补充练习(5)

1. 设环 $R\neq 0$ 有左单位元 e

(1) 若 R 无零因子，则 e 是单位元.

(2) 若 e 是唯一的左单位元，则 e 是单位元.

2. (p-adic 整数) 设 p 是一个素数，$\mathbb{N}$ 是非负整数集.

令 $R=\{(a_1,a_2,\cdots,a_n,\cdots) \mid a_i\in\mathbb{N},\ 0\leq a_n<p^n,$
$a_n\equiv a_{n+1}(\bmod p^n),\ n=1,2,\cdots\}$

规定 R 中加法：对应分量相加后模 p^n
乘法：对应分量相乘后模 p^n

(1) 证明：R 是一个含幺交换环.

(2) ~~求~~ R 中元素是否有逆元？

(3) 令 $\mathbb{Z}_p=\{\alpha=a_0+a_1p+a_2p^2+\cdots \mid 0\leq a_i<p,\ a_i\in\mathbb{Z}\}$

这是一个形式幂级数环，描述 $\mathbb{Z}_p$ 和 R 的关系

(4) $\mathbb{Z}_p$ 是 $\mathbb{Z}$ 的推广，对应 $\mathbb{Z}$ 和 $\mathbb{Q}$ 的关系，定义

$$\mathbb{Q}_p=\{a_{-n}p^{-n}+a_{-n+1}p^{-n+1}+\cdots+a_{-1}p^{-1}+a_0+a_1p+\cdots \mid 0\leq a_i<p\}$$

$\mathbb{Q}_p$ 是一个域.

(5) 刻划 $\hat{\mathbb{Z}}_p$ 的理想.

(6) 定义 $\hat{\mathbb{Q}}_p$ 中长度, 设 $\alpha = a_k p^k + a_{k+1} p^{k+1} + \cdots \in \hat{\mathbb{Q}}_p$, 则 $|\alpha|_p = p^{-k}$ $(a_k \neq 0)$. 证明: 关于这个长度, $\mathbb{Z}$ 在 $\hat{\mathbb{Z}}_p$ 中稠密.

即 $\forall \alpha \in \hat{\mathbb{Z}}_p$, $\forall \varepsilon > 0$, $\exists \alpha_0 \in \mathbb{Z}$, $|\alpha - \alpha_0| < \varepsilon$.

3. (循环环) 设 R 是一个环, 若关于 R 的加法是一个循环群, 则 R 是一个循环环. 证明: (R 是一个循环环)

(1) 循环环是一个交换环, 子加群也是它的理想和子环. 因此 n 阶循环环有 $T(n)$ 个子环, 其中 $T(n)$ 是 n 的正因子个数.

(2) n 阶循环环有 $2^{\psi(n)-\psi(k,n)}$ 个幂等元 $(x^2=x)$, 其中 $\psi(n)$ 是 n 的素因子个数, $\psi(k,n)$ 是 k 与 n 最大公因数素因子个数

(3) 所有 n 阶循环环中, 有且只有 $T(n)$ 个互不同构.

4. (华罗庚定理) 设 $\tau: R \longrightarrow \bar{R}$ 是两个环之间映射, 满足

(1) $\tau(a+b) = \tau(a) + \tau(b)$ $\quad \forall a, b \in R$

(2) $\forall a, b \in R$, $\tau(ab) = \tau(a)\tau(b)$ 或 $\tau(ab) = \tau(b)\tau(a)$

则 τ 是一个环同态或环反同态 (即 $\tau(xy) = \tau(y)\tau(x)$).

解答—补充(5)

1. (1) $\forall x\in R$, $ex=x$ 从而 $e\neq 0$

$(xe-x)e=xe-xe=0$, R 无零因子, $\Rightarrow xe=x$

(注: 实际上只需 R 无右零因子)

(2) $\forall a,b\in R$, $(ae-a+e)b=a(eb)-ab+eb=b$

因此 $ae-a+e$ 也是左单位元, 从而 $ae-a+e=e$

即 $ae=a$ $\Rightarrow e$ 是右单位元.

2. (1) 证明: $\forall a=(a_1,a_2,\cdots)$, $b=(b_1,b_2,\cdots)\in R$

$0\leq a_n<p^n$, $a_n\equiv a_{n+1}\pmod{p^n}$ $\quad n=1,2,3,\cdots$

$0\leq b_n<p^n$, $b_n\equiv b_{n+1}\pmod{p^n}$

$\Rightarrow a_n+b_n\equiv a_{n+1}+b_{n+1}\pmod{p^n}$ $\quad a_nb_n\equiv a_{n+1}b_{n+1}\pmod{p^n}$

$\Rightarrow R$ 关于加法、乘法封闭.

$(0,0,\cdots)$, $(1,1,\cdots)$ 分别是 R 的零元和幺元.

$a=(a_1,a_2,\cdots)$ 的负元 $a'=(a_1',a_2',\cdots,a_n',\cdots)$

$$a_n'=\begin{cases}0 & a_n=0\\ p^n-a_n & 0<a_n<p^n\end{cases}$$

(2) 设 $a=(a_1,a_2,\cdots)\in R$, 且 $a_1\neq 0$ 则 $0<a_1<p$

$0\leq a_2<p^2$, $a_1\equiv a_2\pmod{p}\Rightarrow (a_2,p^2)=1$. 一般地,

设 $a_n \neq 0$，$(a_n, p^n)=1$，由 $a_n \equiv a_{n+1} \pmod{p^n}$

$\Rightarrow (a_{n+1}, p^{n+1})=1$ 即对于 $n=1,2,\cdots$，$(a_n, p^n)=1$，且 $a_n \neq 0$

$0<a_n<p^n$ 存在 $0<s_n<p^n$ $a_n s_n + p^n t_n = 1$

令 $s=(s_1, s_2, \cdots)$ 则 $a_n s_n \equiv 1 \pmod{p^n}$

$a_n s_n + p^n t_n = a_{n+1} s_{n+1} + p^{n+1} t_{n+1} \Rightarrow a_n s_n \equiv a_{n+1} s_{n+1} \pmod{p^n}$

$(a_n, p^n) = (a_{n+1}, p^n) = 1 \Rightarrow s_n \equiv s_{n+1} \pmod{p^n} \Rightarrow s \in R$.

即 $as=1$ 从而 s 是 a 的逆

反之，若 $a=(a_1, a_2, \cdots) \in R$ 可逆，则显然 $a_1 \neq 0$.

(3) $\forall \alpha \in \hat{\mathbb{Z}}_p$，令 $\alpha_k = a_0 + a_1 p + a_2 p^2 + \cdots + \cancel{\alpha_k} a_{k-1} p^{k-1}$

$\alpha_k \in \mathbb{Z}/p^k\mathbb{Z}$，$0 \leq \alpha_k < p^k$，$\alpha_k \equiv \alpha_{k+1} \pmod{p^k}$

令 $R = \left\{ (\alpha_0, \alpha_1, \cdots) \middle| \begin{array}{l} 0 \leq \alpha_k < p^k \\ \alpha_k \equiv \alpha_{k+1} \pmod{p^k} \end{array} \right\}$

定义 $\hat{\mathbb{Z}}_p \xrightarrow{f} R$ f 正如上. 这是一个环同态，

反之，给定 $\alpha = (\alpha_1, \alpha_2, \cdots) \in R$，令 $a_0 = \alpha_0$，$a_1 = (\alpha_1 - \alpha_0)/p$，

$a_2 = (\alpha_2 - \alpha_1)/p^2$，$\cdots$ 令 $a = (a_0, a_1, a_2, \cdots)$ 由此存在

$g: R \longrightarrow \hat{\mathbb{Z}}_p$，$fg = gf = id. \Rightarrow f$ 是一个环同构.

注：任正整数的 p 进制形式对应 $\hat{\mathbb{Z}}_p$ 的元素. $\hat{\mathbb{Z}}_p$ 中元素称成

p-adic 整数，对于负整数

$-1=(p-1)\cdot\frac{1}{(1-p)}=(p-1)+(p-1)p+(p-1)p^2+\cdots \quad \in\hat{\mathbb{Z}}_p$

给定一个有理数 $\frac{a}{b}$ 若 $p\nmid b$，则 $\frac{a}{b}\in\hat{\mathbb{Z}}_p$

这是因为 $b\in\hat{\mathbb{Z}}_p$，$p\nmid b\Rightarrow b=a_0+a_1p+\cdots \quad a_0\neq 0$

$\Rightarrow b$ 在 $\hat{\mathbb{Z}}_p$ 中可逆，逆元 $=\frac{1}{b}\in\hat{\mathbb{Z}}_p$.

但是 $\frac{1}{p}\notin\hat{\mathbb{Z}}_p \Longrightarrow$ 引出 $\hat{\mathbb{Q}}_p$

(4) 只需证任一元 $x\neq 0\in\hat{\mathbb{Q}}_p$ 有逆元.

$x=a_{-n}p^{-n}+a_{-n+1}p^{-n+1}+\cdots+a_{-1}p^{-1}+a_0+a_1p+\cdots$

$a_{-n}\neq 0$.

~~令 $y=b$~~ 令 $y=b_{-n}p^{-n}+b_{-n+1}p^{-n+1}+\cdots+b_0+b_1p+\cdots$

~~$xy=1\Leftrightarrow a_{-n}b_{-n}$~~ $p^nx=a_{-n}+a_{-n+1}p^1+a_{-n+2}p^2+\cdots+a_0p^n+\cdots$

因为 $0<a_{-n}<p$，则 p^nx 有逆，设为 y $\quad p^nx\cdot y=1$

$\Rightarrow x$ 的逆是 p^ny.

注：存在环单同态：$\mathbb{Q}\longrightarrow\hat{\mathbb{Q}}_p$，从而 $\mathbb{Q}$ 是 $\hat{\mathbb{Q}}_p$ 的子域

(5) 设 $I\neq\{0\}$ 是 $\hat{\mathbb{Z}}_p$ 的一个理想，$\alpha\in I$，满足 α 的长度极大 $=\|\alpha\|=p^{-k}$ $\quad k\geq 0$，$\alpha=p^k(a_k+a_{k+1}p+\cdots)$，$a_k+a_{k+1}p+\cdots$ 是可逆元，则 $\underset{(\alpha)}{\alpha\hat{\mathbb{Z}}_p}=p^k\mathbb{Z}_p\subset I$，若存在 $\beta\in I$，$\beta\notin(\alpha)$

$\beta = p^{\ell}(b_\ell + b_{\ell+1}p + \cdots)$ ~~~~ $\ell \geq k \Rightarrow \beta \in p^k\mathbb{Z}_p$.

因此$\hat{\mathbb{Z}}_p$中非零理想形如$p^k\mathbb{Z}_p$

(6) $\forall \alpha \in \hat{\mathbb{Z}}_p$, $\forall \varepsilon > 0$, $\exists$足够大$k>0$, $p^{-k} < \varepsilon$

令$\alpha = a_0 + a_1 p + \cdots + a_{k-1}p^{k-1} + a_k p^k + \cdots$

$\alpha_0 = a_0 + a_1 p + \cdots + a_{k-1}p^{k-1} \in \mathbb{Z}$

则$|\alpha - \alpha_0|_p = |a_k p^k + \cdots|_p \leq p^{-k} < \varepsilon$

3. (1) 设$R = \langle a \rangle$且$a^2 = ka$, $\forall x, y \in R$ 令$x = ma$, $y = na$. $xy = (mn)a^2 = yx$ 设$N = \langle sa \rangle = \{\cdots, -2sa, -sa, 0, sa, 2sa, \cdots\}$是$R$的子加群, 令$x = ma$, $y = nsa$

则$xy = mnsa^2 = (mnk)sa \in N$.

(2) 设$n = p_1^{s_1} \cdots p_m^{s_m}$ p_i互异素数. $R = \{0, a, 2a, \cdots, (n-1)a\}$ $a^2 = ka$

ra是幂等元 $\Leftrightarrow (ra)^2 = ra \Leftrightarrow (kr^2 - r)a = 0 \Leftrightarrow n \mid kr^2 - r$

即$kr^2 - r \equiv 0 \pmod{n}$, $n \mid kr^2 - r$, $\Rightarrow p_i^{s_i} \mid (kr-1)r$ $i = 1, \cdots, m$

~~若$p_i \nmid k$~~ $\Rightarrow p_i^{s_i} \mid kr-1$或$p_i^{s_i} \mid r$,

若$p_i \mid k$, 则$p_i^{s_i} \mid r$

若$p_i \nmid k$, 则$(p_i^{s_i}, k) = 1$, $\exists u, v$, $p_i^{s_i}u + kv = 1$

$(v, p_i^{s_i})=1$，则 $p_i^{s_i} \mid v(kv-1)=kv^2-v$

设 $p_{i_1},\cdots,p_{i_\ell} \mid k$，$p_{i_{\ell+1}},\cdots,p_{i_m} \nmid k$，则 $v = x\cdot p_{i_1}^{s_{i_1}}\cdots p_{i_\ell}^{s_{i_\ell}}$

x 的选择，对于每个 $p_{i_{\ell+1}},\cdots,p_{i_m}$ 有两种选择：$p_{i_j}^{s_{i_j}}$ 或 v $j=\ell+1,\cdots,m$

$\Rightarrow$ x 的选择共 $2^{m-\ell}$ 个.

(3) 首先，n 阶循环环总存在：$\mathbb{Z}_n=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{n-1}\}=\langle\bar{1}\rangle$

设 $R=\langle a\rangle$ 是 n 阶循环环，$a^2=ka$，$1\le k\le n$，R 作为循环群，有 $\varphi(n)$ 个生成元：$r_1a, r_2a,\cdots,r_{\varphi(n)}a$

其中 $r_1=1$，$1\le r_i<n$，$(r_i,n)=1$ $\quad i=1,\cdots,\varphi(n)$.

设 $(k,n)=d$，则存在 $u,s\in\mathbb{Z}$，使得 $ku+ns=d$；可以选择合适的 u，使得 $(u,n)=1$，则 $u=r_i$ $\exists i=1,\cdots,\varphi(n)$ (见注①)

$(r_ia)^2=(r_ik)(r_ia)=(d-ns)(r_ia)=d(r_ia)$

对 n 阶循环环，总存在 r_ia 及 n 的正因子 d，使上式成立.

$\Rightarrow$ 互不同构的 n 阶循环环 $\le T(n)$ 个.

设 $R=\langle a\rangle$ 和 $\bar{R}=\langle b\rangle$ 是两个 n 阶循环环，

$a^2=ka$，$b^2=hb$，$\quad k\mid n$，$h\mid n$，$1\le k,h\le n$，$h\ne k$.

下证 R 和 $\bar{R}$ 没有环同构.

$kr_1,\cdots,kr_{\varphi(n)}$ 与 $hr_1,hr_2,\cdots,hr_{\varphi(n)}$ 中对模 n 无同余的.

否则 设 $kr_i = nq_1 + r$，$hr_j = nq_2 + r$ $0 \le r < n$

则 $k \mid r$，$h \mid r \Rightarrow k \mid hr_j$ 但 $(r_j, n) = 1$，$k \mid n \Rightarrow (k, r_j) = 1$

从而 $k \mid h$ 同理 $h \mid k \Rightarrow h = k$ 矛盾！

注① 设 $(k, n) = d$，$\exists$ 整数 r, s $(r, n) = 1$，$1 \le r \le n$

$kr + ns = d$

这是因为 $k = dk_1$，$n = dn_1$，$(k_1, n_1) = 1$ $\exists r_1, s_1$

$k_1 r_1 + n_1 s_1 = 1 \Rightarrow k_1(r_1 + n_1 t) + n_1(s_1 - k_1 t) = 1$ $\forall t \in \mathbb{Z}$.

$\exists t_0$，$r_1 + n_1 t_0 = p$ 是一个素数（Dirichlet 定理）$(r_1, n_1) = 1$.

$k_1 p + n_1(s_1 - k_1 t_0) = 1$ 令 $s_1 - k_1 t_0 = y_0$

$\Rightarrow kp + ny_0 = d$ 令 $p = nq + r$

$\Rightarrow kr + ns = d$ $(r, n) = 1$ $s = y_0 + kq$.

② 证明思路 $R = \langle a \rangle$ 选择合适的生成元 $b = r_i a$，$R = \langle b \rangle$

$b^2 = db$ $d \mid n \Rightarrow$ 至多 $T(n)$ 个不同构的循环环.

第二步：确有 $T(n)$ 个：(1) 互异的 n 的因子对应的循环环不同构.

(2) $\forall 1 \le k < n$，$R = \langle a \rangle$ $a^2 = ka$

$k = 1$ $R \longrightarrow \mathbb{Z}_n$ 同构.

$k > 1$ $R \hookrightarrow \mathbb{Z}_{nk}$ 嵌入.

$a \longmapsto k$

4. 证明：设τ不是反同态，则存在$c,d\in R$，$\tau(cd)=\tau(c)\tau(d)\neq\tau(d)\tau(c)$.

$\forall x\in R$，若$\tau(cx)=\tau(x)\tau(c)$则

$\tau[c(d+x)]=\tau(cd+cx)=\tau(cd)+\tau(cx)=\tau(c)\tau(d)+\tau(x)\tau(c)$

另一方面，若$\tau[c(d+x)]=\tau(d+x)\tau(c)=\tau(d)\tau(c)+\tau(x)\tau(c)$

$\Rightarrow\tau(c)\tau(d)=\tau(d)\tau(c)$与假设矛盾！因此，

$\tau[c(d+x)]=\tau(c)\tau(d+x)=\tau(c)\tau(d)+\tau(c)\tau(x)$.

则有$\tau(x)\tau(c)=\tau(c)\tau(x)$. 同理$\tau(xd)=\tau(x)\tau(d)$.

$$\Downarrow$$

$\tau(cx)=\tau(c)\tau(x)$.

$\forall x,y\in R$ 若$\tau(xy)=\tau(y)\tau(x)$，仿照以上证明，

$\forall z\in R$，$\tau(xz)=\tau(z)\tau(x)$，$\tau(zy)=\tau(y)\tau(z)$.

考虑$\tau[(x+c)(y+d)]=\tau(xy)+\tau(x)\tau(d)+\tau(c)\tau(y)+\tau(c)\tau(d)$

另一方面，若$\tau[(x+c)(y+d)]=\tau(y+d)\tau(x+c)$

同样讨论，与上式矛盾！因此$\tau[(x+c)(y+d)]=\tau(x+c)\tau(y+d)$

$\Rightarrow\tau(xy)=\tau(x)\tau(y)$