苏州大学 · 数学科学学院

抽象代数学习笔记

Based on lectures of Abstract Algebra

作者：郭利文

时间： 2026 年 1 月 25 日

目录

1 域

例 1.1. 给定 $n \in N^+$ 和素数 p，记 $\alpha = \sqrt[n]{p}$，则

$$\mathbb{Q}(\alpha) = \left\{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in \mathbb{Q}\right\}$$

是域.

证明. 由 Eisenstein 判别，$f = x^n - p$ 在 $\mathbb{Q}$ 上不可约. 则对任意 $g(\alpha) \in \mathbb{Q}(\alpha) \setminus \{0\}$，有 $(f, g) = 1$，即存在 $u, v \in \mathbb{Q}[x]$，使得 $fu + gv = 1$，这样就有

$$1 = f(\alpha)u(\alpha) + g(\alpha)v(\alpha) = g(\alpha)v(\alpha)$$

即 $g(\alpha)$ 有乘法逆元. ■

例 1.2. 设 p 是素数，则 $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$ 是域.

例 1.3. 有

$$\begin{aligned}\mathbb{Q}(\sqrt{2}, \sqrt{3}) &= \left\{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_4\sqrt{6} \mid a_i \in \mathbb{Q}\right\} \\ &= \left\{a_1 + a_2(\sqrt{2} + \sqrt{3}) + a_3(\sqrt{2} + \sqrt{3})^2 + a_4(\sqrt{2} + \sqrt{3})^3 \mid a_i \in \mathbb{Q}\right\} \\ &= \mathbb{Q}(\sqrt{2} + \sqrt{3})\end{aligned}$$

是域.

例 1.4. 设

$$E = \mathbb{Q}\left(\frac{1}{2^{\frac{1}{2^k}}} \middle| k = 1, 2, \cdots\right)$$

则 $E/\mathbb{Q}$ 不是有限生成扩张，但是是代数扩张.

例 1.5. $\mathbb{Q}(\pi)$ 是有限生成扩张，但不是代数扩张.

命题 1.1. *设 F 是域，若 α, β 是 F 代数元，则 $\alpha + \beta, \alpha\beta$ 也是 F 代数元.*

证明. 这里介绍一种不太常见的方法. 设 $f, g \in F[x]$，使得 $f(\alpha) = 0, g(\beta) = 0$. 记 $R(A, B)$ 表示 A, B 的结式. 令 $h(y) = R(f(x), g(y - x)) \in F[y]$，且 $h(\alpha + \beta) = 0$. 再令

$$k(y) = R\left(f(x), x^{\deg g} \cdot g\left(\frac{y}{x}\right)\right) \in F[y]$$

且 $k(\alpha\beta) = 0$ ■

命题 1.2 (维数公式)**.** *设 $F \subset K \subset E$，且 E/F 是有限扩张，则 $K/F, E/K$ 也是有限扩张，且*

$$[E : F] = [E : K] \cdot [K : F].$$

证明. 将 K, E 分别视为 F 上线性空间，则 K 是 E 的子空间，自然 $[K:F] \leq [E:F] < \infty$. 若我们记 $[E:F] = s$，我们断言 $[E:K] \leq s$，否则存在 $\alpha_1, \cdots, \alpha_{s+1} \in E$, 使得它们在 K 上线性无关，注意 $F \subset K$，则 $\alpha_1, \cdots, \alpha_n$ 在 F 上也线性无关，这导出矛盾.

下面不妨假定 $[E:K] = m, [K:F] = n$, 且

$$E = \mathrm{span}_K \{\alpha_1, \cdots, \alpha_m\}, \quad K = \mathrm{span}_F \{\beta_1, \cdots, \beta_n\}$$

则

$$E = \mathrm{span}_F \{\alpha_i \beta_j \mid i \in [1,m]; j \in [1,n]\}$$

下面只需说明 $\{\alpha_i \beta_j\}$ 在 F 线性无关即可. 设 $c_{ij} \in F$ 满足

$$0 = \sum_{i=1}^{m} \sum_{j=1}^{n} c_{ij} \alpha_i \beta_j = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} c_{ij} \beta_j \right) \alpha_i$$

对每个固定 $i \in [1,m]$，由于 $\sum\limits_{j=1}^{n} c_{ij} \beta_j \in K$，于是 $\sum\limits_{j=1}^{n} c_{ij} \beta_j = 0$，最终得到 $c_{ij} = 0$. ■

定理 1.3. 对每个域 F,char$F$ 是 0 或者某个素数，即 F 有子域 $\mathbb{Q}$ 或者子域 $\mathbb{Z}_p$(是在同构意义下，往后不做强调)

例 1.6. 设 F 是域，$\mathrm{char}F = p > 0$，则 $f : F \longrightarrow F, \alpha \longmapsto \alpha^p$ 是域同态, 特别地，当 F 是有限域时，f 是域同构.

命题 1.4. 设有扩张 E/F，其中 $E = F(\alpha_1, \cdots, \alpha_n), \alpha_i$ 是 F 代数元，则 E/F 是有限扩张, 自然也是代数扩张.

证明. E/F 可以看成若干单代数扩张，由有限扩张的传递性 [命题, 1.2]，我们只要证明 $F(\alpha)/F$ 是代数扩张即可，其中 α 是 F 代数元. 设 f 是 α 的极小多项式，记 $\deg f = n$，则

$$F(\alpha) = \left\{ a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1} \mid a_i \in F \right\} = \mathrm{span}_F \left\{ 1_F, \alpha, \cdots, \alpha^{n-1} \right\}$$

即 $[F(\alpha), F] = n < \infty$. ■

命题 1.5. 代数扩张具有传递性，即若 $F \subset K \subset E$，满足 $E/K, K/F$ 是代数扩张，则 E/F 也是代数扩张.

证明. 任意取定 $\alpha \in E$，则存在 $f \in K[x]$，使得 $f(\alpha) = 0$. 不妨设 $f = x^n + \sum\limits_{i=0}^{n-1} a_i x^i$, 记 $K' = F(a_0, a_1, \cdots, a_{n-1})$，则由 [命题，1.4]，$K'/F$ 是有限扩张, 且 $K'(\alpha)/K'$ 也是有限扩张，于是 $K'(\alpha)/F$ 也是有限扩张，自然也是代数扩张. 特别地，α 是 F 代数元. ■

定义 1.1. 设有域扩张 E/F, 记 $\mathrm{Aut}(E)$ 是 E 的自同构群，即 E 到自身的域同构全体，定义

$$\mathrm{Gal}(E/F) = \{\sigma \in \mathrm{Aut}(E) \mid \sigma|_F = \mathrm{id}_F\}$$

则 $\mathrm{Gal}(E/F)$ 是群，称为是 E/F 的 Galois 群.

命题 1.6. 若 E/F 是有限扩张，则 $\mathrm{Gal}(E/F)$ 是有限群.

证明. 不妨设 $[E:F] = n$，且

$$E = \mathrm{span}_F \{\alpha_1, \cdots, \alpha_n\}$$

则对任意 $\sigma \in \mathrm{Gal}(E/F)$，$\sigma$ 完全是由 $(\sigma(\alpha_1), \cdots, \sigma(\alpha_n))$ 决定的. 记 $f_i \in F[x]$ 是 α_i 的极小多项式，则有

$$0 = \sigma(f_i(\alpha_i)) = \sigma\left((\alpha_i)^m + a_1(\alpha_i)^{m-1} + \cdots + a_m\right) = f_i(\sigma(\alpha_i))$$

即 σ 是 $X_i = \{\alpha \in E \mid f_i(\alpha) = 0\}$ 上的一个置换. 注意 $\bigcup_{i=1}^{n} X_i$ 是有限集，其上的置换有限，故而 $|\mathrm{Gal}(E/F)| < \infty$. ∎

定义 1.2. 反之，给定域 E，G 是 $\mathrm{Aut}(E)$ 的有限子群，定义

$$\mathrm{Inv}(G) = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in G\}$$

则 $\mathrm{Inv}(G)$ 是 E 的子域，称为是 G 在 E 上不动域.

命题 1.7. 按 [定义，1.2] 得到的域扩张 $E/\mathrm{Inv}(G)$ 是有限扩张，且 $[E:\mathrm{Inv}(G)] \leq |G|$

证明. 设 $G = \{\sigma_1, \cdots, \sigma_n\}$，我们只需证明对任意取定 $m > n$ 个 E 中元 $\alpha_1, \cdots, \alpha_m$，其在 $\mathrm{Inv}(G)$ 中线性相关即可. 考虑线性方程组

$$\sum_{i=1}^{m} \sigma_j(\alpha_i) x_i = 0, \quad 1 \leq j \leq n. \tag{1.1}$$

(1.1)中方程个数小于未知元个数，且方程系数是 E 中元素，于是方程在 E 中有非零解 $\mathbf{x} = (x_1, \cdots, x_m) \in E^m$. 注意 σ_j 是同构, 则对方程(1.1)的每个属于 $\mathrm{Inv}(G)^m$ 的非零解 $\mathbf{x}$，都有 $\sum_{i=1}^{m} x_i\alpha_i = 0$.

下面我们只需在解空间中找到一个 $\mathrm{Inv}(G)$ 上的非零解. 取解 $\mathbf{x}$ 满足是方程(1.1)的非零解中含有非零元 x_i 最少的一个一个解，由于 $\mathbf{x}$ 非零，故不妨设 $x_1 \neq 0$，因此进一步可不妨设 $x_1 = 1$. 我们断言 $\mathbf{x}$ 是 $\mathrm{Inv}(G)$ 上的解，否则的话，存在 $\sigma \in G$，使得存在某个 x_i，满足 $\sigma(x_i) \neq x_i$，不妨设 $\sigma(x_2) \neq x_2$. 注意 $\sigma(\mathbf{x}) = (\sigma(x_1), \cdots, \sigma(x_m))$ 是方程组

$$\begin{aligned} 0 = \sigma\sigma_j\left(\sum_{i=1}^{m} x_i\alpha_i\right) &= \sum_{i=1}^{m} \sigma\sigma_j(\alpha_i)\sigma(x_i), \quad 1 \leq j \leq n \\ &= \sum_{i=1}^{m} \sigma_k(\alpha_i)\sigma(x_i), \quad 1 \leq k \leq n. \end{aligned} \tag{1.2}$$

的解，且方程 (1.1) 和方程 (1.2) 是同一个方程, 于是 $\sigma(\mathbf{x})$ 也是方程(1.1)的解，且由 $\mathbf{x}$ 取法可知 $\sigma(\mathbf{x})$ 与 $\mathbf{x}$ 的零元位置相同. 但是注意 $\sigma(\mathbf{x})-\mathbf{x}$ 也是方程(1.1)的非零解，且其第一个元素也是零，这与 $\mathbf{x}$ 取法矛盾. ■

引出两个问题：

问题 1

给定域扩张 E/F，则有 $F\subset \mathrm{Inv}(\mathrm{Gal}(E/F))$，进一步是否有 $F=\mathrm{Inv}(\mathrm{Gal}(E/F))$.

问题 2

设 E 是域，给定 $\mathrm{Aut}(E)$ 的有限群 G，则 $G\subset \mathrm{Gal}(E/\mathrm{Inv}(G))$，进一步是否有 $G=\mathrm{Gal}(E/\mathrm{Inv}(G))$.

第一个一般不正确，比如考虑域扩张 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$，第二个我们先做存疑.

2 环

2.1 分式域与中国剩余

设 R 是环，I 是 R 的子环，则 $R/I=\{r+I\mid r\in R\}$ 关于加法是一个 Abel 群，如果我们想在 R/I 上定义乘法，一种自然考虑是

$$(x+I)\cdot(y+I):=xy+I \tag{2.1}$$

如果(2.1)的定义是良定的，则容易验证 R/I 构成一个环. 要使得(2.1)的定义良定，即要保证: 若 $x_1-x_2\in I, y_1-y_2\in I$，要能推出 $x_1y_1-x_2y_2\in I$，即

$$x_1y_1-x_2y_2=\underset{\in I}{(x_1-x_2)}y_1+x_2\underset{\in I}{(y_1-y_2)}\in I$$

自然引出一个概念：设 I 是 R 的子环，如果对任意 $a\in I, r\in R$，有 $ar, ra\in I$，则称 I 为 R 的（双边）理想.

定理 2.1 (同态基本定理). *设 $f: R\longrightarrow S$ 是满的环同态，则 $R/\ker f\cong S$，且 S 中的理想与 R 中包含 $\ker f$ 的理想有一一对应关系.*

证明. 自然定义

$$\begin{aligned}\tilde{f}: R/\ker f &\longrightarrow S\\ r+\ker f &\longmapsto f(r)\end{aligned} \tag{2.2}$$

如果(2.2)的定义是良定的，则 $\tilde{f}$ 是环同态且是双射的验证是平凡的. 若 $x_1-x_2\in f$，则

$$\tilde{f}(x_1+\ker f)-\tilde{f}(x_2+\ker f)=f(x_1)-f(x_2)=f(x_1-x_2)=0$$

所以 $\tilde{f}$ 的定义是良定的，即不依赖于代表元的选取.

下设 R',S' 分别是 R 和 S 的理想，则 $f(R'),f^{-1}(S'):=\{r\in R\mid f(r)\in S\}$ 分别是 S 和 R 中理想，其中 $f(R')$ 是 S 中理想的验证需用到 f 是满的这一条件. 下面我们主要说明对应的唯一性，即若 R' 是 R 中包含 $\ker f$ 的理想，则有事实

$$R'=f^{-1}(f(R'))$$

换句话说即证明：若 R_1,R_2 是 R 中包含 $\ker f$ 的理想，且 $f(R_1)=f(R_2)$，则 $R_1=R_2$：

对任意 $r_1\in R_1$，存在 $r_2\in R_2$，使得 $f(r_1)=f(r_2)$，即 $r_1-r_2\in\ker f\subset R_2$，于是有 $r_1=(r_1-r_2)+r_2\in R_2$，也就是说 $R_1\subset R_2$，同理也有 $R_2\subset R_1$，这就得到 $R_1=R_2$. ■

设 $I_1,\cdots,I_r$ 是 R 的理想，则 $I_1+\cdots+I_r:=\{x_1+\cdots+x_r\mid x_i\in I_i\}$ 和 $\bigcap\limits_{i=1}^{r}I_r$ 都是 R 的理想.

若 $S\subset R$，记 $\langle S\rangle=$ 是包含 S 的 R 中最小理想，若 R 是交换幺环，则

$$\langle S\rangle=\left\{\sum_{i=1}^{m}x_iy_i\mid x_i\in S,y_i\in R,m\in N^+\right\}$$

设 R_1,R_2 是环，在 $R_1\times R_2=\{(r_1,r_2)\mid r_1\in R_1,r_2\in R_2\}$ 中定义如下加法和乘法：

$$\begin{aligned}(x_1,y_1)+(x_2,y_2)&:=(x_1+x_2,y_1+y_2)\\(x_1,y_1)\cdot(x_2,y_2)&:=(x_1x_2,y_1y_2).\end{aligned}\tag{2.3}$$

则 $R_1\times R_2$ 在运算(2.3)下构成环，称为 R_1 与 R_2 的直积. 一个简单的事实是：$R_1\cong R_1\times\{O_{R_2}\}$，$R_2\cong\{O_{R_1}\}\times R_2$，即 R_1,R_2 均可视为 $R_1\times R_2$ 的理想.

命题 2.2. *设 $I\subset J$ 是 R 中的两个理想，则 $I/(I\cap J)\cong(I+J)/J$.*

证明. 自然考虑 $f:I\longrightarrow(I+J)/J,x\longmapsto x+J$，则 f 是满的环同态，且 $\ker f=I\cap J$，由同态基本定理即得. ■

设 R 为交换环，I_1,I_2 是 R 中两个理想，定义

$$I_1I_2:=\left\{\sum_{i=1}^{m}x_iy_i\mid x_i\in I_1,y_i\in I_2\right\}\tag{2.4}$$

则 $I_1I_2\subset I_1\cap I_2$ 也是 R 的理想. 利用定义(2.4)，我们可以归纳定义：若 $I_1,\cdots,I_k$ 是 R 中理想，则

$$\prod_{i=1}^{k}I_k:=I_1(I_2\cdots I_k)=\left\{\sum_{i=1}^{m}x_{i1}x_{i2}\cdots x_{ik}\mid x_{ij}\in I_j\right\}$$

设 I,J 是 R 中理想，若 $R=I+J$，则称 I,J 是互素的.

引理 2.3. 设 R 为环，I, J 是 R 中互素理想，则 $R/(I \cap J) \cong (R/I) \times (R/J)$

证明. 自然考虑

$$f : R \longrightarrow (R/I) \times (R/J)$$
$$r \longmapsto (r + I, r + J)$$

f 是同态，以及 $\ker f = I \cap J$ 都是平凡的，下面我们主要说明 f 是满的. 任取 $r_1, r_2 \in R$，且

$$r_1 = x_1 + y_1$$
$$r_2 = x_2 + y_2$$

其中 $x_i \in I, y_i \in J$, 则有

$$\begin{aligned}(r_1 + I, r_2 + J) &= (x_1 + y_1 + I, x_2 + y_2 + J) = (y_1 + I, x_2 + J) \\ &= (x_2 + y_1 + I, x_2 + y_1 + J) = f(x_2 + y_1)\end{aligned}$$

这就证明了 f 是满射. ■

引理 2.4. 设 R 为交换幺环，$I_1, \cdots, I_n$ 是 R 中两两互素的理想，则 $I_1 \cdots I_{n-1}$ 与 I_n 互素.

证明. 只需注意

$$R \xrightarrow{R\text{中有幺元}} \underbrace{R \cdots R}_{n} = \prod_{k=1}^{n-1} (I_n + I_k) = I_n + I_1 \cdots I_{n-1}$$

■

命题 2.5 (中国剩余). 设 R 是交换幺环，且 $I_1, \cdots, I_n$ 是 R 中两两互素的理想，则

$$R/\left(\prod_{i=1}^{n} I_i\right) \cong (R/I_1) \times \cdots \times (R/I_n) \tag{2.5}$$

证明. 我们先证明 $I_1 I_2 = I_1 \cap I_2$，从而由 [引理，2.4] 可以归纳得到

$$I_1 \cdots I_n = (I_1 \cdots I_{n-1}) I_n = (I_1 \cdots I_{n-1}) \cap I_n = \left(\bigcap_{k=1}^{n-1} I_k\right) \cap I_n = \bigcap_{k=1}^{n} I_k.$$

注意 $I_1 \cap I_2$ 中元素 x 可以写为

$$x = x \cdot 1_R = x(y + z) = yx + xz \in I_1 I_2, \quad y \in I_1, z \in I_2$$

从而即得 $I_1I_2 = I_1 \cap I_2$. 下面我们归纳证明(2.5). 当 $n = 2$ 时，由 [引理，2.3] 已经做好. 对一般情形，由归纳假设则有

$$\begin{aligned} R/\left(\prod_{i=1}^{n} I_i\right) = R/\left(\bigcap_{i=1}^{n} I_i\right) &\cong \left(R/\left(\bigcap_{i=1}^{n-1} I_i\right)\right) \times (R/I_n) \\ &\cong (R/I_1) \times \cdots \times (R/I_n). \end{aligned}$$

■

称环 R 为整环，如果 R 是没有零因子的交换幺环. 令 $R^* = R \setminus \{0\}$ ，在 $R \times R^*$ 中定义关系为：$(r_1, s_1) \sim (r_2, s_2)$，如果 $r_1s_2 = r_2s_1$. 我们说明此关系是一种等价关系，其中自反性和对称性是显然的，下面主要说明传递性. 设 $(r_1, s_1) \sim (r_2, s_2), (r_2, s_2) \sim (r_3, s_3)$，则我们要证明 $r_1s_3 = r_3s_1$，由 $s_2 \neq 0$，我们只要说明 $r_1s_2s_3 = r_3s_1s_2$:

$$r_1s_2s_3 = (r_1s_2)s_3 = (r_2s_1)s_3 = (r_2s_3)s_1 = (r_3s_2)s_1 = r_3s_1s_2.$$

这就证明了上面关系是等价关系，则我们可以记 $F = (R \times R^*)/\sim$ 表示上面等价关系得到的等价类的集合，其中元素记为 $\frac{r}{s}$, 表示以 (r, s) 为代表元的等价类. 在 F 中定义如下加法和乘法

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &:= \frac{r_1s_2 + r_2s_1}{s_1s_2} \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &:= \frac{r_1r_2}{s_1s_2} \end{aligned} \tag{2.6}$$

我们说明(2.6)的定义是良定的，即若 $(r_1, s_1) \sim (r_1', s_1'), (r_2, s_2) \sim (r_2', s_2')$，能有

$$\begin{aligned} (r_1s_2 + r_2s_1, s_1s_2) &\sim (r_1's_2' + r_2's_1', s_1's_2') \\ (r_1r_2, s_1s_2) &\sim (r_1'r_2', s_1's_2') \end{aligned}$$

验证有

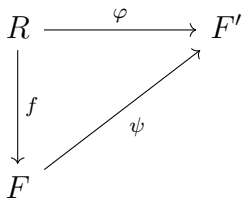
$$\begin{aligned} (r_1s_2 + r_2s_1)s_1's_2' = (r_1s_1')s_2s_2' + (r_2s_2')s_1s_1' = (r_1's_1)s_2s_2' + (r_2's_2)s_1s_1' = (r_1's_2' + r_2's_1')s_1s_2 \\ r_1r_2s_1's_2' = (r_1s_1')(r_2s_2') = (r_1's_1)(r_2's_2) = r_1'r_2s_1s_2. \end{aligned}$$

这样我们就完成了定义良定性的验证，则 F 在(2.6)的加法和乘法下构成一个整环，且

$$\begin{aligned} O_F &= \frac{O_R}{s}, \quad \forall s \in R^* \\ 1_F &= \frac{1_R}{1_R} = \frac{s}{s}, \quad \forall s \in R^* \end{aligned}$$

那么对任意 F 中非零元 $\frac{r}{s}(r \neq 0)$，$\frac{s}{r}$ 是有意义的，且 $\frac{r}{s} \cdot \frac{s}{r} = 1_F$，于是 F 是域，称为 R 的分式域.

命题 2.6. 设 R 是整环，F 是 R 的分式域. 若 φ 是 $R \longrightarrow F'$ 的单同态，其中 F' 是域，则存在唯一的同态 $\psi : F \longrightarrow F'$ 使得如下交换图成立，即分式域唯一.



其中 $f : r \mapsto \dfrac{r}{1}$ 为自然嵌入.

证明. 存在性：定义 $\psi : \dfrac{r}{s} \mapsto \varphi(r)\varphi(s)^{-1}$, 容易验证 ψ 是环同态，且 $\varphi = \psi \circ f$. 下面主要证明唯一性.

若 $F \to F'$ 的域同态 ψ_1, ψ_2 满足 $\varphi = \psi_1 \circ f = \psi_2 \circ f$, 即 $\psi_1\left(\dfrac{r}{1}\right) = \psi_2\left(\dfrac{r}{1}\right), \forall r \in R$, 我们证明 $\psi_1 = \psi_2$. 设 $r \neq 0$，则由域之间同态的性质有

$$\psi_1\left(\frac{1}{r}\right) = \psi\left(\left(\frac{r}{1}\right)^{-1}\right) = \psi_1\left(\frac{r}{1}\right)^{-1} = \psi_2\left(\frac{r}{1}\right)^{-1} = \psi_2\left(\frac{1}{r}\right)$$

于是对于 F 中非零元 $\dfrac{r}{s}(r \neq 0)$，我们有

$$\psi_1\left(\frac{r}{s}\right) = \psi_1\left(\frac{r}{1} \cdot \frac{1}{s}\right) = \psi_1\left(\frac{r}{1}\right) \cdot \psi_1\left(\frac{1}{s}\right) = \psi_2\left(\frac{r}{1}\right) \cdot \psi_2\left(\frac{1}{s}\right) = \psi_2\left(\frac{r}{s}\right)$$

且环同态，都自然的将零元映为零元，于是 $\psi_1 = \psi_2$. ■

设 R 是交换幺环，I 是 R 的理想，则 R/I 是交换幺环，若要求 R/I 是整环，则要求, 若

$$(a + I) \cdot (b + I) = a \cdot b + I = I$$

能够推出 $a + I = I$ 或者 $b + I = I$，换句话说 $ab \in I$，能够推出 $a \in I$ 或者 $b \in I$. 于是引出

定义 2.1. 设 R 是环，$I \neq R$ 是 R 中理想，称 I 是素理想，如果对于 $ab \in I$，能推出 $a \in I$ 或者 $b \in I$.

设 R 是交换幺环，I 是 R 中理想，如果要求 R/I 是域，首先要保证 R/I 只有平凡的理想，这意味着包含 I 的 R 中理想只能是 I 或者是 R. 自然引出

定义 2.2. 设 R 是环，$I \neq R$ 是 R 中理想，称 I 是 R 中极大理想，如果包含 I 的理想只有 I 和 R.

命题 2.7. 在交换幺环 R 中，I 是 R 中理想，则 R/I 是域当且仅当 I 是极大理想.

证明. 当 R/I 是域时，则对任意 $a \notin I$，存在 $b \in R$，使得 $ab - 1_R \in I$. 于是若 R 中理想 J 满足 $J \supsetneq I$，则存在 $a \in J \setminus I$，以及相应的 $b \in R$，使得 $ab - 1_R \in I \subset J$，注意 $ab \in J$，这意味着 $1_R = ab - (ab - 1_R) \in J$，于是 $J = R$.

反之，当 I 是极大理想时，由 R/I 中理想与 R 中包含 I 的理想有一一对应关系，这意味着 R/I 只有平凡理想，则对任意 $a \notin I$，有

$$R/I = \langle a+I \rangle = \{(a+I)(b+I) \mid b \in R\} = \{ab+I \mid b \in R\}$$

特别地，存在某个 $b \in R$, 使得 $1_R + I = (a+I)(b+I)$，这意味着 $a+I$ 有乘法逆元，于是 R/I 是域. ■

2.2 整环上的讨论

设 R 是整环，$a, b \in R$，若存在 $c \in R$，使得 $a = bc$，则称 $b|a$，b 视为 a 的因子. 记 U 是 R 中乘法可逆元全体，其中元素称为单位. 若存在 $c \in U$，使得 $a = bc$，则称 a 与 b 相伴，记为 $a \sim b$. 注意相伴关系是一种等价关系.

设 R 是整环，且 $a \in R$，称与 a 相伴的元素以及单位是 a 的平凡因子. 如果 $a \in R^* \setminus U$(即不考虑单位) 没有非平凡因子，则称 a 是 R 中的不可约元素.

设 R 是整环，如果 $p \in R^* \setminus U$，满足 $p \mid ab$，能够推出 $p \mid a$ 或者 $p \mid b$，则称 p 是 R 中素元素.

设 R 是整环，从理想的角度来看，$a \in R$ 是不可约元当且仅当 $\langle a \rangle$ 是极大主理想.$p \in R$ 是素元，当且仅当 $\langle p \rangle$ 是素理想.

简单事实有：素元都是不可约元.

称整环 R 满足素性条件，如果 R 中不可约元都是素元，即不可约元与素元等价.

设 R 是整环，$a, b \in R$，如果存在 a, b 的公因子 d，满足对任意 a, b 的共因子 d_1，都有 $d_1 \mid d$，则称 d 是 a, b 的最大公因子，简单事实是：最大公因子在相伴意义下唯一，所以如果 d 是 a, b 的一个最大公因子，我们就简记为 $d \sim (a, b)$.

定义 2.3. *设 R 是整环，如果 R 中任何两个元素都有最大公因子，则称 R 是满足最大公因子条件的整环，简称为 GCD 整环.*

在 GCD 整环中，有如下简单性质：$c(a, b) \sim (ca, cb)$; $((a, b), c) \sim (a, (b, c))$; 于是当 $(a, b) \sim 1, (a, c) \sim 1$ 时，

$$(a, bc) \sim ((a, ac), bc) \sim (a, (ac, bc)) \sim (a, c) \sim 1.$$

引理 2.8. *设 R 是 GCD 整环，则 R 满足素性条件.*

证明. 设 p 是 R 中不可约元，若 $p \mid ab$，且 $p \nmid a, p \nmid b$，这意味着 $(p, a) \sim 1, (p, b) \sim 1$，于是 $(p, ab) \sim 1$，这与 $p \mid ab$ 矛盾，于是 p 是素元. ■

定义 2.4. *设 R 是整环，若对任意 $a, b \in R$，存在 $d \in R$，使得 $\langle a \rangle + \langle b \rangle = \langle d \rangle$，即主理想加主理想仍是主理想，则称 R 是 Bezout 整环.*

引理 2.9. *Bezout 整环都是 GCD 整环.*

证明. 对任意 $a,b\in R$，设 $\langle a\rangle+\langle b\rangle=\langle d\rangle$. 由 $\langle a\rangle\subset\langle d\rangle,\langle b\rangle\subset\langle d\rangle$，得 d 是 a,b 的公因子. 且存在 $u,v\in R$，使得 $au+bcv=d$, 这意味着 a,b 的任何公因子都要整除 d，于是 d 就是 a,b 的一个最大公因子. ■

定义 2.5. 设 R 是整环，如果 R 中理想都是主理想，则称 R 是主理想整环，简称为 PID 整环.

由定义，主理想整环是比 Bezout 整环性质更好的环.

定义 2.6. 设 R 是整环，称 R 是唯一分解整环（简称为 UFD 整环），如果对任意 $a\in R^*\setminus U$，a 可分解为有限不可约元素的积，且在相伴意义下，分解唯一，即若

$$a=p_1\cdots p_s=q_1\cdots q_m$$

其中 p_i,q_j 都是不可约元，则 $s=m$, 且存在 $\sigma\in S_m$，使得 $q_i\sim p_{\sigma(i)}$.

定义 2.7. 设 R 是整环，如果 R 中不存在真因子序列 $\{a_i\}_{i=1}^{\infty}$，其中 a_{i+1} 是 a_i 的真因子，则称 R 满足因子链条件.

设整环 R 满足因子链条件，意味着若 $a\in R^*\setminus U$，则 a 从任意方式都可分解为有限不可约元素的乘积. 从理想的角度看，若有主理想升链

$$\langle a_1\rangle\subset\langle a_2\rangle\subset\cdots\subset\langle a_n\rangle\subset\cdots$$

则存在 j，使得当 $k\geq j$ 时，$\langle a_k\rangle=\langle a_j\rangle$.

定理 2.10. 设 R 是整环，则 R 是唯一分解整环当且仅当 R 满足素性条件和因子链条件.

证明. 设 R 是唯一分解整环，则对任意 $a,b\in R$，由唯一有限分解性，R 满足因子链条件，且可以将 a,b 表示为如下形式

$$a=p_1^{r_1}\cdots p_s^{r_s},\quad r_i\geq 0$$
$$b=p_1^{k_1}\cdots p_s^{k_s},\quad k_i\geq 0$$

其中 p_i 是不可约元，且 p_i^0 应视为 R 中幺元或者某个单位. 那么 $d=\prod_{i=1}^{s}p_i^{\min\{r_i,k_i\}}$ 就是 a,b 的一个最大公因子，由 [引理，2.8]，R 满足素性条件.

反之，因子链条件保证对任意 $a\in R^*\setminus U$，a 至少存在一种有限分解. 若

$$a=p_1\cdots p_s=q_1\cdots q_m$$

是 a 的两种不可约分解，则由素性条件，对每个 p_i，存在 q_j，使得 $p_i\sim q_j$，这也意味着 $s\leq m$，否则 p_s 只能是单位，矛盾. 同理，应该也要有 $m\leq s$，于是唯一性即证. ■

命题 2.11. 主理想整环是唯一分解整环.

证明. 设 R 是主理想整环，由 [引理，2.8，2.9]，R 满足素性条件. 若

$$\langle a_1\rangle \subset \langle a_2\rangle \subset \cdots \subset \langle a_n\rangle \subset \cdots$$

是 R 中主理想升链，则 $I = \bigcup_{i=1}^{\infty} \langle a_i\rangle$ 是 R，其中验证最关键的是 I 是否构成子环，即若 $x, y \in I$，设 $x \in \langle a_k\rangle, y \in \langle a_j\rangle$，不妨设 $j \geq k$，则 $x - y \in \langle a_j\rangle \subset I$.

由 I 是主理想，则存在 $d \in I$，使得 $I = \langle d\rangle$，特别地，由 $d \in I$，得到存在 j，使得 $d \in \langle a_j\rangle$，于是 $\langle d\rangle \subset \langle a_j\rangle$，那么就有 $\langle d\rangle = \langle a_j\rangle$. 于是当 $k \geq j$ 时，$\langle a_k\rangle = \langle a_j\rangle$. ■

定义 2.8. 设 R 是整环，若存在映射 $\delta : R^* \longrightarrow N$，满足对任意 $a \in R, b \in R^*$，存在 $q, r \in R$，使得 $a = bq + r$，其中 $r = 0$，或者有 $\delta(b) < \delta(r)$，则称 R 是欧几里得整环，δ 为 R 的一个欧几里得赋值.

命题 2.12. 欧几里得整环是主理想整环，从而是唯一分解整环.

证明. 设 R 是欧几里得整环，δ 为 R 的一个欧氏赋值，I 是 R 中一个理想，则 $\delta(I)$ 是 N 的一个子集，从而存在最小元素，取 $a \in I$，满足 $\delta(a) = \min\{\delta(I)\}$. 则由 a 的取法，对任意 $b \in I$，一定有 $a \mid b$，于是 $I = \langle a\rangle$，即 R 是主理想整环. ■

2.3 唯一分解多项式环

设 R 是环，一个 R 上的多项式是指如下形式

$$p(x) = \sum_{i=0}^{n} a_i x^i, \quad a_i \in R, \quad n \geq 0.$$

a_i 称为多项式系数. 我们记 $R[x]$ 为系数在 R 上的所有多项式全体，即

$$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in R, 0 \leq n \in \mathbb{Z} \right\}.$$

两个多项式相等如果它们的系数完全相同. 如果 $p(x) = \sum_{i=0}^{n} a_i x^i$ 且 $a_n \neq 0$，则我们称 n 是多项式 $p(x)$ 的次数，记为 $\deg p$. 系数 a_n 称为多项式 $p(x)$ 的首项系数. 我们定义零多项式的次数为 $-\infty$.

对于一个多项式 $p(x) = \sum_{i=0}^{n} a_i x^i$，当 $k > \deg p$. 时，我们假定 $a_k = 0$. 那么给定两个多项式 $p(x) = \sum_{i=0}^{n} a_i x^i$ 和 $q(x) = \sum_{i=0}^{m} b_i x^i$，我们就可以定义它们的和 $p(x) + q(x)$ 为

$$(p+q)(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i.$$

定义乘积 $p(x)q(x)$ 为

$$(pq)(x) = \sum_{i=0}^{m+n} c_i x^i,$$

其中

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

则在这两种运算下，$R[x]$ 构成一个环. 且若 1_R 是 R 中幺元，则 1_R 也是 $R[x]$ 中幺元.

当 R 为整环时，对任意 $f, g \in R[x]$，有 $\deg(fg) = \deg f + \deg g$，这意味着 $R[x]$ 也是整环，同时 $R[x]$ 中的单位一定也是 R 中单位，因为若 $\deg f > 0$, 不会存在 $g \in R[x]$，使得

$$\deg(fg) = \deg f + \deg g = \deg(1_R) = 0.$$

引理 2.13. *设 R 是域，则 $R[x]$ 是欧几里得环.*

证明. 我们只要说明对任意 $f \in R[x], 0 \neq g \in R[x]$，使得存在 $q, r \in R[x]$，满足 $f = qg + r$，其中 $r = 0$ 或者 $\deg r < \deg g$，这样 deg 就是 $R[x]$ 中的一个欧氏赋值，从而 $R[x]$ 是欧几里得环.

除去平凡的情况，设 $\deg f = n, \deg g = m$，假定结论对次数小于 n 多项式成立，不妨设

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{i=0}^{m} b_i x^i, \quad n > m$$

则

$$\tilde{f} = f - \frac{a_n}{b_m} \cdot x^{n-m} \cdot g$$

的次数小于 n，由归纳假设即得. ∎

设 R 是唯一分解整环，对于 $f \in R[x]$，下面我们记 $\gcd(f)$ 表示 f 的各项系数的最大公因子，如果 $\deg(f) \sim 1$，则称 f 是本原多项式. 对任意 $f \in R[x]$，f 都可以写成 $f = cf_1$，其中 f_1 是本原多项式，且容易看出在相伴意义下, 这种分解唯一，即若 $f = c_1 f_1 = c_2 f_2$，其中 f_1, f_2 是本原的，则 c_1, c_2 相差一个 R 中单位.

设 R 是唯一分解整环, 若 $f \in R[x]$ 是本原的, 如果 f 有非平凡因子 g, 则 $\deg g > 0$. 那么对任意次数大于零的 $f \in R[x]$，由次数的有限性，f 可有限分解为

$$f = u \cdot f_1 \cdots f_s, \quad \deg f_i > 0, \quad u \in R$$

其中 f_i 是 $R[x]$ 中不可约元 (自然也是本原的)，再由 $u \in R$ 可以唯一有限分解，故 f 在 $R[x]$ 中存在有限不可约分解.

引理 2.14 (Gauss 引理). *设 R 是唯一分解整环，$f_1, f_2 \in R[x]$ 是本原的，则 $f_1 f_2$ 也是本原的.*

证明. 假如 $\gcd(f_1f_2)$ 不是单位，则由 R 是唯一分解整环，可以取 $\gcd(f_1f_2)$ 的一个不可约因子 p，其也是 R 中的素元，于是 $\widetilde{R}=R/\langle p\rangle$ 是整环，则 $\widetilde{R}[x]$ 也是整环. 考虑

$$\varphi : R[x] \longrightarrow \widetilde{R}[x]$$

$$\sum_{i=0}^{m} a_i x^i \longmapsto \sum_{i=0}^{m} (a_i+\langle p\rangle)x^i$$

则 φ 是环同态，且 $O_{\widetilde{R}}=\langle p\rangle=\varphi(f_1f_2)=\varphi(f_1)\varphi(f_2)$，这意味着 $\varphi(f_1)=O_{\widetilde{R}}$ 或者 $\varphi(f_2)=O_{\widetilde{R}}$，即 $p\mid \gcd(f_1)$ 或者 $p\mid \gcd(f_2)$，但是这与 f_1,f_2 本原相矛盾. ■

引理 2.15. *设 R 是唯一分解整环，F 是 R 的分式域，则对任意 $0\neq f\in F[x]$，存在 $r\in F$，和 $f_1\in R[x]$ 是本原的，使得 $f=rf_1$，且此分解在 R 中相伴关系下唯一*

证明. 存在性就是通分，即存在 $b\in R^*$，使得 $f=\dfrac{f'}{b}$，其中 $f'\in R[x]$，于是存在 $c\in R$，使得 $f=\dfrac{c}{b}f_1$，其中 $f_1(x)\in R[x]$ 是本原的，令 $r=\dfrac{c}{b}$ 即得. 若 f 存在两种分解，记为

$$f=\frac{c_1}{b_1}f_1=\frac{c_2}{b_2}f_2,$$

其中 $f_1,f_2\in R[x]$ 是本原的. 则有 $b_2c_1f_1=c_2b_1f_2$，于是存在 R 中单位 u，使得 $b_2c_1=ub_1c_2$，即 $\dfrac{c_1}{b_1}=u\dfrac{c_2}{b_2}$. ■

设 R 是唯一分解整环，F 是 R 的分式域，$f_1,f_2\in R[x]$ 是本原的，且存在 $u\in F$，使得 $f_1=uf_2$，则由 [引理，2.15] 分解的唯一性，一定有 $u\in R$.

引理 2.16. *设 R 是唯一分解整环，F 是 R 分式域，若 $f(\deg f>0)$ 是 $R[x]$ 中的不可约元，则 f 也是 $F[x]$ 中的不可约元.*

证明. 若 f 在 $F[x]$ 中存在真因子，即存在 $f_1,f_2\in F[x]$，满足 $f=f_1f_2$，其中 $\deg f_1>0,\deg f_2>0$. 则由 [引理，2.15]，存在 $r_1,r_2\in F$，使得 $f=r_1r_2f_1'f_2'$，其中 f_1',f_2' 是 $R[x]$ 中次数大于零的本原多项式. 由 [引理，2.14]，$f_1'f_2'$ 也是本原的，那么就有 $r_1r_2\in R$，这意味着 f 在 $R[x]$ 中可分解，矛盾. ■

命题 2.17. *设 R 是唯一分解整环，则 $R[x]$ 也是唯一分解整环.*

证明. 对于非平凡的情形，考虑 $f\in R[x]$，满足 $\deg f>0$，我们已经说明了 f 存在有限分解，若 f 存在两种有限分解

$$f=(u_1\cdots u_k)p_1\cdots p_s=(v_1\cdots v_l)q_1\cdots q_t,\quad u_m,v_n\in R,\quad \deg p_i>0,\quad \deg q_j>0$$

其中 u_m,v_n 是 R 中不可约元；p_i,q_j 是 $R[x]$ 中的不可约元，由 [引理，2.14]，$p_1\cdots p_s$ 与 $q_1\cdots q_t$ 也是 $R[x]$ 中本元多项式，则 $u_1\cdots u_k$ 与 $v_1\cdots v_l$ 相差一个 R 中单位，从而由 R 是唯一分解整环，得 $k=j$，且存在置换 $\sigma\in S_k$，使得 $u_i\sim v_{\sigma(i)}$.

再由 [引理，2.13]，f 在 $F[x]$ 中是唯一分解的，且由 [引理，2.16]，p_i, q_j 也是 $F[x]$ 中的不可约元，故 $s=t$，且对每个 p_i, 存在 q_j，和 $c_i \in F$，使得 $p_i = c_i q_j$，那么由 [引理，2.15] 分解的唯一性，一定有 $c_i \in R$, 且 $c_1 \cdots c_s$ 是 R 中单位，于是每个 c_i 都是 R 中单位，这就证明了唯一性. ■

3 群

3.1 交错单群 $A_n (n \geq 5)$

对任意 $\sigma \in S_n$，σ 都可以写为不相交轮换的乘积：

$$\sigma = (i_1 \cdots i_k) \cdots (j_1 \cdots j_t) \tag{3.1}$$

且在不记顺序情形之下，(3.1)表法唯一, 称为是 σ 的循环分解.

令 m_k 表示 σ 分解式 (3.1) 中长度为 k 的轮换个数，则我们可以记

$$\alpha_\sigma = (m_1, m_2, \cdots, m_n), \quad \sum_{k=1}^{n} k m_k = n.$$

我们用向量 $\vec{m} = (m_1, m_2, \ldots, m_n)$ 表示一种轮换型.

引理 3.1. *设 $\sigma, \tau \in S_n$，且 $\tau = (i_1 \cdots i_k)$，则*

$$\sigma\tau\sigma^{-1} = (\sigma(i_1) \cdots \sigma(i_k)) \tag{3.2}$$

证明. 对于任意 $j \in \{1, \ldots, n\}$, 当 $\sigma^{-1}(j) \notin \{i_1, \cdots, i_k\}$，即 $j \notin \{\sigma(i_1), \cdots, \sigma(i_k)\}$ 时，

$$\sigma\tau\sigma^{-1}(j) = j = (\sigma(i_1) \cdots \sigma(i_k))(j)$$

当 $\sigma^{-1}(j) \in \{i_1, \cdots, i_k\}$，即 $j \in \{\sigma(i_1), \cdots, \sigma(i_k)\}$ 时，不妨设 $j = \sigma(i_s)$，则

$$\sigma\tau\sigma^{-1}(j) = \sigma(i_{s+1}) = (\sigma(i_1) \cdots \sigma(i_k))(j)$$

这样即得. ■

由 [引理，3.1]，我们不难得到

命题 3.2. *设 $\sigma, \tau \in S_n$，则 σ, τ 相互共轭当且仅当 $\alpha_\sigma = \alpha_\tau$，即 σ, τ 要有相同的轮换型.*

群 S_n 是其所有互不相交的共轭类的并集. 因此，群的阶等于所有共轭类大小之和：

$$|S_n| = \sum_{C \in \mathrm{Conj}(S_n)} |C| \tag{3.3}$$

其中 $\mathrm{Conj}(S_n)$ 表示 S_n 共轭类的集合.

对于给定的轮换型 $\vec{m}$，其对应的共轭类 $C_{\vec{m}}$ 中包含的元素个数（即具有该轮换型的置换数量）由以下公式给出：

$$|C_{\vec{m}}| = \frac{n!}{\prod_{k=1}^{n} k^{m_k} \cdot m_k!} \tag{3.4}$$

式(3.4)的组合意义如下：

- 分子 $n!$ 是 n 个元素的全排列；
- 分母 k^{m_k} 消除了每个长度为 k 的轮换内部循环移位带来的重复；
- 分母 $m_k!$ 消除了 m_k 个相同长度轮换之间顺序交换带来的重复；

例 3.1. 对任意 $n \in N^+$，有如下组合恒等式成立

$$1 = \sum_{\substack{0 \le m_k \le n; \\ \sum_{k=1}^{n} k m_k = n}} \prod_{k=1}^{n} \frac{1}{(m_k)! \cdot k^{m_k}}$$

证明. 将共轭类大小公式(3.4)代入式 (3.3) ，就有

$$n! = \sum_{\substack{0 \le m_k \le n \\ \sum_{k=1}^{n} k m_k = n}} \frac{n!}{\prod_{k=1}^{n} k^{m_k} \cdot m_k!}$$

两边同时除以 $n!$ 即得. ■

引理 3.3. *对于 $n \ge 3$，交错群 A_n 由所有的 3-轮换生成.*

证明. A_n 中的元素是偶置换，即偶数个对换的乘积. 因此只需证明任意两个对换的乘积可以写成 3-轮换的乘积即可. 设 i, j, k, l 互不相同，则

$$\begin{aligned} (ij)(jk) &= (ijk) \\ (ij)(kl) &= (ij)(jk)(jk)(kl) = (ijk)(jkl) \end{aligned} \tag{3.5}$$

式(3.5)已经包含了所有可能轮换乘积的情形，这样我们就完成了证明. ■

引理 3.4. *对于 $n \ge 5$，A_n 中所有的 3-轮换在 A_n 中共轭.*

证明. 由 [命题，3.2]，在 S_n 中，所有的 3-轮换属于同一个共轭类. 设 $\tau \in S_n$ 使得 $\tau\sigma_1\tau^{-1} = \sigma_2$，其中 σ_1, σ_2 为任意两个 3-轮换.

- 若 $\tau \in A_n$，则结论显然成立.
- 若 $\tau \notin A_n$ (即 τ 为奇置换)，由于 $n \ge 5$，我们总可以找到两个元素 d, e 不在 σ_1 的变动元中. 令 $\tau' = \tau(de)$. 此时 τ' 为偶置换，即 $\tau' \in A_n$. 且由于 (de) 与 σ_1 不相交，(de) 与 σ_1 可交换，故：

$$\tau'\sigma_1(\tau')^{-1} = \tau(de)\sigma_1(de)^{-1}\tau^{-1} = \tau\sigma_1\tau^{-1} = \sigma_2$$

综上，在 $n \geq 5$ 时，任意两个 3-轮换在 A_n 中也是共轭的. ■

定理 3.5. *当 $n \geq 5$ 时，交错群 A_n 是单群.*

证明. 设 $N \neq \{e\}$ 是 A_n 的正规子群，我们要证明 $N = A_n$. 由 [引理，3.3]，我们只要证明 N 包含 A_n 中所有 3-轮换. 再由 [引理，3.4]，我们只要证明 N 中有一个 3-轮换.

任取 $\sigma \in N, \sigma \neq (1)$. 我们对 σ 的循环分解进行分类讨论：

情形 1：σ 的分解中包含一个长度 $r \geq 4$ 的轮换

不妨设 $\sigma = (1\,2\,3 \ldots r)\tau$，其中 τ 是与其他元素不相交的置换. 令 $\delta = (1\,2\,3) \in A_n$. 考虑换位子 $\rho = \sigma\delta\sigma^{-1}\delta^{-1}$. 由于 $N \trianglelefteq A_n$，故 $\rho \in N$.

$$\begin{aligned}\rho &= \sigma(1\,2\,3)\sigma^{-1}(1\,3\,2)\\ &= (\sigma(1)\,\sigma(2)\,\sigma(3))(1\,3\,2)\\ &= (2\,3\,4)(1\,3\,2)\\ &= (1\,2\,4)\end{aligned}$$

计算结果 $(1\,2\,4)$ 是一个 3-轮换. 故 N 包含 3-轮换.

情形 2：σ 的分解中包含至少两个不相交的 3-轮换

不妨设 $\sigma = (1\,2\,3)(4\,5\,6)\tau$. 令 $\delta = (1\,2\,4) \in A_n$. 同样考虑换位子 $\rho = \sigma\delta\sigma^{-1}\delta^{-1} \in N$.

$$\begin{aligned}\rho &= \sigma(1\,2\,4)\sigma^{-1}(1\,4\,2)\\ &= (\sigma(1)\,\sigma(2)\,\sigma(4))(1\,4\,2)\\ &= (2\,3\,5)(1\,4\,2)\\ &= (1\,4\,2\,3\,5)\end{aligned}$$

此时 ρ 是一个 5-轮换. 这将我们带回了**情形 1**（循环长度 ≥ 4）. 对 ρ 再次应用**情形 1** 的方法，即可得到 N 包含 3-轮换.

情形 3：σ 是若干不相交的对换（2-轮换）之积

由于 σ 是偶置换，它至少包含两个对换. 不妨设 $\sigma = (1\,2)(3\,4)\tau$，其中 τ 固定 $1, 2, 3, 4$. 由于 $n \geq 5$，必然存在元素 5. 令 $\delta = (1\,2\,5) \in A_n$. 构造元素 $\sigma' = \delta\sigma\delta^{-1} \in N$，则

$$\sigma' = (1\,2\,5)[(1\,2)(3\,4)\tau](1\,5\,2) = (2\,5)(3\,4)\tau$$

注意 δ 仅影响 $1,2,5$，而 τ 与这些无关，故 τ 保持不变. 现在考虑 $\sigma'\sigma^{-1} \in N$:

$$\begin{aligned}\sigma'\sigma^{-1} &= [(2\,5)(3\,4)\tau]\cdot[\tau^{-1}(3\,4)(1\,2)]\\ &= (2\,5)(3\,4)(3\,4)(1\,2)\\ &= (2\,5)(1\,2)\\ &= (1\,2\,5)\end{aligned}$$

结果 $(1\,2\,5)$ 是一个 3-轮换. 故 N 包含 3-轮换.

综上所述，无论 σ 属于何种循环类型，N 中必然包含一个 3-轮换. 因此 $N = A_n$，即 A_n 是单群. ■

例 3.2. 当 $n \geq 5$ 时，S_n 的非平凡正规子群只有 A_n.

证明. 设 $\{e\} \neq N$ 是 S_n 的正规子群，则 $A_n \cap N$ 也是 S_n 的正规子群，由 A_n 是单群，只可能是 $A_n \cap N = A_n$ 或者 $A_n \cap N = \{e\}$. 但是另一方面，由第二同构有

$$|NA_n/A_n| = |A_n/(A_n \cap N)| \leq 2$$

这意味着不可能有 $A \cap N = \{e\}$，于是 $A_n \subset N$. 若 $N \neq A_n$，则 N 中有一个奇置换 σ，那么 $\sigma A_n \subset N$ 就是 S_n 的所有奇置换，此时 $N = S_n$. ■

例 3.3. 当 $n \geq 3$ 时，$C(S_n) = \{(1)\}$ 是平凡的.

证明. 对任意 $(1) \neq \sigma \in S_n$，则存在 $i \in \{1, \cdots, n\}$，使得 $\sigma(i) \neq i$，记 $j = \sigma(i)$，于是 $n \geq 3$，可取 k，使得 i, j, k 互不相同. 考虑 $\tau = (jk)$，则 $j = \sigma\tau(i) \neq \tau\sigma(i) = k$，这意味着 $\sigma \notin C(S_n)$，于是 $C(S_n) = \{(1)\}$. ■

3.2 有限群的合成序列

设 G 是群，H, K 是 G 的子群，令

$$HK = \{hk \mid h \in H, k \in K\}$$

若我们要求 HK 是 G 的子群，则首先要有 HK 中元素逆的全体 $KH \subset HK$，即要有 $HK = KH$. 且当 $HK = KH$ 时，

$$(h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1h_2)'k_2' = h_1h_3k_3k_2' \in HK$$

即 HK 是 G 子群，且

$$h_1K = h_2K \Longleftrightarrow h_2^{-1}h_1 \in K \Longleftrightarrow h_2^{-1}h_1 \in H \cap K \Longleftrightarrow h_1(H \cap K) = h_2(H \cap K)$$

这样就得到

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

特别地，当 H 或 K 是 G 正规子群，则 HK 是 G 的子群.

设 G 是群，H_1, H_2, H_3 是 G 的子群，则有

$$H_1 \cap (H_2H_3) \supset (H_1 \cap H_2)(H_1 \cap H_3).$$

特别地，当 $H_2 \subset H_1$ 或者 $H_3 \subset H_1$ 时，有

$$H_1 \cap (H_2H_3) = (H_1 \cap H_2)(H_1 \cap H_3). \tag{3.6}$$

定义 3.1. *设 G 为群，设有 G 的子群列*

$$G = G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_{t+1} = \{e\} \tag{3.7}$$

若 $G_{i+1} \lhd G_i$，则称(3.7)是 G 的次正规序列. 若还有 G_i/G_{i+1} 是单群，则称(3.7)是 G 的合成序列，G_i/G_{i+1} 称为 G 的合成因子.

设 G 是有限群，若 G 不是单群，则取 H_1 是 G 的非平凡正规子群，考虑 G/H_1，记 π_1 是 $G \longrightarrow G/H_1$ 的自然同态. 若 G/H_1 不是单群，取 H_2' 是 G/H_1 的非平凡正规子群，则 $H_2 = \pi_1^{-1}(H_2')$ 是 G 中真包含 H_1 的正规子群，再考虑 G/H_2. 由于群阶的有限性，总能找到 G_1，使得 G/G_2 是单群, 再对 G_2 做相同操作，有限步之后，会得到

$$G_1 = G \supsetneq G_2 \supsetneq \cdots \supsetneq G_{k+1} = \{e\}$$

是 G 的一个合成序列.

命题 3.6 (Jordan-Hölder)**.** *设 G 是群，若*

$$G = G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_{t+1} = \{e\}$$
$$G = H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_{s+1} = \{e\}$$

是 G 的两个合成序列，则 $t = s$，且对每个 i，存在对应 i'，使得 $H_i/H_{i+1} \cong G_{i'}/G_{i'+1}$.

证明. 对每个 H_i，有

$$H_i = (H_i \cap H_1) \supset (H_i \cap G_2) \supset \cdots \supset (H_i \cap G_{t+1}) = \{e\} \tag{3.8}$$

除去其中相同的项，(3.8)就是 H_i 的一个次正规列. 由于 H_i/H_{i+1} 是单群，那么包含 H_{i+1} 的 H_i 中正规子群只有 H_i 和 H_{i+1}，则在

$$H_i = (H_i \cap H_1)H_{i+1} \supset (H_i \cap G_2)H_{i+1} \supset \cdots \supset (H_i \cap G_{t+1})H_{i+1} = H_{i+1}$$

中，对每个 G_k, 要么有 $(G_k \cap H_i)H_{i+1} = H_i$，要么就有 $(G_k \cap H_i)H_{i+1} = H_{i+1}$，于是存在唯一 i'，使得

$$(G_{i'} \cap H_i)H_{i+1} = H_i$$
$$(G_{i'+1} \cap H_i)H_{i+1} = H_{i+1}$$

这样由第二同构定理就有

$$\begin{aligned} H_i/H_{i+1} &= (G_{i'} \cap H_i)H_{i+1}/(G_{i'+1} \cap H_i)H_{i+1} \\ &\cong (G_i' \cap H_i)/((G_i' \cap H_i)) \cap (G_{i'+1} \cap H_i)H_{i+1} \\ &\xlongequal{(3.6)} (G_{i'} \cap H_{i+1})(G_{i'+1} \cap H_i) \end{aligned}$$

对 $G_{i'} \supset G_{i'+1}$，进行类似的操作，得到，存在唯一 j，使得使得

$$(G_{i'} \cap H_j)G_{i'+1} = G_{i'} \quad \text{且} \quad (G_{i'} \cap H_{j+1})G_{i'+1} = G_{i'+1}$$

则

$$G_{i'}/G_{i'+1} \cong (G_{i'} \cap H_j) \Big/ (G_{i'} \cap H_{j+1})(G_{i'+1} \cap H_j)$$

我们断言 $j = i$，这样就有 $H_i/H_{i+1} \cong G_{i'}/G_{i'+1}$.

若 $j \neq i$，不妨设 $i < j$，这意味着 $(G_{i'} \cap H_{i+1})G_{i'+1} = G_{i'}$，于是就有

$$\begin{aligned} H_i &= (H_i \cap G_{i'}) \cdot H_{i+1} \\ &= (H_i \cap (G_{i'} \cap H_{i+1})G_{i'+1})\, H_{i+1} \\ &= (G_{i'} \cap H_{i+1})(G_{i'+1} \cap H_i) \cdot H_{i+1} \\ &= (G_{i'} \cap H_{i+1}) \cdot H_{i+1} \subset H_{i+1} \end{aligned}$$

导出矛盾. 综上我们说明了指标集 $\{i\}$ 与 $\{i'\}$ 之间有一一对应关系，这就证明了我们的命题. ■

3.3 群作用与 Sylow 定理

设 G 是群，Ω 是一个集合，如果 $f : G \times \Omega \to \Omega, (g, x) \mapsto g \cdot x$ 满足

$$e_G \cdot x = x, \quad \forall x \in \Omega$$
$$(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x), \quad \forall g_1, g_2 \in G$$

则称 f 是 G 在 Ω 上的一个作用, 以后简记 $g \cdot x = gx$. 从同态角度来看，G 在 Ω 上作用全体与 $\mathrm{Hom}(G, S_\Omega)$ 有一一对应关系.

设 G 在 Ω 上有个作用，则对任意 $x \in \Omega$，称

$$Gx = \{gx \mid g \in G\}$$

是 x 的轨道. 称

$$G_x = \{g \in G \mid gx = x\} < G$$

是 x 的稳定子群. 在 Gx 中，有

$$g_1 x = g_2 x \Longleftrightarrow g_2^{-1} g_1 \in G_x \Longleftrightarrow g_1 G_x = g_2 G_x$$

于是 $|G_x| = [G : G_x] = \dfrac{|G|}{|G_x|}$(当 G 是有限群时). 如果 $|Gx| = 1$，即 $G_x = G$，则称 x 为 G 的不动点.

对任意 $x, y \in \Omega$，有简单的事实：$Gx = Gy$ 或者 $Gx \cap Gy = \varnothing$，于是有

$$\Omega = \bigcup_{x \in \Omega} Gx = \bigcup_{x \in R} Gx$$

其中 R 表示一个代表系，即对任意 $x, y \in R$，有 $Gx \cap Gy = \varnothing$，最终我们得到

$$|\Omega| = \sum_{x \in R} |Gx| = \sum_{x \in R} \frac{|G|}{|G_x|} = |X_0| + \sum_{x \in R \setminus X_0} \frac{G}{|G_x|} \tag{3.9}$$

其中 X_0 是 G 的不动点集.

设 $y \in Gx$，不妨设 $y = gx$，则若 $h \in G_y$，即有 $hy = h(gx) = (hg)x = y = gx$，这意味着 $g^{-1}hg \in G_x$，即 $h \in gG_xg^{-1}$，即 $G_y \subset gG_xg^{-1}$，比较两边元素个数，即得 $G_y = gG_xg^{-1}$，即稳定子群相互共轭.

我们称 G 在 Ω 上的作用是可迁的，如果 Ω 只有一个轨道，即存在 $x \in \Omega$，满足对任意 $y \in \Omega$，存在 $g \in G$，使得 $y = gx$，或等价刻画为，对任意 $x \in \Omega$，都有 $\Omega = Gx$，此时 $|\Omega|$ 是 $|G|$ 的因子.

我们称 G 在 Ω 上的作用是忠实的，如果

$$\{g \in G \mid gx = x, \forall x \in \Omega\} = \{e_G\}$$

换句话讲，即该作用诱导的同态 $\rho : G \to S_\Omega, \quad \rho(g)(x) := g \cdot x$ 是单同态, 也就是 G 可以视为 S_Ω 的一个子群.

例 3.4 (Burnside 引理)**.** 设有限群 G 作用在集合 X 上，且该作用下轨道个数为 t，对任意 $g \in G$，令

$$F(g) = \sharp\{x \in X \mid gx = x\}$$

则有

$$\sum_{g \in G} F(g) = t|G|$$

证明. 令 $\Omega = \{(g,x) \in G \times X \mid gx = x\}$, 下面我们用两种方法计算 $|\Omega|$. 先固定 g，则 $|\Omega| = \sum_{g\in G} F(g)$. 另外若先固定 x，记 X 的 t 个不同轨道为 $Gx_1, \cdots, Gx_t$，则

$$\Omega = \bigcup_{x\in X} G_x \times \{x\} = \bigcup_{i=1}^{t} \bigcup_{y\in Gx_i} G_y \times \{y\}$$

且当 $y \in Gx_i$ 时，$|G_y| = |G_{x_i}|$，于是得到

$$|\Omega| = \sum_{x\in X} |G_x| = \sum_{i=1}^{t} \sum_{y\in Gx_i} |G_y| = \sum_{i=1}^{t} |Gx_i| \cdot |G_{x_i}| = t|G|.$$

■

引理 3.7. *设 G 是有限群，p 是 $|G|$ 的一个素因子，则 G 中有 p 阶元.*

证明. 考虑集合

$$X = \{(a_1, \cdots, a_p) \mid a_i \in G, a_1 \cdots a_p = e\}$$

则 $|X| = |G|^{p-1}$. 设 $\sigma = (12\cdots p)$，则 $|\langle\sigma\rangle| = p$，考虑 $\langle\sigma\rangle$ 在 X 中的作用为

$$\psi(a_1, \cdots, a_p) := (a_{\psi(1)}, \cdots, a_{\psi(p)}) \in X, \quad \forall \psi \in \langle\sigma\rangle$$

则该作用下每个轨道元素个数只能是 p 或 1，若记 X_0 是 $\langle\sigma\rangle$ 的不动点集，则由(3.9)有，p 整除 $|G|^{p-1} - |X_0|$，于是 $p \mid |X_0|$，且 $|X_0| \neq 0$（因为 $(e, \cdots, e) \in X_0$），所以存在 $a \neq e$，使得 $a^p = e$，这意味着 a 的阶为 p. ■

命题 3.8 (sylow1). *设 G 是有限群，$p^k \mid |G|$，则 G 中有 p^k 阶群.*

证明. 对群 G 的阶进行归纳，假设结论对阶数小于 $|G|$ 的群成立. 考虑 G 到自身的共轭作用，则该作用下 G 的不动点集为 $C(G)$, 由 (3.9)就有

$$|G| = |C(G)| + \sum_{g\in R, g\notin C(G)} [G : C(g)]$$

若 $p||C(G)|$，由 [引理，3.7]，$|C(G)|$ 中有 p 阶元 a，且 $\langle a\rangle \lhd G$，于是可以考虑商群 $G/\langle a\rangle$ ，那么由归纳假设 $G/\langle a\rangle$ 中有 p^{k-1} 阶群 $H/\langle a\rangle$，则 $|H| = |H : \langle a\rangle| \cdot |\langle a\rangle| = p^k$，即 H 是 G 的 p^k 阶群.

若 $p \nmid |C(G)|$，则存在 $g \notin C(G)$，使得 $p \nmid [G : C(g)]$，于是 $p^k \mid C(g)$. 由于 $|C(g) < |G|$，则由归纳假设 $C(g)$ 中有 p^k 阶子群 H, 其自然也是 G 的 p^k 阶子群. ■

设 $|G| = p^k m$，其中 $(p, m) = 1$，则 [命题，3.8] 说明了 G 中 p^k 阶群的存在性，我们称 G 中的 p^k 阶群为 G 的 sylow-p 群.

命题 3.9 (sylow2). *设 G 是有限群，且 $|G| = p^k m, (p, m) = 1$，则 G 的 sylow-p 群相互共轭.*

证明. 设 H 是 G 的一个 sylow-p 群. 对任意 G 的 sylow-p 群 K，考虑 K 在 G/H 上的左诱导作用：

$$k(gH) := (kg)H.$$

记 X_0 为 K 的不动点集，则 $(|K|, |G/H|) = 1$，且由(3.9)有

$$|G/H| \equiv |X_0| \pmod{p},$$

于是 $|X_0| \neq 0$，即 K 有不动点 gH：满足对任意 $k \in K$，有 $kgH = gH$，即 $g^{-1}kg \in H$，即 $k \in gHg^{-1}$，从而 $K \subset gHg^{-1}$，比较两边元素个数就有 $K = gHg^{-1}$. ■

由 [命题，3.9]，$S = \{gHg^{-1} \mid g \in G\}$ 即是 G 所有 Sylow-p 群，且

$$g_1Hg_1^{-1} = g_2Hg_2^{-1} \iff g_2^{-1}g_1 \in N_G(H) \iff g_1N_G(H) = g_2N_G(H)$$

即 $|S| = [G : N_G(H)] \mid m$，是 G 所有不同的 sylow-p 群个数.

命题 3.10 (sylow3). *设 G 是有限群，$|G| = p^k m, (p, m) = 1$，记 n_p 是 G 的 sylow-p 群个数，则 $n_p \equiv 1 \pmod{p}$.*

证明. 设 H 是 G 的一个 sylow-p 群，考虑 H 在 $S = \{gHg^{-1} \mid g \in G\}$ 上的共轭作用：

$$h(gHg^{-1}) := hgH(hg)^{-1}.$$

设 gHg^{-1} 是 H 一个不动点，则对任意 $h \in H$，有 $(hg)H(hg)^{-1} = gHg^{-1}$，即 $g^{-1}Hg \subset N_G(H)$，也就是说 $g^{-1}Hg$ 也是 $N_G(H)$ 的 Sylow-p 群，但注意 $N_G(H)$ 的 sylow-p 群的个数为 $[N_G(H) : N_G(H)] = 1$，且 H 就是 $N_G(H)$ 的一个 sylow-p 群，于是就有 $g^{-1}Hg = H$，那么

$$gHg^{-1} = g(g^{-1}Hg)g^{-1} = H.$$

则 H 的不动点只有一个，由(3.9)就有 $n_p \equiv 1 \pmod{p}$. ■

有了 sylow 相关定理，就引出常见的一类问题，即判断一个群是否是单群，说明一个群不是单群要相对简单的多，下面列举一些常见的说明非单群手段.

例 3.5. 设 G 是交换群，则 G 是单群当且仅当 G 是素数阶的循环群.

例 3.6. 设 G 是一个有限群，其阶为 $|G| = p^n$，其中 p 为素数，且 $n > 1$, 则 G 不是单群. 特别地，当 $n = 2$ 时，G 还是交换群.

证明. 考虑 G 到自身的共轭作用，得到类方程

$$|G| = |C(G)| + \sum_{g \in R \setminus C(G)} [G : C(g)]$$

于是 $p \mid |C(G)|$. 若 $G = C(G)$，此时由 [例，3.5]，G 不是单群. 若 $C(G) \neq G$，则 $C(G)$ 就是 G 的非平凡的正规群.

当 $n = 2$ 时，若 $C(G) \neq G$，则只能是 $|C(G)| = p$. 取 $g \in G \setminus C(G)$，则 $|C(g)| > |C(G)| = p$，于是一定有 $|C(g)| = p^2$，这意味着 $g \in C(G)$，矛盾. ■

例 3.7. 设 $|G| = pq$，其中 p 和 q 是素数，且 $p < q$, 则 G 不是单群.

证明. 由 sylow 第三定理有 $n_q \mid p$，且 $n_q \equiv 1 \pmod{q}$，那么只能是 $n_q = 1$，即 G 的 sylow-q 群是 G 的非平凡正规子，所以 G 不是单群. ■

例 3.8. 设 $|G| = p^2q(p \neq q)$，其中 p, q 为素数，则 G 不是单群.

证明. 当 $p > q$ 时，由 $n_p \mid q$，且 $n_p \equiv 1 \pmod{p}$, 这意味着只能是 $n_p = 1$，故 G 是单群.

当 $p < q$ 时，由 $n_q \mid p^2$，且 $n_q \equiv 1 \pmod{q}$，则可能的情形为 $n_q = 1$ 或者 $n_q = p^2$. 若 $n_q = p^2$, 由于 q 是素数，则任何两个不同 G 的 sylow-q 群的交只能是单位元，于是 G 中有 $p^2(q-1)$ 个 q 阶元，这些元素都不能是 G 的 sylow-p 群中的元素，所以唯一可能的情形是 G 剩下的 p^2 个元素刚好构成 G 的一个 sylow-p 群，即 $n_p = 1$，于是 G 不是单群. ■

例 3.9. 设 H 是 G 的子群，且 $[G : H] = n$，则存在 G 的正规子群 $K \subset H$，使得 $[G : k] \mid n!$. 特别地，当 H 是 G 的真子群，且 $|G| \nmid n!$ 时，K 是 G 的非平凡正规子群，即 G 不是单群.

证明. 考虑 G 在集合 G/H 上的左诱导作用，其诱导了一个同态：$\rho : G \longrightarrow S(G/H)$，记 $K = \ker \rho$，则由同态基本定理，$G/K \cong \mathrm{im}\rho$，取阶数就有 $[G : K] \mid n!$. 另外注意

$$K = \ker \rho = \bigcap_{g \in G} gHg^{-1} \subset H$$

这样就完成了证明. ■

例 3.10. 设 $|G| = p^k m, (m, p) = 1$，若 n_P 表示 G 的 sylow-p 群的个数，则当 $|G| > n_p!$ 时，G 不是单群.

证明. 下面考虑 $n_p > 1$ 情形. 令 $X = \left\{P_1, \cdots, P_{n_p}\right\}$ 是 G 的 sylow-p 群的集合，考虑 G 在 X 上的共轭作用，其诱导了一个同态：$\rho : G \longrightarrow S(X)$，则有

$$1 \leq [G : \ker \rho] = |\mathrm{im}\rho| \leq n_p! < |G|$$

我们下面说明 $[G : \ker \rho] > 1$，从而 $\ker \rho$ 即是 G 的非平凡正规子群，于是 G 不是单群.

若 $[G : \ker \rho] = 1$，这意味着对任意 $g \in G$，有 $gP_1g^{-1} = P_1$, 即 $g \in N_G(P_1)$，也就是 $G = N_G(P_1)$，则 $n_p = 1$，矛盾. ■

3.4 有限生成 Abel 群分类

设 $G_1,\cdots,G_n$ 是群，在 $G=G_1\times\cdots\times G_n$ 上定义乘法运算为

$$(x_1,x_2,\cdots,x_n)\cdot(y_1,y_2,\cdots,y_n):=(x_1y_1,x_2y_2,\cdots,x_ny_n) \tag{3.10}$$

则 G 在(3.10)运算下构成群，称为是 $G_1,\cdots,G_n$ 的外直积. 考虑

$$\pi_i:G_i\longrightarrow G$$

$$g_i\longmapsto(e,e,\cdots,g_i,\cdots,e)$$

则 π_i 是单同态，$G_i'=\mathrm{im}\pi_i$ 是 G 的正规子群，并满足 $G=G_1'\cdots G_n'$，以及

$$G_i'\cap\prod_{j\neq i}^{n}G_j'=\{e_G\},\quad 1\leq i\leq n$$

这引出群内直积的概念

定义 3.2. 设 G 为群，$G_1,\cdots,G_n$ 是 G 的正规子群，且 $G=G_1\cdots G_n$，称 G 是 $G_1,\cdots,G_n$ 的内直积，如果

$$G_i\cap\prod_{j\neq i}^{n}G_j=\{e_G\},\quad 1\leq i\leq n \tag{3.11}$$

设 $G=G_1\cdots G_n$，是 $G_1,\cdots,G_n$ 的内直积，利用同态，

$$\prod_{i=1}^{n}\pi_i:G\longrightarrow G_1\times\cdots\times G_n$$

$$g=g_1\cdots g_n\longmapsto(g_1,\cdots,g_n)$$

我们会得到 $G\cong G_1\times\cdots\times G_n$. 在交换群中，一般将直积写为直和的形式. 值得注意的是，式(3.11)有下面等价判定

1. 对任意 $g\in G$，$g=g_1\cdots g_n,\quad g_i\in G_i$ 的表示是唯一的.
2. 单位元表示唯一.

命题 3.11. 设 $G=\langle a\rangle$，其阶为 $|G|=nm,(n,m)=1$，则 $G\cong\mathbb{Z}_n\times\mathbb{Z}_m$.

证明. 记 $G_1=\langle a^m\rangle,G_2=\langle a^n\rangle$，则 $G_1\cong\mathbb{Z}_n,G_2\cong\mathbb{Z}_m$，且由阶互素可知 $G_1\cap G_2=\{e\}$，下面我们只要说明 $G=G_1G_2$，那么就有

$$G\cong G_1\times G_2\cong\mathbb{Z}_n\times\mathbb{Z}_m$$

由于 $(m,n)=1$，存在 u,v，使得 $mu+nv=1$，则

$$a^k=(a^{mu+nv})^k=(a^m)^{ku}\cdot(a^n)^{kv}\in G_1G_2$$

这样我们就完成了证明. ∎

设 $G=\langle a\rangle$, 且 $|G|=\prod_{i=1}^{s} p_i^{r_i}$ 是 $|G|$ 的标准素分解，则由 [命题，3.11]，就有

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_s^{r_s}}.$$

下面的记号，我们就将直积写为直和了.

命题 3.12. *设 G 是有限生成 Abel 群，则*

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}_{m_i}, \quad (m_i \geq 2,\ m_1 \mid m_2 \mid \cdots \mid m_k)$$

证明. 设 G 的最少生成元的个数为 n，我们对 n 进行归纳. 假设结论对小于 n 的情形成立.

设 $\mathcal{S}$ 为 G 的所有可能的 n 元生成组的集合. 对于任意生成组 $\mathbf{x}=\{x_1,\ldots,x_n\}\in\mathcal{S}$，定义关系集：

$$\mathcal{R}(\mathbf{x})=\left\{(c_1,\ldots,c_n)\in\mathbb{Z}^n \mid \sum_{i=1}^{n} c_i x_i = 0\right\}$$

考虑所有生成组的所有非平凡关系系数集合：

$$C=\bigcup_{\mathbf{x}\in\mathcal{S}} \{|c_i| : (c_1,\ldots,c_n)\in\mathcal{R}(\mathbf{x}), c_i\neq 0\}$$

情形 1：G 无非平凡关系

若对于任意生成组，仅存在全零关系（即所有 $c_i=0$），则生成元线性无关. 此时 G 是秩为 n 的自由 Abel 群，即 $G\cong\mathbb{Z}^n$. 命题得证.

情形 2：G 存在非平凡关系

此时 $C\neq\varnothing$，根据良序原理，可取 $m_1=\min C$. 不妨设该系数对应于生成组 $\{y_1,\ldots,y_n\}$ 及关系式：

$$m_1y_1+m_2y_2+\cdots+m_ny_n=0 \tag{3.12}$$

步骤 A：整除性分析

我们断言 m_1 必须整除该关系中的其他系数 m_i. 假如 $m_1\nmid m_2$，则可作带余除法 $m_2=qm_1+r$，其中 $0<r<m_1$. 作基变换令 $y_1'=y_1+qy_2$，则 $\{y_1',y_2,\ldots,y_n\}$ 仍为 G 的一组生成元. 将其代入 (3.12) 式可得：

$$m_1(y_1'-qy_2)+m_2y_2+\cdots=m_1y_1'+(m_2-qm_1)y_2+\cdots=m_1y_1'+ry_2+\cdots=0$$

此时出现了一个更小的非零系数 r，这与 m_1 的最小性矛盾. 故必有 $m_1\mid m_i$ 对所有 i 成立.

步骤 B：分离循环子群

既然 m_1 整除所有系数，我们可以通过基变换（列变换）将 y_1 以外的项消去. 令 $z_1 = y_1 + \sum_{i=2}^{n} \frac{m_i}{m_1} y_i$，并保持 $z_i = y_i$ $(i \geq 2)$. 显然 $\{z_1, \ldots, z_n\}$ 构成 G 的新生成组，且关系式 (3.12) 简化为：

$$m_1 z_1 = 0$$

这说明 z_1 生成一个阶为 m_1 的循环子群 $\langle z_1 \rangle \cong \mathbb{Z}_{m_1}$.

步骤 C：直和分解与归纳

令 $H = \langle z_2, \ldots, z_n \rangle$. 我们需证明 $G = \langle z_1 \rangle \oplus H$. 由于 G 由 z_i 生成，故 $G = \langle z_1 \rangle + H$. 仅需证明交集为零. 设 $g \in \langle z_1 \rangle \cap H$，则存在整数 u, v_i 使得：

$$g = u z_1 = \sum_{i=2}^{n} v_i z_i \implies u z_1 - \sum_{i=2}^{n} v_i z_i = 0$$

这是一个关于生成组 $\{z_i\}$ 的关系. 根据 m_1 的最小性定义，可知 $m_1 \mid u$（否则取余数会得到更小的系数）. 记 $u = k m_1$，则 $g = k(m_1 z_1)$. 由 $m_1 z_1 = 0$ 可知 $g = 0$. 因此交集平凡，直和成立：

$$G \cong \mathbb{Z}_{m_1} \oplus H$$

由于 H 是由 $n-1$ 个元素生成的 Abel 群，归纳假设即可，这基本完成了证明. ■