第十五周习题课

李文桥

2023 年 12 月 30 日

1 环

回忆: 环、子环和环同态

- 环的定义: 设集合 R 上有两个二元运算(加法和乘法), 其关于加法称为一个交换群, 关于乘法成为一个含幺半群, 且乘法和加法具有分配律, 则称 R 为一个环. 一般记 $0,1$ 为加法和乘法的单位元.
- 子环的定义: 设 $S \subset R$ 含有 $0,1$ 且关于 R 中的加法和乘法是一个环, 则称 S 为 R 的一个子环.
- 设 $\phi:\ R \to R'$ 为一个映射, 且满足:

  (1) $\phi(x+y) = \phi(x) + \phi(y)$, $\forall x, y \in R$;

  (2) $\phi(xy) = \phi(x)\phi(y)$, $\forall x, y \in R$;

  (3) $\phi(1_R) = 1_{R'}$.

  则称 ϕ 为一个环同态. 进一步, 若 ϕ 为双射, 则称 ϕ 为一个环同构.
- 设 $\phi:\ R \to R'$ 为一个环同构, 则 $\mathrm{im}(\phi)$ 为 R' 的一个子环.

回忆: 零因子、可逆元与整环

- 设 R 为一个环, $x \in R\backslash\{0\}$. 若存在 $y \in R\backslash\{0\}$ 使得 $xy = 0$, 则称 x 是一个左零因子; 同样地, 可以定义右零因子.
- 非左零因子的元素具有左消去律; 非右零因子的元素具有右消去律.
- 设 R 为一个环, $x \in R$. 若存在 $y \in R$ 使得 $xy = yx = 1$, 则称 x 为 R 中的可逆元, x 的逆为 y, 记为 x^{-1}.
- 环 R 中可逆元全体关于环 R 的乘法构成一个群.
- 设 R 为一个交换环且无零因子, 则称 R 为整环. 整环具有消去律.

回忆: Fermat 小定理: 设 p 为素数, $a \in \mathbb{Z}$ 且与 p 互素, 则 $a^{p-1} \equiv 1 \mod p$.

习题1: (a) 证明一个事实:

引理 1.1 *$\mathbb{Z}_n$ 的全部子群为 $\{\langle \bar{k} \rangle \mid k \in \mathbb{Z}\} = \{\langle \bar{k} \rangle \mid k \mid n$ 或 $k = 0\}$*

证明: 实际上, $\langle\bar{k}\rangle = \left\langle\overline{\gcd(k,n)}\right\rangle$. 首先, 易见 $\langle\bar{k}\rangle \subseteq \left\langle\overline{\gcd(k,n)}\right\rangle$. 另一方面, 由欧几里得算法, 存在 $u, v \in \mathbb{Z}$ 使得 $uk + vn = \gcd(k,n)$, 这说明 $\bar{u}\bar{k} = \overline{\gcd(k,n)}$, 也即 $\overline{\gcd(k,n)} \in \langle\bar{k}\rangle$, 从而 $\left\langle\overline{\gcd(k,n)}\right\rangle \subseteq \langle\bar{k}\rangle$.□

上述引理告诉我们, 只要取 n 的因子(实际上, 正因子就足够了)作为生成元, 再加上平凡子群 $\langle\bar{0}\rangle$, 我们就得到了所有的子群. 从而本题中应有 6 个子群.

(b) 注意到 71 是素数且 11 与 71 互素, 故由 Fermat 小定理:

$$11^{1752} = 11^{70\times 25+2} \equiv 11^2 \equiv 50 \mod 71.$$

(c) 由于 13 为素数, 所以 $\mathbb{Z}_{13}$ 中除 $\bar{0}$ 以外的元素均可逆. 记 $U = \mathbb{Z}_{13}\backslash\{\bar{0}\}$, 则 U 关于乘法构成一个群, $\mathrm{card}(U) = 12$. 考虑 $\bar{2} \in U$ 的阶. 我们知道 $\bar{2}^{12} = \bar{1}$, 则 $\bar{2}$ 的阶可能为 $2, 3, 4, 6, 12$. 直接计算, $\bar{2}^4 = \bar{3}$, $\bar{2}^6 = \bar{12}$, 所以 $\bar{2}$ 的阶只能是 12. 那么 $U = \langle\bar{2}\rangle$ 为循环群.

习题2: $(a) \Rightarrow (b)$: 设 $v \in R$ 使得 $uv = 1$, 则由 u 不是可逆元知 $vu \neq 1$. 从而 $1+v-vu \neq v$. 而 $u(1+v-vu) = u + uv - uvu = u + 1 - u = 1$, 从而 u 有多于一个右逆;

$(b) \Rightarrow (c)$: 设 v_1, v_2 为 u 的两个不同的右逆, 则 $v_1 - v_2 \neq 0$ 且 $u(v_1 - v_2) = 0$, 从而 u 为左零因子;

$(c) \Rightarrow (a)$: 设 $r \in R\backslash\{0\}$ 使得$ur = 0$. 若 u 为可逆元, 则在上式两侧左乘 u^{-1} , 得 $r = 0$. 矛盾. 所以 u 不是可逆元.

习题3: (a) $1 = 1 - a^n = (1-a)(1 + a + \cdots + a^{n-1}) = (1 + a + \cdots + a^{n-1})(1-a)$, 所以 $1-a$ 可逆;

(b) 设 $c \in R$ 使得 $c(1-ab) = (1-ab)c = 1$, 则 $c - 1 = cab = abc$. 注意到 $(1-ba)bc = bc - babc = bc - b(c-1) = b$, 从而 $(1-ba)bca = ba$, $1-(1-ba)bca = 1-ba$. 进一步, $1 = (1-ba)(1+bca)$. 容易验证 $(1 + bca)(1 - ba) = 1$, 从而 $1 - ba$ 可逆.

习题4: 设 R 为含有有限个元素的整环, 只需证明 R 中每个非零元可逆. 注意到 R 中没有零因子, 所有元素都具有消去律, 故任取 $r \in R\backslash\{0\}$, 由 R 有限知: 存在 $i \neq j \in \mathbb{N}$ 使得 $r^i = r^j$, 不妨设 $i > j$, 则 $r^{i-j} = 1$ (消去律). 则 $r^{i-j-1}r = 1$, 从而 r 可逆.

补充: **定理 1.2** *若 R 为一个环, $r \in R$ 有多于一个右逆, 则 r 有无穷多个右逆.*

证明: 反证法, 设 S 是由 r 的右逆全体构成的集合, 并假设 $S = \{x_1, x_2, \cdots, x_n\}$ 有限, $n \geq 2$. 则由习题 2 知, r 不是单位, 从而 $x_k r \neq 1$, $\forall k = 1, \cdots n$. 那么 $1 - x_k r + x_1$ 是 r 的右逆, 且对于 $1 \leq i, j \leq n$, 若 $1 - x_i r + x_1 = 1 - x_j r + x_1$, 则 $x_i r = x_j r$, 由 r 有右逆知 $x_i = x_j$, 这说明 $1 - x_k r + x_1$ 是 r 的 n 个互不相同的右逆, 从而 $S = \{x_1, \cdots, x_n\} = \{1 - x_1 r + x_1, \cdots 1 - x_n r + x_1\}$, 故存在 k 使得 $1 - x_k r + x_1 = x_1$, 即 $x_k r = 1$. 这说明 r 是单位, 矛盾. □

注: 以上关于右逆的结论对左逆也成立.

2 域

回忆: 域的定义、特征以及域上的线性代数.

- 域: 每个非零元都可逆的整环. p 为素数, 则 $\mathbb{Z}_p$ 为域.

- 域之间的环同态都是单射.
- 设 F 是一个域, 若 1 的加法阶有限, 则定义 F 的特征为 $\mathrm{ord}(1)$; 否则定义 F 的特征为 0. 记 F 的特征为 $\mathrm{char}(F)$. 一个域的特征是 0 或者一个素数.
- 设 $\mathrm{char}(F) = p > 0$, 则 $(x+y)^p = x^p + y^p$.
- 域具有加、减、乘、除的运算封闭性. 除了奇数斜对称行列式矩阵行列式为零以外, 其他所有实数域上线性代数的结论对一般的域均成立.

习题5,6: 只求习题 5(b). 容易求得 $\mathrm{rank}(A) = 2$, 从而 $\dim(V_c(A)) = 2$. 若设 $\boldsymbol{\alpha}, \boldsymbol{\beta}$ 为 $V_c(A)$ 中的一组基, 则 $V_c(A)$ 中的元素形如 $x\boldsymbol{\alpha} + y\boldsymbol{\beta}$, $x, y \in \mathbb{Z}_3$. 由于 $\boldsymbol{\alpha}, \boldsymbol{\beta}$ 线性无关, 所以当 (x, y) 不同时, 其表出的向量也不同(表出的唯一性). 由于 x, y 共有 9 中可能的取值, 所以 $V_c(A)$ 有 9 个向量.

补充: **推论 2.1** *设域 F_q 是含有 q 个元素的有限域, V 为 $(F_q)^n$ 中的 k 维子空间, 则 $\mathrm{card}(V) = q^k$.*

例 2.2 *设 F_q 是含有 q 个元素的有限域.*

(a) 求 $\mathrm{M}_n(F_q)$ 中元素的个数;

(b) 求 $\mathrm{GL}_n(F_q)$ 中元素的个数.

解: 容易看出 $\mathrm{M}_n(F_q)$ 中含有 q^{n^2} 个元素. 而对于 $A \in \mathrm{M}_n(F_q)$, A 可逆当且仅当 A 的行向量线性无关(F_q 上). 那么 A 的第一行有 $q^n - 1$ 种取法(非零向量); 第一行取定后, 第二行需要在第一行生成的子空间外取, 则有 $q^n - q$ 种; 前两行取定后, 第三行要在前两行生成的子空间外取, 则有 $q^n - q^2$ 种;$\cdots$.

由此可得, A 可逆的取法共 $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.

思考: $(F_q)^n$ 中有多少个 k 维子空间?

3 有限域的循环群结构

习题 1(c) 中, 我们证明了 $\mathbb{Z}_{13}$ 中的可逆元具有循环群的结构. 下面我们将这一现象推广到一般的有限群上.

引理 3.1 *设 G 为阿贝尔群, $g, h \in G$ 为有限阶元素. 设 $m = \mathrm{ord}(g)$, $n = \mathrm{ord}(h)$. 若 m, n 互素, 则 gh 的阶为 mn.*

证明: 一方面, $(gh)^{mn} = e$. 另一方面, 若 $s = \mathrm{ord}(gh)$, 则 $(gh)^s = e$. 从而 $g^{ns} = (gh)^{ns} = e$, 从而 $m \mid ns$. 由于 m, n 互素, 所以 $m \mid s$. 同理, $n \mid s$, 所以 $mn \mid s$. 这说明 $s = mn$. □

引理 3.2 *设 G 是一个有限阿贝尔群, $g \in G$ 是 G 中阶最大的元素, 则 $\forall x \in G$, $x^{\mathrm{ord}(g)} = e$.*

证明: 反证法, 设存在 $x \in G$ 使得 $x^{\mathrm{ord}(g)} \neq e$. 令 $m = \mathrm{ord}(g), l = \mathrm{ord}(x)$, $h = \gcd(m, l)$ 则 l 不整除 m, 于是存在某个素数的方幂 p^r 满足 $p^r \mid l$, $p^r \nmid m$. 设 $l = p^r l_1$, $m = p^s m_1$, 其中 $s < r$, m_1 与 p 互素. 令 $h = g^{p^s} x^{l_1}$, 由前引理知 $\mathrm{ord}(h) = p^r m_1 > m$, 与 g 的阶最大矛盾. □

定理 3.3 *设 F_q 是一个含有 q 个元素的有限域, 则记 $F_q^* = F_q \backslash \{0\}$, F_q^* 关于乘法构成一个群, 且为循环群.*

证明: 容易看出 F_q^* 关于乘法构成一个阿贝尔群, 则取 F_q^* 中阶最大的元素 a, 记 $k = \mathrm{ord}(a)$, 则 $k \leq q-1$. 由前引理, F_q^* 中所有元素均为多项式$X^k - 1$ 的根, 这说明 $k \geq q-1$. 故 $k = q-1$, 也即 a 的阶数等于群 F_q^* 的阶数, 所以 $\langle a \rangle = F_q^*$.□

4 环的理想

上次习题中, 我们证明了群同态的核具有交换性, 即 $g\ker(\phi) = \ker(\phi)g$. 这次我们考虑一个环同态的核. 注意到环作为加法群是交换的, 所以同态核作为加法子群必然交换性.

命题 4.1 *设 $\phi: R \to S$ 是一个环同态, 则对任意的 $r \in R$, $a \in \ker(\phi)$, 有 $ra \in \ker(\phi)$, $ar \in \ker(\phi)$.*

反过来, 我们定义环 R 的一个特殊的子集:

定义 4.2 *设 R 为一个环, I 为 R 的一个加法子群. 若对任意的 $r \in R$, $a \in I$, 都有 $ra \in I$, 则称 I 为 R 的一个左理想; 若对任意的 $r \in R$, $a \in I$, 都有 $ar \in I$, 则称 I 为 R 的一右理想. 若 I 为左理想且为右理想, 则称 I 为 R 的一个理想.*

注意到 $(0), R$ 均为 R 的理想.

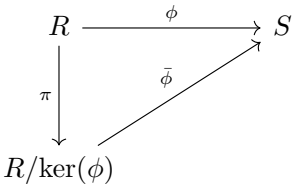
由于交换性, I 为 R 的一个正规子群, 从而可以作商, 得到商群 R/I. 进一步, 我们可以在这个商群上定义乘法, 使其称为一个环: 设 $\overline{r_1}, \overline{r_2} \in R/I$, 定义 $\overline{r_1} \cdot \overline{r_2} := \overline{r_1 r_2}$.

命题 4.3 *上述定义的乘法是良定义的.*

证明是一个很好的练习.

我们称 R/I 为一个商环. 由此, 我们有一个自然的同态: $\pi: R \to R/I$, $r \mapsto \bar{r}$. 容易验证这是一个环同态, 且 $\ker(\pi) = I$. 与上次习题课类似, 我们有:

定理 4.4 (第一同态基本定理) *设 $\phi: R \to S$ 为一个环同态, 则存在唯一一个单的环同态 $\bar{\phi}: R/\ker(\phi) \to S$ 使得 $\phi = \bar{\phi} \circ \pi$.*



证明: 令 $\bar{\phi}: R/\ker(\phi) \to S$, $\bar{r} \mapsto \phi(r)$. 可以验证其良定义, 且满足要求. □

理想实际上是一个很本质的概念, 它能描述许多数学对象之间的联系.

例 4.5 *设 $\mathbb{Z}$ 为整数环. 则全体偶数构成 $\mathbb{Z}$ 的一个理想, 对应商环为 $\mathbb{Z}_2$; 全体 3 的倍数构成 $\mathbb{Z}$ 的一个理想, 对应商环为 $\mathbb{Z}_3$.*

例 4.6 *设 $C[0,1]$ 为定义在闭区间 $[0,1]$ 上的连续实函数全体构成的集合, 则其关于函数的加法和乘法成为一个群. 设 I 为 $C[0,1]$ 的一个理想且 $I \neq C[0,1]$, 则 I 中所有函数有公共零点.*

证明: 反证法: 若 I 中函数没有公共零点, 则对任意的 $\alpha \in [0,1]$, 存在 $f_\alpha \in I$ 使得 $f_\alpha(\alpha) \neq 0$. 由 f_α 的连续性知: 存在包含 α 开区间 U_α 使得 f_α 在 U_α 上非零. 那么 $\{U_\alpha \,|\, \alpha \in [0,1]\}$ 成为 $[0,1]$ 的开覆盖. 由闭区间的有限覆盖性知: 存在 $a_1, \cdots, a_n$ 使得 $[0,1] \subseteq U_{\alpha_1} \cup \cdots \cup U_{\alpha_n}$. 那么令 $g = f_{\alpha_1}^2 + \cdots + f_{\alpha_n}^2 \in I$, g 在 $[0,1]$ 上没有零点. 于是 $\dfrac{1}{g} \in C[0,1]$. 由于 I 为理想, 所以 $1 = \dfrac{1}{g} g \in I$. 进一步, 对任意的 $f \in C[0,1]$, $f = f \cdot 1 \in I$. 这说明 $I = C[0,1]$, 矛盾. □