# 近世代数 (H) 第十五周作业

涂嘉乐 PB23151786

2025 年 6 月 7 日

**Exercise 1** 设 $N_1 \lhd G, N_2 \lhd G$，且 $N_1N_2 = G, N_1 \cap N_2 = \{1_G\}$，则 $G \simeq (G/N_1) \times (G/N_2)$

**Proof** 考虑映射

$$\begin{aligned}\phi : G &\longrightarrow (G/N_1) \times (G/N_2) \\ g &\longmapsto (gN_1, gN_2)\end{aligned}$$

下证 $\phi$ 是群同构

(1) 同态：$\phi(g_1g_2) = (g_1g_2N_1, g_1g_2N_2) = (g_1N_1, g_1N_2)(g_2N_1, g_2N_2) = \phi(g_1)\phi(g_2)$

(2) 单射：若 $(gN_1, gN_2) = (N_1, N_2)$，则 $g \in N_1 \cap N_2 = \{1_G\}$，故 $\mathrm{Ker}\phi = \{1_G\}$，则 $\phi$ 单射

(3) 满射：对 $\forall (aN_1, bN_2) \in (G/N_1) \times (G/N_2)$，由 $G = N_1N_2$，可设 $a = n_{1a}n_{2a}, b = n_{2a}n_{2b}$，其中 $n_{1a}, n_{1b} \in N_1, n_{2a}, n_{2b} \in N_2$

$$\phi(n_{1b}n_{2a}) = (n_{1b}n_{2a}N_1, n_{1b}n_{2a}N_2) = (n_{1b}N_1n_{2a}, n_{1b}N_2) = (N_1n_{2a}, n_{1b}N_2) = (n_{2a}N_1, n_{1b}N_2)$$

$$(aN_1, bN_2) = (n_{1a}n_{2a}N_1, n_{1b}n_{2b}N_2) = (n_{1a}N_1n_{2a}, n_{1b}N_2) = (N_1n_{2a}, n_{1b}N_2) = (n_{2a}N_1, n_{1b}N_2)$$

所以 $\phi(n_{1b}n_{2a}) = (aN_1, bN_2)$，故 $\phi$ 为满射

综上 $\phi$ 为群同构 $\square$

**Exercise 2** 设 $k = \mathbb{F}_p(t_1, t_2)$，$K = (k, (x^p - t_1)(x^p - t_2))$，则在 $K$ 上有 $(x^p - t_1)(x^p - t_2) = (x - a_1)^p(x - a_2)^p$，其中 $a_1, a_2 \in K$，证明

(1) $\dim_k K = p^2$

(2) $\mathrm{Gal}(K/k) = \{\mathrm{Id}_K\}$

(3) $\forall \lambda \in k$，定义 $E_\lambda = k(a_1 + \lambda a_2)$，则

- $\dim_k E_\lambda = p$
- $E_\lambda \neq E_\mu, \forall \lambda \neq \mu$

**Proof** (1). 首先说明 $a_1, a_2$ 是如何得到的：设 $a \in \mathrm{Root}_K(x^p - t_1)$，则 $a^p = t_1$，故

$$x^p - t_1 = x^p - a^p = (x - a)^p \Longrightarrow \mathrm{Root}_K(x^p - t_1) = \{a\}$$

所以 $a_1, a_2 \in K$ 满足 $a_1^p = t_1, a_2^p = t_2$，且它们为 $p$ 重根

因为 $k(t_1, t_2) = \mathrm{Frac}(k[t_1, t_2])$，且 $k[t_1, t_2]$ 为 *UFD*，故只需考虑 $x^p - t_1$ 在 $k[t_1, t_2][x]$ 上的不可约性：在 $k[t_1, t_2][x]$ 上，取 $p = t_1$，由 *Eisenstein* 判别法知 $x^p - t_1$ 在 $k[t_1, t_2][x]$ 上不可约，故

$x^p - t_1$ 在 $k(t_1,t_2)[x]$ 上不可约，同理 $x^p - t_2$ 在 $k(t_1,t_2)[x]$ 上不可约，考虑域扩张塔

$$k \subseteq k(a_1) \subseteq k(a_1,a_2)$$

由 $x^p - t_1$ 在 $k(t_1,t_2)[x]$ 上不可约知，$a_1$ 在 $k[x]$ 上的最小多项式为 $x^p - t_1$，所以 $[k(a_1):k]=p$，又因为 $a_2$ 在 $k(a_1)$ 上的零化多项式为 $x^p - t_2$，假设它可约，则由前面分析知，因子的形式一定是 $(x-a_2)^{p_1}, p_1 < p$，但是 $p_1 < p$ 时，$(x-a_2)^{p_1}$ 的一次项系数为 $-p_1 a_2 \in k(a_1)$，这将推出 $a_2 \in k(a_1)$，矛盾！所以 $x^p - t_2$ 在 $k(a_1)[x]$ 上不可约，故 $[k(a_1,a_2):k(a_1)]=p$，因此

$$[k(a_1,a_2):k] = [k(a_1,a_2):k(a_1)]\cdot[k(a_1):k] = p^2$$

又因为 $(x^p-t_1)(x^p-t_2)$ 的分裂域就是 $k(a_1,a_2)$（要使 $(x^p-t_1)(x^p-t_2)$ 分裂的域必须包含 $a_1,a_2$，因此 $k(a_1,a_2)$ 是最小的使它分裂的域），所以 $\dim_k K = p^2$

(2). 设 $\sigma \in \mathrm{Gal}(K/k)$，则 $\sigma(a_1) \in \mathrm{Root}_K(x^p - t_1) = \{a_1\}$，所以 $\sigma(a_1)=a_1$，同理有 $\sigma(a_2)=a_2$，而 $K = k(a_1,a_2)$，则 $\sigma = \mathrm{Id}$，即 $\mathrm{Gal}(K/k) = \{\mathrm{Id}_K\}$

(3). 对 $\forall \lambda \in k$，因为

$$(a_1 + \lambda a_2)^p = a_1^p + \lambda^p a_2^p = t_1 + \lambda^p t_2$$

所以 $x^p - (t_1 + \lambda^p t_2)$ 零化 $a_1 + \lambda a_2$，假设它可约，则同 (1) 的分析知，$x^p - (t_1+\lambda^p t_2) = (x-(a_1+\lambda a_2))^p$ 的因子必须是 $(x-(a_1+\lambda a_2))^{p_1}, p_1 < p$，但是它的一次项系数为 $-p_1(a_1+\lambda a_2) \in k$，这将推出 $a_1 + \lambda a_2 \in k$，进而 $a_2 \in k(a_1)$，矛盾！所以 $\dim_k E_\lambda = p, \forall \lambda \in k$

假设 $\exists \lambda \neq \mu \in k, \text{s.t.}\ E_\lambda = E_\mu \overset{\text{def}}{=} E$，则 $a_1 + \lambda a_2 \in E, a_1 + \mu a_2 \in E$，解线性方程组可得 $a_1, a_2 \in E$，故 $k(a_1,a_2) \subseteq E$，但是

$$\begin{cases} \dim_k E = p \\ \dim_k k(a_1,a_2) = p^2 \end{cases} \Longrightarrow \dim_E k(a_1,a_2) = \frac{1}{p}$$

这显然矛盾！故 $\forall \lambda \neq \mu, E_\lambda \neq E_\mu$ □

**Exercise 3** 设 $U$ 是 $p$-群，则 $\exists V \leq U, \text{s.t.}\ [U:V]=p$

**Proof** 设 $|U| = p^n$，对 $n$ 归纳：当 $n=1$ 时，显然有 $[U:\{e\}]=p$，假设命题对 $\forall n = k-1$ 成立，下面证明 $n=k$ 时命题成立

因为 $p$-群的中心 $Z(U)$ 非平凡，所以 $|Z(U)| = p^t, 0 < t \leq n$，故 $p \mid |Z(U)|$，由 *Cauchy* 定理知 $Z(U)$ 中有 $p$ 阶元，设为 $g$，则 $|U/(a)| = \frac{|U|}{(a)} = p^{n-1}$，由归纳假设知 $U/(a)$ 存在子群 $S$ 满足 $[U/(a):S]=p$，再由对应定理知，设 $V = \{a \in U | \overline{a} \in S\}$，则 $V \leq U, \text{s.t.}\ S = V/(a)$，且有

$$\big(U/(a)\big)/\big(V/(a)\big) \simeq U/V$$

所以

$$[U:V] = |U/V| = |\big(U/(a)\big)/\big(V/(a)\big)| = [U/(a):V/(a)] = p$$

□

**Exercise 4** 设 $k \subset E_1 \subset \cdots \subset E_n$ 是根式扩张塔，$\mathrm{Char}(k)=0$，则 $E_n = k(\beta)$，记 $\beta$ 在 $k$ 上的最小多项式为 $f(x)$，取 $K=(E_n, f(x))$，设 $\mathrm{Gal}(K/k)=\{\sigma_0=\mathrm{Id}, \sigma_1, \cdots, \sigma_p\}$

验证 $E_n \vee \sigma_1(E_n) \vee \cdots \vee \sigma_p(E_n) = K$

**Proof** 一方面由 $E_n \subseteq K$ 知，$\forall \sigma_i \in \mathrm{Gal}(K/k), \sigma_i(E_n) \subseteq \sigma_i(K) = K$，进而

$$\bigvee_{i=0}^{p} \sigma_i(E_n) \subseteq K$$

另一方面，因为 $f(x)$ 在 $K$ 上分裂，由 $\mathrm{Char}(k)=0$ 知 $K/k$ 是 *Galois* 扩张，所以对 $\forall \alpha \in \mathrm{Root}_K(f), \exists \sigma_i \in \mathrm{Gal}(K/k), \mathrm{s.t.}\ \sigma_i(\beta)=\alpha$，进而 $\alpha \in \sigma_i(E_n)$，所以 $\mathrm{Root}_K(f) \subseteq \bigvee\limits_{i=0}^{p} \sigma_i(E_n)$，即 $f(x)$ 在 $\bigvee\limits_{i=0}^{p} \sigma_i(E_n)$ 上分裂，由 $K$ 的最小性知

$$K \subseteq \bigvee_{i=0}^{p} \sigma_i(E_n)$$

综上 $K = \bigvee\limits_{i=0}^{p} \sigma_i(E_n)$ □

**Exercise 5** 设 $G$ 可解，则

(1) 若 $H \le G$，则 $H$ 可解

(2) 若 $N \trianglelefteq G$，则 $G/N$ 可解

**Proof** 由 $G$ 可解可设 $G = G_0 \trianglerighteq G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_n = \{\mathrm{Id}\}$

(1) 考虑子群降列 $H \ge (H\cap G_1) \ge (H \cap G_2) \ge \cdots \ge (H \cap G_n) = \{1_G\}$，由第二群同构定理（若 $N \trianglelefteq G, H \le G$，则 $H\cap N \trianglelefteq H$）知

$$\begin{cases} (H\cap G_i) \le G_i \\ G_{i+1} \trianglelefteq G_i \end{cases} \implies (H\cap G_1)\cap G_2 \trianglelefteq (H\cap G_1)$$

即 $(H\cap G_{i+1}) \trianglelefteq (H\cap G_i)$，所以 $H \trianglerighteq (H\cap G_1) \trianglerighteq (H\cap G_2) \trianglerighteq \cdots \trianglerighteq (H\cap G_n) = \{1_G\}$，故 $H$ 可解

(2) 由 $N \trianglelefteq G$ 知，$G_iN \le G, \forall 1 \le i \le N$，由对应定理，有子群降列 $G/N \ge (G_1N)/N \ge (G_2N)/N \ge \cdots \ge (G_nN)/N = \{1_{G/N}\}$，接下来证明 $G_iN \trianglelefteq G_{i-1}N$，对 $\forall gn \in G_{i-1}N$，因为

$$\begin{aligned}(gn)(G_iN)(gn)^{-1} &= (gn)(G_iN)(n^{-1}g^{-1}) = gn(G_iN)g^{-1} \\ &= gn(NG_i)g^{-1} = g(NG_i)g^{-1} = (gN)(G_ig^{-1}) \\ &= (Ng)(g^{-1}G_i) = NG_i\end{aligned}$$

所以 $G_iN \trianglelefteq G_{i-1}N$，由对应定理知 $(G_iN)/N \trianglelefteq (G_{i-1}N)/N$，所以 $G/N \trianglerighteq (G_1N)/N \trianglerighteq (G_2N)/N \trianglerighteq \cdots \trianglerighteq (G_nN)/N = \{1_{G/N}\}$，故 $G/N$ 可解 □

**Exercise 6** 若 $G$ 可解，则 $\exists H \lhd G, \text{s.t. } G/H \simeq C_p, p$ 是素数

**Proof** 本题应该要求 $G$ 是有限群，因为考虑 $(\mathbb{Q},+)$，它是 *Abel* 群，故可解，但是它没有指数为 $p$ 的子群，且多项式的 *Galois* 群本身就是有限群

Case 1. 若 $G$ 为 *Abel* 群，由 $G$ 有限知有群同构 $\phi : G \xrightarrow{\sim} \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}$，若 $d_1$ 有因子 $p$，取 $\mathbb{Z}_{d_1}$ 的 $\frac{d_1}{p}$ 阶子群 $H$，则

$$[\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r} : H \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r}] = p$$

再同构回去，即 $[G : \phi^{-1}(H \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_r})] = p$

Case 2. 若 $G$ 不是 *Abel* 群，则考虑 $G$ 的换位子群 $G' = \{xyx^{-1}y^{-1} : x, y \in G\}$，有如下观察

*1.* $G' \trianglelefteq G$：对 $\forall g \in G$

$$\begin{aligned}
aG'a^{-1} &= \{axyx^{-1}y^{-1}a^{-1} : x, y \in G\} \\
&= \{(axa^{-1})(aya^{-1})(axa^{-1})^{-1}(aya^{-1})^{-1} : axa^{-1}, aya^{-1} \in G\} \\
&= \{mnm^{-1}n^{-1} : m, n \in aGa^{-1}\} \xlongequal{aGa^{-1}=G} \{mnm^{-1}n^{-1} : m, n \in G\} \\
&= G'
\end{aligned}$$

*2.* $G/G'$ 是 *Abel* 群：对 $\forall x, y \in G$，因为 $xyx^{-1}y^{-1} \in G'$，所以 $xyG' = yxG'$，即 $(xG')(yG') = (yG')(xG')$

由 $G$ 有限知 $G/G$ 为有限 *Abel* 群，则由 Case 1 知，$G/G'$ 存在指数为 $p$ 的子群，由对应定理可以写作 $H/G'$，其中 $H \leq G$，由于 $H/G' \trianglelefteq G/G'$，故 $H \trianglelefteq G$，且

$$[G : H] = \frac{|G|}{|H|} = \frac{\frac{|G|}{|G'|}}{\frac{|H|}{|G'|}} = \frac{|G/G'|}{|H/G'|} = [(G/G') : (H/G')] = p$$

因此 $H$ 即为所求 $\square$