SOOCHOW UNIVERSITY

Date: Spring 2026

Author: livi

抽象代数

Notes on Abstract Algebra

$$
\begin{tikzcd}
F^n \arrow[rrr, "\mathcal{M}_{\mathbf{v}'}^{\mathbf{w}'}(T)"] \arrow[dr, "\varphi_{\mathbf{v}'}"] \arrow[dd, "P_{\mathbf{v}'}^{\mathbf{v}}"'] & & & F^m \arrow[dl, "\varphi_{\mathbf{w}'}"'] \arrow[dd, "P_{\mathbf{w}'}^{\mathbf{w}}"] \\
& V \arrow[r, "T"] & W & \\
F^n \arrow[ur, "\varphi_{\mathbf{v}}"'] \arrow[rrr, "\mathcal{M}_{\mathbf{v}}^{\mathbf{w}}(T)"'] & & & F^m \arrow[ul, "\varphi_{\mathbf{w}}"]
\end{tikzcd}
$$

前言

该讲义为自用笔记,
主题框架是围绕 Galois 理论做准备
仅供学习与交流使用.

目录

1 域

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

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

则

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

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 $c_{ij}=0$. ■

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 1.1. 设 F 是域，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 1.3. 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

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

即 $[F(\alpha), F] = n < \infty$. ■

命题 1.4. 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，1.3]，$K'/F$ 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 1.5. 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

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

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 $\bigcup\limits_{i=1}^{n} X_i$ 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.

定理 1.6. 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

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

(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 $\sum\limits_{i=1}^{m}x_i\alpha_i=0$.

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

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

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 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$，第二个我们会在 [推论，4.16] 章节做相关解释.

例 1.2. 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 1.3. $\mathbb{Q}(\pi)$ 是有限生成扩张，但不是代数扩张.

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

$$\begin{aligned}f:R&\longrightarrow(R/I)\times(R/J)\\ r&\longmapsto(r+I,r+J)\end{aligned}$$

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

$$\begin{aligned}r_1&=x_1+y_1\\ r_2&=x_2+y_2\end{aligned}$$

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

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

∎

定理 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 $I_1 I_2 = I_1 \cap I_2$. 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 $r_1 s_2 = r_2 s_1$. 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 $r_1 s_3 = r_3 s_1$，由 $s_2 \neq 0$，我们只要说明 $r_1 s_2 s_3 = r_3 s_1 s_2$：

$$r_1 s_2 s_3 = (r_1 s_2) s_3 = (r_2 s_1) s_3 = (r_2 s_3) s_1 = (r_3 s_2) s_1 = r_3 s_1 s_2.$$

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

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

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

$$(r_1s_2+r_2s_1,s_1s_2)\sim(r_1's_2'+r_2's_1',s_1's_2')$$
$$(r_1r_2,s_1s_2)\sim(r_1'r_2',s_1's_2')$$

验证有

$$(r_1s_2+r_2s_1)s_1's_2'=(r_1s_1')s_2s_2'+(r_2s_2')s_1s_1'=(r_1's_1)s_2s_2'+(r_2's_2)s_1s_1'=(r_1's_2'+r_2's_1')s_1s_2$$
$$r_1r_2s_1's_2'=(r_1s_1')(r_2s_2')=(r_1's_1)(r_2's_2)=r_1'r_2s_1s_2.$$

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

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

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.

$$\begin{tikzcd} R \arrow[r, "\varphi"] \arrow[d, "f"] & F' \\ F \arrow[ur, "\psi"] & \end{tikzcd}$$

其中 $f:r\mapsto\frac{r}{1}$ 为自然嵌入.

证明. 存在性：定义 $\psi:\frac{r}{s}\mapsto\varphi(r)\varphi(s)^{-1}$, 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 $\psi_1\left(\frac{r}{1}\right)=\psi_2\left(\frac{r}{1}\right),\forall r\in R$，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 $\frac{r}{s}(r\neq 0)$，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 (这里我们指包含 $\langle a\rangle$ 的主理想只有 $\langle a\rangle$ 和 R).$p\in R$ 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

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

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 $I=\bigcup\limits_{i=1}^{\infty}\langle a_i\rangle$ 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. ■

例 2.1. 整环 $R=\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ 是主理想整环但不是欧几里得环.

证明. 见：An Elementary Proof by Robert A. Wilson (QMUL) ■

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 $p(x) = \sum\limits_{i=0}^{n} a_i x^i$ 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 $p(x) = \sum\limits_{i=0}^{n} a_i x^i$, 当 $k > \deg p$. 时，我们假定 $a_k = 0$. 那么给定两个多项式 $p(x) = \sum\limits_{i=0}^{n} a_i x^i$ 和 $q(x) = \sum\limits_{i=0}^{m} b_i x^i$, 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. *若 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 $\gcd(f)\sim 1$，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 $f=c_1f_1=c_2f_2$，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_1f_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

$$\begin{aligned}\varphi: R[x]&\longrightarrow \widetilde{R}[x]\\ \sum_{i=0}^m a_ix^i&\longmapsto \sum_{i=0}^m (a_i+\langle p\rangle)x^i\end{aligned}$$

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 $f = f_1 f_2$，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 $f = r_1 r_2 f_1' f_2'$，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 $r_1 r_2 \in R$，这意味着 f 在 $R[x]$ 中可分解，矛盾. ■

定理 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 群行列式

定义 3.1. 设 $G = \{g_1, \cdots, g_n\}$ 是 n 阶群，将 g_i 对应变量 x_i，称 n 阶矩阵 $X_G = (x_i x_j^{-1})$ 为 G 的一个群矩阵，其中 $x_i x_j^{-1}$ 表示 $g_i g_j^{-1}$ 所对应的变量，称 X_G 的行列式 D_G 的群行列式.

设 $G = \{g_1, \cdots, g_n\} = \{a_1, \cdots, a_n\}$ 是群 G 的两种排序方式，设 $\sigma \in S_n$，满足 $a_i = g_{\sigma(i)}$，记 $P = (e_{\sigma(1)}, \cdots, e_{\sigma(n)})^T$，其中 e_i 是标准单位列向量，则有

$$PX_G P^{-1} = PX_G P^T = (x_{\sigma(i)} x_j^{-1}) P^T = (x_{\sigma_{(i)}} x_{\sigma_{(j)}}^{-1})$$

于是群矩阵依赖于群元素的排列顺序，但是不同的群矩阵是相似的，因此群行列式与群元素的排列无关，一般将 g_1 写为幺元.

例 3.1. 设 $G=\{g_1,\cdots,g_4\}$ 为 Klein 群，其中 $g_2^2=g_3^2=g_4^2=g_2g_3g_4=g_1$，则其群行列式为

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \\ x_3 & x_4 & x_1 & x_2 \\ x_4 & x_3 & x_2 & x_1 \end{vmatrix} = (x_1+x_2+x_3+x_4)(x_1+x_2-x_3-x_4)(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4).$$

例 3.2. 设 $G=\{s_1,s_2,\ldots,s_n\}$ 为循环群，其中 $s_i=s_2^{i-1}$，则容易得到 G 的群矩阵为循环矩阵

$$X_G=\begin{pmatrix} x_1 & x_n & x_{n-1} & \cdots & x_2 \\ x_2 & x_1 & x_n & \cdots & x_3 \\ x_3 & x_2 & x_1 & \cdots & x_4 \\ \vdots & \vdots & \vdots & & \vdots \\ x_n & x_{n-1} & x_{n-2} & \cdots & x_1 \end{pmatrix}$$

这个矩阵的行列式为

$$D_G=\prod_{i=0}^{n-1}(x_1+x_2\omega^i+\cdots+x_n\omega^{(n-1)i}),$$

其中 ω 是 n 次本原单位根.

例 3.3. 注意 n 阶群 $G=\{g_1,\cdots,g_n\}$ 的群矩阵 X_G 的每行每列都是 $\{x_1,\cdots,x_n\}$ 的全排列，因此 G 可以写为

$$X_G=\sum_{i=1}^n x_iB_i$$

其中 B_i 是置换矩阵，我们称（自称）B_i 是 x_i 在 X_G 中的位置.

由定义 B_1 的第 i 行中，唯一某个第 j 列元素为 1，当且仅当 $x_1=x_ix_j^{-1}$，即 $x_j=x_1^{-1}x_i$，即当且仅当 $x_1x_j=x_i$. 若我们定义

$$\delta(x_k,x_ix_j)=\begin{cases}1, & x_ix_j=x_k\\ 0, & \text{其他}\end{cases}$$

则 B_1 可以表示为 $B_1=(\delta(x_i,x_1x_j))$. 考虑 B_1B_2 的第 (i,j) 元即为

$$d_{ij}=\sum_{k=1}^n \delta(x_i,x_1x_k)\cdot(x_k,x_2x_j)$$

则 $d_{ij}=1\Longleftrightarrow x_1x_k=x_i$ 且 $x_2x_j=x_k$，即当且仅当 $x_1^{-1}x_i=x_2x_j$，即当且仅当 $x_i=(x_1x_2)x_j$. 于是 B_1B_2 就是 x_1x_2 在 X_G 中的位置.

置换矩阵全体构成一个同构于 S_n 的群，不妨就记为 S_n，这样就有一个自然的同态

$$\begin{aligned}\pi: G &\longrightarrow S_n\subset \mathrm{GL}(n,\mathbb{C})\\ g_i &\longmapsto B_i\end{aligned}$$

这个是表示论的起源.

定义 3.2. 设 G 是一个群，称 G 到 $\mathbb{C}^*$ 的函数 χ 为 G 的一个特征，如果对任意 $a,b \in G$，都有 $\chi(ab) = \chi(a)\chi(b)$. 换句话说，$G$ 的特征就是 G 到 C^* 的群同态.

引理 3.1. 记 Abel 群 G 的所有特征的全体为 $\widehat{G}$. 对任意 $\chi, \psi \in \widehat{G}$，定义 $\phi : G \to \mathbb{C}^*$ 为

$$\phi(x) = \chi(x)\psi(x).$$

则 $\phi \in \widehat{G}$，记为 $\phi = \chi \cdot \psi$. 进一步，$(\widehat{G}, \cdot)$ 为 Abel 群，称 $\widehat{G}$ 为 G 的特征群.

证明. 容易验证 $\phi \in \widehat{G}$，即运算 $\cdot$ 是合理的. 这个运算实际上就是函数值的逐点相乘，自然满足交换律和结合律. 于是 $\widehat{G}$ 是一个半群. 记 χ_1 为 G 的主特征，对任意 $\chi \in \widehat{G}$，$\chi_1 \cdot \chi(s) = \chi_1(s)\chi(s) = \chi(s)$. 故 $\chi_1 \cdot \chi = \chi$，即 χ_1 为幺元. 对任意 $\chi \in \widehat{G}$，定义 $\mu(s) = \chi(s^{-1}) = \overline{\chi(s)}$，容易看出 $\mu \in \widehat{G}$，且 $\mu \cdot \chi(s) = \chi(s)\overline{\chi(s)} = 1 = \chi_1(s)$，即 μ 是 χ 的逆元. 于是 $\widehat{G}$ 为 Abel 群. ∎

例 3.4. 设 $G = \langle a \rangle$ 为 n 阶循环群，若 $\chi \in \widehat{G}$，则 $\chi(a)^n = \chi(a^n) = 1$，即 $\chi(a)$ 为 n 次单位根. 而 $\chi(a)$ 的取值决定了 χ. 设 $\omega = e^{\frac{2\pi\sqrt{-1}}{n}}$，令 $\chi_i(a) = \omega^{i-1}$，则 $\chi_i(a^k) = \omega^{(i-1)k}$，其中 $i, k = 1, 2, \cdots, n$. 容易看出 $\widehat{G} = \{\chi_1, \chi_2, \cdots, \chi_n\}$，且 χ_2 为 n 阶元，则 $\widehat{G}$ 为 n 阶循环群，从而 $G \cong \widehat{G}$.

上述例子中的结论并不是偶然的，实际上我们有

命题 3.2. 设 G 是一个有限 Abel 群，则 $G \cong \widehat{G}$.

证明. 有限 Abel 群是循环群的直积，故不妨设 $G = H_1 \times H_2 \times \cdots \times H_k$，其中 H_i 为 n_i 阶循环群. 对任意 $\chi_i \in \widehat{H_i}$，定义

$$\chi(a_1 a_2 \cdots a_k) = \chi_1(a_1)\chi_2(a_2) \cdots \chi_k(a_k).$$

容易验证 $\chi \in \widehat{G}$. 于是有映射

$$\phi : \widehat{H_1} \times \widehat{H_2} \times \cdots \times \widehat{H_k} \to \widehat{G}.$$

可以验证这是一个群同态且是单射. 比较元素个数可知 ϕ 也是满射，从而是同构. 又由 $\widehat{H_i} \cong H_i$ 知 $G \cong \widehat{G}$. ∎

引理 3.1的结论对于非 Abel 群也成立，即非 Abel 群的特征的全体也构成一个 Abel 群，不过我们不用 $\widehat{G}$ 表示这个特征群. 若 χ 为 G 的特征，由于 $\chi(G)$ 为 Abel 群，则由群的同态基本定理可知 $G/\mathrm{Ker}\chi \cong \chi(G)$. 故 $G^{(1)} \subseteq \mathrm{Ker}\chi$，其中 $G^{(1)}$ 为 G 的换位子群. 于是我们自然可以得到

推论 3.3. 设 G 为有限群，则 G 的特征群同构于 $G/G^{(1)}$.

Abel 群的不同特征之间有一个很好的关系——正交关系. 对于 G 的特征 χ，我们考虑 $\sum_{s\in G} \chi(s)$. 若 χ 不是主特征，则存在 $t \in G$ 使得 $\chi(t) \neq 1$. 于是

$$\sum_{s\in G} \chi(ts) = \chi(t) \sum_{s\in G} \chi(s).$$

注意到 $\sum_{s\in G}\chi(ts)=\sum_{s\in G}\chi(s)$，故

$$(\chi(t)-1)\sum_{s\in G}\chi(s)=0.$$

从而我们有

引理 3.4. 设 χ 为有限群 G 的特征，则 $\sum_{s\in G}\chi(s)=\begin{cases}0, & \chi\neq\chi_1,\\ |G|, & \chi=\chi_1.\end{cases}$

进一步，对于特征 χ,ψ，由于 $\phi=\chi\cdot\psi^{-1}$ 也是特征，这里 $\psi^{-1}(s)=\psi(s^{-1})$ 为 ψ 在 $\widehat{G}$ 中的逆元. 利用上述引理可得

命题 3.5. 设 χ,ψ 为有限群 G 的特征，则

$$\sum_{s\in G}\chi(s)\psi(s^{-1})=\begin{cases}0, & \chi\neq\psi,\\ |G|, & \chi=\psi.\end{cases}$$

设 $G=\{s_1,s_2,\cdots,s_n\}$ 为 Abel 群，于是 G 的特征群 $\widehat{G}$ 也有 n 个元，设为 $\{\chi_1,\chi_2,\cdots,\chi_n\}$. 令

$$A=\frac{1}{\sqrt{|G|}}\begin{pmatrix}\chi_1(s_1) & \cdots & \chi_1(s_n)\\ \vdots & & \vdots\\ \chi_n(s_1) & \cdots & \chi_n(s_n)\end{pmatrix}.$$

注意到对于任意特征 ψ 有 $\psi(s^{-1})=\overline{\psi(s)}$，上述命题表明 A 的行向量在 $\mathbb{C}^n$ 的标准内积下是两两正交的，即 A 为酉矩阵. 因此上述命题也称为特征的正交关系.

定理 3.6. 设 $G=\{s_1,s_2,\cdots,s_n\}$ 为 Abel 群，则群行列式 D_G 可以分解为不同的 n 个一次齐次多项式的乘积：

$$D_G=\prod_{\chi\in\widehat{G}}\left(\sum_{i=1}^{n}\chi(s_i)x_i\right).$$

证明. 对任意 $\chi\in\widehat{G}$，将第 i $(i=2,3,\cdots,n)$ 行分别乘以 $\chi(s_i)$ 加到第一行得 $\sum_{i=1}^n\chi(s_i)x_i$ 是 D_G 的因子. 这些因子对于不同的 χ 是两两互素的. 因此，$\prod_{\chi\in\widehat{G}}\left(\sum_{i=1}^n\chi(s_i)x_i\right)$ 是 D_G 的因子. 比较两者的次数和 x_1^n 的系数即得. ■

3.2 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

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

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

引理 3.7. 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，3.7]，我们不难得到

命题 3.8. 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个数）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 3.5. 对任意 $n \in N^+$，有如下组合恒等式成立

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

证明. 将共轭类大小公式(3.4)代入式 (3.3) ，就有

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

两边同时除以 $n!$ 即得. ■

引理 3.9. *对于 $n\geq 3$，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 3.10. *对于 $n\geq 5$，A_n 中所有的 3-轮换在 A_n 中共轭.*

证明. 由 [命题, 3.8], 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 $n\geq 5$，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 3.11. *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，3.9]，我们只要证明 N 包含 A_n 中所有 3-轮换. 再由 [引理，3.10]，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 3.6. 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 3.7. 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 $j = \sigma(i)$. 由于 $n \geq 3$，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 $C(S_n) = \{(1)\}$. ■

例 3.8. 设 G 是置换群，若 G 中有奇置换，则 G 中存在指数为 2 的子群 H.

证明. 令 H 是 G 中所有偶置换的集合，则 $H \lhd G$. 设 σ 是 G 的一个奇置换，则 σH 是 G 的所有奇置换 (对于任意 G 的奇置换 τ，有 $\tau = \sigma(\sigma^{-1}\tau) \in \sigma H$). 于是 $G = H \cup \sigma H$，即 $[G : H] = 2$. ■

例 3.9. 设 G 是阶数为 $2n$ 的群，其中 n 是奇数，则 G 中存在 n 阶子群 H，即 H 是指数为 2 的正规子群. 特别地，当 $|G| \geq 6$，且 $|G| \equiv 2 \pmod 4$，则 G 不是单群.

证明. 考虑 G 在 G 上的左平移作用，其诱导了 $G \to S_G$ 的同态 φ, 且 φ 是单射. 因此可以将 G 等同（群同构）于 S_G 的子群 $\mathrm{im}\varphi$. 设 g 是 G 的一个二阶元，则 $\varphi(g)^2 = \varphi(g^2) = \mathrm{id}$，且 $\varphi(g)$ 没有不动点，因此 $\varphi(g)$ 可以表示为 n 个不相交的 2-轮换之积, 即 $\varphi(g)$ 是一个奇置换，由 [例，3.8]，结论得证. ■

例 3.10. 设 G 是有限群，p 是 G 的最小素因子. 若 $[G : H] = p$，则 $H \lhd G$.

证明. 考虑 G 在左陪集集合 $X = G/H$ 上的左平移作用. $|X| = [G : H] = p$. 设此作用诱导的同态为 $\varphi : G \to S_X \cong S_p$. 设 $K = \ker\varphi$. 根据同态基本定理，$G/K \cong \mathrm{Im}(\varphi) \leq S_p$. 由此可知 $|G/K|$ 能够整除 $|S_p| = p!$. 同时

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

这意味着 $|G/K|$ 是 p 的倍数，且 $|G/K|$ 是 $|G|$ 的因子. 设 $|G/K| = mp$，则 $m \mid (p-1)!$ 且 $m \mid |G|$，但是注意 $(p-1)!$ 的素因子都小于 p，以及 p 是 $|G|$ 的最小素因子，综合只能是 $m = 1$，即 $K = H$. ■

例 3.11. 在 A_4 中，不存在指数为 2 的子群.

证明. 设 $H < A_4$，且 $[A_4 : H] = 2$，这意味着对任意 $g \notin H$，有 $A_4 = H \cup gH$，也就是有 $g^2 \in H$. 注意三轮换的阶为 3，即有

$$(abc) = (abc)^4 = ((abc)^2)^2 \in H$$

但是 A_4 中有 $C_4^3 \times 2 = 8$ 个三轮换，如果将其写出来即是

$$(123), (132), (124), (142), (134), (143), (234), (243)$$

即 $|H| \geq 8$，这与 $|H| = 6$ 矛盾. ■

例 3.12. 6 阶群只有 $\mathbb{Z}_6$ 和 S_3.

证明. 设 G 是 6 阶非循环群，由 sylow 定理 G 有 2 阶和 3 阶群 $\langle a \rangle$ 与 $\langle b \rangle$，则 $\langle a \rangle \cap \langle b \rangle = \{e\}$. 考虑 G 在 $G/\langle a \rangle$ 上的左诱导作用，其诱导了一个同态 $\rho : G \to S_{G/\langle a \rangle} \cong S_3$，我们如果能说明 ρ 是单的，则比较两边阶数就有 $G \cong \mathrm{im}\rho = S_{G/H} \cong S_3$.

若 $g \in \ker \rho$，则 $g\langle a \rangle = \langle a \rangle$，即 $g \in \langle a \rangle$，因此若 $\ker \rho$ 非平凡，则一定有 $g = a$，那么就有 $a(b\langle a \rangle) = b\langle a \rangle$，这意味着一定有 $ab = ba$，那么 ab 的阶即是 6，但是我们已经假定了 G 不是循环群，矛盾. ■

3.3 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

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

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 3.3. 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_2，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.

我们上面的想法就是先找出 G 的一个极大正规子群 G_2，即包含 G_2 的正规子群只有 G_2 和 G，但是过程有点啰嗦. 我们也可以这样来看：假定 $G \neq \{e\}$，令 $\mathcal{S}$ 为 G 的所有真正规子群构成的集合，即

$$\mathcal{S} = \{N \mid N \lhd G, N \neq G\}$$

平凡子群 $\{e\}$ 显然是 G 的真正规子群，故 $\{e\} \in \mathcal{S}$，这意味着 $\mathcal{S}$ 非空且有限. 考虑

$$\mathcal{O} = \{|N| \mid N \in \mathcal{S}\}$$

由于 G 是有限群，$\mathcal{O}$ 是自然数集的一个有限非空子集. 则 $\mathcal{O}$ 中存在最大元素. 设 $m = \max(\mathcal{O})$. 我们在 $\mathcal{S}$ 中选取一个阶数为 m 的子群 M ,即 $|M| = m$,则 M 满足条件.

定理 3.12 (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

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

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，这就完成了我们的证明. ■

3.4 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

$$e_G\cdot x=x,\quad\forall x\in\Omega$$
$$(g_1g_2)\cdot x=g_1\cdot(g_2\cdot x),\quad\forall g_1,g_2\in G$$

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

$$g_1x=g_2x\iff g_2^{-1}g_1\in G_x\iff g_1G_x=g_2G_x$$

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 3.13 (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 3.13 (Cauchy 定理). 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 $|X_0|\neq0$（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. ■

例 3.14. 设 F 是有限域，则 $|F|=p^k$，其中 $p=\mathrm{char}F$.

证明. 将 F 视为加法运算下的交换群，则 $|\langle1\rangle|=p$，且由于 F 中任意非零元的阶都是 p(因为每个非零元都可逆)，[引理，3.13]，告诉我们 $|F|$ 只能有素因子 p，于是 $|F|=p^k$. ■

定理 3.14 (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，3.13], $|C(G)|$ 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 [定理，3.14] 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.

定理 3.15 (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 [定理，3.15]，$S = \{gHg^{-1} \mid g \in G\}$ 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.

定理 3.16 (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 3.15. 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 3.16. 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，3.15]，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 3.17. 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 3.18. 设 $|G| = p^2 q (p \neq q)$，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 3.19. 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 3.20. 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. ■

3.5 二面体群

对于 $n\geq 3$，二面体群 D_n 定义为将正 n 边形变换回自身的刚体运动（rigid motions）[1]组成的群，群运算为变换的复合.

命题 3.17. *D_n 的阶为 $2n$，即 D_n 中元素是 n 个旋转和 n 个翻转（反射）.*

证明. 对于正 n 边形，取定一个顶点，编号为 1，然后按照顺时针给正 n 边形的 n 个顶点依次编号为 $1,\cdots,n$，记 $X=\{1,2,\cdots,n\}$，则 D_n 在 X 上有个自然的作用，且对任意 $x\in X$，如果考虑 D_n 的 n 个旋转，那么这 n 个旋转作用在 x 上，就会带 x 跑遍整个 X，也就是说该作用是可迁的. 记 $\operatorname{stab}(1)$ 是 $x=1$ 的稳定子群，则

$$n=|X|=\frac{|D_n|}{|\operatorname{stab}(1)|}$$

首先恒等变换和沿着过 $x=1$ 的对称轴的翻转是落在 $\operatorname{stab}(1)$，即 $|\operatorname{stab}(1)|\geq 2$. 另一方面，任取 $\sigma\in\operatorname{stab}(1)$，则由于 σ 保持变换前后相邻顶点之间的距离，即可能情形为 $\sigma(2)=2$ 或者 $\sigma(2)=n$，这两种情况刚好分别对应恒等变换和翻转，于是 $|\operatorname{stab}(1)|=2$，则 $|D_n|=2n$. ■

不难看出 D_n 可描述为

$$D_n=\langle r,s\mid r^n=e,s^2=e,srs=r^{-1}\rangle$$

例 3.21. *当 $n\geq 3$ 为奇数时，D_n 的中心是平凡的. 当 $n\geq 3$ 为偶数时，D_n 的中心是 $\{1,r^{n/2}\}$.*

证明. 首先，没有任何反射在 D_n 的中心里，因为反射不与 r 交换：

$$(r^is)r=r^i(sr)=r^ir^{-1}s=r^{i-1}s,\quad r(r^is)=r^{i+1}s$$

所以如果 r^is 与 r 交换，则 $r^{i-1}=r^{i+1}$，这意味着 $r^2=1$，但 r 的阶 $n\geq 3$.

假设旋转 $r^j\in Z(D_n)(0\leq j<n)$，则首先要有 $r^js=sr^j$，这等价于 $r^js=r^{-j}s$，所以 $r^j=r^{-j}$. 即 $r^{2j}=1$. 由于 r 的阶为 n，于是 $n\mid 2j$，且 $0\leq 2j<2n$. 在 $\{0,1,\ldots,2n-1\}$ 中 n 的倍数只有 0 和 n，所以可能的情形是 $2j=0$ 或 $2j=n$.

当 n 是奇数，则唯一的选择是 $j=0$，所以 $r^j=1$. 显然 $1\in Z(D_n)$，所以 $Z(D_n)=\{1\}$.

当 n 是偶数，则 r^j 是 1 或 $r^{n/2}$. 同样，显然 $1\in Z(D_n)$，下面我们验证 $r^{n/2}\in Z(D_n)$. 显然 $r^{n/2}$ 与每个 r^i 交换，故我们只需验证 $r^{n/2}$ 是否与每个反射 r^is 交换，计算就有

$$r^{n/2}(r^is)=r^{n/2+i}s,\quad (r^is)r^{n/2}=r^ir^{-n/2}s=r^ir^{n/2}s=r^{i+n/2}s=r^{n/2+i}s,$$

这样我们就完成了证明. ■

[1] 刚体运动是一种保持距离的变换，如旋转、反射和平移，也被称为等距变换（isometry）.

例 3.22. D_n 中的共轭类如下.

(1) 如果 n 是奇数,

- 单位元: $\{1\}$,
- $(n-1)/2$ 个大小为 2 的共轭类: $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(n-1)/2}\}$,
- 所有反射构成一个共轭类: $\{r^i s : 0 \leq i \leq n-1\}$.

(2) 如果 n 是偶数,

- 两个大小为 1 的共轭类: $\{1\}, \{r^{n/2}\}$,
- $n/2-1$ 个大小为 2 的共轭类: $\{r^{\pm 1}\}, \{r^{\pm 2}\}, \ldots, \{r^{\pm(n/2-1)}\}$,
- 反射分为两个共轭类: $\{r^{2i} s : 0 \leq i \leq \frac{n}{2}-1\}$ 和 $\{r^{2i+1} s : 0 \leq i \leq \frac{n}{2}-1\}$.

证明. D_n 的每个元素都是 r^i 或 $r^i s$ 的形式，其中 i 为某个整数. 因此，为了找到元素 g 的共轭类，我们将计算 $r^i g r^{-i}$ 和 $(r^i s) g (r^i s)^{-1}$.

利用公式

$$r^i r^j r^{-i} = r^j, \quad (r^i s) r^j (r^i s)^{-1} = r^{-j}$$

随着 i 的变化，可以看出 r^j 在 D_n 中的共轭元仅有 r^j 和 r^{-j}.

为了找到 s 的共轭类，我们计算

$$r^i s r^{-i} = r^{2i} s, \quad (r^i s) s (r^i s)^{-1} = r^{2i} s.$$

随着 i 的变化，$r^{2i} s$ 跑遍了那些 r 的指数可被 2 整除的反射. 如果 n 是奇数，那么在模 n 的运算下，每个整数都是 2 的倍数（这是因为 2 在模 n 下是可逆的，对于给定的 k，我们可以通过解 $k \equiv 2i \pmod{n}$，来求出 i）. 因此当 n 是奇数时

$$\{r^{2i} s : i \in \mathbb{Z}\} = \{r^k s : k \in \mathbb{Z}\},$$

所以 D_n 中的所有反射都与 s 共轭.

当 n 是偶数时，我们只能得到一半的反射作为 s 的共轭元. 另一半与 rs 共轭:

$$r^i (rs) r^{-i} = r^{2i+1} s, \quad (r^i s)(rs)(r^i s)^{-1} = r^{2i-1} s.$$

随着 i 的变化，这给出了 $\{rs, r^3 s, \ldots, r^{n-1} s\}$. ■

推论 3.18. 设 D_n 是二面体群，则

(1) 当 n 为奇数时，D_n 的所有正规子群为 D_n 和旋转子群 $\langle r^d \rangle$，其中 $\mid d \mid n$.

(2) 当 n 为偶数时，D_n 的所有正规子群为 $D_n, \langle r^2, s \rangle, \langle r^2, rs \rangle$ 以及旋转子群 $\langle r^d \rangle$.

3.6 有限生成 Abel 群分类

例 3.23. 设 G 是有限 Abel 群，且 $|G| = mn, (m,n) = 1$，则有直积 $G = G_1G_2$，其中 $|G_1| = m, |G_2| = n$.

证明. 由 G 是 Abel 群，则

$$G_1 = \{g \in G \mid g^m = e\} \quad G_2 = \{g \in G \mid g^n = e\}$$

是 G 的子群. 且由 $(m,n) = 1$，存在 u, v，使得 $mu + nv = 1$，即对任意 $g \in G$，有

$$g = g^{mu+nv} = (g^{nv}) \cdot (g^{mu}) \in G_1G_2$$

则 $G = G_1G_2$，且若 $g \in G_1 \cap G_2$，则 $o(g) \mid n$，且 $o(g) \mid n$，那只能是 $o(g) = 1$，即 $g = e$. 这样我们就证明了直积. 下面我们只要说明 $(|G_1|, n) = 1$，$(|G_2|, m) = 1$，即可说明 $|G_1| = m, |G_2| = n$. 若 $(|G_1|, n) > 1$，则取其一个公共素因子 p，由 Cauchy 定理，G_1 中有 p 阶元 g，但是由定义要有 $g^m = 1$，这意味着 $o(g) = p$ 要整除 m，矛盾. ■

推论 3.19. 设 G 是有限 Abel 群，且 $|G| = p_1^{r_1} \cdots p_s^{r_s}$，则存在直积分解 $G = G_1 \cdots G_s$，使得 $|G_i| = p_i^{r_i}$.

定理 3.20 (分类定理). 设 G 是有限生成 Abel 群. 则 G 同构于以下形式的直和:

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{d_1} \oplus \mathbb{Z}_{d_2} \oplus \cdots \oplus \mathbb{Z}_{d_k} \tag{3.10}$$

其中:

1. $r \geq 0$ 是整数（G 的自由秩）.
2. $d_1, \ldots, d_k$ 是满足 $d_i \geq 2$ 且 $d_1 \mid d_2 \mid \cdots \mid d_k$ 的整数.

且若

$$G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}_{d_i} \cong \mathbb{Z}^s \oplus \bigoplus_{j=1}^{m} \mathbb{Z}_{c_j}$$

其中 d_i 和 c_j 均满足整除链条件. 则 $r = s$, $k = m$，且对于所有 i，有 $d_i = c_i$.

证明. 见 David McKinnon 的讲义：Classification of Finitely Generated Abelian Groups. ■

3.7 pq 阶群

例 3.24 (第一类 pq 阶群). 设有限群 G 的阶为 $|G| = pq (p < q)$，且 $q \not\equiv 1 \pmod p$，则 G 是循环群.

证明. 记 H, K 分别是 G 的 sylow-p 和 sylow-q 群，则 $n_q = 1$ 且 $n_p = 1$(因为 $q \not\equiv 1 \pmod p$)，即 H, K 都是 G 的正规子群，且 $H \cap K = \{e\}$，那么 $|HK| = pq = |G|$，即有直积 $G = HK$. 又因为 H, K 都是素数阶群，则可设 $H = \langle a \rangle$，$K = \langle b \rangle$，那么有

$$[a, b] = a^{-1}b^{-1}ab \in H \cap K = \{e\}$$

这意味着 $ab = ba$，于是 $o(ab) = o(a)o(b) = pq$，即 G 是循环群. ■

例 3.25 (第二类 pq 阶群). 当 $q \equiv 1 \pmod p$ 时，可以作仿射群 $\mathrm{Aff}(\mathbb{Z}_q)$ 的子群：

$$A_{p,q} = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathrm{Aff}(\mathbb{Z}_q) : x^p = 1 \text{ in } \mathbb{Z}_q \right\}. \tag{3.11}$$

这里 1 是 $\mathbb{Z}_q$ 中的幺元. 则 $|A_{p,q}| = pq$，且群 $A_{p,q}$ 是非阿贝尔群，因为矩阵 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 和 $\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$ 不交换，其中 x 是 $\mathbb{Z}_q$ 中阶为 p 的元素.

证明. 注意 y 有 q 种选择，由于 $x \in \mathbb{Z}_q^*$ 且假设 $p|(q-1)$，由 Cauchy 定理，在 $\mathbb{Z}_q^*$ 中存在一个阶为 p 的元素，因此它的幂次在 $\mathbb{Z}_q$ 中给出至少 p 个 $x^p = 1$ 的解. 另一方面，作为 $\mathbb{Z}_q$ 上的多项式 $x^p - 1$，其在 $\mathbb{Z}_q$ 中的根不能超过 p 个，所以 $x^p = 1$ 在 $\mathbb{Z}_q$ 上恰好有 p 个解. 于是 $|A_{p,q}| = pq$. ■

命题 3.21. 设 p 和 q 为素数，且 $p < q$ 和 $q \equiv 1 \pmod p$. 在同构意义下，(3.11) 中的群 $A_{p,q}$ 是唯一的大小为 pq 的非 Abel 群.

证明. 见 Keith Conrad 的讲义：Applications of Cauchy's Theorem. ■

推论 3.22. 对于奇素数 q，$2q$ 阶群只有 $\mathbb{Z}_{2q}$ 和二面体群 D_q.

3.8 可解群

设 G 是群，记 $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$, $G^{(0)} = G$，若 $\varphi : G \to H$ 是群同态，则 $[\varphi(g_1), \varphi(g_2)] = \varphi([g_1, g_2])$，这意味着 $\varphi(G^{(k)}) \subset H^{(k)}$，特别地当 φ 是满的，则 $\varphi(G^{(k)}) = H^{(k)}$.

定义 3.4. 我们称群 G 是可解群，如果 G 满足如下之一条件

(i) 存在 k，使得 $G^{(k)} = \{e\}$，即有

$$G = G^{(0)} \rhd G^{(1)} \rhd \cdots \rhd G^{(k)} = \{e\}$$

(ii) 存在 G 的次正规列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_t = \{e\}$$

使得 G_i / G_{i+1} 是 Abel 群.

引理 3.23. 若 G 是可解群，则 G 的子群 H 是可解的，且若 $H \lhd G$，则 G/H 是可解的. 反之，若 $H \lhd G$，且 $H, G/H$ 都是可解的，则 G 也是可解的.

证明. 若 H 是 G 的子群，那么 $H^{(k)} \subseteq G^{(k)}$. 如果 H 是正规子群，考虑自然同态 $\pi : G \to G/H$，则 $\pi(G^{(k)}) = (\pi(G))^{(k)} = (G/H)^{(k)}$. 这说明若 G 可解，则 H 和 G/H 都可解.

再证第二个结论. 若 G/H 可解，则存在 $k \in \mathbb{N}$，使得 $(G/H)^{(k)} = \{\bar{e}\}$. 于是

$$\pi(G^{(k)}) = (\pi(G))^{(k)} = (G/H)^{(k)} = \{\bar{e}\}.$$

因此 $G^{(k)} \subseteq \operatorname{Ker} \pi = H$. 而 H 可解，故其子群 $G^{(k)}$ 也可解，从而存在 $l \in \mathbb{N}$ 使得 $(G^{(k)})^{(l)} = \{e\}$，于是

$$G^{(k+l)} = (G^{(k)})^{(l)} = \{e\},$$

故 G 可解. ∎

定理 3.24. 设 G 是有限群，则 G 是可解群当且仅当 G 的合成因子都是素数阶循环群.

证明. 设 G 是有限阶可解群，则其存在合成序列

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_k = \{e\}$$

其中 G_i/G_{i+1} 是单群. 由 [引理, 3.23]，G_i/G_{i+1} 也是可解群，从而只能是 $(G_i/G_{i+1})^{(1)} = \{\bar{e}\}$，这意味着 G_i/G_{i+1} 是 Abel 群，从而是素数阶的循环群. ∎

4 Galois 理论

4.1 分裂域

设有域扩张 E/F，取定 $\alpha \in E$，定义 $F[\alpha] = \{\sum_{i=0}^{m} a_i \alpha^i \mid m \geq 0, a_i \in F\}$. 考虑映射

$$\begin{aligned} f : F[x] &\longrightarrow F[\alpha] \\ \sum_{i=0}^{n} a_i x^i &\longmapsto \sum_{i=0}^{n} a_i \alpha^i \end{aligned} \tag{4.1}$$

(4.1)是一个满的环同态. 当 α 是 F 代数元时，记 $g(x) \in F[x]$ 是 α 极小多项式，则 $F[x]/\langle g(x)\rangle \cong F[\alpha]$，由于 $g(x)$ 是 $F[x]$ 中的不可约元，则 $\langle g(x)\rangle$ 是极大主理想，又因为 $F[x]$ 是主理想整环，从而 $\langle g(x)\rangle$ 是极大理想，则 $F[x]/\langle g(x)\rangle$ 是域，于是此时 $F[\alpha] = F(\alpha)$.

当不存在 $F[x]$ 中的非零多项式 $g(x)$，使得 $g(\alpha) = 0$ 时，即 α 是 F 中超越元，此时 $F[x] \cong F[\alpha]$.

定义 4.1. 给定域 F 和 $f(x) \in F[x]$，称 E 是 f 在 F 的一个分裂域，如果 E 满足

1) f 可以在 E 中分解为一次因式的乘积

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \quad c, \alpha_i \in E.$$

2) $E = F(\alpha_1, \cdots, \alpha_n)$.

引理 4.1. 设 $f \in F[x]$ 是不可约的，则存在 F 的有限扩张 E，使得 f 在 E 中有根.

证明. 令 $K = F[x]/\langle f(x)\rangle$，由于 $\langle f(x)\rangle$ 是极大理想，则 F 是域. 定义自然嵌入 $\sigma : F \to K$ 为:

$$\sigma(a) = a + \langle f(x)\rangle, \quad \forall a \in F$$

记 $F' = \sigma(F) = \{a + \langle f(x)\rangle \mid a \in F\}$，则 F' 是 K 的一个子域，且 $F \cong F'$. 定义集合 E 为 F 与 K 中除去 F 像的部分的并集:

$$E = F \cup (K \setminus F')$$

令 $\varphi : E \to K$ 如下:

$$\varphi(u) = \begin{cases} \sigma(u) = u + \langle f(x)\rangle, & u \in F \\ u, & u \in K \setminus F' \end{cases}$$

显然 φ 是双射. 其逆映射 $\varphi^{-1} : K \to E$ 为:

$$\varphi^{-1}(v) = \begin{cases} \sigma^{-1}(v), & v \in F' \\ v, & v \in K \setminus F' \end{cases}$$

利用双射 φ，我们将 K 上的加法 $+_K$ 和乘法 $\cdot_K$ 拉回到 E 上. 对任意 $x, y \in E$，定义:

$$x +_E y = \varphi^{-1}(\varphi(x) +_K \varphi(y))$$
$$x \cdot_E y = \varphi^{-1}(\varphi(x) \cdot_K \varphi(y))$$

首先，由于 $(K, +_K, \cdot_K)$ 是域，且 φ 是双射，故 $(E, +_E, \cdot_E)$ 必然构成一个域. 其次，我们需要验证 F 确实是 E 的子域（即 E 上的运算限制在 F 上与 F 原有运算一致）. 设 $a, b \in F$. 注意到 $\varphi(a) = \sigma(a)$ 且 σ 是域同态，则

$$\begin{aligned} a +_E b &= \varphi^{-1}(\sigma(a) +_K \sigma(b)) \\ &= \varphi^{-1}(\sigma(a+b)) \\ &= a + b \end{aligned}$$

同理可验证乘法 $a \cdot_E b = a \cdot b$.

最后，对于 $f(x)$ 的根. 在 K 中，根为 $\bar{x} = x + \langle f(x)\rangle$. 由于 $\bar{x} \notin F'$（因为 f 不可约且 $\deg(f) \geq 1$），故 $\bar{x} \in K \setminus F'$. 根据 φ 的定义，该元素对应 E 中的元素即为它自身. ■

注记 4.1. 一般教科书都直接将 F 视为 $F[x]/\langle f(x)\rangle$ 的子域，并未做过多解释，因为是第一次出现，我们稍稍解释，以后我们也将 F 直接视为 $F[x]/\langle f(x)\rangle$ 的子域.

定理 4.2. 设 $f\in F[x]$ 是首一的，且 $\deg f>0$，则存在 f 在 F 上的一个分裂域.

证明. 对 $\deg f=n$ 进行归纳，当 $n=1$ 时，取 $E=F$ 即可. 现在假设结论对 $F[x]$ 中次数小于 n 的多项式成立. 取 f 在 $F[x]$ 中的一个不可约因式为 p，则 $\deg p>1$，由 [引理，4.1]，存在 K/F，使得 $p(x)$ 在 K 中有根 α_1，假定

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_r)g(x),\quad \alpha_i\in K,\quad r\geq 1$$

为 f 在 K 中分解，不妨设 $K=F(\alpha_1,\cdots,\alpha_r)$, 否则考虑其子域 $F(\alpha_1,\cdots,\alpha_r)$. 因为 $g(x)\in F[x]\subset K[x]$，则由归纳假设，存在 $g(x)$ 在 K 中的分裂域 E，则 f 可以在 E 中分解为一次因式的乘积 $f(x)=\prod_{i=1}^{n}(x-\alpha_i)$，且

$$E=K(\alpha_{r+1},\cdots.\alpha_n)=F(\alpha_1,\cdots,\alpha_r)(\alpha_{r+1},\cdots,\alpha_n)=F(\alpha_1,\cdots,\alpha_n)$$

这意味着 E 是 f 在 F 中的一个分裂域. ■

推论 4.3. 设 $f\in F[x]$, 且 $\deg f=n$，E 是 f 的一个分裂域，则 $[E:F]\leq n!$.

设 $\eta:F\to\widetilde{F}$ 是域同构，其诱导了 η 的一个满的扩张同态：

$$\begin{aligned}\widetilde{\eta}:F[x]&\longrightarrow \widetilde{F}[x]\\ \textstyle\sum_{i=0}^{n}a_ix^i&\longmapsto \textstyle\sum_{i=0}^{n}\eta(a_i)x^i\end{aligned}\tag{4.2}$$

现在考虑 $g(x)$ 是 $F[x]$ 中的一个不可约元，那么 $\widetilde{g}(x)=\widetilde{\eta}(g)$ 是 $\widetilde{F}[x]$ 的不可约元，记 π 是 $\widetilde{F}[x]\to\widetilde{F}[x]/\langle\widetilde{g}(x)\rangle$ 的自然投影，那么 $\pi\circ\widetilde{\eta}:F[x]\to\widetilde{F}[x]/\langle\widetilde{g}(x)\rangle$ 是满的同态，且 $\ker\pi\circ\widetilde{\eta}=\langle g(x)\rangle$，则 $F[x]/\langle g(x)\rangle\cong\widetilde{F}[x]/\langle\widetilde{g}(x)\rangle$. 在这个过程中，我们始终保持 η 的作用不变.

引理 4.4. 设有域同构 $\eta:F\to\widetilde{F}$，和域扩张 $E/F,\widetilde{E}/\widetilde{F}$，设 $\alpha\in E$ 是 F 的代数元，记 $g(x)\in F[x]$ 是 α 的极小多项式，则 η 可以开拓为 $F(\alpha)\to\widetilde{E}$ 的同态当且仅当 $\widetilde{g}$ 在 $\widetilde{E}$ 中有根，于是这样的同态个数等于 $\widetilde{g}$ 在 $\widetilde{E}$ 中不同根的个数，即这样的同态个数小于等于 $\deg\widetilde{g}=\deg g=[F(\alpha):F]$，于是等号成立当且仅当 $\widetilde{g}(x)$ 在 $\widetilde{E}$ 中可以完全分解，且没有重根.

证明. 设 $\xi:F(\alpha)\to\widetilde{E}$ 是由 η 开拓得到的群同态，则 $0=\xi(g(\alpha))=\widetilde{g}(\xi(\alpha))$，这意味着 $\xi(\alpha)$ 是 $\widetilde{g}$ 在 $\widetilde{E}$ 中的根. 反过来，设 $\widetilde{\alpha}\in\widetilde{E}$ 是 $\widetilde{g}(x)$ 的一个根，则由 $\widetilde{g}$ 的不可约性，$\widetilde{g}(x)$ 即是 $\widetilde{\alpha}$ 的极小多项式，那么由式(4.1)和(4.2)有

$$F(\alpha)\xrightarrow{\cong}F[x]/\langle g(x)\rangle\xrightarrow{\cong}\widetilde{F}[x]/\langle\widetilde{g}(x)\rangle\xrightarrow{\cong}\widetilde{F}(\widetilde{\alpha})\longrightarrow\widetilde{E}$$

这个过程保持 η 的作用，合起来即得到一个从 $F(\alpha)\to\widetilde{E}$ 的由 η 开拓的同态. ■

定理 4.5. 设 $\eta_0 : F \to \widetilde{F}$ 是同构，且 E 和 $\widetilde{E}$ 分别是 $f \in F[x]$ 和 $\widetilde{f} \in \widetilde{F}[x]$ 的一个分裂域，则存在 η_0 的开拓 $\eta : E \to \widetilde{E}$ 是同构，且这样的同构个数小于等于 $[E : F]$，且等号成立当且仅当 f 在 $F[x]$ 中的任一不可约因式在 E 中没有重根.

证明. 不妨假定在 $E[x]$ 中有 $f(x) = \prod_{i=1}^{n}(x - \alpha_i)$. 记 $F_0 = F$，$F_i = F_{i-1}(\alpha_i)$，由 [引理，4.4]，存在 $\eta_i : F_i \to \widetilde{F}_i$，使得 $\eta_i|_{F_{i-1}} = \eta_{i-1}(i = 1, \cdots, n)$，即有

$$\begin{array}{ccccccccc} F & \longrightarrow & F_1 & \longrightarrow & F_2 & \longrightarrow & \cdots & \longrightarrow & E \\ \downarrow{\scriptstyle \eta_0} & & \downarrow{\scriptstyle \eta_1} & & \downarrow{\scriptstyle \eta_2} & & & & \downarrow{\scriptstyle \eta=\eta_n} \\ \widetilde{F} & \longrightarrow & \widetilde{F}_1 & \longrightarrow & \widetilde{F}_2 & \longrightarrow & \cdots & \longrightarrow & \widetilde{E} \end{array} \tag{4.3}$$

注意

$$\widetilde{f}(x) = \widetilde{\eta}_0(f) = \widetilde{\eta}(f) = \widetilde{\eta}\left(\prod_{i=1}^{n}(x - \alpha_i)\right) = \prod_{i=1}^{n}(x - \eta(\alpha_i)) \tag{4.4}$$

由 $\widetilde{E}$ 是 $\widetilde{f}$ 的分裂域，于是 $\widetilde{E} = \widetilde{F}(\eta(\alpha_1), \cdots, \eta(\alpha_n))$. 这样就有

$$\begin{aligned} \eta(E) = \eta(F_{n-1}(\alpha_n)) = \eta_{n-1}(F_{n-1})(\eta(\alpha_n)) &= \cdots = \eta_0(F_0)(\eta(\alpha_1))\cdots(\eta(\alpha_n)) \\ &= \widetilde{F}(\eta(\alpha_1), \cdots, \eta(\alpha_n)) = \widetilde{E} \end{aligned}$$

这意味着 η 是满的，自然也是同构. 下面我们主要讨论 η_0 的开拓同构 $\eta : E \to \widetilde{E}$ 的个数. 若 η 是这样的同构，则令 $\eta|_{F_i} = \eta_i$，则有 $\eta_i|_{F_{i-1}} = \eta_{i-1}$，于是我们看 η 有多少个，就是看每一步的 η_i 有多少个.

记 $g_i(x) \in F_{i-1}[x]$ 为 α_i 的极小多项式，则由于 $f(x) \in F_{i-1}[x]$，且 $f(\alpha_i) = 0$，这意味着 $g_i(x) \mid f(x)$，也就是说 $g_i(x)$ 其实就是 $f(x)$ 在 $F_{i-1}[x]$ 中的一个不可约因式，那么 $\widetilde{g}_i(x)$ 就是 $\widetilde{f}$ 在 $\widetilde{F}_{i-1}[x]$ 的一个不可约因式. 又因为 $\eta(\alpha_i)$ 是 $\widetilde{g}_i(x)$ 的根，则 $\{\widetilde{g}_1(x), \cdots, \widetilde{g}_n(x)\}$ 包含了 $\widetilde{f}$ 的所有根.

现在设 $\widetilde{p}(x)$ 是 $\widetilde{f}(x)$ 在 $\widetilde{F}[x]$ 的任一不可约因式，则存在某个 $\widetilde{g}_i(x)$ 使得 $\widetilde{p}(x)$ 与 $\widetilde{g}_i(x)$ 在 $\widetilde{E}$ 中有公共根 β. 于是，若 $\widetilde{g}_i(x) \nmid \widetilde{p}(x)$，则 $(\widetilde{p}(x), \widetilde{g}_i(x))_{\widetilde{F}_{i-1}[x]} = 1$，即存在 $u(x), v(x) \in \widetilde{F}_{i-1}[x]$，使得 $\widetilde{p}(x)u(x) + \widetilde{g}_i(x)v(x) = 1$，将 $x = \beta$ 代入即得 $0 = 1$，这是矛盾的. 于是有 $\widetilde{g}_i(x) \mid \widetilde{p}(x)$.

即 $\widetilde{f}(x)$ 在 $\widetilde{F}[x]$ 中的任一不可约因式都包含某个 $\widetilde{g}_i(x)$ 作为因式. 反过来，对每个 $\widetilde{g}_i(x)$，其必定与 $\widetilde{f}(x)$ 在 $\widetilde{F}[x]$ 中的某个不可约因式 $\widetilde{p}(x)$ 有公共根，即 $\widetilde{g}_i(x)$ 是 $\widetilde{p}(x)$ 的因式.

由 [引理，4.4]，每个 η_i 的个数小于等于 $[F_i : F_{i-1}] = \deg \widetilde{g}_i(x)$，这样就有

$$|\mathrm{Iso}(E, \widetilde{E})| \leq [F_1 : F_0] \cdot [F_2 : F_1] \cdots [F_n : F_{n-1}] = [E : F] \tag{4.5}$$

其中 $|\mathrm{Iso}(E, \widetilde{E})|$ 表示满足条件的同构个数，且等号成立当且仅当 $\widetilde{g}_i(x)(1 \leq i \leq n)$ 在 $\widetilde{E}$ 中没有重根.

当 $\tilde{f}$ 在 $\tilde{F}[x]$ 中的任一不可约因式 $\tilde{p}(x)$ 在 $\tilde{E}$ 中没有重根时，$\tilde{g}_i(x)$ 作为某一个 $\tilde{p}(x)$ 的因式，自然在 $\tilde{E}$ 中没有重根. 反过来，每个 $\tilde{f}(x)$ 在 $\tilde{F}[x]$ 中的不可约因式 $\tilde{p}(x)$，都可以视为 (在调整顺序后)$\tilde{g}_1(x)$，即作为(4.3)的第一步 η_1 中的极小多项式，所以当(4.5)取等号时，$\tilde{p}(x)$ 在 $\tilde{E}$ 中没有重根.

于是(4.5)等号成立当且仅当 $\tilde{f}$ 在 $\tilde{F}[x]$ 中的任一不可约因式在 $\tilde{E}$ 中没有重根，由 (4.4) 和 η 是双射，这也等价于 $f(x)$ 的任一不可约因式在 E 中没有重根. ■

> **注记 4.2.** 此定理深刻地揭示了代数结构的内蕴性（Intrinsic Nature）. 它表明，分裂域 E 的代数结构完全由基域 F 及多项式 $f(x)$ 的内在代数性质所决定，而与元素的具体记号无关. 同构 η_0 就像一座桥梁，它保证了在 F 中成立的一切代数运算关系，在映射到 $\tilde{F}$ 后依然成立；而定理 4.5 进一步断言，这种"结构的保真性"在扩域过程中不会丢失——E 与 $\tilde{E}$ 作为 f 与 $\tilde{f}$ 的分裂域，在代数意义下是不可分辨的（Indistinguishable）. 这体现了抽象代数的核心思想：我们在乎的不是元素是什么，而是元素之间如何相互作用.

推论 4.6. $f \in F[x], (\deg f > 0)$ 的分裂域存在, 且在同构意义下唯一.

推论 4.7. 设 E, E_1 是 $f \in F[x]$ 的两个分裂域，则 $\eta : E \to E_1, \eta|_F = \mathrm{id}$ 这样的同构个数不超过 $[E : F]$，且等号成立当且仅当 f 在 $F[x]$ 中的任一不可约因式在 E 中没有重根.

设 $f \in F[x]$，若 f 的任一不可约因式在其分裂域 E 中没有重根，则我们称 f 是可分多项式. 若有代数扩张 K/F，对任意 $\alpha \in K$，记 $g(x) \in F[x]$ 是 α 的极小多项式，若 $g(x)$ 是可分多项式，则称 K/F 是可分扩张，α 称为 F 的可分元. 若对任意 $f \in F[x]$（默认次数大于零），f 都是可分多项式，则称 F 是完全域.

定义 4.2. 设 $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$，定义 $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$，称为是 $f(x)$ 的形式导数.

当 $f'(x) = 0$ 时，意味着 $a_1 = 2a_2 = \cdots = na_n = 0$. 若 $\mathrm{char}F = 0$，则此时 $a_1 = \cdots = a_n = 0$，即 $f = a_0$. 若 $\mathrm{char}F = p > 0$，则当 $p \nmid k$ 时，$a_k = 0$，此时有 $f(x) = a_0 + \sum_{k=1}^{s} b_k x^{kp}$.

命题 4.8. 设 $f(x) \in F[x]$，则 f 在其分裂域 E 上没有重根当且仅当 $(f, f')_{F[x]} = 1$.

证明. 以下不妨假定 f 是首一的. 若 α 是 f 的重根，则设在 $E[x]$ 中有分解 $f = (x-\alpha)^2 g(x)$，则

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x)$$

于是有 $f'(\alpha) = 0$，此时不会有 $(f, f') = 1$. 若 $(f, f') \neq 1$，取 (f, f') 在 E 中的一个根，记为 β，设 $f = (x-\beta)h(x)$，则

$$f'(x) = h(x) + (x-\beta)h'(x)$$

由 $f'(\beta) = 0$，即有 $h(\beta) = 0$，这意味着 β 是 f 在 E 中的重根. ■

于是若 $\mathrm{char}F = 0$，则 F 一定是完全域. 当 $\mathrm{char}F = p > 0$ 时，$g(x) \in F[x]$ 是不可约元，则 $g(x)$ 不可分当且仅当 $g'(x) = 0$.

引理 4.9. 设 $\mathrm{char}F = p > 0$，对任意 $a \in F$，则 $f(x) = x^p - a$ 要么在 $F[x]$ 中不可约，要么存在 $b \in F$，使得 $f(x) = (x-b)^p$.

证明. 若 f 在 $F[x]$ 中可约，设 $g(x)$ 是 $f(x)$ 的一个真因式，记 b 为 g 在 E 中的一个根，则有 $f(b) = 0$，即 $a = b^p$. 于是 $f(x) = x^p - b^p = (x-b)^p$. 那么 $g(x)$ 在 $E[x]$ 中的分解一定形如 $g(x) = (x-b)^k (k < p)$，则 $g(x)$ 的常数项为 $(-b)^k \in F$，这意味着 $b^k \in F$. 又因为 $(k,p) = 1$，则存在整数 u, v，使得 $1 = ub + pv$，于是

$$b = b^{uk+pv} = (b^k)^u \cdot (b^p)^v \in F$$

■

命题 4.10. 设 $\mathrm{char}F = p > 0$，则 F 是完全域当且仅当 $F^p = F$，即由 [例，1.1] 诱导的 Frobenius 同态是同构. 特别地，有限域都是完全域.

证明. 当 $F^p \neq F$ 时，即存在 $a \in F$，满足对任意 $b \in F$，都有 $a \neq b^p$，由 [引理，4.9]，$f(x) = x^p - a$ 是不可约的，且 $f' = 0$，于是 f 是不可分多项式，即 F 不是完全域.

当 F 不是完全域时，取 $F[x]$ 中的不可约的不可分多项式 $f(x)$，由 $f'(x) = 0$，可以不妨设

$$f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np}$$

若对每个 a_i，都存在对应的 $b_i \in F$，使得 $a_i = b_i^p$，则

$$f(x) = b_0^p + b_1^p x^p + \cdots + b_n^p x^{np} = (b_0 + b_1 x + \cdots + b_n x^n)^p$$

这与 f 不可约矛盾，于是存在某个 a_i，使得对任意 $b \in F$，都有 $a_i \neq b^p$，即 $F^p \neq F$. ■

定理 4.11. 设 p 为素数，k 为正整数，令 $q = p^k$，则存在唯一的 q 阶域，记为 $\mathbb{F}_q$.

证明. 考虑素域 $\mathbb{Z}_p$ 上的多项式 $f(x) = x^q - x \in \mathbb{Z}_p[x]$，设 K 是 $f(x)$ 在 $\mathbb{Z}_p$ 上的分裂域. 令

$$S = \{\alpha \in K \mid \alpha^q - \alpha = 0\} = \{\alpha \in K \mid \alpha^q = \alpha\}.$$

显然 $0, 1 \in S$，对于任意 $\alpha, \beta \in S$，由于 K 的特征为 p，则

$$(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta,$$

$$(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta.$$

若 $\beta \neq 0$，则 $(\beta^{-1})^q = (\beta^q)^{-1} = \beta^{-1}$. 这说明集合 S 对域的四则运算封闭，故 S 是 K 的一个子域. 对任意 $a \in \mathbb{Z}_p$，由费马小定理有 $a^p = a$，这样就有 $a^q = a$，这意味着 $\mathbb{Z}_p \subseteq S$. 即 S 是

$\mathbb{Z}_p$ 的一个扩域. 又因为 $f'(x)=qx^{q-1}-1=p^kx^{q-1}-1=-1$，于是 $(f,f')=1$. 因此，$f(x)$ 在分裂域 K 中没有重根，即 $|S|=q$. 又因为 S 是 $\mathbb{Z}_q$ 的扩域且包含 $f(x)$ 的所有根，则只能是 $S=K$.

现在设 F 是任意一个阶为 $q=p^k$ 的有限域，其特征为 p，即 F 包含了一个 p 阶子域 $\mathbb{F}'_p$. 考虑 F 的乘法群 $F^*=F\setminus\{0\}$，这是一个阶为 $q-1$ 的群. 由 Lagrange 定理，对任意 $\alpha\in F^*$，有 $\alpha^{q-1}=1$. 两边同乘 α，得 $\alpha^q=\alpha$. 对于零元 0，显然也有 $0^q=0$. 因此，F 中的全部 q 个元素都是多项式 x^q-x 的根，这意味着 F 是 $f(x)\in\mathbb{F}'_p[x]$ 的一个分裂域. 因为 $\mathbb{Z}_p\cong\mathbb{F}'_p$，由 [定理，4.5]，$K$ 与 F 同构. ■

> **注记 4.3.** 通过 [例，3.14] 和 [定理，4.11]，我们实际上找出了所有的有限域.

定义 4.3. 设有代数扩张 E/F，若对任意 $F[x]$ 中的不可约多项式，要么 $g(x)$ 在 E 中没有根，要么 $g(x)$ 在 E 中可以完全分解，则称 E/F 为正规扩张.

> **定理 4.12.** 设 E/F 是有限扩张，则 E/F 是正规扩张当且仅当 E 是某个 $f\in F[x]$ 的分裂域.

证明. 假设 E 是 $f\in F[x]$ 的分裂域. 设 $g\in F[x]$ 不可约，若 g 在 E 中有根 α，我们证明 g 在 E 中可以完全分解. 设 K 是 $g\in E[x]$ 的分裂域，任意取定 g 在 K 中的根 β，我们只要证明 $E=E(\beta)$. 在 [定理，4.5] 中，取 $\eta_0: F\to F$ 为恒等映射，此时 $g=\tilde{g}$，则 η_0 可以开拓为同构 $\eta_1: F(\alpha)\to F(\beta)$，注意 E 和 $E(\beta)$ 分别是 $f\in F(\alpha)[x]$ 和 $\tilde{f}=f\in F(\beta)[x]$ 的分裂域，则 η_1 又可开拓为同构 $\eta: E\to E(\beta)$. 则有

$$\begin{aligned} &\sum_{i=1}^n x_ie_i=0,\quad x_i\in F, e_i\in E\\ \Longleftrightarrow\ &\eta\left(\sum_{i=1}^n x_ie_i\right)=\sum_{i=1}^n x_i\eta(e_i)=0\end{aligned}$$

这意味着 $[E:F]=[E(\beta):F]$，从而一定有 $E=E(\beta)$.

反过来，设 E/F 是正规扩张，且 $[E:F]=n$，以及 $E=\mathrm{span}_F\{\alpha_1,\cdots,\alpha_n\}$，记 $g_i\in F[x]$ 是 α_i 的极小多项式，则 g_i 在 E 中可以完全分解，令 $f=\prod\limits_{i=1}^n g_i$，则 E 是 $f\in F[x]$ 的分裂域. ■

定义 4.4. 设 E/F 是有限扩张，类似上面证明与记号，我们令 K 是 $f=\prod\limits_{i=1}^n g_i(x)\in F[x]$ 的分裂域，则 E/F 包含于正规扩张 K/F，因此我们可以定义包含 E/F 的最小正规扩张，称为是 E/F 的正规闭包.

定理 4.13. 设 E/F 是有限的正规扩张，K 是 E/F 的中间域，则如下条件等价：

(1) K/F 是正规扩张.

(2) 对任意 $\eta \in \mathrm{Gal}(E/F)$，有 $\eta(K) \subset K$.

(3) 对任意 $\eta \in \mathrm{Gal}(E/F)$，有 $\eta(K) = K$.

证明. 假定 K/F 是正规扩张，任取 $\alpha \in K$，记 $g(x) \in F[x]$ 为 α 的极小多项式，则 g 在 K 中可以完全分解，对任意 $\eta \in \mathrm{Gal}(E/F)$，则有 $0 = \eta(g(\alpha)) = g(\eta(\alpha))$，这意味着 $\eta(\alpha) \in K$，从而 $\eta(K) \subset K$. 另外作为 F-线性空间，又有 $[\eta(K) : F] = [K : F]$，这样就有 $\eta(K) = K$.

反过来，假定对任意 $\eta \in \mathrm{Gal}(E/F)$，都有 $\eta(K) = K$. 对任意 $\alpha \in K$，设 $g(x) \in F[x]$ 是 α 的极小多项式，我们证明 g 在 K 中可以完全分解. 由于 E/F 是正规扩张，则 g 在 E 中可以完全分解. 设 β 是 g 在 E 中的任意一根，在 [定理，4.5] 中，取 $\eta_0 : F \to F$ 为恒等映射，其可以开拓为 $\eta_1 : F(\alpha) \to F(\beta)$，由于 E 分别可以视为 $f \in F(\alpha)[x]$ 和 $f \in F(\beta)[x]$ 上的分裂域，则 η_1 可以开拓为 $\eta \in \mathrm{Gal}(E/F)$，这意味着 $\beta = \eta_1(\alpha) = \eta(\alpha) \in K$，于是 $g(x)$ 在 F 中可以完全分解. ■

定理 4.14. 设 $f \in F[x]$ 是可分多项式，E 是 $f \in F[x]$ 的分裂域，则 E/F 是可分扩张.

证明. 对任意 $\alpha \in E$，设 $g(x) \in F[x]$ 是 α 的最小多项式，由 [定理，4.12]，E/F 是正规扩张，则 g 在 E 中可以完全分解，记 g 在 E 中有 k 个互异根，由 [引理，4.4]，其诱导了从 $F(\alpha) \to E$ 的 k 个不同嵌入，记为 $\eta^{(1)}, \cdots, \eta^{(k)}$, 注意 E 可以视为可分多项式 $f \in F(\alpha)[x]$ 的分列域，由 [定理，4.5]，对每个 $\eta^{(i)}$，有 $[E : F(\alpha)]$ 个由 $\eta^{(i)}$ 开拓的同构：$\eta : E \to E$，于是

$$|\mathrm{Gal}(E/F)| = [E : F] = k \cdot [E : F(\alpha)]$$

又因为 $[E : F] = [E : F(\alpha)] \cdot [F(\alpha) : F] = [E : F(\alpha)] \cdot \deg(g)$，于是就有 $\deg(g) = k$，即 $g(x)$ 是可分多项式，于是 E/F 是可分扩张. ■

4.2 Galois 扩张

定义 4.5. 设 E/F 是代数扩张，我们称 E/F 是 Galois 扩张，如果 E/F 是可分扩张也是正规扩张.

定理 4.15. 设 E/F 是有限扩张，则如下条件等价

(1) E/F 是 Galois 扩张.

(2) E 是某个可分多项式 $f \in F[x]$ 的分裂域.

> **(3)** F 是 $\mathrm{Aut}(E)$ 的某个有限子群的不动域.

证明. 假定 E/F 是有限 Galois 扩张，则由 [定理，4.12]，E 是某个 $f \in F[x]$ 的分裂域，不妨设 f 在 E 中可分解为 $\prod_{i=1}^{n}(x-\alpha_i)$，对每个 α_i，设 $g_i \in F[x]$ 是 α_i 的极小多项式，由 E/F 是可分扩张，则 g_i 是可分多项式. 又因为 $\{g_i\}_{i=1}^{n}$ 跑遍了 f 的不可约因式，即 f 是可分多项式.

假定 E 是可分多项式 $f \in F[x]$ 的分裂域，记 $G = \mathrm{Gal}(E/F)$ 以及 $F' = \mathrm{Inv}(G)$，则由不动域的定义有 $\mathrm{Gal}(E/F') = \mathrm{Gal}(E/F) = G$. 于是有

$$|\mathrm{Gal}(E/F')| \xlongequal{\text{by } 4.5} [E:F'] \overset{\text{by } 1.6}{\leq} |G| \xlongequal{\text{by } 4.5} [E:F] = |\mathrm{Gal}(E/F')| \tag{4.6}$$

即

$$[E:F] = [E:F'] \cdot [F':F] = [E:F']$$

于是 $F = F'$.

假定 F 是 $G = \{\eta_1, \cdots, \eta_n\} < \mathrm{Aut}(E)$ 的不动域. 对任意 $\alpha \in E$，设 $g \in F[x]$ 是 α 的最小多项式，则 $\eta_i(\alpha)$ 是 g 在 E 中的根，不妨设 $\eta_1(\alpha), \cdots, \eta_k(\alpha)(\eta_1(\alpha) = \alpha)$ 是互异根，则 $k \leq \deg(g)$. 令 $f = \prod_{i=1}^{k}(x - \eta_i(\alpha))$，则 $\eta_i(f(x)) = f(x)(1 \leq i \leq n)$，这意味着 $f(x) \in F[x]$，从而 $g \mid f$，于是只能是 $g = f$，即在 g 在 E 中可完全分解且无重根，于是 E/F 是有限 Galois 扩张. ■

推论 4.16. 设 E 是域，G 是 $\mathrm{Aut}(E)$ 的有限子群，则 $E/\mathrm{Inv}(G)$ 是有限 Galois 扩张，于是

$$|\mathrm{Gal}(E/\mathrm{Inv}(G))| = [E:\mathrm{Inv}(G)] \leq |G|$$

即有 $G = \mathrm{Gal}(E/\mathrm{Inv}(G))$.

推论 4.17. 设 E/F 是有限 Galois 扩张，由(4.6)就有 $\mathrm{Inv}(\mathrm{Gal}(E/F)) = F$.

索引