环

1. 在$\mathbb{Z}\times\mathbb{Z}$中定义加法和乘法: 对于任意$(a,b),(c,d)\in\mathbb{Z}\times\mathbb{Z}$,

$$(a,b)+(c,d)=(a+c,b+d)$$
$$(a,b)(c,d)=(ac,bd)$$

证明$\mathbb{Z}\times\mathbb{Z}$是一个有零因子的交换环.

证明:

(a) $\mathbb{Z}\times\mathbb{Z}$对加法构成Abel群;

(b) $\mathbb{Z}\times\mathbb{Z}$对乘法构成交换半群;

(c) 分配律.

零因子$(0,a),(b,0),\ a,b\neq 0$.

2. 证明$(\mathbb{Q}(\sqrt{2}),+,\times)$是整环也是域.

证明:

(a) $(\mathbb{Q}(\sqrt{2}),+)$是Abel群;

(b) $(\mathbb{Q}(\sqrt{2})\setminus\{0\},+)$是Abel群;

(c) 分配律.

域是整环. (先说明无零因子, 再证明是域亦可)

3. 设C是实数域$\mathbb{R}$上的所有实函数构成的集合, 定义加法与乘法为: 对于任意$f,g\in C,\ x\in\mathbb{R}$,

$$(f+g)(x)=f(x)+g(x)$$

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

试问C对于上述加法、乘法是否构成环?

解: 不构成环. 令$f(x)=x, g(x)=x^2, h(x)=x^2$, 有$h(f+g)(x)=(x+x^2)^2, (hf)(x)+(hg)(x)=x^2+x^4$, 不满足分配律.

4. 设在非空集合R中定义了加法与乘法两种运算, 且

1) R对加法为群;

2) R对乘法为幺半群;

3) 加法与乘法间有分配律.

证明R为幺环.

证明: 需要证明加法满足交换律. $\forall a,b\in R$, 有$(a+1)(b+1)=a(b+1)+(b+1)=ab+a+b+1,\ (a+1)(b+1)=(a+1)b+(a+1)=ab+b+a+1$, 故$a+b=b+a$.

5. 若环R的非零元素e满足$e^2=e$, 则称e为**幂等元**. 证明若无零因子环R 有幂等元e, 则R为整环, 且e为R的幺元.

证明: 即要证明R中存在幺元, 且幺元为e. $e^2=e\Rightarrow e^2a=ea\Rightarrow e(ea-a)=0$, 由于$R$ 中无零因子, 于是$ea-a=0$, 即$ea=a$, 同理可证$ae=a$. 故R是整环, e 是幺元.

6. 设R是交换整环, $R[x]$是R上的一元多项式环, $f, g \in R[x]$. 证明deg$fg =$ deg$f +$ deg$g$.

证明: 设$f(x) = \sum\limits_{i=0}^{n} a_i x^i, g(x) = \sum\limits_{j=0}^{m} b_j x^j, (a_n, b_m \neq 0)$, 即deg$f = n$, deg$g = m$. $f(x)g(x) = \sum\limits_{k=0}^{m+n} (\sum\limits_{i+j=k} a_i b_j x^k)$. 因为$R$是交换整环, 所以$a_n b_m \neq 0$, 从而$\deg(fg) = m + n =degf+degg$.

7. 证明交换环R的任意一族理想的交是R的理想.

证明: 设$I_1, \ldots, I_k$为R的理想.

① $0 \in I_j \Rightarrow 0 \in \cap_{j=1}^{k} I_j$.

② $\forall a, b \in \cap_{j=1}^{k} I_j$, 有$a, b \in I_j$. 因为$I_j$都是理想, 所以有$a - b \in I_j$, 故$a - b \in \cap_{j=1}^{k} I_j$.

③ $\forall r \in R, a \in \cap_{j=1}^{k} I_j. \therefore a \in I_j, \because I_j$都是理想$, \therefore ra \in I_j, \therefore ra \in \cap_{j=1}^{k} I_j$.

综上, $\cap_{j=1}^{k} I_j$仍是理想.

8. 设R是环, $a \in R$. 若$\exists m \in \mathbb{N}$使得$a^m = 0$, 则称a是一个**幂零元**. 证明交换环R的幂零元集合是R的理想.

证明: 设幂零元集合为I.

① $0^m = 0, \therefore 0 \in I$.

② $\forall a, b \in I, \exists m, n,$ s.t. $a^m = 0, b^n = 0$, 有$(a-b)^{n+m} = \sum C_{n+m}^{k} a^k (-b)^{n+m-k}$, 当$k \geq m$时, $a^k = 0$; 当$k < m$时, $(-b)^{n+m-k} = 0, \therefore a - b \in I$.

③ $\forall r \in R, a \in I, \exists m,$ s.t. $a^m = 0$, 有$(ra)^m = r^m a^m = 0, \therefore ra \in I$.

综上, I是R的理想.

9. 证明$\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$.

证明:

(a) $\mathbb{Z}[x]/\langle x\rangle = \{[a]|a\in\mathbb{Z}\}$. 设映射$\phi:\mathbb{Z}[x]/\langle x\rangle \to \mathbb{Z}, [a]\mapsto a$. 证明映射$\phi$是单射、满射、满足同态性.

(b) 设映射$\varphi:\mathbb{Z}[x]\to\mathbb{Z}, f(x)\mapsto f(0)$. $\forall a\in\mathbb{Z}, \exists f(x)\in\mathbb{Z}[x]$, s.t. $\varphi(f(x)) = a, \therefore \varphi$是满射. $\forall f(x), g(x)\in\mathbb{Z}[x]$, 有$\varphi(f(x)+g(x)) = f(0)+g(0) = \varphi(f(x))+\varphi(g(x)), \varphi(f(x)g(x)) = f(0)g(0) = \varphi(f(x))\varphi(g(x))$, 故$\varphi$是满同态映射. 易知ker$\varphi = \{f(x)|\varphi(f(x)) = 0\} = \langle x\rangle$, 根据同态基本定理, $\mathbb{Z}[x]/\langle x\rangle \cong \mathbb{Z}$.

10. 证明$u=\sqrt{2}+\sqrt{3}$在$\mathbb{Q}$上是代数的, 并求出$\mathbb{Q}[x]$中的理想I, 使得$\mathbb{Q}[u]\cong\mathbb{Q}[x]/I$.

证明: $\because u^4-10u^2+1=0, \therefore u$是代数元.

设$\varphi:\mathbb{Q}[x]\to\mathbb{Q}[u], f(x)\mapsto f(u)$.

① 易知φ是满射.

② $\varphi(f(x)+g(x)) = f(u)+g(u) = \varphi(f(x))+\varphi(g(x)), \varphi(f(x)g(x)) = f(u)g(u) = \varphi(f(x))\varphi(g(x))$

故φ是满同态. 又知ker$\varphi = \{f(x)|\varphi(f(x))=0\} = \langle x^4-10x^2+1\rangle$, 根据同态基本定理, $\mathbb{Q}[x]/\langle x^4-10x^2+1\rangle \cong \mathbb{Q}[u]$. 故所求的$I = \langle x^4-10x^2+1\rangle$

11. 设$\omega = -\frac{1}{2}+\frac{\sqrt{-3}}{2}$, 证明$\mathbb{Q}[\omega]\cong\mathbb{Q}[x]/\langle x^2+x+1\rangle$.

证明: 证明过程类似于上题.

12. 证明$\sqrt{-3}$是$\mathbb{Z}[\sqrt{-3}]$的素元素.

证明: 定义范数$N(a+b\sqrt{-3}) = a^2+3b^2, a,b \in \mathbb{Z}$. 若$\sqrt{-3} \mid \alpha\beta$, 则$3 \mid N(\alpha)N(\beta)$, 从而$3 \mid N(\alpha)$或$3 \mid N(\beta)$. $\mathbb{Z}[\sqrt{-3}]$ 中范数为3 的只有$\sqrt{-3}$或$-\sqrt{-3}$, 所以$\sqrt{-3} \mid \alpha$或$\sqrt{-3} \mid \beta$. 故$\sqrt{-3}$ 是$\mathbb{Z}[\sqrt{-3}]$的素元素.

13. 在高斯整数环中, 对2,3,5进行素元素分解.

解: 因为高斯整数环是唯一析因环, 所以素元素与不可约元素是等价的, 且若可分解, 分解方式在相伴的意义下唯一. 单位群$U = \{1, -1, i, -i\}$.

(a) $2 = (1+i)(1-i)$. 需证明$1+i$和$1-i$是不可约元素. 假设$1+i$可约, 则必有非平凡真因子$a+bi$, s.t. $(a+bi)\cdot\alpha = 1+i$. 两边取范数有$(a^2+b^2)N(\alpha) = 2$, 那么$a^2+b^2 = 1$或2.

若$a^2+b^2 = 1$, 则$a+bi \in U$, 是平凡因子, 矛盾.

若$a^2+b^2 = 2$, 则$N(\alpha) = 1$, 则$\alpha \in U$, 从而$a+bi \sim 1+i$, 不是真因子, 矛盾.

故$1+i$为不可约元素. 同理可证$1-i$为不可约元素.

(b) $5 = (2+i)(2-i) = (1-2i)(1+2i)$. 证明过程类似. **注：这两个分解方式在相伴意义下是一种, 因为$\mathbf{2+i \sim 1-2i}$, $\mathbf{2-i \sim 1+2i}$.**

(c) 3是素元素. 证明过程类似.

14. 证明$\mathbb{Z}[\sqrt{-3}]$不是唯一析因环.

证明: $4 = (1+\sqrt{-3})(1-\sqrt{-3}) = 2\times 2$. 易证$1+\sqrt{-3}, 1-\sqrt{-3}, 2$都是$\mathbb{Z}[\sqrt{-3}]$中的不可约元素, 且2与$1+\sqrt{-3}$不相伴, 故$\mathbb{Z}[\sqrt{-3}]$不是唯一析因环.

15*. 设R是主理想整环, I是R的理想, 且$I \neq \{0\}$. 试证:

(1) R/I的每个理想都是主理想;

(2) R/I中仅有有限多个理想.

证明:

*自然同态: 设I是R的理想, π是R到商环R/I的同态映射, 该同态映射被称作自然同态, ker$\pi = I$.

*利用选做题第1题的结论可知, π建立了R中包含ker$\pi = I$的子环与R/I的子环的一一对应, 把理想对应到理想.

(1) 由于R是主理想整环, 设$I = \langle a \rangle, a \in R$, R/I中的每个理想与R中每个包含$\langle a \rangle$的理想一一对应. 设$\langle b \rangle \supseteq \langle a \rangle$, 下面观察$\langle b \rangle$对应的$R/I$中的理想是什么. $\langle b \rangle = \{xb | x \in R\}, \pi(\langle b \rangle) = \{\pi(xb) | x \in R\} = \{xb + I | x \in R\}$. 已知商环$R/I$中有运算$xb + I = (x + I)(b + I)$, 于是$\pi(\langle b \rangle) = \{(x + I)(b + I) | x \in R\} = \{(x + I)(b + I) | x + I \in R/I\} = \langle b + I \rangle$是主理想, 故$R/I$的每个理想都是主理想.

(2) 在R中, 若$\langle b \rangle \supseteq \langle a \rangle$, 则$b \mid a$. 因为$R$是主理想整环, 所以$R$是唯一析因环, 故$a$在相伴意义下只有有限个因子, 从而$R$只有有限个理想, 于是$R/I$也只有有限多个理想.

16. 设R是交换整环, 但不是域. 证明$R[x]$不是主理想整环.

证明: 设$a \in R$且$a \notin U$. 观察理想$\langle a, x \rangle$. 假设$\langle a, x \rangle$是主理想, $\langle a, x \rangle = \langle b \rangle$, 那么$b \mid a, b \mid x$. $b \mid a \Rightarrow b \in R, b \in R, b \mid x \Rightarrow b \sim 1$, 于是$\langle b \rangle = \langle 1 \rangle = R$. 显然$\langle a, x \rangle \neq R$, 故假设不成立.

17. 证明$R=\{a+\frac{b}{2}(1+\sqrt{-3})|a,b\in\mathbb{Z}\}$为Euclid环.

证明: 观察$a+\frac{b}{2}(1+\sqrt{-3})=\frac{1}{2}(2a+b+b\sqrt{-3})$, 令$c=2a+b, d=b$, 于是有$R=\{\frac{1}{2}(c+d\sqrt{-3})|c,d\in\mathbb{Z}, c\equiv d \bmod 2\}$.

设$\alpha=\frac{1}{2}(a+b\sqrt{-3}), a\equiv b \bmod 2, \quad \beta=\frac{1}{2}(c+d\sqrt{-3}), c\equiv d \bmod 2$, 定义$\delta(\alpha)=\frac{1}{4}(a^2+3b^2)\in\mathbb{Z}^+$, $\delta(\alpha\beta)=\delta(\alpha)\delta(\beta)$. 若$\beta\neq 0$, 则有

$$\alpha\beta^{-1}=\frac{a+b\sqrt{-3}}{c+d\sqrt{-3}}=u+v\sqrt{-3},\ u,v\in\mathbb{Q}.$$

于是有

$$u=e+\epsilon,\ v=f+\eta,\quad e,f\in\mathbb{Z},\quad 0\leq\epsilon,\eta\leq\frac{1}{2}.$$

令$\gamma=\beta(\epsilon+\eta\sqrt{-3})=\alpha-\beta(e+f\sqrt{-3})\in R$, 于是

$$\alpha=\beta(e+f\sqrt{-3})+\gamma.$$

若$\epsilon=\eta=\frac{1}{2}$或0, 则$u+v\sqrt{-3}\in R, \beta\mid\alpha$. 否则, 不妨设$k_1<\frac{1}{2}$, 于是$\delta(\gamma)=(\epsilon^2+3\eta^2)\delta(\beta)<\left(\frac{1}{4}+\frac{3}{4}\right)\delta(\beta)=\delta(\beta)$. 由此可知$R$是Euclid环.

18. 设R为Euclid环, 且$\delta(ab)=\delta(a)\delta(b)$. 证明$a\in U\Leftrightarrow\delta(a)=\delta(1)$.

证明: 由于$1a=a$, 所以$\delta(1a)=\delta(1)\delta(a)=\delta(a)$, 故$\delta(1)=1$.

"$\Rightarrow$": 若$a\in U$, 则$\delta(aa^{-1})=\delta(a)\delta(a^{-1})=\delta(1)=1$, 所以$\delta(a)=1$.

"$\Leftarrow$": 若$\delta(a)=1, 1=a_0a+r, \delta(r)<\delta(a)=1$, 故$\delta(r)=0$, 即$r=0$, 因此$a\in U$.

19. 试证$\langle x\rangle$是$\mathbb{Z}[x]$中的素理想而非极大理想.

证明: 教材(机械工业出版社)定理7.4.1. 因为$\mathbb{Z}[x]/\langle x\rangle\cong\mathbb{Z}$ 是整环而不是域, 所以$\langle x\rangle$是$\mathbb{Z}[x]$中的素理想而非极大理想.

20. 取$m \in \mathbb{N}, m > 1$, 令$A = \{f(x) | f(x) \in \mathbb{Z}[x], m | f(0)\}$, 证明:

(1) A是$\mathbb{Z}[x]$的理想;

(2) $\langle x \rangle \subset A \subset \mathbb{Z}[x]$;

(3) m为素数时, A是素理想.

证明:

(1) $m \mid 0$, 所以$0 \in A$. 设$f(x), g(x) \in A, h(x) \in \mathbb{Z}[x]$, 有$m \mid f(0), m \mid g(0)$, 从而有

$$m \mid f(0) - g(0) = (f - g)(0), \qquad m \mid h(0)f(0) = (hf)(0),$$

即$f(x) - g(x), h(x)f(x) \in A$. 故$A$是理想.

(2) $\langle x \rangle = \{f(x) \cdot x | f(x) \in \mathbb{Z}[x]\}$. 对于$\forall f(x) \cdot x \in \langle x \rangle$有$m | f(0) \cdot 0$, 所以$\langle x \rangle \subseteq A$. 而$x + m \in A$, 但$x + m \notin \langle x \rangle$, 所以$\langle x \rangle \neq A$. 又因为$1 \in \mathbb{Z}[x], m \nmid 1$, 所以$1 \notin A$, 所以$A \neq \mathbb{Z}[x]$. 综上$\langle x \rangle \subset A \subset \mathbb{Z}[x]$.

(3) 记π为$\mathbb{Z}$到$\mathbb{Z}_m$的自然同态(自然同态是满同态). 设映射$\varphi : \mathbb{Z}[x] \to \mathbb{Z}_m$, $f(x) \mapsto \pi(f(0))$. 于是有

① $\varphi(f(x) + g(x)) = \pi(f(0) + g(0)) = \pi(f(0)) + \pi(g(0)) = \varphi(f(x)) + \varphi(g(x))$

② $\varphi(f(x)g(x)) = \pi(f(0)g(0)) = \pi(f(0))\pi(g(0)) = \varphi(f(x))\varphi(g(x))$

③ $\varphi(a) = \pi(a), \quad a \in \mathbb{Z} \subset \mathbb{Z}[x]$

因此φ是满同态. $\ker\varphi = \{f(x) \in \mathbb{Z}[x] | \varphi(f(x)) = \pi(f(0)) = 0 + m\mathbb{Z}\} = \{f(x) \in \mathbb{Z}[x] | m \mid f(0)\} = A$, 故$\mathbb{Z}[x]/A \cong \mathbb{Z}_m$. 当$m$为素数时, $\mathbb{Z}_m$为整环, 从而$\mathbb{Z}[x]/A$也是整环, 故此时A为素理想.

选做题

1. 设f是环R到环R'的同态映射, $K = \ker f$, 证明:

(1) f建立了R中包含K的子环与R'的子环的一一对应;

(2) f把理想映射为理想;

(3) 若I是R的理想且$K \subseteq I$, 则$R/I \cong R'/f(I)$.

2. (中国剩余定理) 若R的理想I, J满足$I + J = R$, 则称I, J互素. $I_1, \ldots, I_n$是R中两两互素的理想, 证明:

$$R/\cap_{i=1}^{n} I_i \cong R/I_1 \times \cdots \times R/I_n$$

3. 设R是一个无限的主理想整环. 试证若R中只有有限个可逆元, 则R中有无限多个素理想.

4. 证明$\mathbb{Z}_p[x]$(p 为素数)有无限多个不可约多项式.