第十五周作业参考解答及补充

作业

1. (习题 4.3.1)

设 $G=\langle\alpha\rangle$ 是 n 阶循环群, 试证明:

(1) α^m 是 G 的生成元 (即 $G=\langle\alpha^m\rangle$) $\Leftrightarrow (m,n)=1$;

(2) 若 $\mathbb{Z}/n\mathbb{Z}$ 表示模 n 的剩余类环, $U(\mathbb{Z}/n\mathbb{Z})$ 是它的单位群, 则

$$\overline{m}\in U(\mathbb{Z}/n\mathbb{Z})\Leftrightarrow (m,n)=1;$$

(3) 设 $\mathrm{Aut}(G)$ 表示群 G 的自同构群, 则 $\mathrm{Aut}(G)\cong U(\mathbb{Z}/n\mathbb{Z})$.

proof

该题在 3.1.6 的注记有提及. 已经指出 G 是 n 阶循环群即 $G\cong\mathbb{Z}/n\mathbb{Z}$, 因此只需证 (2), 而 (2) 是 1.2.9. 因此只证 (3).
对 $\sigma\in\mathrm{Aut}(G)$, 注意到 $\sigma(\overline{m})=m\sigma(\overline{1})$, 故可以验证映射

$$\mathrm{Aut}(G)\to U(\mathbb{Z}/n\mathbb{Z}),\quad \sigma\mapsto\sigma(\overline{1})$$

是一个群同构. 事实上只需要验证 $(\sigma_1\circ\sigma_2)(\overline{1})=\sigma_1(\overline{1})\cdot\sigma_2(\overline{1})$, 这由群同态的定义得到. 而 $\sigma\in\mathrm{Aut}(G)$ 可逆, 因此 $\sigma(\overline{1})\in\mathbb{Z}/n\mathbb{Z}$ 关于乘法可逆, 必须有 $\sigma(\overline{1})\in U(\mathbb{Z}/n\mathbb{Z})$. $\square$

2. (习题 4.3.2)

设 F 是一个域, $F^*=F\setminus\{0\}$, 证明乘法群 F^* 的任何有限子群都是循环群.

proof

任意 F^* 的有限子群 G, 设 $|G|=n$, 那么 $\forall\alpha\in G$, 有 $\alpha^n=1$. 因此 G 是 $U_n(F)$ 的一个子群, 而循环群的子群一定是循环群. $\square$

注:

$\mathbb{Z}$ 的子群一定是 $n\mathbb{Z}$, n 为该子群中最小的自然数. 循环群是 $\mathbb{Z}$ 的一个商群, 因此对同态 $\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ 用 4.1.3, 那么 $\mathbb{Z}/n\mathbb{Z}$ 的子群是某个 $d\mathbb{Z}$ 的像, 这里要求 $n\mathbb{Z}\subseteq d\mathbb{Z}$, 即 $d\mid n$. 从而该子群就是 $\langle\overline{d}\rangle$.

3. (习题 4.3.3)

设 K 是特征零的域, L 是多项式 $x^n-1\in K[x]$ 的分裂域. 试证明: $\mathrm{Gal}(L/K)$ 同构于 $U(\mathbb{Z}/n\mathbb{Z})$ 的一个子群. 特别地, $\mathrm{Gal}(L/K)$ 总是交换群.

proof

这是分圆域的一般情形 (3.1.6), 设 $\theta \in L$ 是 n 次本原单位根, 即 $x^n - 1$ 的根, $\sigma \in \mathrm{Gal}(L/K)$. 那么 $x^n - 1 = (x-1)(x-\theta)\cdots(x-\theta^{n-1})$. 对等式两边以 σ 作用, 就有 $x^n - 1 = (x-1)(x-\sigma(\theta))\cdots(x-\sigma(\theta)^{n-1})$. 因此 $\sigma(\theta)$ 也是本原单位根, 则有同态

$$\mathrm{Gal}(L/K) \to U(\mathbb{Z}/n\mathbb{Z}) = \langle\theta\rangle, \sigma \mapsto \sigma(\theta)$$

因此 $\mathrm{Gal}(L/K)$ 同构于 $U(\mathbb{Z}/n\mathbb{Z})$ 的一个子群, 即它的像. 而交换群的子群自然是交换的. $\square$

注:

若 K 特征零或特征 p 满足 $(p,n)=1$, 则 $x^n - 1$ 是可分多项式, 因此无重根, 此时单位根群 $U_n(K) \cong \mathbb{Z}/n\mathbb{Z}$. 这时有

$$\mathrm{Gal}(L/K) = \begin{cases} U(\mathbb{Z}/n\mathbb{Z}) & \theta \notin K, \\ \{\mathrm{id}\} & \theta \in K. \end{cases}$$

4. (习题 4.5.1)

设 $\mathrm{Aut}(X)$ 表示集合 X 的自同构群. 试证明:

(1) 若 $G \times X \to X$, $(g,x) \mapsto g\cdot x$, 是群 G 在 X 上的一个作用, $\forall g \in G$, 定义映射 $X \xrightarrow{\rho(g)} X$, $x \mapsto g\cdot x$. 则 $\rho(g) \in \mathrm{Aut}(X)$ 且映射

$$\rho : G \to \mathrm{Aut}(X),\ g \mapsto \rho(g)$$

是群同态.

(2) 若 $\rho : G \to \mathrm{Aut}(X)$ 是一个群同态, 则映射

$$G \times X \to X,\ (g,x) \mapsto \rho(g)(x)$$

是一个群作用.

proof

(1) 由于 G 是群, g^{-1} 是存在的, 从而这里定义的左乘映射 $\rho(g)$ 自然是一个双射. 只需验证 ρ 是保持乘法的. 对 $\forall x \in X$

$$\rho(g_1g_2)(x) = (g_1g_2)\cdot x = g_1\cdot(g_2\cdot x) = \rho(g_1)(\rho(g_2)(x)) = (\rho(g_1)\circ\rho(g_2))(x).$$

因此有 $\rho(g_1g_2) = \rho(g_1)\circ\rho(g_2)$ 保持乘法, ρ 是群同态.

(2) 反过来, 若 ρ 是群同态, 则 $\rho(1)=1$, 即 $\rho(1)=\mathrm{id}_X$. 那么对 $\forall x \in X$ 自然

有 $1\cdot x=\rho(1)(x)=\mathrm{id}_X(x)=x$. 另一方面,

$$(g_1g_2)\cdot x=\rho(g_1g_2)(x)=(\rho(g_1)\circ\rho(g_2))(x)=\rho(g_1)(\rho(g_2)(x))=g_1\cdot(g_2\cdot x)$$

因此 $G\times X\to X$, $(g,x)\mapsto\rho(g)(x)$ 是一个群作用.

$\square$

注:

这题是群作用的两种表述, 若看成一个群同态 $\rho: G\to\mathrm{Aut}(X)$ 则更贴近表示论的观点. 比如同态

$$\rho: G\to\mathrm{GL}(V),\quad g\mapsto\rho(g)$$

称为群 G 的一个 k-表示 (a k-representation, or a representation over field k). 其中 V 是一个 k-线性空间, $\mathrm{GL}(V)$ 为 V 上所有可逆线性变换构成的群.

一般地, 对于范畴 $\mathcal{C}$ 中的对象 X, 群 G 在 X 上的作用是群同态

$$\rho: G\to\mathrm{Aut}_{\mathcal{C}}(X)$$

此观点在模的定义中也是类似的, 见 5.1.3, 即一个 R-模实际上是环 R 在 Abel 群 M 上的一个作用.