补充练习 11.1

设 F 是域，R 是 F 的子环，且 $|R| \geq 2$。令 $S = \{ab^{-1} \mid a, b \in R, b \neq 0\}$，证明 S 是 F 中包含 R 的最小子域。

解答.

证明. 我们需要证明两点：(1) S 是 F 的一个子域；(2) S 是包含 R 的最小子域。

1. **证明 S 是 F 的一个子域**。
   我们使用子域判别法。

   (a) S **非空**：因为 $|R| \geq 2$ 且 R 是子环，所以 R 中必有非零元。设 $b \in R$ 且 $b \neq 0$。由于 R 是环，所以 $b \in R$。因此 $bb^{-1} = 1_F \in S$。所以 S 非空。

   (b) **对减法封闭**：任取 $x, y \in S$。则存在 $a, c \in R$ 和 $b, d \in R, b \neq 0, d \neq 0$ 使得 $x = ab^{-1}, y = cd^{-1}$。

   $$x - y = ab^{-1} - cd^{-1} = (ad - cb)(bd)^{-1}$$

   因为 R 是环，所以 $ad, cb, ad - cb \in R$。同时 $bd \in R$。又因为 F 是域，没有零因子，且 $b \neq 0, d \neq 0$，所以 $bd \neq 0$。因此，$x - y$ 的形式是 R 中一个元素乘以 R 中一个非零元的逆。故 $x - y \in S$。

   (c) **对乘法封闭**：任取 $x, y \in S$，符号同上。

   $$xy = (ab^{-1})(cd^{-1}) = (ac)(bd)^{-1}$$

   因为 R 是环，所以 $ac \in R$ 且 $bd \in R$。如前述，$bd \neq 0$。故 $xy \in S$。

   (d) **对求逆元封闭**：任取 $x \in S$ 且 $x \neq 0$。则 $x = ab^{-1}$，其中 $a, b \in R, b \neq 0$。因为 $x \neq 0$，所以必有 $a \neq 0$。

   $$x^{-1} = (ab^{-1})^{-1} = ba^{-1}$$

   因为 $b \in R$ 且 $a \in R, a \neq 0$，所以 $x^{-1} \in S$。

   根据子域判别法，(a), (b), (c), (d) 证明了 S 是 F 的一个子域。

2. **证明 S 是包含 R 的最小子域**。

   (a) **证明** $R \subseteq S$：任取 $r \in R$。因为 $|R| \geq 2$，所以 R 不是零环，故 $1_F \in R$ 且 $1_F \neq 0$。我们可以将 r 写成 $r = r \cdot 1_F = r \cdot (1_F)^{-1}$。因为 $r \in R$ 且 $1_F \in R, 1_F \neq 0$，根据 S 的定义，$r \in S$。所以 $R \subseteq S$。

(b) **证明最小性**：设 K 是 F 的任意一个包含 R 的子域，即 $R \subseteq K$。我们需要证明 $S \subseteq K$。任取 $s \in S$。根据定义，$s = ab^{-1}$，其中 $a, b \in R, b \neq 0$。因为 $R \subseteq K$，所以 $a \in K$ 且 $b \in K$。因为 K 是一个域，且 $b \in K, b \neq 0$，所以 b 在 K 中有乘法逆元 $b^{-1} \in K$。又因为 K 是域，对乘法封闭，所以 $a \cdot b^{-1} \in K$，即 $s \in K$。由于 s 是 S 中的任意元素，所以 $S \subseteq K$。

综合以上两点，S 是 F 中包含 R 的最小子域。

补充练习 11.2

在模 15 剩余类环 $\mathbb{Z}_{15} = \{\overline{0}, \overline{1}, \ldots, \overline{14}\}$ 中，求方程 $x^2 - \overline{1} = \overline{0}$ 的全部根。

解答. 方程 $x^2 - \overline{1} = \overline{0}$ 在环 $\mathbb{Z}_{15}$ 中等价于求解同余方程：

$$x^2 \equiv 1 \pmod{15}$$

因为 $15 = 3 \times 5$，且 $\gcd(3, 5) = 1$，根据中国剩余定理，上述同余方程等价于求解下面的同余方程组：

$$\begin{cases} x^2 \equiv 1 \pmod{3} \\ x^2 \equiv 1 \pmod{5} \end{cases}$$

1. **求解** $x^2 \equiv 1 \pmod{3}$，解为 $x \equiv 1, 2 \pmod{3}$。
2. **求解** $x^2 \equiv 1 \pmod{5}$，解为 $x \equiv 1, 4 \pmod{5}$。

组合解： 共有 $2 \times 2 = 4$ 种组合。

- $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases} \implies x \equiv 1 \pmod{15}$
- $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \end{cases} \implies x \equiv 4 \pmod{15}$
- $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \end{cases} \implies x \equiv 11 \pmod{15}$
- $\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \end{cases} \implies x \equiv 14 \pmod{15}$

因此，方程 $x^2 - \overline{1} = \overline{0}$ 在 $\mathbb{Z}_{15}$ 中的全部根为 $\overline{1}, \overline{4}, \overline{11}, \overline{14}$。

补充练习 11.3

设 $R = \{2z \mid z \in \mathbb{Z}\}$ 是所有偶数关于整数加法和乘法构成的环，令 $D = \{4z \mid z \in \mathbb{Z}\}$，证明 D 是 R 的理想，并给出商环 R/D 的元素。

解答.

证明. 要证明 D 是 R 的理想，需验证 $(D, +)$ 是 $(R, +)$ 的子群，且 D 对 R 的乘法有吸收性。

1. $(D, +) \leq (R, +)$：D 非空。对任意 $4z_1, 4z_2 \in D$，有 $4z_1 - 4z_2 = 4(z_1 - z_2) \in D$。故成立。
2. 吸收性：对任意 $r = 2z_1 \in R$ 和 $d = 4z_2 \in D$，有 $rd = (2z_1)(4z_2) = 4(2z_1z_2) \in D$。故成立。

因此，D 是 R 的理想。商环 R/D 的元素是 R 中元素关于 D 的陪集。

- $0 + D = D = 4\mathbb{Z}$
- $2 + D = \{2 + 4z \mid z \in \mathbb{Z}\}$

因为任何偶数 $2z$ 要么是 4 的倍数（z 为偶数），要么是 $2 + 4k$ 的形式（z 为奇数），所以商环 R/D 只有这两个元素：$R/D = \{D, 2 + D\}$。

补充练习 11.4

给出模 12 剩余类环 $\mathbb{Z}_{12} = \{\overline{0}, \ldots, \overline{11}\}$ 的所有理想及相应的商环。

解答. $\mathbb{Z}_{12}$ 的理想由 12 的正因子 $d = 1, 2, 3, 4, 6, 12$ 生成，理想为 $I_d = \langle \overline{d} \rangle$，商环为 $\mathbb{Z}_{12}/I_d \cong \mathbb{Z}_d$。

- $I_1 = \langle \overline{1} \rangle = \mathbb{Z}_{12}$。商环 $\cong \mathbb{Z}_1$。
- $I_2 = \langle \overline{2} \rangle = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}\}$。商环 $\cong \mathbb{Z}_2$。

- $I_3 = \langle \overline{3} \rangle = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}$。商环 $\cong \mathbb{Z}_3$。
- $I_4 = \langle \overline{4} \rangle = \{\overline{0}, \overline{4}, \overline{8}\}$。商环 $\cong \mathbb{Z}_4$。
- $I_6 = \langle \overline{6} \rangle = \{\overline{0}, \overline{6}\}$。商环 $\cong \mathbb{Z}_6$。
- $I_{12} = \langle \overline{12} \rangle = \{\overline{0}\}$。商环 $\cong \mathbb{Z}_{12}$。

补充练习 11.5

证明 $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$。

解答.

证明. 使用环的第一同构定理。定义求值同态 $\phi : \mathbb{R}[x] \to \mathbb{C}$ 为 $\phi(p(x)) = p(i)$。

1. **证明 ϕ 是满射**：对任意 $a+bi \in \mathbb{C}$，取多项式 $p(x) = a + bx \in \mathbb{R}[x]$，则 $\phi(p(x)) = p(i) = a + bi$。故 ϕ 是满射。
2. **确定核** $\ker(\phi)$：$\ker(\phi) = \{p(x) \in \mathbb{R}[x] \mid p(i) = 0\}$。根据实系数多项式共轭根定理，若 i 是根，则 $-i$ 也是根。因此 $(x-i)(x+i) = x^2+1$ 是 $p(x)$ 的因子。所以 $p(x) \in \langle x^2+1 \rangle$。故 $\ker(\phi) = \langle x^2+1 \rangle$。

根据第一同构定理，$\mathbb{R}[x]/\ker(\phi) \cong \mathrm{im}(\phi)$，即 $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$。

补充练习 11.6

证明 $\langle 1+2i \rangle$ 是高斯整环 $\mathbb{Z}[i]$ 的极大理想。

解答.

证明. 我们证明商环 $\mathbb{Z}[i]/\langle 1+2i \rangle$ 是一个域。如果商环是域，则理想是极大理想。考虑高斯整数的范数 $N(a+bi) = a^2+b^2$。计算范数 $N(1+2i) = 1^2+2^2 = 5$。因为 5 是一个素数，根据高斯整环的性质，由范数为素数的元素生成的主理想是极大理想。具体地，商环 $\mathbb{Z}[i]/\langle 1+2i \rangle$ 同构于有限域 $\mathbb{Z}_5$。在商环中，$1+2i \equiv 0 \implies 2i \equiv -1$。两边平方得 $(2i)^2 \equiv (-1)^2 \implies -4 \equiv 1 \implies 5 \equiv 0$。这表明商环的特征为 5。任意元素

$a+bi+\langle 1+2i\rangle$ 都可以被化简。由 $2i \equiv -1 \pmod{\langle 1+2i\rangle}$，乘以 3 得 $6i \equiv -3 \implies i \equiv 2 \pmod 5$。所以 $a+bi \equiv a+2b \pmod{\langle 1+2i\rangle}$。这表明商环中的每个元素都等价于 $\mathbb{Z}_5$ 中的一个元素。因为 $\mathbb{Z}_5$ 是域，所以商环 $\mathbb{Z}[i]/\langle 1+2i\rangle$ 是域，因此 $\langle 1+2i\rangle$ 是 $\mathbb{Z}[i]$ 的极大理想。

补充练习 11.7

证明 $\langle z^2+z+1\rangle$ 是多项式环 $\mathbb{Z}_2[z]$ 的极大理想。

解答.

证明. 在域 F 上的多项式环 $F[x]$ 中，主理想 $\langle p(x)\rangle$ 是极大理想当且仅当多项式 $p(x)$ 在 F 上是不可约的。这里 $F=\mathbb{Z}_2=\{\overline{0},\overline{1}\}$，多项式是 $p(z)=z^2+z+1$。我们检查 $p(z)$ 在 $\mathbb{Z}_2$ 中是否有根：

- $p(\overline{0})=\overline{0}^2+\overline{0}+\overline{1}=\overline{1}\neq\overline{0}$
- $p(\overline{1})=\overline{1}^2+\overline{1}+\overline{1}=\overline{3}=\overline{1}\neq\overline{0}$

因为 $p(z)$ 是二次多项式且在 $\mathbb{Z}_2$ 中没有根，所以它在 $\mathbb{Z}_2$ 上是不可约的。因此，由它生成的理想 $\langle z^2+z+1\rangle$ 是 $\mathbb{Z}_2[z]$ 的极大理想。

补充练习 11.8

给出有限域 $F=\mathbb{Z}_3[z]/\langle z^2+2z+2\rangle$ 的元素，加法运算表和乘法运算表，非零元素构成的乘法群的生成元，以及它的所有子域。

解答. 令 $I=\langle z^2+2z+2\rangle$，记 $\alpha=z+I$。在商环 F 中，有 $\alpha^2+2\alpha+2=0$，即 $\alpha^2=-2\alpha-2=\alpha+1$ (在 $\mathbb{Z}_3$ 中)。

1. **元素**：F 的元素形如 $a+b\alpha$，其中 $a,b\in\mathbb{Z}_3$。共有 $3\times3=9$ 个元素：$\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}$。

2. **加法运算表** ($|F| = 9$)

$+$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	1	2	0
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	α	$\alpha+1$	$\alpha+2$
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	0	$\alpha+1$	$\alpha+2$	α
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1	$\alpha+2$	α	$\alpha+1$

3. **乘法运算表** ($|F| = 9$)

$\times$	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$\alpha+1$	$2\alpha+1$	1	$2\alpha+2$	2	$\alpha+2$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$2\alpha+1$	2	α	2α	$\alpha+2$	1
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	1	α	2α	$\alpha+1$	$2\alpha+2$	2
2α	0	2α	α	$2\alpha+2$	2α	$\alpha+1$	$\alpha+2$	1	$2\alpha+1$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	2	$\alpha+2$	$2\alpha+2$	1	2α	α
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$\alpha+2$	1	2	$2\alpha+1$	α	2α

4. **乘法群的生成元**：非零元乘法群 F^* 是一个 8 阶循环群。我们检验 α 的阶：$\alpha^1 = \alpha$
   $\alpha^2 = \alpha + 1$
   $\alpha^3 = \alpha(\alpha+1) = \alpha^2 + \alpha = (\alpha+1) + \alpha = 2\alpha + 1$
   $\alpha^4 = \alpha(2\alpha+1) = 2\alpha^2 + \alpha = 2(\alpha+1) + \alpha = 2\alpha + 2 + \alpha = 2$
   $\alpha^5 = 2\alpha$
   $\alpha^6 = 2\alpha^2 = 2(\alpha+1) = 2\alpha + 2$
   $\alpha^7 = \alpha(2\alpha+2) = 2\alpha^2 + 2\alpha = 2(\alpha+1) + 2\alpha = \alpha + 2$
   $\alpha^8 = \alpha(\alpha+2) = \alpha^2 + 2\alpha = (\alpha+1) + 2\alpha = 1$
   α 的阶是 8，所以 α 是 F^* 的一个生成元。

5. **子域**：有限域的子域的阶数必须是 p^k 的形式，其中 k 整除域阶的指数。F 的阶是 $9 = 3^2$。2 的因子是 1 和 2。

   - $k = 1$: 阶为 $3^1 = 3$ 的子域，即素子域 $\mathbb{Z}_3 = \{0, 1, 2\}$。

- $k = 2$: 阶为 $3^2 = 9$ 的子域，即 F 本身。

所以 F 只有一个真子域，就是它的素子域 $\mathbb{Z}_3$。

补充练习 11.9

有限域 $K = \mathbb{Z}_2[z]/\langle z^2 + z + 1\rangle$ 的加法群与 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 同构，请写出它们之间的一个同构映射。

解答.

证明. K 作为一个向量空间，其基为 $\{1, \alpha\}$，其中 $\alpha = z + \langle z^2 + z + 1\rangle$。$K$ 的元素为 $\{0, 1, \alpha, 1 + \alpha\}$。$\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 的元素为 $\{(0,0), (1,0), (0,1), (1,1)\}$。我们可以定义一个基于基映射的同构 $\psi : K \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$。令 $\psi(1) = (1,0)$ 且 $\psi(\alpha) = (0,1)$。由于 ψ 是加法群同态，它必须满足 $\psi(x + y) = \psi(x) + \psi(y)$。我们可以将此映射扩展到所有元素：

- $\psi(0) = \psi(0 \cdot 1 + 0 \cdot \alpha) = 0\psi(1) + 0\psi(\alpha) = (0,0)$
- $\psi(1) = \psi(1 \cdot 1 + 0 \cdot \alpha) = 1\psi(1) + 0\psi(\alpha) = (1,0)$
- $\psi(\alpha) = \psi(0 \cdot 1 + 1 \cdot \alpha) = 0\psi(1) + 1\psi(\alpha) = (0,1)$
- $\psi(1 + \alpha) = \psi(1) + \psi(\alpha) = (1,0) + (0,1) = (1,1)$

这个映射 ψ 将 K 的四个元素一一映射到 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ 的四个元素，因此是双射。它也保持了加法运算，所以是一个群同构。