NIS2312-01 Fall 2023-2024

信息安全的数学基础 (1)

Answer 12-13

2023 年 11 月 3 日

Assignment 12

Problem 1

假设 D 是一个有理数且不是完全平方数, 定义集合

$$\mathbf{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbf{Q}\}.$$

那么集合 $\mathbf{Q}(\sqrt{D})$ 在通常数的加法乘法的运算下是否构成环, 如果构成环是否构成 $\mathbf{C}$ 的子环?

解:

(1) 显然 $\mathbf{Q}(\sqrt{D})$ 是非空集合;

(2) 验证加法的封闭性: 对任意 $x = a + b\sqrt{D}, y = c + d\sqrt{D} \in \mathbf{Q}(\sqrt{D})$, 我们有 $x + y = (a + c) + (b + d)\sqrt{D} \in \mathbf{Q}(\sqrt{D})$;

(3) 验证加法的结合律: 对任意 $x, y, z \in \mathbf{Q}(\sqrt{D})$ 有 $x + (y + z) = (x + y) + z$ 成立;

(4) 单位元显然是 0: 对任意 $x \in \mathbf{Q}(\sqrt{D})$, 有 $x + 0 = 0 + x = x$;

(5) 任意 $x \in \mathbf{Q}(\sqrt{D})$ 的负元是 $-x$;

(6) 通常数的加法显然满足交换律;

(7) 验证乘法的封闭性: 对任意 $x = a + b\sqrt{D}, y = c + d\sqrt{D} \in \mathbf{Q}(\sqrt{D})$, 我们有 $xy = (ac + bdD) + (ad + bc)\sqrt{D} \in \mathbf{Q}(\sqrt{D})$;

(8) 通常数的加法和乘法满足分配律.

故 $\mathbf{Q}(\sqrt{D})$ 在通常数的加法乘法的运算下构成环.

又因为 $\mathbf{C}$ 关于通常数的加法和乘法构成环, $\mathbf{Q}(\sqrt{D}) \subseteq \mathbf{C}$ 且 $\mathbf{Q}(\sqrt{D})$ 关于通常数的加法和乘法构成环, 故 $\mathbf{Q}(\sqrt{D})$ 构成 $\mathbf{C}$ 的子环.

Problem 2

证明在任意无零因子有单位元的有限交换环中, 非零元素均是单位 (本质上是证明有限整环是域).

解: 先证明对任意非零 $c \in R$, 有 $cR = R$: 显然 $cR \subseteq R$, 假设 $|cR| < |R|$, 则有 $cr_i = cr_j$, 其中 $r_i, r_j \in R$, 即 $r_i = r_j$, 因此 $|cR| = |R|$, 故 $cR = R$. 又因为 R 中有乘法单位元, 则 $\exists d \in R$, 有 $cd = e$, 即 c 是单位, 所以非零元素均是单位.

Problem 3

如果一个元素 $x \in R$ 满足等式 $x^n = 0, n \in \mathbf{Z}^+$, 那么称其幂零元 (简单的例子是线性代数中的幂零矩阵). 证明: 在交换环 R 中, 有 $x \in R$ 是幂零元, 那么:

(1) x 不是零元素就是零因子;

(2) rx 仍然是幂零元, 其中 $r \in R$;

(3) $1+x$ 是单位 (hint: 构造系数在 R 上的多项式 $f(x)$ 使得 $(1+x)f(x) = 1+g(x^n) = 1$ 即可).

解:

(1) 因为 $x^n = x \cdot x^{n-1} = 0$, 显然 $x = 0$ 满足等式. 假设 $x \neq 0$, 则 $x^{n-1} = 0$ 或者 x 是零因子, 以此类推, 得到 $x = 0$ 或者 x 是零因子.

(2) 显然 $(rx)^n = r^n x^n = 0$

(3) 显然 $(1+x)(1-x)(1+x^2)(1+x^4)\cdots(1+x^{2^m}) = 1 - x^{2^{m+1}} = 1$, 其中 $2^{m+1} > n$, 且 $(1-x)(1+x^2)(1+x^4)\cdots(1+x^{2^m}) \in R$, 因此 $1+x$ 是单位.

(4) 也可 $(1+x)(1-x+x^2-x^3+\cdots+(-1)^{n-1}x^{n-1}) = 1+(-1)^n x^n = 1$

Problem 4

证明: 如果环 R 的元素满足 $r^2 = r$, 其中 $r \in R$, 那么 R 是一个交换环.

解: 令 $r = x + y$ 其中 $x, y, r \in R$, 那么 $r^2 = (x+y)^2 = x^2 + xy + yx + y^2 = x+xy+yx+y$, 即 $xy+yx = 0$. 同时将 $y = x$ 带入 $xy+yx = 0$, 有 $2x^2 = 2x = x+x = 0$, 因为 x 的任意性, 可以得到 $xy + xy = 0$. 综上, $xy = yx$, 那么 R 是一个交换环.

Assignment 13

Problem 1

设 S 是 R 的子环, I 是 R 的理想, 且 $I \subseteq S$. 证明:

(1) S/I 是 R/I 的子环;

(2) 如果 S 是 R 的理想, 则 S/I 是 R/I 的理想.

解:

(1) S/I 显然是非空子集. 设 $x+I, y+I \in S/I$, 则有 $x, y \in S$, 根据 S 是 R 的子环可知 $x-y, xy \in S$, 因此有

$$(x+I)-(y+I) = (x-yu)+I \in S/I \text{ and } (x+I)(y+I) = xy+I \in S/I,$$

故 S/I 是 R/I 的子环.

(2) 设 $x+I \in S/I$ 和 $r+I \in R/I$, 则有 $x \in S$, 根据 S 是 R 的理想可知 $rx, xr \in S$, 因此有

$$\begin{aligned}(r+I)(x+I) &= rx+I \in S/I\\ (x+I)(r+I) &= xr+I \in S/I,\end{aligned}$$

结合 S/I 是 R/I 的子环可知 S/I 是 R/I 的理想.

Problem 2

设 R 是交换环, I 是 R 的理想. 令

$$\sqrt{I} = \{r \in R \mid \exists n \in N, \text{ 使 } r^n \in I\}.$$

证明: $\sqrt{I}$ 是 R 的理想.

解: 显然 $\sqrt{I}$ 集合非空. 设 $a, b \in \sqrt{I}$, 故 $\exists m, n \in \mathbf{Z}$ 使得 $a^m, b^n \in I$. 因此对任意的 $r \in R$, 都有

$$\begin{aligned}(a-b)^{m+n} &= a^{m+n} + \sum_{k=1}^{m+n-1} (-1)^k \mathrm{C}_{m+n}^k a^{m+n-k} b^k + (-1)^{m+n} b^{m+n} \in I\\ (ra)^m &= r^m a^m \in I\\ (ar)^m &= a^m r^m \in I,\end{aligned}$$

所以 $a-b, ra, ar \in \sqrt{I}$, 因此 $\sqrt{I}$ 是 R 的理想.

Problem 3

设 R_1, R_2 是环, $R = R_1 \oplus R_2$. 记 $R_1' = \{(a,0) \in R \mid a \in R_1\}$, $R_2' = \{(0,b) \in R \mid b \in R_2\}$. 证明:

(1) R_1', R_2' 是 R 的理想;

(2) $R = R_1' + R_2'$.

解:

(1) 对任意的 $x = (a,0), y = (b,0) \in R_1', r = (r_1, r_2) \in R$, 有

$$\begin{aligned} x - y &= (a-b, 0) \in R_1' \\ rx &= (r_1 a, 0) \in R_1' \\ xr &= (ar_1, 0) \in R_1'. \end{aligned}$$

所以 R_1' 为 R 的理想. 同理可证 R_2' 为 R 的理想.

(2) 对任意的 $(a,b) \in R$, 有 $(a,b) = (a,0) + (0,b) \in R_1' + R_2'$, 所以 $R = R_1' + R_2'$.

Problem 4

设 $R = \mathbf{Z}$ 为整数集. 对任意的 $x, y \in R$, 规定

$$x \oplus y = x + y + 1, \quad x \odot y = xy + x + y.$$

(1) 证明: $(R, \oplus, \odot)$ 构成一个环;

(2) 证明: R 与整数环 $\mathbf{Z}$ 同构.

解:

(1) (a) 显然 $\oplus$ 满足封闭性;

(b) 对任意的 $x, y \in R$, 有

$$\begin{aligned} x \oplus y &= x + y + 1 = y + x + 1 = y \oplus x, \\ x \odot y &= xy + x + y = yx + y + x = y \odot x, \end{aligned}$$

所以 R 的两个运算都满足交换律;

(c) 对任意的 $x, y, z \in R$, 有

$$\begin{aligned}
(x \oplus y) \oplus z &= (x + y + 1) \oplus z = (x + y + 1) + z + 1 = x + y + z + 2, \\
x \oplus (y \oplus z) &= x \oplus (y + z + 1) = x + (y + z + 1) + 1 = x + y + z + 2, \\
(x \odot y) \odot z &= (xy + x + y) \odot z = (xy + x + y)z + (xy + x + y) + z \\
&= xyz + xy + xz + yz + x + y + z, \\
x \odot (y \odot z) &= x \odot (yz + y + z) = x(yz + y + z) + x + (yz + y + z) \\
&= xyz + xy + xz + yz + x + y + z,
\end{aligned}$$

所以 R 的两个运算都满足结合律;

(d) 对任意的 $x \in R$, 有

$$x \oplus (-1) = x + (-1) + 1 = x,$$

所以 -1 为 R 的零元.

(e) 对任意的 $x \in R$, 有

$$x \oplus (-2 - x) = x + (-2 - x) + 1 = -1,$$

所以 $-2 - x$ 为 x 的负元.

(f) 对任意的 $x \in R$, 有

$$x \odot 0 = x \cdot 0 + x + 0 = x,$$

所以 0 为 R 的单位元.

(g) 对任意的 $x, y, z \in R$, 有

$$\begin{aligned}
(x \oplus y) \odot z &= (x + y + 1) \odot z = (x + y + 1)z + (x + y + 1) + z \\
&= xz + yz + x + y + 2z + 1, \\
(x \odot z) \oplus (y \odot z) &= (xz + x + z) \oplus (yz + y + z) \\
&= xz + yz + x + y + 2z + 1,
\end{aligned}$$

所以 $\odot$ 对 $\oplus$ 满足分配律. 因此 $(R, \oplus, \odot)$ 构成一个有单位元的交换环.

(2) 令

$$\begin{aligned}
\phi : R &\longrightarrow \mathbf{Z} \\
x &\longmapsto x + 1.
\end{aligned}$$

(a) 显然 ϕ 为 R 到 $\mathbf{Z}$ 的单且满映射.

(b) 对任意的 $x, y \in R$, 有

$$\begin{aligned}\phi(x \oplus y) &= \phi(x+y+1) = x+y+2 = (x+1)+(y+1)\\ &= \phi(x)+\phi(y)\\ \phi(x \odot y) &= \phi(xy+x+y) = xy+x+y+1 = (x+1)(y+1)\\ &= \phi(x)\phi(y)\end{aligned}$$

所以 ϕ 为 R 到 $\mathbf{Z}$ 的同构映射, 即 $R \cong \mathbf{Z}$.

Problem 5

设 S 为 R 的子环, I 为 R 的理想, 则 $S \cap I$ 是 S 的理想且

$$\frac{S}{S \cap I} \cong \frac{S+I}{I}.$$

解: 显然 I 为环 $S+I$ 的理想, 从而有自然同态.

$$\eta : S+I \longrightarrow (S+I)/I.$$

因而 η 在 S 上的限制

$$\begin{aligned}\eta|_S : S &\longrightarrow (S+I)/I,\\ s &\longmapsto \eta(s)\end{aligned}$$

是一个 S 到 $(S+I)/I$ 的同态. 又对任意的 $\overline{s+x} \in (S+I)/I (s \in S, x \in I)$, 有

$$\eta|_S(s) = \eta(s) = \bar{s} = \overline{s+x},$$

所以 $\eta|_S$ 为满同态. 而

$$\text{Ker } \eta|_S = \{s \in S \mid \eta(s) = \overline{0}\} = \{s \in S \mid s \in I\} = S \cap I.$$

从而 $S \cap I$ 是 S 的理想. 由环同态基本定理知, 有环同构

$$S/(S \cap I) \cong (S+I)/I.$$