{b_1}{a_1}, \frac{b_2}{a_2} \in P'$
   $\Rightarrow \frac{b_1}{a_1} \cdot \frac{a_1}{a_2} = \frac{b_1}{a_2} \in P'$
   $\therefore \frac{b_1}{a_2} - \frac{b_2}{a_2} = \frac{b_1 - b_2}{a_2} \in P' \Rightarrow b_1 - b_2 \in P.$

   (ii) $\forall\, r \in R \quad \frac{b_1}{a_1} \cdot \frac{r}{a_1} = \frac{b_1 r}{a_1^2} \in P' \Rightarrow b_1 r \in P.$

   (iii) if $b_1, b_2 \in P$,
   $\Rightarrow \exists\, a \in S$ such that $\frac{b_1 b_2}{a} \in P'$.
   $\Rightarrow \frac{b_1 b_2}{a} \cdot \frac{a}{a_2} \in P'$.
   $\Rightarrow \frac{b_1}{a} \cdot \frac{b_2 a}{a_2} \in P'$.
   Case (i): $\frac{b_1}{a} \in P' \Rightarrow b_1 \in P$, (done)
   Case (ii): $\frac{b_2 a}{a_2} \in P' \Rightarrow \begin{cases} \frac{a}{a} \in P',\ P' = S^{-1}R. \ (\rightarrow\leftarrow) \\ \frac{b_2}{a} \in P' \Rightarrow b_2 \in P. \text{ (done)} \end{cases}$

2) $P' = S^{-1}R = PS^{-1}R$. $ab \in P \Rightarrow a \in P$ or $b \in P$. (prime)

5. SOLUTION:

a) 這一小題要利用上課證過的定理:

   Theorem. Let R be a ring and $S \subseteq R$ be multiplicative closed. Set $U = \{P \mid P \text{ is a prime in } R \text{ with } P \cap S = \varnothing\}$, $V = \{P' \mid P' \text{ is a prime in } S^{-1}R\}$. Then there exist a bijection from U to V.

   取 $S = R - P$, 令 $U = \{Q \mid Q \text{ is a prime in } R \text{ with } Q \cap S = \varnothing\}$, $V = \{Q' \mid Q' \text{ is a prime in } S^{-1}R\}$. 即可得證。

b) Let M be a maximal ideal of R_P. Since $R_P^2 = R_P$, by *Theorem 2.19* M is also a prime ideal. by (a) $\exists Q \subseteq P$ such that $Q_P = M$.

$\because Q \subseteq P, \therefore Q_P \subseteq P \Rightarrow M \subseteq P_P$.

Claim: $P_p \neq R_p$. Suppose $P_P = R_P$, i.e. $S^{-1}P = S^{-1}R$ where $S = R - P$. Define a map $\tau_s : R \to R_P$ by $\tau_s(r) = (r, 1)$ for $r \in R \Rightarrow \tau_s^{-1}(P_P) = \tau_s^{-1}(R_P) = R, 1 \in R$. Let $\tau_s(1) = \overline{(a, s)} \in P_P$ for some $a \in P, s \in S$. $\tau_s(1) = \overline{(1, 1)}$, $\therefore \overline{(a, s)} = \overline{(1, 1)}$. Then $\exists \rho \in S$ such that $1s\rho = 1a\rho \Rightarrow S \cap P \neq \varnothing$. This contradicts $S = R - P$.

c) $R = \mathbb{Z}, \{0\} = Q \subseteq P = \{2\}$.

6. Solution:

It suffices to show that each nonunit is a nilpotent. Let $r + M^n$ be a nonunit, if $r \in M$, then $(r + M^n)^n = r^n + M^n = 0 + M^n$. Suppose $r \notin M$, since R/M is a field, there exists $s \in R$ such that $(r + M)(s + M) = 1 + M$. Then $rs - 1 \in M$, hence $r(t) + (-1)^n = (rs - 1)^n \in M^n$, for some $t \in R$. Then $r + M^n$ is a nonunit in R/M^n, a contradiction.

7. Solution:

($\Rightarrow$) Since R is local, the maximal ideal $M = \{a \mid a \text{ is nonunit in } R\ \forall a \in R\}$. $\forall a, b \in M, a + b \in M$, since M is ideal, i.e. $a + b$ is nonunit. That is, if a and b are nonunit, then $a + b$ is nonunit. This is equivalent to the statement "If $a + b$ is unit, then a or b is a unit."

($\Leftarrow$) Let $M = \{a \in R \mid a \text{ is nonunit}\}$.

Claim: M is a maximal ideal in R. Let $a, b \in M$. (i)$a + b \in M$. (ii)$\forall r \in R, ra \in M$. If $ra \notin M$, then ra is unit, i.e. $\exists c$ such that $(ra) \cdot c = 1_R$.

$\Rightarrow a \cdot (rc) = 1_R$

$\Rightarrow rc$ is unit of a.

This contradicts the fact $a \in M$.