近世代数笔记

作者：吕浩哲（Lucas Shen）

时间：July 13, 2025

封面：https://www.pixiv.net/artworks/100631860

悟已往之不谏，知来者之可追。——陶渊明

目录

第 1 章 群

1.1 群的定义

1.1.1 半群、幺半群与群

定义 1.1 (半群 (semigroup))

称带有二元运算 $\cdot$ 的集合 G 为半群，若其满足：

1. 封闭性（或 $\cdot$ 为 G 上的二元运算）：对任意 $a,b\in G$ 有 $ab\in G$.
2. 结合律：对任意 $a,b,c\in G$ 有 $(ab)c=a(bc)$.

若 G 为有限集，则称 $|G|$ 为 G 的阶.

♣

定义 1.2 (幺半群 (monoid))

称带有二元运算 $\cdot$ 的集合 G 为幺半群，若其满足：

1. 封闭性（或 $\cdot$ 为 G 上的二元运算）：对任意 $a,b\in G$ 有 $ab\in G$.
2. 结合律：对任意 $a,b,c\in G$ 有 $(ab)c=a(bc)$.
3. 单位元（幺元）：存在 $e\in G$，对任意 $a\in G$ 都有 $ae=ea=a$.

若 G 为有限集，则称 $|G|$ 为 G 的阶.

♣

注 实际上，幺半群就是“带有幺元的半群”.

定义 1.3 (群 (group))

称带有二元运算 $\cdot$ 的集合 G 为群，若其满足：

1. 封闭性（或 $\cdot$ 为 G 上的二元运算）：对任意 $a,b\in G$ 有 $ab\in G$.
2. 结合律：对任意 $a,b,c\in G$ 有 $(ab)c=a(bc)$.
3. 单位元（幺元）：存在 $e\in G$，对任意 $a\in G$ 都有 $ae=ea=a$.
4. 逆元：对任意 $a\in G$，存在 $a^{-1}\in G$ 使得 $aa^{-1}=a^{-1}a=e$.

若 G 为有限集，则称 $|G|$ 为 G 的阶.

♣

注 实际上，群就是对于逆运算封闭的幺半群，或者说带有幺元与逆元的半群.

直积可以通过已有群构造出新群.

命题 1.1 (群的直积)

设 $(G,\cdot_1),(H,\cdot_2)$ 为群，则集合 $G\times H=\{(g,h):g\in G,h\in H\}$ 在运算 $\cdot_3$：

$$(g_1,h_1)\cdot_3(g_2,h_2)=(g_1\cdot_1 g_2,h_1\cdot_2 h_2) \tag{1.1}$$

下为群.

♠

1.1.2 同态与子群

定义 1.4 (群同态)

设 G,H 为群，若映射 $f:G\to H$ 满足对任意 $a,b\in G$ 都有

$$f(ab)=f(a)f(b), \tag{1.2}$$

则称 f 为 G 到 H 的一个群同态. 在此基础上若 f 为单射，则称 f 为单同态；若 f 为满射，则称 f 为满同

态.

注 将其中群改为半群，则可以得到半群同态的定义.

容易验证，若 G,H,K 为群，$f:H\to K, g:G\to H$ 为群同态，则 $fg:G\to K$ 也为群同态.

定义 1.5 (群同构)

设 G,H 为群，若映射 $f:G\to H$ 为同态，且 f 为双射，则称 f 为 G,H 之间的群同构，此时称 G,H 同构，记为 $G\cong H$.

定义 1.6 (核、像与原像)

设 $f:G\to H$ 为群同态，则定义 f 的核与像分别为

$$\operatorname{Ker} f=\{g\in G:f(g)=e\in H\}\subset G, \tag{1.3}$$

$$\operatorname{Im} f=\{f(g):g\in G\}\subset H. \tag{1.4}$$

对于子集 $B\subset H$，可以定义 B 在 f 下的原像为

$$f^{-1}(B)=\{g\in G:f(g)\in B\}. \tag{1.5}$$

命题 1.2

设 $f:G\to H$ 为群同态，则

1. f 为单同态当且仅当 $\operatorname{Ker} f=e$.
2. f 为满同态当且仅当 $\operatorname{Im} f=H$.
3. f 为群同构当且仅当存在映射 $f^{-1}:H\to G$，使得 $ff^{-1}=\mathrm{Id}_H, f^{-1}f=\mathrm{Id}_G$.

定义 1.7 (子群)

设 $(G,\cdot)$ 为群，若非空集合 $K\subset G$，并且 $(K,\cdot)$ 为群，则称 K 为 G 的子群，记为 $K\leqslant G$.

命题 1.3

设 $(G,\cdot)$ 为群，K 为 G 的非空子集，则 $K\leqslant G$ 当且仅当对任意 $a,b\in K$，$ab^{-1}\in K$.

引理 1.1

设 G 为群，$\{H_i:i\in I\}$ 为 G 的子群，则 $\cap_{i\in I}H_i$ 也为 G 的子群.

定义 1.8 (生成群)

设 G 为群，$X\subset G$，则定义由 X 生成的群为

$$\langle X\rangle=\bigcap_{X\subset H_i\leqslant G}H_i. \tag{1.6}$$

注 根据定义立得，$\langle X\rangle$ 是任何包含 X 的 G 的子群的子群，也就是包含 X 的“最小”的群.

循环群

根据生成的概念，可以得到一类结构非常简单的群：循环群，它是由一个元素生成的群.

定义 1.9 (循环群)

设 S 为非空集合，$a \in G$，$\cdot$ 为其上的二元运算，则定义

$$\langle a \rangle = \langle \{a\} \rangle = \{a^n : n = 0, 1, \cdots\} \tag{1.7}$$

为由 a 生成的循环群. 若 $|\langle a \rangle| = n < \infty$，则称之为 n 阶循环群 C_n.

一类最经典的循环群的例子就是 $\mathbb{Z}_m$，而借助这一类群可以通过同构给出所有循环群的刻画.

定理 1.1

任何无限循环群同构与 $(\mathbb{Z}, +)$，任何有限（n 阶）循环群同构于 $\mathbb{Z}_m$.

定义 1.10 (元素的阶)

设 G 为群，则定义 $a \in G$ 的阶为

$$\operatorname{ord} a = |a| = \min\{k : a^k = e\}, \tag{1.8}$$

也就是由 a 生成的循环群的阶，若任意 a^k 两两不同，则称 a 的阶为 0.

命题 1.4

设循环群 $C_n = \langle a \rangle$，则

$$|a^k| = \frac{n}{\gcd(n, k)}. \tag{1.9}$$

1.2 陪集与正规子群

1.2.1 陪集与计数

定义 1.11 (左/右同余)

设群 $H \leqslant G$，$a, b \in G$，那么

1. 称 a 与 b 模 H 的右同余，若 $ab^{-1} \in H$，记为 $a \equiv_r b (\operatorname{mod} H)$.
2. 称 a 与 b 模 H 的左同余，若 $a^{-1}b \in H$，记为 $a \equiv_l b (\operatorname{mod} H)$.

容易验证，左同余与右同余均为等价关系，若 G 为 Abel 群，则左同余与右同余等价.

定义 1.12 (陪集)

设 G 为群，$H \leqslant G$，则对任意 $a \in G$，可以定义 H 的左、右陪集为

$$aH = \{ah : h \in H\}, \quad Ha = \{ha : h \in H\}. \tag{1.10}$$

借助陪集，可以更好地描述左右同余的概念：

$$a \equiv_r b (\operatorname{mod} H) \iff a \in Hb \tag{1.11}$$

$$a \equiv_l b (\operatorname{mod} H) \iff a \in bH \tag{1.12}$$

由于左右同余为等价关系，因此陪集恰好可以看作等价类，这种等价类给出了群 G 的一个划分，有如下命题：

命题 1.5

设群 $H \leqslant G$，则

1. 对任意 $a,b \in G$，$aH = bH$ 当且仅当 $a \equiv_l b (\mathrm{mod}\, H)$，$Ha = Hb$ 当且仅当 $a \equiv_r b (\mathrm{mod}\, H)$.
2. 对任意 $a,b \in G$，$aH = bH, aH \cap bH = \emptyset$ 有且仅有一者成立.

♠

定义 1.13 (指数)

设群 $H \leqslant G$，则定义子群 H 关于 G 的指数为 G 中 H 的陪集的个数，记为 $[H:G]$.

♣

由上述命题可知，G 中元素可以由子群 H 的左陪集或右陪集划分，即

$$G = \bigsqcup_{a \in G} aH \tag{1.13}$$

若考虑两边的数量，可知 $|H||G|$，更精确地，可以得到如下定理.

定理 1.2 (Lagrange)

设群 $H \leqslant G$（均为有限群），则

$$|G| = |H| \cdot [G:H]. \tag{1.14}$$

♡

推论 1.1

设群 $K \leqslant H \leqslant G$，则

$$[G:K] = [G:H][H:K]. \tag{1.15}$$

♡

推论 1.2

设群 $H, K \leqslant G$，则 $|HK| = |H| \cdot |K| / |H \cap K|$.

♡

证明 由于 $H \cap K \subset K$，根据 Lagrange 定理可得 $[K : H \cap K] = |K|/|H \cap K|$，并且 $H(H \cap K) = H$，由此对任意 $k \in K$ 都有 $Hk = H(H \cap K)k$. 对 K 陪集分解可得

$$K = \bigsqcup_{k \in K} (H \cap K)k, \tag{1.16}$$

这里共有 $[K : H \cap K]$ 个陪集，进一步有

$$HK = H \bigsqcup_{k \in K} (H \cap K)k = \bigsqcup_{k \in K} H(H \cap K)k = \bigsqcup_{k \in K} Hk \tag{1.17}$$

根据无交并计数可得

$$|HK| = |H|[K : H \cap K] = \frac{|H||K|}{|H \cap K|}. \tag{1.18}$$

推论 1.3

设群 $H, K \leqslant G$，则 $[G : H \cap K] = [G:H][G:K]$.

♡

1.2.2 正规子群与商群

在陪集的基础上，可以进一步讨论一种特殊的子群：正规子群.Abel 群的左陪集等于右陪集，但一般的群中也会有左陪集等于右陪集的情况，这就是正规子群.

定义 1.14 (正规子群)

设群 $H \leqslant G$，称 H 为 G 的正规子群，若对任意 $a \in G$ 有 $aH = Ha$，记为 $H \triangleleft G$.

♣

需要注意的是，上面的 $aH = Ha$ 并不代表对任意 $h \in H$ 都有 $ah = ha$，这只是集合整体的相等. 进一步可以给出正规子群的多种刻画.

命题 1.6

设群 $H \leqslant G$，则下述命题等价：

1. $H \triangleleft G$.
2. 对任意 $h \in H$，存在 $h' \in H$ 使得 $ah = h'a$.
3. 对任意 $a \in G$，$aHa^{-1} := \{aha^{-1} : h \in H\} \subset H$.
4. 对任意 $a \in G$，$aHa^{-1} := \{aha^{-1} : h \in H\} = H$.

♠

定理 1.3

设 $K \leqslant G, N \triangleleft G$，则

1. $N \cap K \triangleleft K$.
2. $N \triangleleft \langle N \cup K \rangle$.
3. $NK = \langle N \cup K \rangle = KN$.
4. 若 $K \triangleleft G$，$K \cap N = \{e\}$，则对任意 $k \in K, n \in N$ 都有 $nk = kn$.

♡

证明

1. 继承 N 的性质.
2. 显然（因为 $N \leqslant \langle N \cup K \rangle$）.
3. N 的正规性保证了 NK 为群，并且显然有 $N \cup K \subset NK$. 假设有群 $A \leqslant G, A \supset N \cup K$，则必有 $NK \leqslant A$，故得证.
4. 对任意 $n \in N, k \in K$，考虑 $nkn^{-1}k^{-1}$ 有

$$nkn^{-1}k^{-1} = (nkn^{-1})k^{-1} \in K, \quad nkn^{-1}k^{-1} = n(kn^{-1}k^{-1}) \in N, \tag{1.19}$$

故 $nkn^{-1}k^{-1} = e$，即 $nk = kn$.

借助正规子群，可以讨论一类非常重要的群结构：商群.

定义 1.15 (商群)

设群 $H \triangleleft G$，则定义集合及其上的运算为

$$G/H = \{aH : a \in G\}, \quad (aH) \cdot (bH) = (ab)H \tag{1.20}$$

则 $(G/H, \cdot)$ 为群，称为 G 商 H 的群.

♣

定义商运算时最重要的一步就是验证其良定性，即不同代表元得到相同等价类. 而商群之所以只能取正规子群，正是因为正规子群保证了

$$(aH)(bH) = a(Hb)H = a(bH)H = (ab)H, \tag{1.21}$$

也就是商运算的无矛盾性.

每个正规子群都能自然诱导出一个商群，而每个商群都能诱导出一个同态，称为**典范映射**

定理 1.4 (典范映射)

设群 $H \triangleleft G$，定义映射 $\pi : G \to G/H$，$\pi(a) = aH$，则称 π 为典范映射.

♡

典范映射实际上是将 G 中一坨元素粘到一起的过程，这一坨元素构成了一个等价类，所有的等价类就构成了商群.

1.2.3 同构基本定理

命题 1.7

设 $f:G\to H$ 为群同态，则 $\operatorname{Ker} f\triangleleft G$.

定理 1.5 (第一同构定理)

设 $f:G\to H$ 为群同态，则 $G/\operatorname{Ker} f\cong H$.

定理 1.6 (第二同构定理)

设 $K\leqslant G, N\triangleleft G$，则 $K/(N\cap K)\cong NK/N$.

证明 构造满同态 $f:K\to NK/N$，$f(k)=kN$，则 $\operatorname{Ker} f=N\cap K$.

定理 1.7 (第三同构定理)

设 $H,K\triangleleft G$，$K<H$，则 $(G/K)/(H/K)\cong G/H$.

证明 构造满同态 $f:G/K\to G/N$，$f(gK)=gH$，则 $\operatorname{Ker} f=H/K$.

1.3 群的经典例子

1.3.1 置换群

有限集合上的双射可以看作其中元素的一个重新排列（如果确定某种初始顺序），因此置换可由有限集合上的双射自然诱导.

定义 1.16 (置换)

设 $\Sigma=\{1,\cdots,n\}$，称其上的一个双射 τ 为一个置换，可记为

$$\tau=\begin{pmatrix}1,2,\cdots,n\\ \tau(1),\tau(2),\cdots,\tau(n)\end{pmatrix}. \tag{1.22}$$

特别的，对于 $1\leqslant i_1,\cdots,i_r\leqslant n(r\leqslant n, i_r\neq i_s)$，可记置换 $\sigma=(i_1,\cdots,i_r)$，使得 $\sigma(i_k)=\sigma(i_{k+1}),\sigma(i_r)=i_1$，称为轮换. 置换的表示不是唯一的，如果将 $1,\cdots,n$ 的顺序打乱，则对应的像也会有不同的顺序，例如轮换 $\sigma=(i_1,i_2,\cdots,i_r)=(i_2,\cdots,i_r,i_1)$.

固定 n，所有置换之间可以复合，此时所有置换构成**置换群**.

定义 1.17 (置换群)

集合 $\sum=\{1,\cdots,n\}$ 中的所有置换在映射的复合下构成一个群，称为 n 阶置换群 S_n，易得 $|S_n|=n!$.

定理 1.8

任何非单位 $\sigma\in S_n$ 都可以分解为一系列不相交轮换的乘积（每个轮换长度至少为 2），并且这种分解在不考虑次序前提下唯一.

证明 设 $\sigma\in S_n$，$\sigma\neq(1)$，则如下定义等价关系：对任意 $1\leqslant i\neq j\leqslant n$，称 $i\sim j$ 若存在 $k\in\mathbb{N}$ 使得 $\sigma^k(i)=(j)$.

容易验证这是一个等价关系，它们构成 $\{1\leqslant k\leqslant n:\sigma(k)\neq k\}$ 的一个划分，取每个等价类中的一个元素 $x_1,\cdots,x_p$，则

$$\sigma=(x_1,\cdots,\sigma^{k_1-1}(x_1))\cdots(x_p,\cdots,\sigma^{k_p-1}(x_p)) \tag{1.23}$$

得证，反过来唯一性易得.

上面的分解还有一种良好的性质，若 $\sigma=\sigma_1\cdots\sigma_p$ 为如上分解，则 σ_i 都是可交换的，即对任意 $\tau\in S_p$

$$\sigma=\sigma_{\tau(1)}\cdots\sigma_{\tau(p)}. \tag{1.24}$$

引理 1.2

任何非单位 $\sigma\in S_n$ 都可以分解为一系列对换的乘积，且这种对换的奇偶性是唯一的.

证明 分解是易得的，只需证明奇偶的唯一性. 定义式

$$\prod_{1\leqslant i<j\leqslant n}(\sigma(j)-\sigma(i)) \tag{1.25}$$

的符号为置换 σ 的符号，则只需证明，每次复合一个对换后，置换都会变号.

定义 1.18 (奇/偶置换)

设 $\sigma\in S_n$，若 σ 能分解为奇数/偶数个对换的乘积，则称 σ 为奇置换/偶置换.

定理 1.9

设 $n\geqslant 2$，A_n 为 S_n 中所有偶置换的全体，则 $A_n\triangleleft S_n$，并且 $[S_n:A_n]=2$，或者说 $|A_n|=n!/2$，A_n 称为交错群.

类比整数中的素数，群中也有结构相似的对象，称为单群.

定义 1.19 (单群)

群 G 称为单群，若其只有平凡正规子群（$\{e\}$ 和 G）.

命题 1.8

剩余类群 $\mathbb{Z}_n$ 为单群当且仅当 n 为素数.

下面证明一个略显复杂的命题：绝大多数 A_n 都是单群，首先证明一些引理.

引理 1.3

设 $\tau=(a_1a_2\cdots a_m),\sigma\in S_n$，则

$$\sigma\tau\sigma^{-1}=(\sigma(a_1)\sigma(a_2)\cdots\sigma(a_m)). \tag{1.26}$$

注 该引理给出了置换群中共轭元的关系，非常直观.

引理 1.4

固定 $r\neq s\in\{1,2,\cdots,n\}$，则 $A_n(n\geqslant 3)$ 由三循环 $\{(rsk):1\leqslant k\leqslant n,k\neq r,s\}$ 生成.

证明 不妨设 $n>3$，根据定义可知 A_n 中任何元素都能表示为（偶数个）对换的乘积，有形式 $(ab)(cd)$ 或 $(ab)(ac)$，而 $(ab)(cd)=(acb)(acd)$，$(ab)(ac)=(acb)$，因此 A_n 中任何元素都能表示为三循环的乘积，这些三循环有形式 $(rsa),(ras),(rab),(sab),(abc)$，其中 $a,b,c\neq r,s$，并且

$$(ras)=(rsa)^2,\quad (rab)=(rsb)(rsa)^2, \tag{1.27}$$

$$(sab)=(rsb)^2(rsa),\quad (abc)=(rsa)^2(rsc)(rsb)^2(rsa), \tag{1.28}$$

因此 A_n 中元素均由置换 (rsk) 生成.

引理 1.5

若 $N\triangleleft A_n(n\geqslant 3)$ 且 N 包含一个三循环，则 $N=A_n$.

证明 若 $(rsc)\in N$，则对任意 $k\neq r,s;c$ 有

$$(rsk)=[(rs)(ck)](rsc)^2[(rs)(ck)]^{-1}\in N \tag{1.29}$$

因此根据上一条引理有 $N=A_n$.

定理 1.10

交错群 A_n 为单群，当且仅当 $n\neq 4$.

证明 Step 1. 证明 A_5 为单群，设 $\{e\}\neq N\triangleleft A_5$，由于 A_5 中的型只有 $1^5,1^23^1,1^12^2,5^1$，因此分如下类讨论.

1. 若 N 包含一个三循环，则有引理可得 $N=A_5$.
2. 若 N 包含一个五循环，不妨设 $(12345)\in N$，则

$$(124)=(123)(12345)(123)^{-1}(12345)^{-1}\in N, \tag{1.30}$$

故 N 包含一个三循环，$N=A_5$.

3. 若 N 包含一个 2^2 型置换，不妨设 $(12)(34)\in N$，则

$$(243)=(123)[(12)(34)](123)^{-1}[(12)(34)]^{-1}\in N, \tag{1.31}$$

故 N 包含一个三循环，$N=A_5$.

Step 2. 证明 A_n 为单群可推出 A_{n+1} 为单群（$n\geqslant 5$）.

设 $H\triangleleft A_{n+1}$ 非平凡，先证明存在 $\sigma\in H$ 使得 $\sigma(1)=1$，取 $e\neq\tau\in H$，若 $\tau(1)=i\neq 1$，则取 $j\in\{2,\cdots,n\}$ 使得 $j\neq i,\sigma(j)\neq j$，再取 $k,l\notin\{1,i,j,\sigma(j)\}$，则

$$\sigma=(jkl)\sigma'^{-1}(jkl)^{-1}\sigma'\in H \tag{1.32}$$

满足要求（这里构造 $ABA^{-1}B^{-1}$ 式的结构是为了保证封闭）. 因此 $H\cap A_n\neq\{e\}$，A_n 为单群说明 $H\cap A_n=A_n$，即 $H\geqslant A_n$，故 H 中包含三循环，即 $H=A_{n+1}$，得证.

1.3.2 二面体群

置换群 S_n 还有一种重要子群，称为二面体群.

定义 1.20 (二面体群)

设 $n\geqslant 3$，定义二面体群 D_n 为由满足如下条件的 a,b 生成的阶为 $2n$ 的群：

1. $a^n=b^2=e$，对任意 $0<k<n$ 都有 $a^k\neq e$.
2. $ba=a^{-1}b$.

下面的定理说明，这种定义是良好的.

定理 1.11

任意由满足上述定义中的 a,b 生成的阶为 $2n$ 的群都同构于 D_n.

证明 由于 $D_n=\{a^ib^j:0\leqslant i<n;j=0,1\}$，设 G 由 a_1,b_1 生成，下证 $f:D_n\to G$，$f(a^ib^j)=a_1^ib_1^j$ 是一个群同构. 显然 f 为双射，只需证明其为同态，对任意 $a^ib^j,a^ub^v\in D_n$，有

$$f((a^ib^j)(a^ub^v))=f(a^{i-u}b^{j+v})=a_1^{i-u}b_1^{j+v}=(a_1^ib_1^j)(a_1^ub_1^v)=f(a^ib^j)f(a^ub^v) \tag{1.33}$$

1.4 初探范畴

下面初步介绍一些范畴的概念，范畴是一种重要的数学语言，可以概括不同场景中不同数学对象的相同结构. 我们过去讨论过许多数学对象（如集合、群、环、线性空间等），以及其中的态射（集合间的映射、群/环之

间的同态、线性变换），它们具有一些共有的特性：态射都具有结合律，并且每个对象都有一个到自身的单位态射（恒等映射）.

定义 1.21 (范畴)

设 $\mathbf{C}$ 为一个类，且对其中任意对象 A,B 都有一个集合 $[A,B]=\{A\to B\}$（或 $hom(A,B)$），且有如下性质

1. 态射的合成：对 $\mathbf{C}$ 中任意对象 A,B,C，有映射

$$[B,C]\times[A,B]\longrightarrow[A,C] \tag{1.34}$$

$$(g,f)\longmapsto g\circ f=gf \tag{1.35}$$

2. 结合律：若 $f\in[A,B],g\in[B,C],h\in[C,D]$，则

$$(fg)h=f(gh). \tag{1.36}$$

3. 单位元：对 $\mathbf{C}$ 中任意对象 B，存在态射 $1_B\in[B,B]$，使得对任意 $f\in[A,B],g\in[B,C]$ 有

$$1_B\circ f=f,\quad g\circ 1_B=g. \tag{1.37}$$

则称 $\mathbf{C}$ 为范畴.

定义 1.22 (对象的等价)

设 $\mathbf{C}$ 为范畴，A,B 为其对象，称 $f\in[A,B]$ 为等价，若存在 $g\in[B,A]$ 使得

$$f\circ g=1_B,\quad g\circ f=1_A. \tag{1.38}$$

定义 1.23 (积)

设 $\mathbf{C}$ 为范畴，$\{A_i:i\in I\}$ 是 $\mathbf{C}$ 中的一族对象，则定义 $\{A_i:i\in I\}$ 的积为 $\mathbf{C}$ 中的一个对象 P，带有一族态射 $\{\pi_i\in[P,A_i]:i\in I\}$ 使得对任意对象 B 以及一族态射 $\{\varphi_i\in[B,A_i]:i\in I\}$，存在唯一态射 $\varphi\in[B,P]$ 使得对任意 $i\in I$ 都有 $\pi_i\circ\varphi=\varphi_i$.

定义中的 π_i 在实际对象中常以投影映射出现. 借助交换图，可以较清楚地理解上述定义

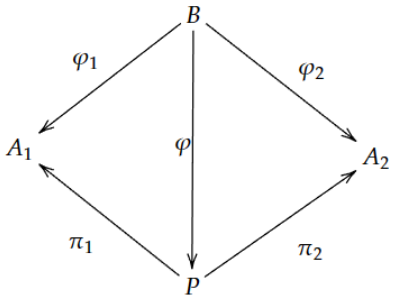

图 1.1: 积

积在许多数学对象中都有出现，比如集合的卡氏积，以及下一节会讨论的群的积.

定理 1.12

设 $(P,\{\pi_i\}),(Q,\{\psi_i\})$ 为范畴 $\mathbf{C}$ 中一族对象 $\{A_i:i\in I\}$ 的积，则 P,Q 等价.

证明 根据积的定义，存在态射 $f\in[P,Q],g\in[Q,P]$ 使得如下交换图成立

这说明 $g\circ f$ 满足对任意 i 有 $\pi_i\circ(g\circ f)=\pi_i$ 成立. 根据积的定义，这里的 $g\circ f$ 是唯一的，而 Id_P 恰好也满足这一关系，故 $g\circ f=\mathrm{Id}_P$，同理可得 $f\circ g=\mathrm{Id}_Q$，故 P,Q 等价.

下面考虑积的一个对偶定义：余积.

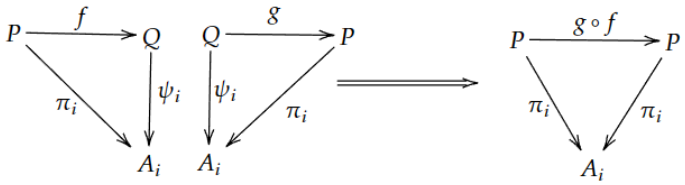

图 1.2: 交换图

定义 1.24 (余积)

设 $\mathbf{C}$ 为范畴，$\{A_i : i \in I\}$ 是 $\mathbf{C}$ 中的一族对象，则定义 $\{A_i : i \in I\}$ 的余积为 $\mathbf{C}$ 中的一个对象 S，带有一族态射 $\{\tau_i \in [A_i, S] : i \in I\}$ 使得对任意对象 B 以及一族态射 $\{\psi_i \in [A_i, B] : i \in I\}$，存在唯一态射 $\psi \in [S, B]$ 使得对任意 $i \in I$ 都有 $\psi \circ \tau_i = \psi_i$.

如果从交换图来看，余积实际上是将积中的箭头全部反向.

定理 1.13

设 $(S, \{\tau_i\}), (S', \{\lambda_i\})$ 为范畴 $\mathbf{C}$ 中一族对象 $\{A_i : i \in I\}$ 的余积，则 S, S' 同构.

在许多例子中，范畴的对象是一些集合，而态射对应集合间的映射，在这种考虑下，可以给出具体范畴的定义.

定义 1.25 (具体范畴)

具体范畴是带有一个函数 σ 的范畴 $\mathbf{C}$，对任意 $\mathbf{C}$ 中的对象 A 赋予一个集合 $\sigma(A)$（称为 underlying set）满足如下性质：

1. 任何态射 $A \to B$ 是 underlying set 上的映射 $\sigma(A) \to \sigma(B)$.
2. 对象 A 中的恒等态射是 $\sigma(A)$ 中的恒等映射.
3. 范畴 $\mathbf{C}$ 中态射的复合与对应 underlying set 中映射的复合相同.

具体范畴既具有范畴的性质，也具有集合的性质，大多时候我们省略 σ，采用相同的记号表示对象与其 underlying set，不过要注意在使用时分辨范畴对象的态射与集合间的映射.

定义 1.26 (自由对象)

设 F 为具体范畴 $\mathbf{C}$ 中的对象，X 为一个非空集合，$i : X \to F$ 为一个映射（集合意义），称 F 在集合 X 上自由，若对任意 $\mathbf{C}$ 中的对象 A 以及映射 $f : X \to A$（集合意义），存在唯一态射 $\bar{f} \in [F, A]$ 使得 $\bar{f} \circ i = f$.

若 F 在集合 X 上自由，则考虑 X 在某映射下的像时，只需要考虑集合 $i(X)$ 的像即可.

例 1.1 考虑如下事实：设 G 为群，$g \in G$，则 $\mathbb{Z}$ 到 G 的同态可仅由在 1 处的取值确定，这种同态有形式 $\bar{f} : \mathbb{Z} \to G$，$\bar{f}(n) = g^n$. 若令 $X = \{1\}$，i 为 X 到 $\mathbb{Z}$ 的嵌入映射，考虑群范畴，则上面的事实可以表述为：任意映射 $f : X \to G$，存在唯一的群同态 $\overline{f} : \mathbb{Z} \to G$，使得 $f = \bar{f} \circ i$，即 $\mathbb{Z}$ 在 X 上自由.

换句话说，这种映射 f 与同态 $\bar{f}$ 之间存在一一对应，因此任何同态都可以仅由 X 在某个映射 f 下的像确定.

定理 1.14

设 $\mathbf{C}$ 为具体范畴，F, F' 为其中两个对象，分别在集合 X, X' 上自由，且 $|X| = |X'|$，则 F, F' 等价.

证明

上面的积、余积、自由对象都借助某种**泛性质** (universal mapping property) 定义（根据某种“存在唯一”性确定某一映射的性质），并且给定（一族）对象的两个积（或余积、自由对象）实际上是等价的.

定义 1.27 (终对象/始对象)

称范畴 $\mathbf{C}$ 中的对象 I 是始对象，若对任意 $\mathbf{C}$ 中的对象 C，$[I,C]$ 中存在唯一态射.$\mathbf{C}$ 中的对象 T 称为终对象，若对任意 $\mathbf{C}$ 中的对象 C，$[I,C]$ 中存在唯一态射.

定理 1.15

范畴 $\mathbf{C}$ 中任何两个始对象（或终对象）等价.

1.5 直和与直积

本节讨论群范畴中的积与 Abel 群范畴的余积，这不仅是一种构造新群的方法，更是一种描述群结构的方法.

一开始的几节中介绍过两个群的直积 $G\times H$，很容易将其推广为任意多群的直积 $\prod_{i\in I}G_i$，其上的运算也很容易推广（每一分量对应的运算），这样的群以及其上的运算称为这一族群 $\{G_i:i\in I\}$ 的**直积**.

定理 1.16

设 $\{G_i\}$ 为一族群，则

1. 直积 $\prod_{i\in I}G_i$ 仍然是一个群.
2. 对任意 $k\in I$，映射 $\pi_i:\prod_{i\in I}G_i\to G_k$，$\pi_i(\{a_i:i\in I\})=a_k$ 是一个满同态.

注 上述定义中的 π_k 称为直积的**典范映射**.

证明 只证明 2，

$$\pi_i(\{a_i\}\{b_i\})=a_ib_i=\pi_i(\{a_i\})\pi_i(\{b_i\}) \tag{1.39}$$

对任意 $g\in G_i$，取 $g_j=e_j\in G_j,j\neq j$，并记 $g=g_i$ 则 $\pi_i(\{g_i\})=g_i$. 故为满射.

定理 1.17

设 $\{G_i:i\in I\}$ 为一族群，$\{\varphi_i:H\to G_i:i\in I\}$ 为一族群同态，则存在唯一的同态 $\varphi:H\to\prod_{i\in I}G_i$，使得对任意 $i\in I$ 都有 $\pi_i\circ\varphi=\varphi_i$，换句话说，$\prod_{i\in I}G_i$ 为群范畴中的积.

证明 容易构造 + 验证.

特别地，由于 Abel 群的直积也是一个 Abel 群，因此这也是 Abel 群范畴中的一个积.

定义 1.28 ((外) 弱直积)

一族群 $\{G_i:i\in I\}$ 的外弱直积定义为 $\prod_{i\in I}^wG_i=\{g\in\prod_{i\in I}G_i\}$，且除了有限项外，均有 $g_i=e_i\in G_i$. 若每个 G_i 均为 Abel 群，则 $\prod_{i\in I}^wG_i$ 也被称为外直和，表示为 $\sum_{i\in I}G_i$.

注 特别地，当 I 为有限集时，弱直积与直积相同.

定理 1.18

设 $\{G_i:i\in I\}$ 为一族群，则

1. $\prod_{i\in I}^wG_i\triangleleft\prod_{i\in I}G_i$.
2. 对任意 $k\in I$，定义映射 $\tau_k:G_k\to\prod_{i\in I}^wG_i$，使得 $\tau_k(a)=\{a_i\}$，其中 $a_i=a,a_j=e_j,j\neq i$，则 τ_i 为单同态.
3. 对任意 $i\in I$，$\tau_i(G_i)\triangleleft\prod_{i\in I}G_i$.

注 上述定义中的 τ_i 称为**典范单射**.

证明

1. 设 $\{g_i\}\in\prod_{i\in I}$，则对任意 $\{h_i\}^w\in\prod_{i\in I}^w G_i$，当 $h_i=e_i$ 时，$g_ih_ig_i^{-1}=e_i$，因此共轭运算的结果仍然只有有限项不为单位元，因此
$$\{g_i^{-1}\}\prod_{i\in I}^w G_i\{g_i\}=\prod_{i\in I}^2 G_i. \tag{1.40}$$
2. 这里的 τ 可以看作嵌入映射，这种嵌入是唯一的，因此 τ 为单射，同态是容易验证的.
3. 与 1 类似，共轭运算后，$\tau_i(G_i)$ 的指标 $j\neq i$ 仍然为 e_j，因此仍然为 $\tau_i(G_i)$.

定理 1.19

设 $\{A_i:i\in I\}$ 为一族 Abel 群，若 B 为 Abel 群且 $\{\psi_i:A_i\to B:i\in I\}$ 为一族同态，则存在唯一的同态 $\psi:\sum_{i\in I}A_i\to B$ 使得 $\psi\circ\tau_i=\psi_i$，换句话说，$\sum_{i\in I}A_i$ 为 Abel 群范畴的余积.

证明 定义 $\psi(\{a_i\})=\sum_{i\in I}\psi_i(a_i)$，根据外直和的定义可知求和只有有限项（因为仅有限个 $a_i\neq 0_i$，$\psi_i(a_i)\neq 0$），由此可知
$$\psi\circ\tau_i(a)=\psi_i(a),\quad \psi(\{a_i\}+\{b_i\})=\sum_{i\in I}\psi_i(a_i+b_i)=\sum_{i\in I}\psi_i(a_i)+\sum_{i\in I}\psi_i(b_i)=\psi(\{a_i\})+\psi(\{b_i\}) \tag{1.41}$$
为了证明唯一性，假设还存在 ϕ 满足条件，则
$$\phi(\{a_i\})=\phi\left(\sum_{i\in I}\tau_i(a_i)\right)=\sum_{i\in I}\psi_i(a_i)=\psi(\{a_i\}) \tag{1.42}$$
得证.

下面的定理给出了一个群 G 与正规子群的弱直积同构的条件.

定理 1.20

设 $\{N_i:i\in I\}$ 为一族 G 的正规子群，若满足

1. $G=\langle\bigcup_{i\in I}N_i\rangle$.
2. 对任意 $k\in I$，$N_k\cup\langle\bigcup_{i\neq k}N_i\rangle=\langle e\rangle$.

则 $G\cong\prod_{i\in I}^w N_i$.

证明 根据定理1.3中正规子群的交换性，任意 $\{n_i\}\in\prod_{i\in I}^w N_i$ 可以唯一定义一个元素 $\prod_{i\in I}n_i=\phi(\{n_i\})\in G$，根据外直积的定义可知乘积仅有限项，只需证明 ϕ 为一个群同构，而其显然为同态（正规子群的交换性），只需证明其单且满.

设 $\prod_{i\in I}n_i=e=n_i\tilde{n}_i$，其中 $\{n_i\}\in\prod_{i\in I}^w N_i$，则由条件 2，可知 $n_i=\tilde{n}_i=e$，因此单射得证.

根据条件 1，可知任意 $g\in G$ 可表示为 $g=\prod_{i\in I}n_i$，其中 $n_i\in N_i$，其仅有限个 $n\neq e$，ϕ 单使得这种表示唯一，综上得证.

推论 1.4

设 $N_1,\cdots,N_r\lhd G$ 使得 $G=N_1\cdots N_r$，并且对任意 $1\leqslant k\leqslant r$ 都有 $N_k\cap(N_1\cdots\hat{N}_k\cdots N_r)=\langle e\rangle$，则 $G\cong\prod_{i=1}^r N_i$.

定义 1.29 (内弱直积)

设 $\{N_i:i\in I\}$ 为 G 的一族正规子群，并且 $G=\langle\bigcup_{i\in I}N_i\rangle$，对任意 $k\in I$ 有 $N_k\cap\langle\bigcup_{i\neq k}N_i\rangle=\langle e\rangle$，则 G 称为这一族群的内弱直积，记为 $G=\prod_{i\in I}^w N_i$. 若 G 为 Abel 群，则也称为内直和.

定理 1.21

设 $\{N_i : i \in I\}$ 为 G 的一族正规子群，则 G 为这一族群的内弱直积当且仅当任何 $g \neq e, g \in G$ 都能唯一表示为 $\prod_{i\in I} n_i$，且其中仅有限项不为 e.

定理 1.22

设 $\{f_i : G_i \to H_i : i \in I\}$ 为一族群同态，且 $f = \prod f_i$ 表示映射 $\prod_{i\in I} G_i \to \prod_{i\in I} H_i, \{g_i\} \mapsto \{f_i(g_i)\}$，则 f 为群同态，且

$$\operatorname{Ker} f = \prod_{i\in I} \operatorname{Ker} f_i, \quad \operatorname{Im} f = \prod_{i\in I} \operatorname{Im} f_i \tag{1.43}$$

并且 f 为单同态当且仅当每个 f_i 为单同态.

推论 1.5

设 $\{G_i : i \in I\}, \{H_i : i \in I\}$ 为一族群，且每个 $N_i \triangleleft G_i$，则

1. $\prod_{i\in I} N_i \triangleleft \prod_{i\in I} G_i$，并且 $\prod_{i\in I} G_i / \prod_{i\in I} N_i \cong \prod_{i\in I} G_i/N_i$.
2. $\prod^w_{i\in I} N_i \triangleleft \prod^w_{i\in I} G_i$，并且 $\prod^w_{i\in I} G_i / \prod^w_{i\in I} N_i \cong \prod^W_{i\in I} G_i/N_i$.

1.6 自由群与自由积

本节中将讨论群范畴中的自由对象：自由群，并借此描述群的结构.

给定集合 X，可以构造其上的自由群 F. 若 $X = \emptyset$，则 $F = \langle e \rangle$，若不然，则考虑与 X 无交的集合 $X^{-1} = \{x^{-1} : x \in X\}$, $|X| = |X^{-1}|$，再取 $1 \notin X \cup X^{-1}$，则称 X 中的一个**字**为序列 $a_1 a_2 \cdots a_k$，其中 $a_i \in X \cup X^{-1} \cup \{1\}$，1 称为**空字**，两个字 $a_1 \cdots a_k, b_1 \cdots b_l$ 相等当且仅当 $k = l$，且每个 $a_i = b_i$. 接着在这个集合上定义群结构：

1. 乘法：$(a_1 \cdots a_k)(b_1 \cdots b_l) = a_1 \cdots a_k b_1 \cdots b_l$.
2. 单位元：$(a_1 \cdots a_k)1 = 1(a_1 \cdots a_k) = a_1 \cdots a_k$.
3. 逆元：$(a_1 \cdots a_k)^{-1} = a_k^{-1} \cdots a_1^{-1}$，特别的，$xx^{-1} = x^{-1}x = 1$.

借助这些运算，字可以进行化简，即 $abb^{-1}c = ac$，我们自然希望字能尽可能简化，由此定义

定义 1.30 (既约字)

若字 $w \neq 1$ 中无形如 $a^{-1}a$ 或 1 的子串，则称其为既约字.

引理 1.6

任一字 w 存在唯一既约形式.

证明

既约字自然会诱导出一个等价关系，而上述引理保证了这种等价关系的良定性，即字 $w_1 \sim w_2$ 当且仅当 w_1, w_2 能化简到同一既约形式. 且容易验证这种等价关系下字之间运算的良定性，即若 $w_1 \sim w_2, u_1 \sim u_2$，则 $w_1 u_1 \sim w_2 u_2$.

定理 1.23

设 X 非空，$F = F(X)$ 为 X 中任意既约字的集合，则 F 在上述运算下为一个群，且 $F = \langle X \rangle$.

定义 1.31 (自由群)

如上定义的群 $F = F(X)$ 称为 X 上的自由群.

下面的定理表明，自由群是群范畴中的一种自由对象.

定理 1.24

设 F 为 X 上的自由群，$\tau: X \to F$ 为嵌入映射，若 G 为群，$f: X \to G$ 为映射，则存在唯一群同态 $\bar{f}: F \to G$ 使得 $\bar{f} \circ \tau = f$. 换句话说，群范畴中的对象 F 为集合 X 上的自由对象.

证明 对任意 $w = x_1 \cdots x_k \in F$，定义映射

$$\bar{f}(w) = \bar{f}(x_1) \cdots \bar{f}(x_k), \tag{1.44}$$

$$\bar{f}(x_k) = \begin{cases} f(x_k), x_k \in X \\ f(x_k^{-1})^{-1}, x_k \in X^{-1} \end{cases} \tag{1.45}$$

则不难验证 $\bar{f}$ 满足条件.

推论 1.6

任意群 G 都是一个自由群的同态像.

证明 设 X 为 G 的生成元的集合，F 为 X 上的自由群，则对于嵌入映射 $X \hookrightarrow G$，存在唯一同态 $\bar{f}: F \to G$ 使得 $\bar{f}(x) = x \in G$，而 $G = \langle X \rangle$，故 $\bar{f}$ 为满同态.

结合上述推论以及第一同构定理，可知任何群 G 同构于商群 $F/N = F/\operatorname{Ker} \bar{f}$，记号同上，也就是说只要确定集合 X、自由群 F、同态及其核，就能确定群 G 的结构，这种思想称为**群的表现**.

定义 1.32 (群的表现)

若 $G \cong F(X)/N$，则记 G 的表现为

$$\langle X | r = e, r \in N \rangle, \tag{1.46}$$

其中 X 的元素称为 G 的生成元，N 的元素构成生成元的生成关系.

定理 1.25 (Van Dyck)

设 X 为集合，Y 为 X 中一些既约字的集合，$G = \langle X | w = e, \forall w \in Y \rangle$，若群 $H = \langle X \rangle$ 且满足关系 $w = e, \forall w \in Y$，则存在 G 到 H 的满同态.

证明 设 $F = F(X)$，由于存在嵌入映射 $X \hookrightarrow H$，则根据泛性质可诱导出（满）同态 $\varphi: F \to H$，而 $Y \subset \operatorname{Ker} \varphi$，设 N 为由 Y 生成的正规子群，则存在满同态 $f: F/N \to H$，$f(gN) = \varphi(g)$，而 $G \cong F/N$，得证.

定义 1.33 (自由积)

第 2 章 群的结构

本章继续讨论群的结构.

2.1 自由 Abel 群

对于 Abel 群，运算常用 $+$ 表示，逆常用 $-a$ 表示，单位元常用 0 表示.

定义 2.1 (基)

对于 Abel 群 F，若存在集合 X 使得 $F=\langle X\rangle$，且对任意 $x_1,\cdots,x_k\in X$，$n_i\in\mathbb{Z}$，若 $\sum_{i=1}^k n_ik_i=0$ 必有 $n_i=0$，则称 X 中的元素为 F 的一组基. ♣

注

1. 这种形式与向量空间非常相似，这实际上是一个 $\mathbb{Z}$-**模**，并且易知任何 Abel 群都对应了一个 $\mathbb{Z}$-模.
2. 基的定义实际上说明，任何 $x_k\in X$ 的阶都是 0，即 $\langle x_k\rangle$ 为无限循环群（否则存在 $n\neq 0$ 使得 $nx_k=0$）.

命题 2.1

对于 Abel 群 F，如下陈述等价

1. F 有一组非空基.
2. F 为一族无限循环子群的 (内) 直和.
3. F 同构于一族整数加群的直和.
4. F 为 Abel 群范畴的一个自由对象，即自由 Abel 群.

♠

证明 $1\Rightarrow 2$: 设 F 基为 X，考虑一族群 $\{\langle x_i\rangle:x_i\in X\}$，则任何 $z\in F$ 都能表示为有限个基的线性组合，即 $F=\bigoplus_{x\in X}\langle x\rangle$（反过来的包含性是显然的）.

$2\Rightarrow 3$: 根据无限循环群与整数加群的同构可得.

$3\Rightarrow 1$: 设 $F\cong\sum\mathbb{Z}$，指标集为 X，则对任意 $x\in X$，令 $\theta_x=\{u_i\}\in\sum\mathbb{Z}$，其中 $u_x=1,u_i=0(i\neq x)$，则 $\{\theta_x:x\in X\}$ 为 $\sum\mathbb{Z}$ 的一组基.

$1\Rightarrow 4$: 设 X 为 F 的一组基，则 F 为 X 上的自由群，存在嵌入映射 $\iota:X\to F$，且对任意群 G，同态 $f:X\to G$，可以构造出同态 $\bar{f}:F\to G$（与定理1.24类似），得证.

$4\Rightarrow 3$: 设 F 为 X 上的自由群，则根据 X 的指标构造同等数量的 $\mathbb{Z}$ 的直和，再构造 $Y=\{\theta_x:x\in X\}$ 为 $\sum\mathbb{Z}$ 的一组基，由定理1.24，可以构造对于函数 $f:X\to\sum\mathbb{Z},f(x)=\theta_x$，存在唯一同态 $\bar{f}:F\to\sum\mathbb{Z}$，且 $f=\bar{f}\circ\tau$（τ 为嵌入映射），且 $F/\operatorname{Ker}\bar{f}\cong\sum\mathbb{Z}$，由基的性质可知，若 $\bar{f}(g)=0$，则必有 $g=e$，因此 $\operatorname{Ker}\bar{f}=\{e\}$，得证.

上述证明也给出了一个构造 X 上自由 Abel 群的方法.

定理 2.1

自由 Abel 群 F 的任何两个基都是等势的，由此可定义 F 的秩为其基的势. ♡

证明 设 F 基为 X，$|X|=n<\infty$，则若 $F\cong\mathbb{Z}^n$，$2F\cong(2\mathbb{Z})^n$，因此有 $F/2F\cong(\mathbb{Z}/2\mathbb{Z})^n$，说明 $|F/2F|=2^n$，若 Y 为另一组基且 $|Y|=m$，则 $|F/2F|=2^m$，因此 $m=n$，得证.

若 F 有一组基 X 无限，则根据上述讨论可知其所有基都无限，下面证明 $|X|=|F|$，易知 $|X|\leqslant|F|$，根据 Schroeder-Bernstein 定理只需证明 $|F|\leqslant|X|$. 令 $S=\bigcup_{n\in\mathbb{N}}X^n$，则对任意 $s=(x_1,\cdots,x_n)\in S$，令

$G_s=\langle x_1,\cdots,x_n\rangle$，则 $G_s\cong\bigoplus_{k\leqslant t}\mathbb{Z}y_k$，因此 $|G_s|=|\mathbb{Z}^t|=|Z|=\aleph_0$，而 $F=\bigcup_{s\in S}G_s$，因此

$$|F|=\left|\bigcup_{s\in S}G_s\right|\leqslant|S||G_s|=|S|\aleph_0=|S|=|X|, \tag{2.1}$$

得证.

推论 2.1

设 F_1,F_2 为自由 Abel 群，则 $F_1\cong F_2$ 当且仅当 $\mathrm{rk}F_1=\mathrm{rk}F_2$.

定理 2.2

设自由 Abel 群 F 有一组基 $X=\{x_1,\cdots,x_n\}$，$G\leqslant F$ 非空，则存在 $r\in\mathbb{N}$，$d_1|d_2|\cdots|d_r\in\mathbb{N}$ 使得 G 为以 $\{d_1x_1,\cdots,d_rx_r\}$ 为基的自由群.

证明 $n=1$ 显然成立，设命题对所有小于 n 的自由 Abel 群成立，考虑 n 的情形. 令

$$S=\{s\in\mathbb{Z}:\text{存在基}\{y_1,\cdots,y_n\}\text{使得}G\text{中存在形如}sy_1+k_2y_2+\cdots+k_ny_n\text{的元素}\}, \tag{2.2}$$

由于 $G\neq\emptyset$，故 $S\neq\emptyset$；根据对称性可知此时 $k_2,\cdots,k_n\in S$；因此 S 存在最小正元素 d_1，使得存在一组基 $\{y_1,\cdots,y_n\}$ 使得

$$v=d_1y_1+k_2y_2+\cdots+k_ny_n\in G \tag{2.3}$$

$$=d_1(y_1+q_2y_2+\cdots+q_ny_n)+r_2y_2+\cdots+r_ny_n \tag{2.4}$$

$$=d_1x_1+r_2y_2+\cdots+r_ny_n \tag{2.5}$$

其中 $k_i=q_id_1+r_i,0\leqslant r_i<d_1$，且 $W=\{x_1,y_2,\cdots,y_n\}$ 为 F 的一组基，因此 d_1 的最小性使得 $r_2=\cdots=r_n=0$，也即 $v=d_1x_1\in G$.

令 $H=\langle y_2,\cdots,y_n\rangle$，则 H 为秩 $n-1$ 的自由 Abel 群且 $F=\langle x_1\rangle\oplus H$，进一步我们断言

$$G=\langle v\rangle\oplus(G\cap H)=\langle d_1x_1\rangle\oplus(G\cap H), \tag{2.6}$$

基的性质保证了 $\langle v\rangle\cap(G\cap H)=0$，设 $u=t_1x_1+t_2y_2+\cdots+t_ny_n\in G$，则 d_1 的最小性保证了 $d_1|t_1$，而 $t_2y_2+\cdots+t_ny_n\in G\cap H$，因此 $G=\langle v\rangle+(G\cap H)$.

下面不妨设 $G\cap H\neq0$，因此则根据归纳假设存在 H 的一组基 $\{x_2,\cdots,x_n\}$，以及 $d_2|\cdots|d_n$ 使得 $G\cap H$ 基为 $\{d_2x_2,\cdots,d_nx_n\}$，因此最后只需证明 $d_1|d_2$，而这根据 d_1 的最小性是显然的.

推论 2.2

设 G 为有限生成 Abel 群，则任何子群 $H\leqslant G$ 都能由 $m\leqslant n=\mathrm{rk}G$ 个元素生成.

注 该结论对非 Abel 群不一定成立.

2.2 有限生成 Abel 群

本节将证明刻画有限生成 Abel 群结构的定理，特别地包含一个唯一性定理，它说明两个有限生成 Abel 群具有某种相同的属性当且仅当其同构. 由于 Abel 群可以看作一个 $\mathbb{Z}$-模，因此本节的许多结构在后面章节中主理想整环 (PID) 上的模中会有推广形式.

定理 2.3

任何有限生成 Abel 群 G 满足 $G\cong\sum_{k=1}^n\mathbb{Z}_{m_k}$，其中 $1<m_1|m_2|\cdots|m_n$（这里认为 $\mathbb{Z}$ 阶为 ∞）.

证明 设 G 由 n 个元素生成，则存在秩为 n 的自由群 F 以及满同态 $\pi:F\to G$，若 π 恰好为同构，则 $G\cong F\cong\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}(n\text{ 项})$；若不然，则子群 $K=\mathrm{Ker}\,\pi$ 存在一组基 $\{d_1x_1,\cdots,d_rx_r\}$ 满足 $d_1|\cdots|d_r$，因此 $K=\sum_{i=1}^r\langle d_ix_i\rangle$，

令 $d_{r+1}=\cdots=d_n=0$，则根据推论1.5可得

$$G\cong F/K=\sum_{i=1}^{n}\langle x_i\rangle\Big/\sum_{i=1}^{n}\langle d_ix_i\rangle\cong\sum_{i=1}^{n}\langle x_i\rangle/\langle d_ix_i\rangle\cong\sum_{i=1}^{n}\mathbb{Z}_{d_i}\tag{2.7}$$

特别地，若 $d_i=1$，则 $\mathbb{Z}/\mathbb{Z}\cong\{0\}$；若 $d_i=0$，则 $\mathbb{Z}/\{0\}\cong\mathbb{Z}$，故上述结果也可写成

$$G\cong\mathbb{Z}_{m_1}\oplus\cdots\oplus\mathbb{Z}_{m_t}\oplus(\mathbb{Z}\oplus\cdots\oplus\mathbb{Z}),\tag{2.8}$$

其中 $m_1|\cdots|m_t$，并且 $\mathbb{Z}$ 共有 $s=n-r$ 个.

上面的定理给出了有限生成 Abel 群的分解定理，如果考虑如下引理，还可以进行更细致的分解.

引理 2.1

设 $m=p_1^{n_1}\cdots p_t^{n_t}\in\mathbb{N}$，则

$$\mathbb{Z}_m\cong\sum_{i=1}^{t}\mathbb{Z}_{p_i^{n_i}}=\mathbb{Z}_{p_1^{n_1}}\oplus\cdots\oplus\mathbb{Z}_{p_t^{n_t}},\tag{2.9}$$

♡

事实上，只需证明若 $(r,n)=1$，则 $\mathbb{Z}_{rn}\cong\mathbb{Z}_r\oplus\mathbb{Z}_n$.

证明 由于 $n\in\mathbb{Z}_{rn}$ 阶为 r，$r\in\mathbb{Z}_{rn}$ 阶为 n，因此 $\langle n\rangle\cong\mathbb{Z}_r,\langle r\rangle\cong\mathbb{Z}_n$，考虑如下两个单同态

$$\psi_r:\mathbb{Z}_r\to\mathbb{Z}_{rn},\quad\psi_r(k)=nk,\tag{2.10}$$

$$\psi_n:\mathbb{Z}_r\to\mathbb{Z}_{rn},\quad\psi_n(k)=rk,\tag{2.11}$$

由此构造映射 $\psi:\mathbb{Z}_r\oplus\mathbb{Z}_n\to\mathbb{Z}_{rn}$，$\psi(x,y)=\psi_r(x)+\psi_n(y)=nx+ry$（良定性易得），进一步可得 $\operatorname{Ker}\psi=\{(0,0)\}$，并且由 Bezout 定理可知 $1\in\operatorname{Im}\psi$，因此 ψ 为群同构（单满同态），得证.

注 进一步也可证明 $(r,n)=1$ 当且仅当 $\mathbb{Z}_{rn}\cong\mathbb{Z}_r\oplus\mathbb{Z}_n$，只需考虑两个群中元素最大阶即可.

综合上述结果，可以给出如下定理.

定理 2.4

任何有限生成 Abel 群同构于有限个循环群的直和，这些循环群或为无限，或为素数幂阶.

♡

由于有限 Abel 群必为有限生成的，因此将有限 Abel 群分解再重组，可以得到如下推论.

推论 2.3

设 G 为阶为 n 的有限 Abel 群，则对任意 $m|n$，G 有一个 m 阶子群.

♡

证明 证明要用到下面引理的结论，即 $\mathbb{Z}_{p^{n-m}}\cong p^m\mathbb{Z}_{p^n}\leqslant\mathbb{Z}_{p^n}$.

接下来证明进一步的结论，即上面循环分解的顺序实际上可以由群 G 本身确定，首先考虑一些琐碎的引理.

引理 2.2

设 G 为 Abel 群，m,p 分别为一个整数和素数，则下述均为 G 的子群：

1. $mG=\{mu:u\in G\}$.
2. 阶整除 m 的元素：$G[m]=\{u\in G:mu=0\}$.
3. 阶等于 p^n 的元素：$G(p)=\{u\in G:|u|=p^n\}$.
4. 有限阶元素：$G_t=\{u\in G:|u|<\infty\}$.

特别地，存在同构 $\mathbb{Z}_{p^n}[p]\cong\mathbb{Z}_p$，$p^m\mathbb{Z}_{p^n}\cong\mathbb{Z}_{p^{n-m}}$，设 $H,G_i(i\in I)$ 为 Abel 群，则

1. 若 $g:G\to\sum_{i\in I}G_i$ 为同构，则存在限制在 $mG,G[m]$ 上的同构 $mG\cong\sum_{i\in I}mG_i$，$G[m]\cong\sum_{i\in I}G_i[m]$.
2. 若 $f:G\to H$ 为同构，则存在限制在 $G_t,G(p)$ 上的同构 $G_t\cong H_t$，$G(p)\cong H(p)$.

♡

注 其中 G_t 称为群 G 的**扭子群**，若 $G=G_t$ 则称 G 为扭群，若 $G_t=0$ 则称 G “无扭”(torsion-free).

前面几个子群是显然的（容易验证），由于

$$\mathbb{Z}_{p^n}[p] = \{p^{n-1}, 2p^{n-1}, \cdots, (p-1)p^{n-1}\} \tag{2.12}$$

$$p\mathbb{Z}_{p^n} = \{px : x \in \mathbb{Z}_{p^{n-1}}\} \tag{2.13}$$

因此同构也容易得到，最后两个也可以直接构造得到.

定理 2.5

设 G 为有限生成 Abel 群，则

1. G 的循环分解中自由 Abel 群的秩唯一.
2. 若 G 不为自由 Abel 群，则存在唯一整数列 $1 < m_1 | \cdots | m_t$ 使得

$$G \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_t} \oplus F, \tag{2.14}$$

   其中 F 为自由 Abel 群.
3. 若 G 不为自由 Abel 群，则存在素幂 $p_1^{s_1}, \cdots, p_k^{s_k}$ 使得

$$G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{s_k}} \oplus F, \tag{2.15}$$

   其中 F 为自由 Abel 群，这些素幂不考虑次序下是唯一的.

♡

证明

1. G 的任何分解都给出了同构 $G \cong H \oplus F$，其中 H 为有限循环群的直和，F 为秩 $s < \infty$ 的自由 Abel 群. 设 $\tau : H \to H \oplus F$ 为嵌入映射 $\tau(h) = (h, 0)$，则易知 $\tau(H)(\cong H)$ 为 $H \oplus F$ 的扭子群，即在同构 $G \cong H \oplus F$ 下有 $G_t \cong \tau(H)$（根据引理），因此

$$G/G_t \cong (F \oplus H)/\tau(H) \cong F, \tag{2.16}$$

   即 G/G_t 为自由 Abel 群，且该群的秩仅与 G 有关，因此 F 的秩是唯一的.
2. 可以由 3 直接构造.
3. 假设

$$G \cong \sum_{i=1}^{r} \mathbb{Z}_{n_i} \oplus F \cong \sum_{j=1}^{r} \mathbb{Z}_{k_j} \oplus F, \tag{2.17}$$

   其中 n_i, k_j 都是素幂，F 为自由 Abel 群，由第一问易知

$$\sum_{i=1}^{r} \mathbb{Z}_{n_i} \cong G_t \cong \sum_{j=1}^{r} \mathbb{Z}_{k_j}, \tag{2.18}$$

   则根据引理，对任意素数 p 有 $(\sum \mathbb{Z}_{n_i})(p) \cong (\sum \mathbb{Z}_{k_j})(p)$，因此只需说明，对每个固定的素数 p，这种分解中的幂（不考虑次序）是唯一的，即不妨设 $G = G_t$，且

$$G \cong \sum_{i=1}^{r} \mathbb{Z}_{p^{a_i}} \cong \sum_{j=1}^{d} \mathbb{Z}_{p^{c_j}}, \quad 1 \leqslant a_1 \leqslant \cdots \leqslant a_r; 1 \leqslant c_1 \leqslant \cdots \leqslant c_d, \tag{2.19}$$

   根据引理 $G[p] \cong (\mathbb{Z}_p)^r \cong (\mathbb{Z}_p)^d$，说明 $r = d$，设 v 是最小的使得 $a_v \neq c_v$ 的整数，不妨设 $a_v < c_v$，再次根据引理有

$$p^{a_v}G \cong \sum_{i=1}^{r} p^{a_v}\mathbb{Z}_{p^{a_i}} \cong \sum_{i=v+1}^{r} \mathbb{Z}_{p^{a_i - a_v}} \cong \sum_{i=v}^{r} \mathbb{Z}_{p^{c_i - a_v}}, \tag{2.20}$$

   由此得到了 $p^{a_v}G$ 的两个分解，但其中循环群的数量不同，则根据前文的讨论可知矛盾，故得证.

对于有限生成 Abel 群 G，上面的 $m_1, \cdots, m_t$ 称为 G 的**不变因子**，上面的素幂称为 G 的**初等因子（组）**，易知初等因子组实际上是每个不变因子的初等因子.

2.3 群在集合上的作用

研究群的一种极为重要的方法就是群的表示，其动机在于建立群到常见群之间的同态，由此通过熟悉的结构理解未知群的结构. 这里的“常见群”大多考虑两种：置换群、矩阵群，它们分别对应了两种理论：**群作用**（置换表示）、**群表示**（线性表示），本节将讨论群作用，并由此给出 Sylow 定理的证明.

定义 2.2 (群作用/置换表示)

设群 G，集合 Σ，$S(\Sigma)$ 为 Σ 上的对称群，则称同态 $\tau: G \to S(\Sigma)$ 为 G 在集合 Σ 上的一个置换表示（或群作用）.

♣

上述定义看似抽象，但将其剥开后会发现一些自然之处：$S(\Sigma)$ 实际上同构于 Σ 上所有双射的集合，因此对任意 $g \in G$，$\tau(g) = \tau_g$ 实际上是 Σ 上的双射，因此减少一些记号，可以将群作用表示为映射 $G \times \Sigma \to S$，$g \cdot s \mapsto s$，且该映射须满足[1]

$$e \cdot s = s, \quad g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s \tag{2.21}$$

在无歧义的情况下，上面的 $\cdot$ 有时会省略.

例 2.1 对称群 S_n 中元素的表示实际上就是在集合 $\{1, 2, \cdots, n\}$ 上的作用.

例 2.2 如果考虑群 G 到自身的作用，则根据定义，可以立即给出两种自然的作用：

1. 左乘作用：$\tau_g(s) = gs$.
2. 共轭作用：$\tau_g(s) = gsg^{-1}$.

例 2.3 类似地，设 $H \leqslant G$，也可以考虑群 G 在陪集 $\Sigma = \{aH : a \in G\}$ 上的左乘作用：$\tau_g(aH) = (ga)H$，但此时共轭作用不那么自然，留与后文讨论.

根据上面的讨论，足以得到一个重要的定理.

定理 2.6 (Caylay)

任何群 G 都同构于一个置换群（对称群的子群）.

♡

证明 令 G 左乘作用于 G 上，则

$$\tau_g = \tau_h \iff gs = hs, \forall s \in G \iff g = h, \tag{2.22}$$

因此 $\tau: G \to S(G)$ 为单同态，根据同态基本定理可得 $G \cong \operatorname{Im}\tau \leqslant S(G)$，得证.

下面讨论借助群作用给出的两个重要对象：轨道与稳定子（不变子群），以及一个计数定理.

¶ 轨道与稳定子

如果将集合 Σ 中的元素看作空间中的散点，集合 G 的作用看作使每个点运动到另一个位置，那么轨道的概念也很容易理解：一个点能运动到的点的集合可称轨道，每一点都在轨道中运动.

定义 2.3 (轨道)

设群 G 作用于集合 Σ 上，则记任意 $x \in \Sigma$ 的轨道为

$$O_x = \{g \cdot x \in \Sigma : g \in G\}. \tag{2.23}$$

♣

注 根据前文的引入，不难验证轨道诱导出了集合 Σ 中的一个一个等价关系：

$$x \sim y \iff \exists g \in G : g \cdot x = y \iff O_x = O_y, \tag{2.24}$$

轨道描述了集合 Σ 中某一元素在作用下的“运动”，对应地可以考虑保持某一元素“不变”的作用，从而给出稳定子的概念.

[1] 事实上，这里 $g_1 \cdot (g_2 \cdot s) = (g_1 g_2) \cdot s$ 并不是必须的，如果将其改为 $g_1 \cdot (g_2 \cdot s) = (g_2 g_1) \cdot s$ 同样也满足定义，二者是对称的.

定义 2.4 (稳定子/不变子群/固定子群)

设群 G 作用于集合 Σ 上，则记任意 $x \in \Sigma$ 的不变子群为

$$G_x = \{g \in G : g \cdot x = x\}. \tag{2.25}$$

♣

注 根据群作用的定义，不难验证 $G_x \leqslant G$.

关于轨道的计数定理来自这样的观察：对任意 $x \in \Sigma$，其稳定子越小，轨道则越大，反之亦然. 特别地，若 $G_x = \{e\}$ 则任何 $g \in G$ 都对应了 O_x 中的元素 $g \cdot x$，此时 $|G| = |O_x|$；若 $O_x = \{x\}$，则任何 $g \in G_x$ 都保持 x 不变，因此 $G = G_x$. 这里已经有了一些苗头，借助一些简单的记号，可以进一步考虑轨道与稳定子间的关系：

$$O_x = Gx, \quad G_x x = x \Longrightarrow gG_x x = g \cdot x \tag{2.26}$$

这里实际上给出了 G_x 的左陪集与 O_x 之间的对应，也就是如下定理：

定理 2.7 (轨道定理)

设群 G 作用于集合 Σ 上，则对任意 $x \in \Sigma$ 有

$$|G| = |G_x| \cdot |O_x|. \tag{2.27}$$

♡

证明 只需证明 $[G : G_x] = |O_x|$，也即构造出 $\{gG_x : g \in G\}$ 与 $O_x = \{g \cdot x : g \in G\}$ 之间的双射，令

$$f : \{gG_x : g \in G\} \longrightarrow \{g \cdot x : g \in G\} \tag{2.28}$$

$$gG_x \longmapsto g \cdot x \tag{2.29}$$

由于

$$gG_x = hG_x \Longleftrightarrow g^{-1}h \in G_x \Longleftrightarrow (g^{-1}h) \cdot x = x \Longleftrightarrow g \cdot x = h \cdot x. \tag{2.30}$$

因此 f 为双射.

除了计数定理，轨道与稳定子还有一些有趣的结论，整理如下（都是易证的）：

命题 2.2

设群 G 作用在 Σ 上，τ 为对应的同态，则

1. 对任意 $x \in \Sigma$，有

$$G_{g\cdot x} = gG_x g^{-1}, \tag{2.31}$$

即同轨道元素的稳定子彼此共轭.

2. $G_x \triangleleft G$ 当且仅当 G_x 中元素保持 O_x 中每个元素不变.
3. $\operatorname{Ker}\tau = \{g \in G : g = \mathrm{Id}_\Sigma \Leftrightarrow g \cdot x = x, \forall x \in \Sigma\} = \bigcap_{x\in\Sigma} G_x$.
4.

♠

接下来讨论**中心化子**和**正规化子**的概念，但看二者定义会感到复杂，但从群作用的角度看，它们有自然之处.

设群 $H \leqslant G$ 共轭作用于 G 自身，即 $\tau_h(x) = hxh^{-1}$，则此时

$$H_x = \{h \in G : hxh^{-1} = x\} = \{h \in G : hx = xh\}, \tag{2.32}$$

这就是（x 关于 H 的）中心化子.

定义 2.5 (中心化子)

设子群 $H \leqslant G$，则对任意 $x \in G$，定义

$$C_H(x) = \{h \in H : hxh^{-1} = x\} = \{h \in H : hx = xh\} \tag{2.33}$$

为 x 关于 H 的中心化子（群），当 $H = G$ 是简称 x 的中心化子.

♣

注

1. 应用前面的结论可知 $C_H(h\cdot x)=C_H(hxh^{-1})=hC_H(x)h^{-1}$.
2. 对于集合 $A\subset G$，可以推广中心化子的概念：$C_H(A)=\{h\in H:hxh^{-1}=x,\forall x\in A\}$，此时容易验证有

$$C_H(A)=\bigcap_{x\in A}C_H(x). \tag{2.34}$$

如果考虑上述作用 τ 的核（并且 $H=G$），利用前面的结论可以得到

$$\operatorname{Ker}\tau=\{g\in G:gxg^{-1}=x,\forall x\in G\}=\bigcap_{x\in G}G_x=\bigcap_{x\in G}C_G(x) \tag{2.35}$$

这就是群的中心.

定义 2.6 (群的中心)

设群 G，定义其中心

$$C(G)=\{g\in G:ga=ag,\forall a\in G\}=C_G(G), \tag{2.36}$$

也即与所有 $a\in G$ 可交换的元素的集合.

注 特别地，当且仅当 $C(G)=G$ 时 G 为 Abel 群；并且易证 $C(G)$ 的交换性使得 $C(G)\triangleleft G$.

注意到 $g\in C(G)$ 当且仅当 $\tau_g=\mathrm{Id}_G$，此时对任意 $x\in G$ 有 $\tau_x(g)=g$，因此 $O_g=\{g\}$，根据共轭类的划分可得

$$|G|=\sum_{x\in G}|O_x|=|C(G)|+\sum_{x\in G,|O_x|>1}|O_x|, \tag{2.37}$$

该等式也被称为类方程，稍作推广，令 $H\leqslant G$ 共轭作用到 G 上可得

$$|G|=\sum_{x\in G}|O_x|=|C_H(G)|+\sum_{x\in G,|O_x|>1}|O_x|, \tag{2.38}$$

上面的式子有一些迷惑性，因为 $C_H(G)$ 实际上同时是两种集合：$\operatorname{Ker}\tau$ 以及 G 中轨道大小为 1 的元素集合，而上述方程实际上对后者成立，对前者不成立. 考虑一般情况，若 G 作用于 Σ 上，令

$$\Sigma_0=\{x\in\Sigma:h\cdot x=x,\forall h\in H\}=\{x\in\Sigma:|O_x|=1\}\subset\Sigma, \tag{2.39}$$

则同样考虑可得

$$|\Sigma|=\sum_{x\in\Sigma}|O_x|=|\Sigma_0|+\sum_{x'\in\Sigma,|O_{x'}|>1}|O_{x'}|. \tag{2.40}$$

2.4 Sylow 定理

¶ 准备工作

Sylow 定理的动机来自一个非常自然的问题（可以看作 Lagrange 定理的逆）：若 $n\big||G|$，G 中是否存在 n 阶子群？整数可以唯一分解为素数的幂，根据这种思路可以首先考虑素数（幂）阶群，首先定义 p-群.

定义 2.7 (p-群)

设群 G 的阶为 p^n，p 为素数，则称 G 为 p-群；若 $H\leqslant G$ 为 p-群，则称 H 为 G 的 p-子群.

延续上一部分，可以给出一个重要的同余引理，它的使用将贯穿 Sylow 定理的证明.

引理 2.3

设 p-群 H 作用在 Σ 上，记 $\Sigma_0=\{x\in\Sigma:h\cdot x=x,\forall h\in H\}$，则 $|\Sigma|\equiv|\Sigma_0|(\mathrm{mod}\,p)$.

注

1. 这种同余关系对一般群 G 的某些情况也成立，只是考虑 p-群更有代表性.
2. 容易看出（根据包含关系或利用轨道定理），若 $x \in \Sigma_0$，则 $H = H_x$.

证明 对任意 $x \in \Sigma$，若 $|O_x| > 1$，则 $|O_x| = [H : H_x] \big| H$ 说明 $p \big| |O_x|$，因此

$$|\Sigma| = |\Sigma_0| + \sum_{x' \in \Sigma, |O_{x'}|>1} |O_{x'}| \equiv |\Sigma_0| (\mathrm{mod}\, p). \tag{2.41}$$

下面的推论给出了使用同余引理的一个例子.

推论 2.4

非平凡 p-群的中心 $C(G)$ 包含多于一个元素.

♡

证明 显然 $|C(G)| \geqslant 1$，令 G 共轭作用于自身，则根据同余引理有

$$|C(G)| \equiv |G| \equiv 0 (\mathrm{mod}\, p), \tag{2.42}$$

这说明 $|C(G)| > 1$.

最后的准备工作是考虑群在陪集上的作用，并且重复前面的诸多讨论，这以例子的方式呈现.

例 2.4 设 $H \leqslant G$，则可以考虑 G 在集合 $S = \{gH : g \in G\}$ 上的自然左乘作用 τ，即

$$\tau_g(aH) = (ga)H, \tag{2.43}$$

容易计算

$$G_{aH} = aHa^{-1}, \quad \mathrm{Ker}\, \tau = \bigcap_{a \in G} aHa^{-1}, \tag{2.44}$$

考虑 S_0，由于

$$aH \in S_0 \Longleftrightarrow g \in G_{aH}, \forall g \in G \Longleftrightarrow G = G_{aH} = aHa^{-1}, \tag{2.45}$$

但是 $H \leqslant G$，$|aHa^{-1}| = |H|$，因此 $S_0 = \emptyset$.

例 2.5 设 $H \leqslant G$，也可以考虑 H 在集合 $S = \{gH : g \in G\}$ 上的自然左乘作用 τ，即

$$\tau_h(aH) = (ha)H, \tag{2.46}$$

下面的计算也是类似的

$$H_{aH} = (aHa^{-1}) \cap H, \quad \mathrm{Ker}\, \tau = \bigcap_{a \in G} aHa^{-1}, \tag{2.47}$$

继续考虑 S_0，此时

$$aH \in S_0 \Longleftrightarrow h \in G_{aH}, \forall h \in H \Longleftrightarrow H = H_{aH} = aHa^{-1} \cap H \Longleftrightarrow a \in N_G(H) \tag{2.48}$$

[2] 这里就自然引出了正规化子的概念

定义 2.8 (正规化子)

设子群 $H \leqslant G$，则对任意 $K \leqslant G$，定义

$$N_H(K) = \{h \in H : hKh^{-1} = K\} = \{h \in H : hK = Kh\} \tag{2.49}$$

为 K 关于 H 的正规化子.

♣

注 易得当 $H = G$ 时，$K \triangleleft N_G(K)$.

关于正规化子还有许多要谈，暂且继续主题.

这时 S_0 不再平凡，并且有 $|S_0| = [N_G(H) : H] = |N_G(H)/H|$，由此自然得到如下推论.

推论 2.5

设 H 为 G 的 p-子群，则 $[N_G(H) : H] \equiv [G : H] (\mathrm{mod}\, p)$.

♡

[2] 这里由 $H \subset aHa^{-1}$ 可推出 $H = aHa^{-1}$ 是因为二者大小相等.

证明 由于 $|S|=\#\{gH:g\in G\}=[G:H]$，$|S_0|=[N_G(H):H]$，根据同余引理得证.

推论 2.6

设 H 为 G 的 p-子群且 $p\big|[G:H]$，则 $N_G(H)\neq H$.

证明 此时 $0\equiv[G:H]\equiv[N_G(H):H](\mathrm{mod}\,p)$，而 $[N_G(H):H]\geqslant 1$ 说明 $[N_G(H):H]>1$，得证.

¶Sylow 三定理

首先证明 Cauchy 的结果，这一定理的证明中构造了一个非常精巧的群作用.

定理 2.8 (Cauchy)

设 G 为有限群，素数 $p||G|$，则 G 有 p 阶群（或者说 G 中有 p 阶元）.

证明 设 $|G|=n$，构造 p 元组集合

$$S=\{(a_1,\cdots,a_p):a_i\in G,a_1\cdots a_p=e\},\tag{2.50}$$

根据定义可知 a_p 由前 $p-1$ 个元素决定，因此 $|S|=n^{p-1}\equiv 0(\mathrm{mod}\,p)$. 令 $\mathbb{Z}_p$ 以轮换作用于 S 上，即

$$k\cdot(a_1,\cdots,a_p)=(a_{k+1},\cdots,a_p,a_1,\cdots,a_k)\in S,\tag{2.51}$$

容易验证这确实是一个群作用 $(0x=x,(k_1+k_2)x=k_1(k_2x))$，而 $(a_1,\cdots,a_p)\in S_0$ 当且仅当对任意 k 都有

$$k(a_1,\cdots,a_p)=(a_1,\cdots,a_p),\tag{2.52}$$

这说明 $a_1=\cdots=a_p=a$，根据 S 的定义可知 $a^p=1$，并且 $(e,\cdots,e)\in S_0$ 说明 $|S_0|>0$，根据上述引理可知 $|S_0|\equiv|S|(\mathrm{mod}\,p)$，即 S_0 中存在非平凡元素，其对应的 $a\in G$ 恰好为 p 阶元，得证.

从 Cauchy 定理出发进行归纳，可以一气呵成 Sylow 定理.

定理 2.9 (第一 Sylow 定理)

设群 G 满足 $|G|=p^nm,n\geqslant 1,(p,m)=1$，则对任意 $1\leqslant i\leqslant n$，G 中存在 p^i 阶子群.

证明 对 i 归纳，由 Cauchy 定理可知 G 中存在 p 阶子群，设 H 为 G 的 $p^i<p^n$ 阶子群，则 $p\big|[G:H]$，根据上面的引理可知

$$[N_G(H):H]\equiv[G:H]\equiv 0(\mathrm{mod}\,p),\tag{2.53}$$

这说明 $p\big|[N_G(H):H]=|N_G(H)/H|$，根据 Cauchy 定理 $N_G(H)/H$ 包含一个 p 阶子群 H_1/H，计算阶可知 $|H_1|=p^{i+1}$，这里

$$H\lhd H_1\leqslant N_G(H)\leqslant G,\tag{2.54}$$

得证.

上面的证明过程隐含的一个直接的推论.

推论 2.7

设群 G 满足 $|G|=p^nm,n\geqslant 1,(p,m)=1$，则 G 的任何 p^i 阶群都是某个 p^{i+1} 阶群的正规子群 $(0\leqslant i\leqslant n-1)$.

第一 Sylow 定理保证了对 $|G|$ 的任意素因子 p，群 G 中存在一个极大的 p-群，这为 **Sylow p-子群**.

定义 2.9 (Sylow p-子群)

设 G 为有限群，称其极大 p-子群 P 为 Sylow p-子群.

注

1. 根据 Sylow 定理可知 $|P|=p^m$，这里 $(|G|/p^m,p)=1$.
2. 进一步也可知 P 为 G 的 Sylow p-子群当且仅当 $|P|=p^m$.
3. 进一步还可知 Sylow 子群的共轭也是 Sylow 子群.

概括来说，第一定理给出了 p-子群/Sylow p-子群的存在性，第二定理进一步刻画了 p-子群之间的关系，第三定理做了更细致的工作：给出了 p-子群的数量关系. 后面两个定理证明需要的工具仍然是前面的那些讨论.

定理 2.10 (第二 Sylow 定理)

设 H 为 G 的 p-子群，P 为 G 的 Sylow p-子群，则存在 $x\in G$ 使得 $H\leqslant xPx^{-1}$. 特别地，G 的任意两个 Sylow p-子群彼此共轭.

证明 设 $S=\{gP:g\in G\}$，令 H 左乘作用于 S 上，根据 P 的极大性有 $p\nmid[G:P]=|S|$，而根据同余引理有

$$|S_0|\equiv|S|(\mathrm{mod}\,p),\tag{2.55}$$

因此 $|S_0|>0$，这说明存在 $xP\in S_0$，即 $H=H_{xP}=(xPx^{-1})\cap H\leqslant xPx^{-1}$，得证.

特别地，若 H 也为 G 的 Sylow p-子群，则根据阶以及包含关系可得 $H=xPx^{-1}$.

推论 2.8

群 G 的 Sylow p-子群 P 为 G 的正规子群当且仅当 P 为 G 的唯一 Sylow p-子群.

推论 2.9

若 P 为 G 的 Sylow p-子群，则 P 是 $N_G(P)$ 的唯一 Sylow p-子群.

定理 2.11 (第三 Sylow 定理)

设 G 为群，p 为 $|G|$ 的素因子，则 G 的 Sylow p-子群的个数整除 $|G|$，且有形式 $kp+1$（或者说模 p 余 1）。

证明 根据第二定理可知 G 的所有 Sylow p-子群的个数就是某个 Sylow p-子群 P 共轭类的个数，即 $[G:N_G(P)]$，这显然整除 $|G|$. 为了证明进一步的结论，设 P 为 G 的 Sylow p-子群，记 G 的所有 Sylow p-子群的集合为

$$S=\{gPg^{-1}:g\in G\},\quad |S|=[G:N_G(P)],\tag{2.56}$$

令 P 共轭作用于 S 上，则 $P_{gPg^{-1}}=(gN_G(P)g^{-1})\cap P$，这说明 $gPg^{-1}\in S_0$ 当且仅当

$$P=P_{gPg^{-1}}=gN_G(P)g^{-1}\cap P,\quad P\leqslant gN_G(P)g^{-1}=N_G(gPg^{-1}),\tag{2.57}$$

由于 $gPg^{-1}\lhd N_G(gPg^{-1})$，因此 $N_G(gPg^{-1})$ 中包含 P,gPg^{-1} 两个 Sylow p-子群，由上一条推论它们相等，因此 $g\in N_G(P),gPg^{-1}=P$，即 $S_0=\{P\}$，根据同余引理有

$$|S|=[G:N_G(P)]\equiv|S_0|\equiv1(\mathrm{mod}\,p),\tag{2.58}$$

得证.

定理 2.12

设 P 为有限群 G 的一个 Sylow p-子群，则 $N_G(N_G(P))=N_G(P)$.

证明 左边包含右边是显然的，只需证明反过来的包含关系. 易得 P 为 $N=N_G(P)$ 的一个 Sylow p-子群，并且是 N 中的唯一 Sylow p-子群（正规性），因此若 $x\in N_G(N)$，则 $xNx^{-1}=N$，而 $P\lhd N$，故

$$xPx^{-1}\subset xNx^{-1}\subset N,\tag{2.59}$$

根据 P 的唯一性可知 $xPx^{-1}=P$，故 $x\in N$，即 $N_G(N)\subset N$，得证.

2.5 有限群的分类

借助 Sylow 定理/自由群等理论，可以对一些有限群进行分类，特别是阶不超过 15 的小阶群.

命题 2.3

设 p,q 为素数，若 $q\nmid p-1$，则 pq 阶群只有 $\mathbb{Z}_{pq}$；若 $q|p-1$，则除此之外还有

$$K=\langle c,d:c^p=d^q=1,dc=c^sd\rangle, \tag{2.60}$$

其中

$$s\not\equiv 1(\mathrm{mod}\,p),\quad s^q\equiv 1(\mathrm{mod}\,p). \tag{2.61}$$

证明 不妨设 $2<q<p$，G 中 p,q 阶群的个数为 n_p,n_q，则

$$n_p|q,n_p\equiv 1(\mathrm{mod}\,p),\quad n_q|p,n_q\equiv 1(\mathrm{mod}\,q) \tag{2.62}$$

故 $n_p=1$，若 $q\nmid p-1$ 则 $n_q=1$，设 a,b 分别为 p,q 阶元，则由于 $\langle a\rangle\cap\langle b\rangle=\{1\}$，二者均正规，因此 $\langle a\rangle,\langle b\rangle$ 中元素可交换，易得 $G\cong\mathbb{Z}_{pq}$.

若 $q|p-1$，则 $n_p=1,n_q=p$，设 c,d 分别为 p,q 阶元，设 $dcd^{-1}=c^s$，则

$$c=d^qcd^{-q}=c^{s^q},\quad s^q\equiv 1(\mathrm{mod}\,p), \tag{2.63}$$

若加上 G 非交换的条件，则有 $s\not\equiv 1(\mathrm{mod}\,p)$，取 $\mathbb{Z}_p^*$ 的原根 g，可知

$$s=g^{\frac{p-1}{q}m},\quad m=1,2,\cdots,q-1, \tag{2.64}$$

但对于不同的 s，得到的群是同构的，因为 $\langle c\rangle=\langle c^k\rangle,(k,p)=1$，因此选择合适的 k 可以做到同构.

命题 2.4

设 p 为奇素数，则任何 $2p$ 阶群 G 必然同构于 $\mathbb{Z}_{2p}$ 或 D_p.

证明 不妨设 G 为非 Abel 群，则由 Sylow 定理可知 G 中仅有一个 Sylow p-子群 $\langle a\rangle\triangleleft G$，且 $|G/\langle a\rangle|=2$，因此设 $b\notin\langle a\rangle$，则 $bab^{-1}=a^k$，由于

$$a=b^2ab^{-2}=b(bab^{-1})b^{-1}=ba^kb^{-1}=a^{k^2}, \tag{2.65}$$

故 $p\big|k^2-1=(k+1)(k-1)$，因此必有 $k=1$ 或 $k=p-1$，而前者表示 G 可交换，故 $k=p-1$，$bab^{-1}=a^{-1}$，即 $G\cong D_p$.

命题 2.5

只有两个 8 阶非 Abel 群：四元数群 Q_8 和 D_4.

证明 设 G 为 8 阶非 Abel 群，则 G 中无 8 阶元但有 4 阶元 a（否则元素阶均为 2，易得矛盾），类似对 $2p$ 阶群的讨论可知 $|G/\langle a\rangle|=2$，$b\notin\langle a\rangle$ 满足 $bab^{-1}=a^k$（否则若设 $bab^{-1}=ba^k$，则 $b\in\langle a\rangle$ 矛盾）.

1. 若 $\mathrm{ord}\,b=2$，则仿照 $2p$ 阶群的讨论可知 $G=D_4$（已假设 G 非 Abel）.
2. 若 $\mathrm{ord}\,b=4$，则重复相同的过程可知 $k=3$，即 $bab^{-1}=a^{-1}$，此时 $b^{-1}a^2b^{-1}=abab^{-1}=aa^{-1}=1$，因此 $a^2=b^2$，故 $G=Q_8$.

注 最后的相等可以根据生成群的定义验证：即任何包含 a,b 的群都包含 XXX

命题 2.6

只有三个 12 阶非 Abel 群：D_6,A_4 和

$$T=\langle a,b:|a|=6,b^2=a^3,ba=a^{-1}b\rangle. \tag{2.66}$$

证明 取 G 的一个 Sylow 3-子群 $P=\langle c\rangle$，令 G 左乘作用于 $S=\{gP:g\in G\}$，则有诱导同态 $\tau:G\to S_4$. 由于

$\operatorname{Ker}\tau=\bigcap_{g\in G}gPg^{-1}\leqslant P$，因此 $\operatorname{Ker}\tau=\{1\}$ 或 P.

1. 若 $\operatorname{Ker}\tau=\{1\}$，则 G 为单同态，$G\cong\operatorname{Im}G\leqslant S_4$，而 S_4 的 12 阶子群只有 A_4，故 $G\cong A_4$.
2. 若 $\operatorname{Ker}\tau=P$，则 P 是 G 的唯一 Sylow 3-子群，$P\triangleleft G$，即 G 中 3 阶元素只有 c,c^2，因此 c 的共轭元的个数为 $[G:C_G(c)]=1$ 或 2，即 $|C_G(c)|=12$ 或 6，故 $C_G(c)$ 中必有 2 阶元素 d，令 $a=cd=dc$，容易验证 $\operatorname{ord}a=6$，因此 G 有 6 阶元.

若 G 有 6 阶元 a，则显然 $\langle a\rangle\triangleleft G$，取 $b\notin\langle a\rangle$，$bab^{-1}=a^k$，此时 $G=\langle a,b\rangle$，则

1. 若 $\operatorname{ord}b=2$，则仿照 $2p$ 阶群的讨论可知 $G=D_6$.
2. 若 $\operatorname{ord}b=3$，则讨论可知只有 $k=1$，G 是 Abel 群，不予考虑.
3. 若 $\operatorname{ord}b=4$，则讨论可知 $k=-1$，即 $bab^{-1}=a^{-1}$，根据阶可得 $b^2=a^3$，即 $G=T$.
4. 若 $\operatorname{ord}b=6$，则讨论可知 $k=-1$，此时 a,b 地位对等，因此 $b^2=a^2$，这将导致

$$a^3=b^2a=a^{-2}b^2=1, \tag{2.67}$$

与 $\operatorname{ord}a=6$ 矛盾.

2.6 幂零群与可解群

考虑如下群（可能具有）的性质：

1. G 是自身 Sylow 子群的直积.
2. 若 $m\big||G|$，则 G 有 m 阶子群.
3. 若 $|G|=mn,(m,n)=1$，则 G 有 m 阶子群.

容易发现 $1\Rightarrow2\Rightarrow3$ 是简单的. 反过来，A_4 满足 3 但不满足 2；S_3 满足 2 但不满足 1，而有限 Abel 群、p-群同时满足 $1,2,3$，本节将讨论满足 1 或 3 的群.

幂零群

设 G 为群，则其中心 $C(G)$ 是 G 的正规子群，记 $C_1(G)=C(G)$，设 $\pi_1:G\to G/C_1(G)$ 为典范映射，再令

$$C_2(G)=\pi_1^{-1}(C(G/C(G)))\leqslant G, \tag{2.68}$$

实际上有 $C_1(G)\triangleleft C_2(G)\triangleleft G$，首先 $1C_1(G)\in C(G/C_1(G))$，$\pi(C_1(G))=1C_1(G)$，故

$$C_1(G)\subset\pi_1^{-1}(C(G))\subset\pi^{-1}(C(G/C_1(G)))=C_2(G), \tag{2.69}$$

因此 $C_1(G)\triangleleft C_2(G)$，并且

$$C_2(G)/C_1(G)=C(G/C_1(G))\triangleleft G/C_1(G), \tag{2.70}$$

因此 $C_2(G)\triangleleft G$（根据定义易证）. 以此类推，令

$$\pi_k:G\to G/C_k(G),\quad C_{k+1}(G)=\pi_k^{-1}(C(G/C_k(G))), \tag{2.71}$$

则可以得到**升中心列**

$$\{1\}\triangleleft C_1(G)\triangleleft C_2(G)\triangleleft\cdots\triangleleft G, \tag{2.72}$$

由此可以定义幂零群

定义 2.10 (幂零群)

群 G 称为幂零的，若存在 n 使得 $C_n(G)=G$.

♣

注 Abel 群都是幂零的，因为 $G=C(G)=C_1(G)$.

命题 2.7

任何有限 p-群都是幂零的.

♠

证明 根据推论??，p-群的中心为非平凡群，因此若 $G \neq C_k(G)$，则

$$C_{k+1}(G)/C_k(G) = C(G/C_k(G)) \tag{2.73}$$

也是非平凡的，即必有 $C_k(G) < C_{k+1}(G)$，自然得证.

定理 2.13

有限个幂零群的直积是幂零的.

证明 根据归纳法，只需证明两个群直积的情形成立即可. 设 $G = H \times K$，H, K 都幂零，只需证明对任意 i 成立

$$C_i(G) = C_i(H \times K) = C_i(H) \times C_i(K). \tag{2.74}$$

根据中心的定义，易证 $i = 1$ 时命题成立，现设 $C_i(G) = C_i(H) \times C_i(K)$，考虑 $i+1$ 的情形，对于同态 $\pi : G \to G/C_i(G)$，可以分解为如下几步：

$$G = H \times K \xrightarrow{\varphi} H/C_i(H) \times K/C_i(K) \xrightarrow{\phi} \frac{H \times K}{C_i(H) \times C_i(K)} = \frac{H \times K}{C_i(H \times K)} = G/C_i(G), \tag{2.75}$$

使得 $\pi = \phi \circ \varphi$，其中 $\varphi = \varphi_H \times \varphi_K$ 为各自的同态，ϕ 为同构，因此根据定义有

$$\begin{aligned} C_{i+1}(G) &= \pi^{-1}(C(G/C_i(G))) && (2.76)\\ &= \varphi^{-1} \circ \phi^{-1}(\frac{H \times K}{C_i(H) \times C_i(K)}) && (2.77)\\ &= \varphi^{-1}(H/C_i(H) \times K/C_i(K)) && (2.78)\\ &= \varphi_H^{-1}(H/C_i(H)) \times \varphi_K^{-1}(K/C_i(K)) && (2.79)\\ &= C_{i+1}(H) \times C_{i+1}(K), && (2.80) \end{aligned}$$

得证.

引理 2.4

若 $H < G$，G 幂零，则 $H < N_G(H)$（真子群）.

证明 只需找到一个元素 $a \in N_G(H), a \notin H$ 即可. 约定 $C_0(G) = \{1\}$，设 n 为满足 $C_n(G) < H$ 的最大者，任取 $a \in C_{n+1}(G), a \notin H$，则 $aC_n(G) \in C_{n+1}(G)/C_n(G) = C(G/C_n(G))$，因此对任意 $h \in H$ 有

$$ahC_n(G) = (aC_n(G))(hC_n(G)) = (hC_n(G))(aC_n(G)) = haC_n(G), \tag{2.81}$$

因此 $a^{-1}ha \in hC_n(G) \subset H$，$a \in N_G(H), a \notin H$，得证.

上面给出幂零群的等价条件.

定理 2.14

有限群 G 幂零当且仅当它是自身 Sylow 子群的直积.

证明 若 G 为自身 Sylow 子群的直积，则显然 G 幂零；反之设 G 幂零且其自身不为 Sylow 子群，$P < G$ 为 Sylow p-子群，则 $P \triangleleft N_G(P)$，但过去证明过 $N_G(N_G(P)) = N_G(P)$，因此再次使用上一条引理可知 $N_G(P) = G$，说明 $P \triangleleft G$，P 也是唯一的 Sylow p-子群，设

$$|G| = p_1^{n_1} \cdots p_k^{n_k}, \tag{2.82}$$

$P_1, \cdots, P_k$ 为对应于 $p_1, \cdots, p_k$ 的 Sylow 子群，注意到若 $x \in P_i \cap P_j$，则 $\operatorname{ord} x | p_i, \operatorname{ord} x | p_j$，只有 $x = 1$，因此 $P_i \cap P_j = \{1\}$，利用相同的思路可知 $P_1 \cdots P_n = P_1 \times \cdots \times P_n$，比较阶数可知

$$G = P_1 \cdots P_n = P_1 \times \cdots \times P_n, \tag{2.83}$$

得证.

可以看出，幂零群的等价条件是有某种分解，这种分解与有限生成 Abel 群有相似之处，因此立得如下推论：

推论 2.10

若 G 为有限幂零群，且 $m\big||G|$，则 G 有 m 阶群. ♡

可解群

下面讨论可解群，首先定义交换子的概念.

定义 2.11 (交换子/交换子群)

对于群 G，$a,b\in G$，定义 a,b 的交换子为 $[a,b]=aba^{-1}b^{-1}$，由 $\{[a,b]:a,b\in G\}$ 的生成的群 G' 称为 G 的交换子群. ♣

正如其名，交换子刻画了元素的交换性：$[a,b]=1$ 当且仅当 a,b 可交换；交换子群刻画了群的交换性：$G'=\{1\}$ 当且仅当 G 为 Abel 群.

定理 2.15

设 G 为群，则 $G'\triangleleft G$，且 G/G' 为 Abel 群. 对于 $N\triangleleft G$，G/N 为 Abel 群当且仅当 N 包含 G'. ♡

证明 对于 G 的自同构 f，注意到

$$f([a,b])=[f(a),f(b)], \tag{2.84}$$

如果考虑 $\tau_g:x\mapsto gxg^{-1}$，则可知

$$g[a,b]g^{-1}=[gag^{-1},gbg^{-1}]\in G', \tag{2.85}$$

这说明 $gG'g^{-1}\leqslant G'$，故 $G'\triangleleft G$. 若 $N\triangleleft G,G/N$ 为 Abel 群则对任意 $aN,bN\in G/N$ 有 $abN=baN$，因此 $[a,b]=aba^{-1}b^{-1}\in N$，$G'\leqslant N$，得证，反过来也是容易的.

仿照升中心列，记 $G^{(1)}=G'$，$G^{(k)}=(G^{(k-1)})'$ 称为 G 的 k 阶**导群**，则有

$$G\triangleright G^{(1)}\triangleright G^{(2)}\triangleright\cdots\triangleright\{1\}, \tag{2.86}$$

且任何 $G^{(k)}\triangleleft G$（归纳易证），由此可以定义可解群.

定义 2.12 (可解群)

群 G 称为可解的，若存在 n 使得 $G^{(n)}=\langle e\rangle$. ♣

命题 2.8

任何幂零群都是可解的. ♠

证明 设 G 幂零，$G=C_n(G)$，则 $G/C_{n-1}(G)=C(G/C_{i-1}(G))$ 为 Abel 群，因此

$$G^{(1)}\leqslant C_{n-1}(G)\leqslant G, \tag{2.87}$$

同理，$C_i(G)/C_{i-1}(G)=C(G/C_{i-1}(G))$ 为 Abel 群，因此 $C_i(G)'\leqslant C_{i-1}(G)$，再借助一个很基本的事实：$A\leqslant B\Rightarrow A'\leqslant B'$ 可得

$$G^{(2)}=(G^{(1)})'\leqslant C_{n-1}(G)'\leqslant C_{n-2}(G)\leqslant G, \tag{2.88}$$

$$G^{(3)}=(G^{(2)})'\leqslant C_{n-2}(G)'\leqslant C_{n-3}(G)\leqslant G, \tag{2.89}$$

以此类推，最终可得

$$G^{(n)}=(G^{(n-1)})'\leqslant C_1(G)'=C(G)'=\{1\}, \tag{2.90}$$

故 $G^{(n)}=\{1\}$，即 G 可解.

定理 2.16

1. 任何可解群的子群/同态像都是可解的.
2. 设 $N \triangleleft G$，则 $N, G/N$ 可解当且仅当 G 可解.

♡

证明

1. 设 G 可解，$G^{(n)} = \{1\}$，子群的情形是显然的；设 $f : G \to H$ 为满同态，则 $f([a,b]) = [f(a), f(b)]$，归纳易证 $f(G^{(i)}) = f(G)^{(i)} = H^{(i)}$（双边包含），故 $f(G^{(n)}) = \{1\} = H^{(n)}$，即 $f(G) = H$ 可解.
2. 设 G 可解，则 N 显然可解，考虑满同态 $f : G \to G/N$ 可知 G/N 可解；反之同样考虑这一同态，G/N 可解说明存在 n 使得 $f(G^{(n)}) = (G/N)^{(n)} = \{1\}$，因此 $G^{(n)} \leqslant N$，N 可解说明 $G^{(n)}$ 可解，即 G 可解.

推论 2.11

当 $n \geqslant 5$ 时，S_n 不可解.

♡

证明 若 S_n 可解，则 $A_n \leqslant S_n$ 可解，但当 $n \geqslant 5$ 时 A_n 为单群，显然 $A_n' \neq \{1\}$，因此 $A_n' = A_n$，故 A_n 不可解，得证.

为了将 Sylow 定理在有限可解群上推广，需要做一些准备工作.

定义 2.13 (特征子群/全不变子群)

$H \leqslant G$ 称为 G 的特征子群（全不变子群），若对任意 $f \in \mathrm{Aut}(G)$（$f \in \mathrm{End}(G)$）有 $f(H) \leqslant H$.

♣

引理 2.5

设 $N \triangleleft G$，G 为有限群，$H \leqslant G$，则

1. 若 H 为 N 的特征子群，则 $H \triangleleft G$.
2. G 的任何正规 Sylow 子群都是全不变的.
3. 若 G 可解，N 为极小正规子群，则 N 是一个 Abel p-群.

♡

证明

1. 考虑 N 中的自同构 $(g \in G)$ $\tau_g : x \mapsto gxg^{-1}$，则根据特征子群的定义可知 $\tau_g(H) = ghg^{-1} \leqslant H$，故 $H \triangleleft G$，得证.
2. 设 P 为 G 的正规 Sylow p-子群，$f \in \mathrm{End}(G)$，则由于
$$f(P) \cong P/(P \cap \mathrm{Ker}\, f), \tag{2.91}$$
因此 $f(P)$ 为 p-群，$f(P) \leqslant P$（根据 Sylow 子群的唯一性），得证.
3. 显然 $N' \triangleleft N$，并且 N' 是 N 的全不变子群，由 1 得 $N' \triangleleft G$，根据 N 的极小性可得 $N' = \{1\}$ 或 $N' = N$，N 的可解性说明 $N' \neq N$，故 $N' = \{1\}$，即 N 为 Abel 群.
再设 P 为 N 的非平凡 Sylow p-子群，则 N 的交换性使得 $P \triangleleft N$，这说明 P 是 N 的特征子群，再次由 1 可得 $P \triangleleft G$，根据 P 的非正规性可知 $P = N$，得证.

命题 2.9 (Hall)

设 G 为有限可解群，$|G| = mn, (m,n) = 1$，则

1. G 有 m 阶子群.
2. G 中任何两个 m 阶子群彼此共轭.
3. 设 $k \mid m$，则 G 的任何 k 阶子群都包含在一个 m 阶子群中.

♠

2.7 正规列与子正规列

上一节讨论升中心列与导群列得到了许多良好的结论，将这一概念推广，可以研究一般的正规子群列，并且最终得到著名的 Jordan-Holder 定理.

定义 2.14 (次正规列)

称 G 的正规子群列

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n \tag{2.92}$$

为 G 的一个次正规列，其中 $G_i \triangleright G_{i+1}$，所有 G_i/G_{i+1} 称为因子，真包含的个数称为长度. 特别地，若每个 $G_i \triangleleft G$，则称之为一个正规列.

♣

注 容易发现，导群列与（有限）升中心列都是正规列.

定义 2.15 (加细)

设 $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n$ 为一个次正规列，若其中可以插入一个满足 $G_{i+1} \triangleleft N \triangleleft G_i$ 的子群 N 得到新的次正规列，则称该操作为一步加细. 次正规列 S 的任何有限步加细称为其加细，称 S 的一个加细是真的，若其长度大于 S.

♣

定义 2.16 (合成列/可解列)

称一个次正规列 $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{1\}$ 为一个合成列，若每个因子 G_i/G_{i+1} 都是单群；称其为可解列，若每个因子都是 Abel 群.

♣

若 $N \triangleleft G$，则 G/N 的任何子群都有 H/N 的形式，因此 G/N 为单群当且仅当 N 为 G 的极大正规子群（即 G 中真包含 N 的正规子群只有 G）.

定理 2.17

1. 任何有限群 G 都有合成列.
2. 可解列的任何加细仍然是可解列.
3. 一个次正规列是合成列当且仅当它没有真加细.

♡

证明

1. 取 G 的一个极大正规子群 G_1，则 G/G_1 是单群，若 $G_1 \neq \{1\}$ 则重复这一操作，即得合成列.
2. 设添加了 $G_{i+1} \triangleleft N \triangleleft G_i$，由于 G_i/G_{i+1} 为 Abel 群，其子群 N/G_{i+1} 也为 Abel 群，并且

$$G_i/N \cong (G_i/G_{i+1})/(N/G_{i+1}) \tag{2.93}$$

也为 Abel 群，得证.

3. 次正规列是合成列当且仅当每个 G_i/G_{i+1} 为单群，若在 G_i, G_{i+1} 之间可以做一步加细，则必有 $N \triangleleft G_i$ 使得 $N/G_{i+1} \triangleleft G_i/G_{i+1}$，根据单群可知必有 $N = G_i$ 或 $N = G_{i+1}$，因此长度没有变化，不存在 proper 加细 s. 反之若无 proper 加细 s，则添加任何 N 都不会改变长度，类似可得.

下面的命题表明，“可解列”确实与“可解”有密切联系.

定理 2.18

群 G 可解当且仅当其有可解列.

♡

证明 若 G 可解，显然其导群列给出了一个可解列；反之若 G 有可解列，则 G/G_1 为 Abel 群说明

$$G \triangleright G_1 \triangleright G^{(1)}, \tag{2.94}$$

G_1/G_2 为 Abel 群说明

$$G_2 \triangleright G_1' \triangleright G^{(2)}, \tag{2.95}$$

以此类推可得 $G^{(n)} = \{e\}$.

命题 2.10

有限群 G 可解当且仅当 G 存在一个合成列，其所有因子都是素数阶循环群.

♠

证明 若 G 有这样的合成列，则显然所有因子都是 Abel 群，即 G 有可解列，是可解群. 反之若 G 可解，则 G 有可解列，下面将其 refine 为一个满足条件的合成列. 首先取 G 的极大正规子群 $H_1 \triangleright G_1$，若 $H_1 \neq G_1$，则再取 H_1 的极大正规子群 $H_2 \triangleright G_1$，以此类推，可得

$$G \triangleright H_1 \triangleright \cdots \triangleright H_k \triangleright G_1, \tag{2.96}$$

其中 $G/H_1, H_i/H_{i+1}, H_k/G_1$ 均为单群，而 G/G_1 为 Abel 群说明这里的每个因子都是 Abel 群，而有限单 Abel 群必然是素数阶循环群，用相同的方法处理 G_i, G_{i+1}，即得一个合成列，所有因子都是素数阶循环群.

定义 2.17 (次正规类的等价)

称 G 的两个次正规列 S, T 等价，若存在 S, T 的非平凡因子间（在同构意义下）的一一对应.

♣

注 这里只要求因子的一一对应，不要求顺序.

引理 2.6

若 S 为群 G 的合成列，则 S 的任何加细都与 S 等价.

♡

证明 合成列无 proper 加细，因此任何添加都不改变长度，因此非平凡因子不变.

下面证明一个技术性的引理

引理 2.7 (Zassenhaus)

设 A, A^*, B, B^* 为 G 的子群，且 $A^* \triangleleft A, B^* \triangleleft B$，则

1. $A^*(A \cap B^*) \triangleleft A^*(A \cap B)$.
2. $B^*(A^* \cap B) \triangleleft B^*(A \cap B)$.
3. $$\frac{A^*(A \cap B)}{A^*(A \cap B^*)} \cong \frac{A \cap B}{(A \cap B^*)(A^* \cap B)} \cong \frac{(A \cap B)B^*}{(A^* \cap B)B^*}. \tag{2.97}$$

♡

证明 $B^* \triangleleft B$ 说明 $(A \cap B^*) \triangleleft (A \cap B)$，而正规子群的乘积仍然是正规子群，因此 1,2 都是易得的.

令 $D = (A \cap B^*)(A^* \cap B) \triangleleft (A \cap B)$，定义满射

$$f : A^*(A \cap B) \longrightarrow (A \cap B)/D \tag{2.98}$$

$$ak \longmapsto Dk, \tag{2.99}$$

其中 $a \in A^*, k \in A \cap B$，注意到 $a_1k_1 = a_2k_2$ 当且仅当 $a_1^{-1}a_2 = k_1k_2^{-1}$，此时

$$D = f(a_1^{-1}a_2) = f(k_1k_2^{-1}) = Dk_1k_2^{-1}, \quad f(a_1k_1) = Dk_1 = Dk_2 = f(a_2k_2), \tag{2.100}$$

因此 f 良定，根据 A^* 的正规性有

$$f(a_1k_1a_2k_2) = f(a_1a_2'k_1k_2) = Dk_1k_2 = (Dk_1)(Dk_2) = f(a_1k_1)f(a_2k_2), \tag{2.101}$$

故 f 为同态，因此根据同态基本定理有

$$A^*(A \cap B)/\mathrm{Ker}\, f \cong A \cap B/D, \tag{2.102}$$

其中 $ak \in \operatorname{Ker} f$ 当且仅当 $k \in D$，因此

$$\operatorname{Ker} f = A^*(A \cap B^*)(A^* \cap B) = A^*(A \cap B^*), \tag{2.103}$$

得证，另一半同理.

如下定理说明，同群中的此正规列都是等价的，也即可以将此作为群的某种性质.

定理 2.19 (Schreier)

群 G 的任何两个次正规列（正规列）都可以 refine 为等价的次正规列（正规列）.

♡

证明 设 G 有两个次正规列

$$G = G_0 > G_1 > \cdots > G_n, \quad G = H_0 > H_1 > \cdots > H_m, \tag{2.104}$$

约定 $G_{n+1} = H_{m+1} = \{1\}$，则对任意 $0 \leqslant i \leqslant n$ 有

$$G_i = G_{i+1}(G_i \cap H_0) > G_{i+1}(G_i \cap H_1) > \cdots > G_{i+1}(G_i \cap H_m) > G_{i+1}(G_i \cap H_{m+1}) = G_{i+1}, \tag{2.105}$$

暂且不考虑其中是否有平凡元素，则添加这些元素后 G 列中群个数为

$$(n+1) + (n+1) * m = (n+1)(m+1) \tag{2.106}$$

同理，对 H 列添加这些元素后群个数为 $(m+1)(n+1)$，根据 Zassenhaus 定理可得

$$\frac{G_{i+1}(G_i \cap H_k)}{G_{i+1}(G_i \cap H_{k+1})} \cong \frac{(G_i \cap H_k)H_{k+1}}{(G_{i+1} \cap H_k)H_{k+1}}, \tag{2.107}$$

这就建立起了两个 refine 列因子之间的同构对应，抛去相同数量的平凡因子后，即得二者的加细等价.

定理 2.20 (Jordan-Holder)

群 G 的任何两个合成列都是等价的，因此有合成列的群都能唯一确定一个正规子群列.

♡

注 该定理并不保证一般群合成列的存在性.

证明 G 的任何两个合成列不能进一步 refine，但根据 Schreier 两个次正规列都可以 refine 为两个等价的次正规列，因此这两个合成列是等价的.

第 3 章 环

3.1 环与理想

环的定义

环实际上是在群的基础上添加了另一种运算，并要求其中一种运算可交换的结构.

定义 3.1 (环)

定义环为集合 R 与其上运算 $+,\cdot$，满足：

1. $(R,+)$ 为 Abel 群，$(R,\cdot)$ 为半群.
2. 分配律：$a(b+c)=ab+ac,(a+b)c=ac+bc$.

♣

注 若 $(R,\cdot)$ 为幺半群则称 R 为含幺环；若乘法也是交换的则称 R 为交换环. 一般用 $0,1$ 分别代表环中的加法、乘法单位元.

定义 3.2 (零因子)

设环 R 有非零元 $a\in R$，则称 a 为左（右）零因子，若存在 $b\in R,b\neq 0$ 使得 $ab=0$（$ba=0$）.

♣

注 容易验证，环中无零因子当且仅当该环满足左、右消去律.

定义 3.3 (可逆元/单位)

称 $a\in R$ 左（右）可逆，若存在 $b\in R$ 使得 $ba=1$（$ab=1$）. 若 a 同时左右可逆则称 a 可逆，或者说 a 是 R 中一个单位.

♣

根据上面的定义，可以给出环论中几种重要对象的定义.

定义 3.4 (整环/除环（体）/域)

定义满足 $1\neq 0$，且无零因子的交换环为整环；定义满足 $1\neq 0$，且任何非零元均可逆的环为除环（或体）；定义交换除环为域.

♣

定义 3.5 (环同态)

设 R,S 为环，映射 $f:R\to S$ 称为环同态，若对任意 $a,b\in R$ 满足

$$f(a+b)=f(a)+f(b),\quad f(ab)=f(a)f(b). \tag{3.1}$$

进一步，若 f 可逆，则称 f 为环同构.

♣

注 根据环同态，同样可以定义核、像，单同态、满同态等概念.

定义 3.6 (环的特征)

设 R 为环，若存在 $n\in\mathbb{N}$ 使得对任意 $a\in R$ 有 $na=0$，则称其为 R 的特征，记为 $\operatorname{char}R=a$；若不存在这样的 n，则称 R 为零特征.

♣

命题 3.1

1. 对任意 $a\in R$ 有 $\operatorname{ord}a\mid\operatorname{char}R$.
2. 特别当 R 含幺时，$\operatorname{char}R=\operatorname{ord}1$.
3. 若 R 为整环且 $\operatorname{char}R>0$，则 $\operatorname{char}R$ 为素数.

♠

对于交换环，可以考虑如下同态

定义 3.7 (Frobenius 自同态)

设 R 为交换环，$\mathrm{char}\, R = p$ 为素数，定义

$$F : R \longrightarrow R \tag{3.2}$$

$$a \longmapsto a^p, \tag{3.3}$$

则 F 为 R 的一个自同态，称为 Frobenius 自同态.

♣

同态是容易验证的，容易验证当 $R = \mathbb{Z}_p$ 时，F 为一个自同构.

理想

在群中，借助正规子群可以进行商运算，但这对于环而言会有些古怪：商环借助的不是“正规子环”，而是“理想”，并且大多情况下理想不会是一个子环（除非为整个环），下面来讨论理想.

定义 3.8 (子环)

设 R 为环，则称 $S \subset R$ 为 R 的子环，若其在 R 中的加法、乘法下依然是一个环，记为 $S \leqslant R$.

♣

定义 3.9 (理想)

设 R 为环，则称 $I \subset R$ 为 R 的左（右）理想，若 $(I,+) \leqslant (R,+)$，并且对任意 $r \in R, x \in I$ 都有 $rx \in I$ $(xr \in I)$，这称为左（右）吸收律，称 I 为理想若其同时为左、右理想，记为 $I \triangleleft R$.

♣

注 R 中有两个平凡理想，即 $\{0\}, R$.

理想的吸收律从定义来看非常古怪，其内涵将在讨论商环/环同态定理时揭示.

推论 3.1

设 $\{A_i : i \in I\}$ 为环 R 的一族理想，则 $\bigcap_{i\in I} A_i$ 也是 R 的理想.

♡

注 类似可考虑左/右理想的交.

定义 3.10 (生成的理想)

设 $X \subset R$，则定义由 X 生成的理想 (X) 为包含 X 的最小理想，即

$$(X) = \bigcap_{X \subset A_i \triangleleft R} A_i. \tag{3.4}$$

♣

X 中的元素称为 (X) 的生成元，若 $X = \{x_1, \cdots, x_n\}$，则 $(X) = (x_1, \cdots, x_n)$ 称为**有限生成**的，仅由一个元素生成的理想称为**主理想**，若环中所有理想都是主理想，则称其为主理想环（特别地，**主理想整环**称为 PID）.

命题 3.2

设 R 为环，$a \in R, X \subset R$，则

1. 主理想 (a) 中的元素形如 $ra + as + na + \sum_{i=1}^{r} r_i a s_i$，其中 $r, s, r_i, s_i \in R$，$m \in \mathbb{N}, n \in \mathbb{Z}$. 若 R 含幺，则
$$(a) = \left\{ \sum_{i=1}^{n} r_i a s_i : r_i, s_i \in R, n \in \mathbb{N} \right\}. \tag{3.5}$$
2. 若 a 处于 R 的中心（与所有元素可交换），则 $(a) = \{ra + na : r \in R, n \in \mathbb{Z}\}$.
3. $Ra = \{ra : r \in R\}$ 为 R 的左理想，$aR = \{ar : r \in R\}$ 为 R 的右理想. 若 a 处于 R 的中心，则 $aR = Ra \triangleleft R$.

♠

注 对于不含幺的环，(a) 未必包含 a.

理想之间可以进行运算，如

$$A+B=\{a+b:a\in A,b\in B\}, \tag{3.6}$$

$$AB=(\{ab:a\in A,b\in B\})=\left\{\sum_{k=1}^{n}a_kb_k:a_k\in A,b_k\in B\right\} \tag{3.7}$$

归纳可得任意有限个理想之间的加、乘.

命题 3.3

设 $A_1,\cdots,A_n,A,B,C\triangleleft R$，则

1. $A_1+\cdots+A_n,A_1\cdots A_n\triangleleft R$.
2. 结合律：$(A+B)+C=A+(B+C)$，$(AB)C=A(BC)$.
3. 分配律：$B(A_1+\cdots+A_n)=BA_1+\cdots+BA_n$，$(A_1+\cdots+A_n)C=A_1C+\cdots+A_nC$.

♠

事实上，关于有两个理想产生的新理想有如下命题:

命题 3.4

设 $A,B\triangleleft R$，则

1. $A+B=(A\cup B)$.
2. $AB\subset A\cap B\subset(A\cup B)=A+B$.

♠

商环与同构定理

下面根据理想来讨论商环.

定义 3.11 (商环)

设 R 为环，$I\triangleleft R$，则定义 R/I 为商环，其中运算

$$(a+I)+(b+I)=(a+b)+I,\quad (a+I)(b+I)=ab+I. \tag{3.8}$$

♣

作商最重要的是验证良定性，上面的加法部分是容易的（因为 $(I,+)\triangleleft(R,+)$），因此只需要验证乘法，设 $a,a'\in a+I$，$b,b'\in b+I$，则

$$a'b'-ab=a'(b'-b)+(a'-a)b\in a'I+Ib\subset I, \tag{3.9}$$

说明 $a'b'+I=ab+I$，因此乘法是良定的. 由此可以看出吸收律的效用，如果直接拆括号可得

$$(a+I)(b+I)=ab+aI+Ib+II\subset ab+I \tag{3.10}$$

注意到同态的核就是一个理想，因此仿照群同构定理，可以给出类似的环同构三定理.

定理 3.1 (第一同构定理)

设 $f:R\to S$ 为满同态，则 $R/\operatorname{Ker}f\cong S$.

♡

定理 3.2 (第二同构定理)

设 $I,J\triangleleft R$，则 $I/(I\cap J)\cong(I+J)/J$.

♡

定理 3.3 (第三同构定理)

设 $I,J\triangleleft R$，$I<J$，则 $(R/I)/(J/I)\cong R/J$.

♡

素理想与极大理想

整数环有如下性质：素数 $p|ab$ 蕴含 $p|a$ 或 $p|b$，类比这种性质，可以定义环中的素理想.

定义 3.12 (素理想)

理想 $P \triangleleft R$ 称为素理想，若对任意 $ab \in P$，必有 $a \in P$ 或 $b \in P$.

♣

素理想的性质体现在其商环中：

定理 3.4

设交换环 R 中 $1 \neq 0$，则 P 为素理想当且仅当 R/P 为整环.

♡

证明 注意到

$$(a+P)(b+P) = P \Longleftrightarrow ab \in P, \tag{3.11}$$

因此若 P 为素理想，则可不妨设 $a \in P$，此时 $a+P=P$，故 R/P 为整环；反之若 R/P 为整环，则可不妨设 $a+P=P$，即 $a \in P$，故 P 为素理想.

还有一种特殊的理想，称为极大理想，它可以看作 R 中某个非平凡理想链的终点.

定义 3.13 (极大理想)

理想 $M \triangleleft R$ 称为极大理想，若对任意满足 $M \subset N \subset R$ 的理想 N 都有 $N = M$ 或 $N = R$.

♣

极大理想可以看作包含关系的偏序集中的极大元，因此在承认 Zorn 引理的情况下，极大理想必定存在.

定理 3.5

非零环 R 中的极大理想存在，并且任何理想都包含在一个极大理想中.

♡

证明 对任意 $A \triangleleft R$，考虑集合

$$\mathcal{S} = \{B \triangleleft R : A \subset B \neq R\}, \tag{3.12}$$

$A \in \mathcal{S}$ 说明则该集合非空，只需证明 $\mathcal{S}$ 中任何链 (非空全序子集) 都有上界 (Zorn 引理). 设 $\{B_i : i \in I, B_i \in \mathcal{S}\}$ 为一个非空全序子集，令

$$B = \bigcup_{i \in I} B_i, \tag{3.13}$$

则对任意 $a, b \in B$，存在 i, j 使得 $a \in B_i, b \in B_j$，不妨设 $B_i \subset B_j$ 则 $a, b \in B_j, a-b \in B_j \subset B$，吸收律同理，因此 B 为理想且 $A \subset B \neq R$ (否则 $1 \in B_i$，矛盾)，故 $B \in \mathcal{S}$ 为该子集的上界，根据 Zorn 引理，$\mathcal{S}$ 中存在极大元，该极大元就是 R 中包含 A 的极大理想.

命题 3.5

若交换环 R 满足 $R^2 = R$，则 R 中任何极大理想都是素理想.

♠

证明 设 $M \triangleleft R$ 极大，假设存在 $ab \in M$，$a, b \notin M$，由于 $M \triangleleft M + (a), M + (b) \triangleleft R$，根据 M 的极大性可知 $M + (a) = M + (b) = R$，但 $ab \in M$ 说明此时 $(a)(b) \subset (ab) \subset M$，因此

$$R = R^2 = (M + (a))(M + (b)) \subset M^2 + (a)M + M(b) + (a)(b) \subset M \tag{3.14}$$

这与 M 的极大性矛盾，得证.

与素理想类似，极大理想的性质也能体现在其商环中：

定理 3.6

设 $M \triangleleft R$，$1 \neq 0$，则

1. 若 M 为极大理想，R 为交换环，则商环 R/M 为域.
2. 若商环 R/M 为除环，则 M 为极大理想.

♡

证明

1. 设 $a \notin M$，则 $a+M \neq M$，M 的极大性说明 $(a)+M=R$，因此存在 $r \in R, m \in M$ 使得 $ar+m=1$，因此

$$1+M=ra+M=(r+M)(a+M), \tag{3.15}$$

故 R/M 为除环，R 的交换性使得 M 为域.

2. 若 R/M 为除环，则 $1+M \neq M$，设 $M \subset N \triangleleft R$，则取 $a \in N, a \notin M$，存在 $b \in R$ 使得 $(a+M)(b+M)=ab+M=1+M$，这说明 $ab-1 \in M$，而 $a \in N$，因此 $1 \in N$，这说明 $N=R$，即 M 是极大的.

推论 3.2

对于交换环 R，$1 \neq 0$，如下陈述等价：

1. R 为域.
2. R 无非平凡理想.
3. 0 为 R 的极大理想.
4. 任何非零环同态 $R \to S$ 都是单同态.

♡

证明 此时 $R \cong R/\{0\}$ 为域当且仅当 $\{0\}$ 为 R 的极大理想，当且仅当 R 无非平凡理想；而到域的同态均为单同态，另一方面若 4 成立，假如 R 存在非平凡理想，则考虑其上的商映射，导出矛盾，得证.

3.2 环的积与余积

定义 3.14 (直积)

设 $\{R_i : i \in I\}$ 为环，则定义其直积为 $\prod_{i \in I} R_i$.

♣

注 容易验证直积在自然乘法、加法下也为环.

容易验证，若 $A_i \triangleright R_i$，则 $\prod_{i \in I} A_i \triangleleft \prod_{i \in I} R_i$.

定理 3.7 (直积的泛性质)

设 $\{R_i : i \in I\}, S$ 为环，$\{\varphi_i \in [S, R_i] : i \in I\}$，则存在唯一同态 $\varphi : S \to \prod_{i \in I} R_i$，使得 $\varphi_i = \pi_i \circ \varphi$.

♡

定理 3.8

设 $A_1, \cdots, A_n \triangleleft R$ 使得

1. $A_1 + \cdots + A_n = R$.
2. 对任意 k，$A_k \cap (A_1 + \cdots + \widehat{A_k} + \cdots + A_n) = 0$.

则 $R \cong A_1 \times \cdots \times A_n$.

♡

证明 只需证明 R 中元素可唯一表示为 $A_1, \cdots, A_n$ 中元素和的形式即可.

讨论直积的一个重要目的是讨论中国剩余定理，这在数论中出现过，首先仿之定义同余.

定义 3.15 (同余)

设 $A \triangleleft R$，则称 $a, b \in R$ 模 A 同余，若 $a-b \in A$，记为 $a \equiv b (\mathrm{mod}\, A)$.

♣

注 容易验证，这样得到的同余也是一个等价关系，且 $a_1 \equiv b_1(\mathrm{mod}\, A), a_2 \equiv b_2(\mathrm{mod}\, A)$ 可得

$$a_1 + a_2 \equiv b_1 + b_2(\mathrm{mod}\, A), \quad a_1 a_2 \equiv b_1 b_2(\mathrm{mod}\, A). \tag{3.16}$$

定理 3.9 (中国剩余定理)

设 $A_1, \cdots, A_n \triangleleft R$，且 $R^2 + A_i = R, A_i + A_j = R(i \neq j)$，则对于任意 $b_1, \cdots, b_n \in R$，存在 $b \in R$ 使得

$$b \equiv b_i(\mathrm{mod}\, A_i), \quad i = 1, \cdots n. \tag{3.17}$$

♡

注 若 R 含幺，则 $R^2 = R$，此时对任意理想 I 都有 $R^2 + I = R$.

证明 由于 $A_1 + A_2 = A_1 + A_3 = R$，因此

$$R^2 = (A_1 + A_2)(A_1 + A_3) = A_1^2 + A_1 A_3 + A_2 A_1 + A_2 A_3 \subset A_1 + A_2 A_3, \tag{3.18}$$

另一方面由于 $R = A_1 + R^2$，因此

$$R = A_1 + R^2 \subset A_1 + (A_1 + A_2 A_3) = A_1 + A_2 A_3 \subset R, \tag{3.19}$$

这说明 $R = A_1 + A_2 A_3$，若假设 $R = A_1 + A_2 \cdots A_{k-1}$ 则

$$R^2 = (A_1 + A_2 \cdots A_{k-1})(A_1 + A_k) \subset A_1 + A_2 \cdots A_k \tag{3.20}$$

$$R = R^2 + A_1 \subset A_1 + A_2 \cdots A_k \subset R, \tag{3.21}$$

即得 $R = A_1 + A_2 \cdots A_k$，因此根据归纳可得

$$R = A_1 + A_2 \cdots A_n, \tag{3.22}$$

对于 $b_1 \in R$，存在 $a \in A_1, b \in A_2 \cdots A_n$ 使得 $b_1 = a + b$，令 $x_1 = b - a$ 则

$$x_1 \equiv b_1(\mathrm{mod}\, A_1), \quad x_1 \equiv 0(\mathrm{mod}\, A_k), k = 2, \cdots, n, \tag{3.23}$$

对每个 $1 \leqslant k \leqslant n$ 重复上述过程，得到 x_k，令 $x = x_1 + \cdots + x_k$ 满足条件，得证.

从上面的一般形式也很容易得到数论中的 CRT

推论 3.3

设 $m_1, \cdots, m_n$ 为两两互素的正整数，则对任意 $b_1, \cdots, b_n$，方程组

$$x \equiv b_i(\mathrm{mod}\, m_i), \quad i = 1, \cdots, n \tag{3.24}$$

在模 $m = m_1 \cdots m_n$ 意义下有唯一解.

♡

中国剩余定理还有如下的同态形式

推论 3.4

设 $A_1, \cdots, A_n \triangleleft R$，则存在单同态

$$\theta : R \Big/ \bigcap_{i=1}^{n} A_i \longrightarrow \prod_{i=1}^{n} R/A_i \tag{3.25}$$

$$r + \bigcap_{i=1}^{n} A_i \longmapsto (r + A_1, \cdots, r + A_n) \tag{3.26}$$

特别当 $R^2 + A_i = R$，$A_i + A_j = R(i \neq j)$ 时 θ 为满同态，即同构.

♡

证明 注意到 $(r + A_1, \cdots, r + A_n) = (r' + A_1, \cdots, r' + A_n)$ 当且仅当对任意 i 有 $r - r' \in A_i$，即

$$r - r' \in \bigcap_{i=1}^{n} A_i, \tag{3.27}$$

故 θ 为单同态，当这些理想满足更多条件时考虑同态

$$f : R \longrightarrow \prod_{i=1}^{n} R/A_i \tag{3.28}$$

$$r \longmapsto (r + A_1, \cdots, r + A_n), \tag{3.29}$$

根据中国剩余定理，对任意 $(r_1 + A_1, \cdots, r_n + A_n)$，存在 $r \in R$ 使得 $r \equiv r_k (\mathrm{mod}\, A_k)$，也即

$$f(r) = (r_1 + A_1, \cdots, r_n + A_n), \tag{3.30}$$

故 f 为满同态，且此时 $\mathrm{Ker}\, f = \bigcap_{i=1}^{n} A_i$，由第一同构定理可知 θ 恰好为同构.

推论 3.5 (插值公式)

设 F 为域，$t_1, \cdots, t_n \in F$ 两两不同，则对于任意 $a_1, \cdots, a_n \in F$，存在唯一 $f(x) \in F[x]$ 使得 $\deg f < n$，$f(t_i) = a_i$.

♡

证明 令 $I_i = (x - t_i)$，则根据 CRT 可得.

3.3 交换环的因子分解

定义 3.16 (整除/相伴)

设 R 为交换环，$a, b \in R$，若存在 $x \in R$ 使得 $ax = b$，则称 a 整除 b，记为 $a|b$，此时称 a 为 b 的一个因子. 若 $a|b, b|a$，则称 a, b 相伴，记为 $a \sim b$

♣

注 容易验证整除为偏序关系，相伴是等价关系.

定理 3.10

设 R 为交换幺环，$a, b, u \in R$ 则

1. $a|b$ 当且仅当 $(b) \subset (a)$.
2. $a \sim b$ 当且仅当 $(a) = (b)$.
3. $u \in R^*$ 当且仅当对任意 $r \in R$ 有 $u|r$，当且仅当 $(u) = R$.
4. 若存在 $r \in R^*$ 使得 $a = br$，则 $a \sim b$，当 R 为整环时反之成立.

♡

定义 3.17 (不可约/素元)

设 R 为交换幺环，则

1. 称 $c \in R$ 不可约，若 $c = ab \Rightarrow a \in R^* \vee b \in R^*$.
2. 称 $p \in R$ 为素元，若 $p \notin R^* \cup \{0\}$ 且 $p|ab \Rightarrow p|a \vee p|b$.

♣

虽然在 $\mathbb{Z}$ 中，不可约与素性等价，但二者大多是不等价的.

例 3.1 在 $\mathbb{Z}_6$ 中，2 为素元，但 $2 = 2 \cdot 4$ 说明 2 可约.

例 3.2 考虑 $\mathbb{Z}[\sqrt{-5}]$，则其中 $3, 2 \pm \sqrt{-5}$ 均不可约，但

$$3|9 = (2 + \sqrt{-5})(2 - \sqrt{-5}), \tag{3.31}$$

显然 $3 \nmid 2 \pm \sqrt{-5}$.

定理 3.11

设 R 为整环，$p, c \in R, p, c \neq 0$，则

1. p 为素元当且仅当 (p) 为 R 的素理想.
2. c 不可约当且仅当 (c) 为所有主理想集合中的极大元.

3. R 中任何素元不可约.
4. 若 R 为主理想整环，则其中素性与不可约等价.
5. 不可约元（或素元）的相伴类都是不可约（或素）的.
6. R 中不可约元的因子只有单位.

♡

注意到 $\mathbb{Z}$ 中每个元素都可以唯一分解为素数幂的乘积形式，而上面已经讨论了整环中“素元”与“不可约元”的性质，因此可以将这种唯一分解定理提取出来，给出**唯一分解整环的定义**.

定义 3.18 (唯一分解整环 (UFD))

称整环 R 为唯一分解整环，若其满足下面的唯一分解性质：

1. R 中任意非零元都能写作 $a=c_1\cdots c_n$ 的形式，其中 c_k 均为不可约元.
2. 若有两种分解 $a=c_1\cdots c_n=d_1\cdots d_m$，则必有 $m=n$，且存在置换 $\sigma\in S(n)$ 使得 $c_i\sim d_{\sigma(i)}$（即各因子差一个置换下等价）.

♣

注 事实上，上面的定义保证了 UFD 中的不可约元均为素元.

定义 3.19 (最大公因子)

设 R 为整环，$a,b\in\mathbb{R}-\{0\}$，称 d 为 a,b 的最大公因子，若其满足

1. $d|a,d|b$.
2. 若 $d'|a,d'|b$，则 $d'|d$.

记为 $d\sim\gcd(a,b)$. 特别地，若 $\gcd(a,b)\sim 1$，则称 a,b 互素.

♣

注

1. 一般元素的最大公因子不是唯一的，因为与 d 相伴的元素也都是最大公因子，所以上面使用相伴的记号.
2. 上面的定义并不保证最大公因子的存在性.

引理 3.1

设 R 为整环，$a,b,c\in R-\{0\}$，则

1. $\gcd(\gcd(a,b),c)\sim\gcd(a,\gcd(b,c))$.
2. $c\gcd(a,b)\sim\gcd(ca,cb)$.
3. 若 $\gcd(a,b)\sim\gcd(a,c)\sim 1$，则 $\gcd(a,bc)\sim 1$.

♡

证明

1. 设 $d_1\sim\gcd(a,b),d_2\sim\gcd(d_1,c)$，易验证 $d_2|\gcd(a,\gcd(b,c))$.
2. 设 $d\sim\gcd(a,b),a=da_1,b=db_1$，则 $ca=cda_1,cb=cdb_1$，故
$$cd|\gcd(ca,cb), \tag{3.32}$$
再设 $cD'=D\sim\gcd(ca,cb),ca=cD'a_2,cb=cD'b_2$，则由整环的性质可得 $D'a_2=da_1=a,D'b_2=db_1=b$，故
$$D'|a,D'|b\Rightarrow D'|d,D=cD'|cd, \tag{3.33}$$
得证.
3. $\gcd(a,b)\sim 1$ 说明 $\gcd(ac,bc)\sim c$，显然有 $\gcd(a,ac)\sim a$，因此
$$\gcd(a,bc)\sim\gcd(\gcd(a,ac),bc)\sim\gcd(a,\gcd(ac,bc))\sim\gcd(a,c)\sim 1. \tag{3.34}$$

定义 3.20 (Noether 性质)

若整环环 R 中的主理想升链均会终止，即若

$$(a_1) \subset (a_2) \subset \cdots, \tag{3.35}$$

则必有 n 使得 $(a_n) = (a_{n+1}) = \cdots$，则称 R 具有 Noether 性质.

♣

注 这也相当于整除链 $a_2|a_1, a_3|a_2, \cdots$ 有终止.

定理 3.12

整环 R 的下述三条命题等价：

1. R 为 UFD.
2. R 满足 Noether 性质且任意两元素均有最大公因子.
3. R 满足 Noether 性质且其中不可约元与素元等价.

♡

证明 $1 \Rightarrow 2$：考虑一个引理：对于一个 UFD，若 $b|a = up_1^{k_1} \cdots p_n^{k_n}$，则 $b = vp_1^{l_1} \cdots p_n^{l_n}$，且 $l_i \leqslant k_i$，且所有等号同时成立当且仅当 $a \sim b$，由此可知 UFD 中的理想升链必有终止，且任何对于任意两个 a, b，其最大公因子

$$\gcd(a, b) \sim p_1^{\min\{k_1, l_1\}} \cdots p_n^{\min\{k_n, l_n\}}, \tag{3.36}$$

得证.

$2 \Rightarrow 3$：只需证不可约元为素元. 设 $p \in R$ 不可约，$p|ab$，断言 $\gcd(p, a) \sim 1, \gcd(p, b) \sim 1$ 不可能同时发生（否则 $\gcd(p, ab) \sim 1$，矛盾），不妨设 $\gcd(p, a) \sim d \not\sim 1$，则 $p = dc \sim d$（不可约性，c 为单位），故 $p|a$，得证.

$3 \Rightarrow 1$：依次证明分解的存在性与唯一性即可，任取非零非单位的 $a \in R$，设 X 表示 R 中有不可约分解的元素全体，易知 X 对乘法封闭，若 $a \notin X$，则设 $a = a_1 b_1$，其中 a_1, b_1 均为真因子且不妨设 $a_1 \notin X$，以此类推，可得严格无限升链

$$(a) \subset (a_1) \subset (a_2) \subset \cdots, \tag{3.37}$$

由 Noether 性质可知必有终点，即得矛盾. 再证明唯一性，设

$$a = up_1 \cdots p_n = vq_1 \cdots q_m, \tag{3.38}$$

其中 $u \sim v \sim 1, p_i, q_j$ 不可约（根据条件这也为素元），由于 $p_1|vq_1 \cdots q_m$，不妨设 $p_1|q_1$，由于 q_1 不可约，故 $p_1 \sim q_1$，因此上面的分解中可以消去 p_1, q_1，归纳可得 $m = n$，且两个分解的元素成对相伴，即分解是唯一的.

推论 3.6

任何 PID 都是 UFD.

♡

证明 只需验证 R 满足 Noether 性质且素元与不可约元等价（这在前面给出过），设有理想升链

$$(a_1) \subset (a_2) \subset \cdots, \tag{3.39}$$

则 $I = \bigcup_{i=1}^{\infty}(a_i)$ 为理想，可设 $I = (a)$，而 $a \in I$ 说明必然存在某个 (a_n) 包含 a，这就是升链的终点.

事实上，也可以证明 PID 中任意两元素均有最大公因子，只需注意到

$$(a) + (b) = (\gcd(a, b)) \tag{3.40}$$

即可.

命题 3.6

设 R 为含幺交换环，则

1. 若 $d \sim \gcd(a_1, \cdots, a_n)$，则存在 $x_1, \cdots, x_n$ 使得 $d = a_1x_1 + \cdots + a_nx_n$ 当且仅当 $(d) = (a_1) + \cdots + (a_n)$.
2. 若 R 为 PID，则 $d \sim \gcd(a_1, \cdots, a_n)$ 当且仅当存在 $x_1, \cdots, x_n$ 使得 $d = a_1x_1 + \cdots + a_nx_n$.
3. 若 R 为 UFD，则最大公因子存在.

♠

定义 3.21 (欧式环)

若环 R 上存在映射 $\varphi: R-\{0\} \to \mathbb{N}$，满足

1. 对任意 $a,b \in R, ab \neq 0$ 有 $\varphi(a) \leqslant \varphi(ab)$.
2. 对任意 $a,b \in R, b \neq 0$，存在 $q,r \in R$ 使得 $a = qb + r$，且必有 $r = 0$ 或 $r \neq 0, \varphi(r) < \varphi(b)$.

则称 R 为欧式环，若 R 还为整环则称其为欧式整环.

♣

欧式整环也可如下定义

定义 3.22 (欧式整环 (ED))

若整环 R 上存在映射 $\varphi: R \to \mathbb{N}$，满足：

1. $\varphi(x) = 0 \Leftrightarrow x = 0$.
2. 对任意 $a,b \in R, b \neq 0$，存在 $q,r \in R$ 使得 $a = qb + r$ 并且 $\varphi(r) < \varphi(b)$.

则称 R 为欧式整环.

♣

可以看出，欧式整环其实就是可作“带余除法”的环，这种带余除法被抽象为了 Euclid 函数 φ.

例 3.3 $\mathbb{Z}$ 为 ED，函数 $\varphi(x) = |x|$.

例 3.4 若 F 为域，则 $F[x]$ 为 ED，函数 $\varphi(f(x)) = \deg f$.

例 3.5 $\mathbb{Z}[i]$ 为 ED（也被称为 Gauss 整环），函数 $\varphi(a+bi) = |a+bi| = a^2 + b^2$.

对任意 $\beta = a + bi \neq 0, \alpha = c + di$，设

$$\frac{\alpha}{\beta} = u + iv, \quad u, v \in \mathbb{Q}, \tag{3.41}$$

则可取 $u_1, v_1 \in \mathbb{Z}$ 使得 $|u - u_1|, |v - v_1| \leqslant 1/2$，令 $q = u_1 + iv_1$ 则

$$\gamma = \alpha - q\beta \in \mathbb{Z}[i], \tag{3.42}$$

则

$$\frac{|\gamma|^2}{|\beta|^2} = \left|\frac{\alpha}{\beta} - q\right|^2 \leqslant \frac{1}{2}, \tag{3.43}$$

即 $\alpha = q\beta + \gamma$ 满足条件.

定理 3.13

所有 ED 均为 PID.

♡

证明 设 R 为 ED，$I \triangleleft R$，记集合 $\varphi(I) \subset \mathbb{N}$ 的极小元为 m，即存在 $b \in I$ 使得 $\varphi(b) = m$，下证 $I = (b)$，显然 $(b) \subset I$，对任意 $a \in I$ 作带余除法 $a = qb + r$，由于 $r = a - qb \in I$，因此必有 $r = 0$（否则 $\varphi(r) < \varphi(b) = m$，与 m 的最小性矛盾），故 $a = qb \in (b)$，即 $I \subset (b)$，得证.

3.4 商环与局部化

定义 3.23 (可乘)

称环 R 的非空子集 S 是可乘的，若 S 关于乘法封闭.

♣

注 环 R 中可逆元素的全体 R^* 是可乘的；整环 R 中非零元素的全体 $R - \{0\}$ 也是可乘的；若 P 为交换环 R 的素理想，则 $P, R - P$ 都是可乘的.

商环的思想来自于有理数的构造，任何有理数都能表示为两个整数的商，即可以使用 $\mathbb{Z} \times \mathbb{Z}^*$ 表示所有有理数. 此外，不同表示之间可以进行约分，即考虑等价关系

$$\frac{a}{b} \sim \frac{c}{d} \Longleftrightarrow ad - bc = 0, \tag{3.44}$$

这时就有

$$\mathbb{Q} \cong \mathbb{Z} \times \mathbb{Z}^* / \sim, \tag{3.45}$$

由此也可以给出 $\mathbb{Z}$ 到 $\mathbb{Q}$ 的嵌入：$a \mapsto a/1$.

定理 3.14

设 S 为交换环 R 的可乘集，则 $R \times S$ 上的关系

$$(r,s) \sim (r',s') \Longleftrightarrow \exists s_1 \in S : s_1(rs' - r's) = 0 \tag{3.46}$$

是一个等价关系. 特别地，若 R 无零因子且 $0 \notin S$，则

$$(r,s) \sim (r',s') \Longleftrightarrow rs' - r's = 0. \tag{3.47}$$

♡

在上述定理的基础上，$R \times S$ 中的元素 (r,s) 可表示为 r/s，$R \times S/\sim$ 也记为 $S^{-1}R$.

定理 3.15

设 S 为交换环 R 的可乘集，则

1. $S^{-1}R$ 是一个交换幺环，其中加法与乘法定义为
$$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}, \quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}. \tag{3.48}$$
2. 若 R 无零因子且 $0 \notin S$，则 $S^{-1}R$ 为整环.
3. 若 R 无零因子且 $S = R - \{0\}$，则 $S^{-1}R$ 为域.

♡

上面的 $S^{-1}R$ 称为 R 关于 S 的商环（或分式环）；若 R 为整环，$S = R - \{0\}$，则 $S^{-1}R$ 为域，它称为 R 的分式域，记为 $\mathrm{Frac}R$，特别的 $\mathrm{Frac}R = \mathbb{Q}$，这时有一个自然的嵌入 $n \mapsto n/1$，对于一般的环有

定理 3.16

设 S 为交换环 R 的可乘集，则

1. 映射 $\varphi_S : R \to S^{-1}R, r \mapsto rs/s$ 为一个单同态，且 $\varphi_S(S) \subset S^*$.
2. 若 S 中无零因子，则 φ_S 为单同态，即任何整环都可以被嵌入到其商域中.
3. 若 R 含幺，$S = R^*$，则 φ_S 为同构，特别的，域 F 的分式域同构于自身.

♡

证明 (3). 注意到对任意 $r/s \in S^{-1}R$ 有

$$\frac{r}{s} = \varphi_S(rs^{-1}). \tag{3.49}$$

即得同构.

下面的定理说明，分式环可以借助某种“泛性质”定义.

定理 3.17

设 S 为交换环 R 的可乘集，T 为交换幺环，$f : R \to T$ 为一个同态且 $f(S) \subset T^*$，则存在唯一同态 $\bar{f} : S^{-1}R \to T$ 满足 $\bar{f} \circ \varphi_S = f$.

♡

证明 注意到良定的同态

$$\bar{f} : S^{-1}R \longrightarrow T \tag{3.50}$$

$$r/s \longmapsto f(r)f(s)^{-1} \tag{3.51}$$

满足条件 $f = \bar{f} \circ \varphi_S$. 假设还有另一个同态 $g : R^{-1}S \to T$ 满足 $f = g \circ \varphi_S$，则对任意 $r/s \in R^{-1}S$ 有

$$g(r/s) = g(\varphi_S(r)\varphi_S(s)^{-1}) = g(\varphi_S(r))g(\varphi_S(s))^{-1} = f(r)f(s)^{-1} = \bar{f}(r/s), \tag{3.52}$$

故 $g = \bar{f}$.

如果固定 S, R，将所有 (f,T) 视为范畴 $\mathbf{C}$ 的对象，这里 T 为交换幺环，f 为 R 到 T 的同态且将 S 映到 T^*

中，$\mathbf{C}$ 中的态射由同态 $g:T_1\to T_2$ 诱导，满足

$$g(f,T_1)=(g\circ f,T_2), \tag{3.53}$$

那么上面的定理实际上说明 $(\varphi_S,S^{-1}R)$ 为该范畴中的一个始对象.

推论 3.7

设 R 为整环，将其视为自身分式域 F 的子环，则若 E 为域且 $f:R\to E$ 是一个同态，则存在唯一同态 $\bar{f}:F\to E$ 使得 $\bar{f}\big|_R=f$. 特别的，任何包含 R 的域 E_1 都包含一个域 $F_1\cong F$.

♡

下面讨论分式环中的理想.

定理 3.18

设 S 为交换环 R 的可乘集，则

1. 若 $I\triangleright R$，则 $S^{-1}I=\{a/s:a\in I,s\in S\}\triangleright S^{-1}R$.
2. 若 $I,J\triangleleft R$，则

$$S^{-1}(I+J)=S^{-1}I+S^{-1}J \tag{3.54}$$

$$S^{-1}(IJ)=(s^{-1}I)(S^{-1}J) \tag{3.55}$$

$$S^{-1}(IJ)=S^{-1}I\cap S^{-1}J. \tag{3.56}$$

♡

定理 3.19

设 S 为交换环 R 的可乘集，$I\triangleleft R$，则 $S^{-1}I=S^{-1}R$ 当且仅当 $S\cap I\neq\emptyset$.

♡

引理 3.2

♡

3.5 多项式环与形式幂级数

定义 3.24 (多项式环)

设 R 为环，x 为变元，定义 R 上的多项式环为

$$R[x]=\{a_nx^n+\cdots+a_0:a_i\in R,a_n\neq 0\}. \tag{3.57}$$

其中有自然的加法与乘法.

♣

注

1. 多项式环的加法是自然的，但乘法并不那么自然，设

$$(a_nx^n+\cdots+a_0)(b_mx^m+\cdots+b_0)=c_px^p+\cdots+c_0, \tag{3.58}$$

其中 $c_k=\sum_{i=0}^{k}a_ib_{k-i}$，注意这里的系数的次序.

2. 若 R 为交换幺环，则 $R[x]$ 也是.
3. 进一步可以定义多元多项式环 $R[x_1,\cdots,x_n]\cong R[x_1]\cdots[x_n]$.

多项式在许多地方都出现过，可能更多的是在分析中作为多项式函数出现，这实际上说明多项式环上存在一类非常重要的赋值同态.

定义 3.25 (赋值同态/代入同态)

设 R,E 为交换幺环，$R\subset E$，取 $c\in E$，可定义赋值同态

$$\phi_c:R[x]\longrightarrow E \tag{3.59}$$

$$f(x)\longmapsto f(c), \tag{3.60}$$

可记 $\operatorname{Im}\phi_c=R[c]$.

3.6 多项式环的分解

设 D 为 UFD，K 为 Frac$D$，本节讨论 $D[x]$ 上的因子分解.

定义 3.26 (容积/本原多项式) 设 $f(x)=a_nx^n+\cdots+a_0$，称 $C_f\sim\gcd(a_n,\cdots,a_0)$ 为 f 的容积. 特别当 $C_f\sim 1$ 是称 f 为本原多项式.

对任意 $f\in D[x]$，可知存在 $g\in D[x]$ 使得 $f=C_fg$，容易证明这里的 g 就是本原多项式.

命题 3.7

1. 设 $f\in D[x]$，$\deg f>0$，则存在本原多项式 $g\in D[x]$ 使得 $f=cg(x)$，且 c,g 在相伴意义下唯一.
2. 设 $\varphi\in K[x]$，则存在 $f(x)$ 为本原多项式，$a,b\in D,\gcd(a,b)\sim 1$ 使得 $\varphi(x)=(a/b)f(x)$，且 a,b,f 在相伴意义下唯一.

证明

1. 设 $f(x)=cg(x)=c'h(x)$，则 $C_f\sim cC_g\sim c'C_h$，故 $C_g\sim C_h$，故 $g\sim h$.
2. 记

$$\varphi(x)=\frac{r_n}{s_n}x^n+\cdots+\frac{r_0}{s_0} \tag{3.61}$$

$$=\frac{r}{s}f_1(x) \tag{3.62}$$

$$=\frac{rC_{f_1}}{s}f(x), \tag{3.63}$$

消去公因子可以得到满足条件的表达. 若存在另一种表达，即

$$\varphi(x)=\frac{c}{d}g(x)=\frac{a}{b}f(x),\quad \gcd(c,d)\sim\gcd(a,b)\sim 1, \tag{3.64}$$

由此可得 $bcg(x)=adf(x)$，由本原得到 $bc\sim ad$，根据对称性只需验证 $c|a$，事实上

$$\gcd(c,d)\sim 1\Rightarrow\gcd(ac,ad)\sim a, \tag{3.65}$$

而显然 $c|ac,c|ad$，故 $c|\gcd(ac,ad)\sim a$，得证.

引理 3.3 (Gauss) 若 $f,g\in D[x]$ 为本原多项式，则 $f(x)g(x)$ 也为本原多项式.

证明 若 fg 非本原，则取 C_{fg} 的素因子 p，设

$$f(x)=a_nx^n+\cdots+a_0,\quad g(x)=b_mx^m+\cdots+b_0, \tag{3.66}$$

则 fg 的 k 次项系数为 $\sum_{i+j=k}a_ib_j$，设

$$p|a_0,\cdots,a_{i-1},p\nmid a_i,\quad p|b_0,\cdots,b_{j-1},p\nmid b_j, \tag{3.67}$$

f,g 本原说明这样的 i,j 必定存在，容易验证 p 不整除 x^{i+j} 的系数.

命题 3.8 设 $f\in D[x],\deg f>0$，则 f 在 $D[x]$ 中不可约当且仅当 f 为本原多项式（即在 $K[x]$ 中不可约）.

证明 设 f 在 $D[x]$ 中不可约，若 f 在 $K[x]$ 中可约，则设

$$f(x)=\frac{a_1}{b_1}\frac{a_2}{b_2}f_1(x)f_2(x), \tag{3.68}$$

其中 f_1,f_2 为本原，故 f_1f_2 为本原，即得 $a_1a_2\sim b_1b_2$，故 $f\sim f_1f_2$，矛盾.

反之若 f 在 $K[x]$ 不可约，若 $f(x)=g(x)h(x)$，则由其在 $K[x]$ 中的不可约性有 g,h 中至少一个次数为 0，不妨设 $g=a\in D$，则由本原性可知 $a\sim 1$.

命题 3.9

设 $f,g\in D[x]$ 为本原多项式，则在 $D[x]$ 中 $f\sim g$ 当且仅当在 $K[x]$ 中 $f\sim g$.

定理 3.20

设 D 为 UFD，则 $D[x]$ 也为 UFD.

证明 任取非零非单位的 $f\in D[x]$，若 $f\in D$ 则显然有分解；若 $\deg f>0$ 则不妨设 f 本原（否则先根据容积分解），首先在 $K[x]$ 中分解为不可约因子乘积

$$f(x)=\varphi_1(x)\cdots\varphi_n(x) \tag{3.69}$$

$$=\frac{a}{b}g_1(x)\cdots g_n(x), \tag{3.70}$$

其中 $g_1,\cdots,g_n$ 为本原，由此可得 $u=a/b\in U(D)$，且在 $D[x]$ 中 $g\sim g_1\cdots g_n$，因此

$$f(x)=ug_1(x)\cdots g_n(x), \tag{3.71}$$

得证. 再证明唯一性，设

$$f=up_1\cdots p_mg_1(x)\cdots g_n(x)=vq_1\cdots q_{m'}h_1(x)\cdots h_{n'}(x), \tag{3.72}$$

其中 $u,v\in U(D),p_i,q_j$ 在 D 中不可约，g_i,h_j 在 $K[x]$ 中不可约（为本原），则易知

$$up_1\cdots p_m\sim vq_1\cdots q_n, \tag{3.73}$$

由 D 的 UFD 性质可知上面的分解是唯一的，另外由于 $K[x]$ 为 UFD，因此 $n=n'$，且可以调次序使得在 $K[x]$ 中 $g_i\sim h_i$，因此在 $D[x]$ 中 $g_i\sim h_i$，得证.

定义 3.27 (根)

设 $R\subset E$（为交换幺环），称 $c\in E$ 为 $f(x)\in R[x]$ 的根，若 $f(c)=0$.

注 借助带余除法可知这等价于 $f(x)=(x-c)g(x)$，若 $f(x)=(x-c)^mg(x)$ 且 $g(c)\neq 0$，则称 c 为 f 的 m 重根.

定义 3.28 (形式导数)

设 $R\subset E$ 为整环，定义 $f(x)=a_0+\cdots+a_nx^n\in R[x]$ 的形式导数为

$$f'(x)=a_1+\cdots+na_nx^{n-1}. \tag{3.74}$$

注 容易验证，形式导数也满足线性性、乘法原理/Leibniz 法则.

命题 3.10

设 $R\subset E$ 为域，$f(x)\in R[x],c\in E$，则

1. 若 $\operatorname{char}R=0$，则 c 为 f 的 m 重根当且仅当
$$f(c)=f'(c)=\cdots=f^{(m-1)}(c)=0,f^{(m)}(c)\neq 0. \tag{3.75}$$
2. 若在 $R[x]$ 中 $\gcd(f,f')\sim 1$，则 f 在 E 中无重根；尤其若 $\operatorname{char}R=0$ 且 f 不可约，则 f 无重根.

只证明 2.

证明 若 f 在 E 中有重根 c，则 f, f' 在 $E[x]$ 中有非平凡公因子，由此可得 f, f' 在 $R[x]$ 中也有非平凡公因子，与 $R[x]$ 中 $\gcd(f, f') \sim 1$ 矛盾.

定理 3.21 (Eisenstein 判别法)

设 D 为 UFD，$f(x) = a_n x^n + \cdots + a_0 \in D[x]$，若 f 本原，素元 p 满足

$$p | a_0, \cdots, a_{n-1}, \quad p \nmid a_n, \quad p^2 \nmid a_0, \tag{3.76}$$

则 $f(x)$ 不可约.

♡

第 4 章 域扩张与 Galois 理论

4.1 域扩张基本理论

命题 4.1

设 D 为 PID，$p \in D$ 不可约，则 (p) 为极大理想.

推论 4.1

设 K 为域，$K[x]$ 为 PID，设 $f(x) \in K[x]$ 不可约，则 $(f(x))$ 在 $K[x]$ 中极大，故 $K[x]/(f(x))$ 为域.

定义 4.1 (域扩张)

设 K 为域 L 的子域，则称 L 为 K 的扩域，可简记为 L/K.

域扩张有很多例子，比如最熟悉的 $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$；多项式 x^3-5 在 $\mathbb{Q}[x]$ 中不可约，因此 $\mathbb{Q}[x]/(x^3-5)$ 也是域，如果考虑映射（嵌入映射复合商映射）

$$\mathbb{Q} \longrightarrow \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]/(x^3-5), \tag{4.1}$$

因此 $\mathbb{Q}[x]/(x^3-5)$ 也可以看作 $\mathbb{Q}$ 的扩域，事实上扩域也可看作线性空间，因此有时候可以计算维数

$$\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt{2}] = 2, \quad \dim_{\mathbb{Q}} \mathbb{Q}[x]/(x^2-3) \leqslant 3. \tag{4.2}$$

还有一种作域扩张的方法，是考虑商域，即

$$\mathbb{Q} \subset \mathbb{Q}[x] \subset \mathbb{Q}(x) = \{[\frac{f(x)}{g(x)}] : g \neq 0\}. \tag{4.3}$$

下图给出了一些常见域之间的关系：

定义 4.2 (生成多项式环)

设 L/K 为域扩张，$u_1, \cdots, u_n \in L$，称

$$K[u_1, \cdots, u_n] = \{\sum a_{i_1 \cdots i_n} u_1^{i_1} \cdots u_n^{i_n} : a \in K, i_k \in \mathbb{N}\} \tag{4.4}$$

为 $u_1, \cdots, u_n$ 生成的多项式环.

注 这实际上是 $K[x]$ 中赋值同态的像.

定义 4.3 (生成扩域)

设 L/K 为域扩张，$u_1, \cdots, u_n \in L$，定义 $K(u_1, \cdots, u_n)$ 为包含 $u_1, \cdots, u_n$ 的最小的扩域，称为 $u_1, \cdots, u_n$ 生成的扩域. 特别的，若 $L = K(u_1, \cdots, u_n)$，则称 L 为有限生成的；更特别的，当 $n=1$ 时称 L 为单扩张.

生成多项式环与生成扩域之间有关系

$$K(u_1, \cdots, u_n) = \mathrm{Frac} K[u_1, \cdots, u_n], \tag{4.5}$$

有时候二者相等，比如 $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$，也有时不相等，比如 $\mathbb{Q}[x^2] \neq \mathbb{Q}(x^2)$.

定义 4.4 (代数元/超越元)

设 $L/K, u \in L$，若存在 $f(x) \in K[x], f(x) \neq 0$ 使得 $f(u) = 0$，则称 u 为 K 上的代数元，否则称 u 为超越元.

例 4.1 $\sqrt{2}$ 是 $\mathbb{Q}(\sqrt{2})$ 的代数元；t 在 $\mathbb{Q}[t]/(t^3-5)$ 是代数元；π 为 $\mathbb{Q}$ 中的超越元.

定义 4.5 (代数扩张/超越扩张)

若 L/K，L 中每个元素在 K 上代数，则称 L/K 为代数扩张，否则称为超越扩张.

定义 4.6 (无限/有限扩张)

若 L/K，则可以将 L 视为 K-线性空间，称 $[L:K]=\dim_K L$ 为扩张次数，若 $[L:K]<\infty$ 则为有限扩张，否则为无限扩张.

命题 4.2

若 L/K 为有限扩张，则 L/K 为有限生成扩张.

证明 可取 L/K 基 $u_1,\cdots,u_n$，以其线性组合唯一表示 L 的元素，因此

$$L=K(u_1,\cdots,u_n). \tag{4.6}$$

命题 4.3

若 L/K 为有限扩张，则必为代数扩张.

证明 设 $\dim_K L=n<\infty$，则任取 $u\in L$，$1,u,u^2,\cdots,u^n$ 线性相关，故存在 u 的零化多项式 $f(x)\in K[x]$.

借助上述命题，可以很方便地判别代数扩张. 对于域扩张的次数，也有类似群论中 Lagrange 定理的结论

定理 4.1

设 $E/L/K$ 为域扩张，则 E/K 有限当且仅当 $E/L,E/K$ 均有限，且

$$[E:K]=[L:K][E:L]. \tag{4.7}$$

证明 若 E/K 有限，则 L/K 为 E/K 的有限子线性空间，故 $[L:K]\leqslant[E:K]<\infty$，考虑 E/K 的基有

$$E=\mathrm{Span}_K(u_1,\cdots,u_n)=\mathrm{Span}_L(u_1,\cdots,u_n) \tag{4.8}$$

故 $[E:L]$ 有限. 反之若 $[E:L],[L:K]$ 有限，则设

$$E=\mathrm{Span}_L(u_1,\cdots,u_n),L=\mathrm{Span}_K(v_1,\cdots,v_m), \tag{4.9}$$

那么必然有

$$E=\mathrm{Span}_L(u_iv_j:1\leqslant i\leqslant n,1\leqslant j\leqslant m), \tag{4.10}$$

故 $[E:L]$ 有限，这些元素的线性无关性也易得.

为讨论有限扩张，可以先从单扩张开始.

定理 4.2

设 $L=K(u)$ 为单扩张，

1. 若 u 为超越元，则 $K(u)\cong K(x)$ 不可约，这里 $K(x)=\mathrm{Frac}K[x]$.
2. 若 u 为代数元，则存在唯一的不可约多项式 $f(x)\in K[x]$ 使得 $f(u)=1$，且

$$K(u)\cong K[x]/(f(x)),\quad [K(u):K]=\deg f. \tag{4.11}$$

注 对于代数元的情形，该多项式称为 u 在 K 中的的极小多项式.

证明

1. 考虑赋值同态 $\phi_u:K[x]\to L,\phi_u(f)=f(u)$，$u$ 的超越性说明 $\mathrm{Ker}\,\phi_u=\{0\}$，而 $\mathrm{Im}\,\phi_u=K[u]$，考虑分式域 $K(x)$，根据泛性质，存在唯一同态 $\tilde{\phi}_u:K(x)\to L$ 使得 $\tilde{\phi}_u\circ\varphi_K=\phi_u$，注意到 $\mathrm{Im}\,\tilde{\phi}_u=K(u)=L$，故

$$\mathrm{Ker}\,\phi_u=\{0\}\Rightarrow\mathrm{Ker}\,\tilde{\phi}_u=\{0\}\Rightarrow K(u)/\mathrm{Ker}\,\tilde{\phi}_u\cong\mathrm{Im}\,\tilde{\phi}_u=K(u). \tag{4.12}$$

得证.

2. 同样考虑赋值同态 ϕ_u，u 为代数元说明存在多项式零化 u，故 $\phi_u \neq \{0\}$，$K[x]$ 为 PID 说明存在 $f(x)$ 使得 $\operatorname{Ker}\phi_u = (f(x))$，其中 f 首一，由同态基本定理有

$$K[x]/(f(x)) \cong K[u], \tag{4.13}$$

$k[u]$ 为整环说明 $(f(x))$ 为 $K[x]$ 的素理想，即 f 为素元，同时不可约，故 $(f(x))$ 为极大理想，因此 $K[u]$ 为域，故 $K[u] \cong K(u)$，最后计算扩张次数，设 $n = \deg f$，则 $(1, \bar{x}, \cdots, \bar{x}^{n-1})$ 是 $K[x]/(f(x))$ 的一个无关张成组，故 $[K(u) : K] = n$.

推论 4.2

设 L/K 为域扩张，$u_1, \cdots, u_n \in L$ 为 K 上的代数元，则 $K(u_1, \cdots, u_n)/K$ 为有限扩张，从而是代数扩张，且 $K(u_1, \cdots, u_n) = K[u_1, \cdots, u_n]$.

♡

证明 令 $L_0 = K, L_i = K(u_1, \cdots, u_i)$，则 $L_{i+1} = L_i(u_{i+1})$，u_{i+1} 是 $L_1 \supset K$ 上的代数元，故 $[L_{i+1} : L_i] < \infty$，因此

$$[K(u_1, \cdots, u_n) : K] = [L_n : K] = [L_n : L_{n-1}] \cdots [L_2 : L_1][L_1 : L_0] < \infty. \tag{4.14}$$

推论 4.3

设 $E/L, L/K$ 为代数扩张，则 E/K 为代数扩张.

♡

证明 取 $u \in E$ 为 L 上的代数元，则存在 $f(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0 \in L[x]$ 使得 U 在 $K(\alpha_1, \cdots, \alpha_{n-1})$ 上代数，故

$$K(\alpha_1, \cdots, \alpha_{n-1}, u)/K \tag{4.15}$$

为有限扩张，进而是代数扩张.

定义 4.7 (代数闭域)

设 K 为域，称之为代数闭域，若其满足如下等价条件之一：

1. $K[x]$ 中次数大于等于 1 的多项式都在 K 中有根.
2. $K[x]$ 中次数大于等于 1 的多项式都可以分解为一次因式乘积（即不可约元只有一次多项式）.
3. K 无非平凡代数扩张.

♣

定理 4.3

设 K 为域，则有

1. 存在性：存在代数扩张 $\overline{K}/K$，且 $\overline{K}$ 为代数闭域.
2. 极大性：若 L/K 为代数扩张，则存在嵌入 $\eta : L \to \overline{K}$，使得。。。。
3. 唯一性：若 $\tilde{K}/K$ 为代数封闭的代数扩张，则 $\tilde{K} \cong \overline{K}$.

♡

证明 存在性：考虑集合 $\{L : L/K\text{为代数扩张}\}$，则集合的包含关系是该集合中的偏序关系，根据 Zorn 引理，其中任何链都有极大元 $\overline{K}$（易验证任何链的上界为其并），易证 $\overline{K}$ 为代数闭域.

4.1.1 有限域

若 F 为有限域，则其特征必然非零，进一步可证明其特征为素数，这是因为存在同态

$$\phi : \mathbb{Z} \longrightarrow F \tag{4.16}$$

$$n \longmapsto n \cdot 1_F \tag{4.17}$$

根据整数环的性质可知存在 p，使得 $\operatorname{Ker}\phi = (p)$，故 $p \cdot 1_F = 0$，即得 $\operatorname{char} F = p$，并且根据同态基本定理

有嵌入 $\mathbb{Z}_p \hookrightarrow F$，也就是说 F 必然包含一个 p 元子域，在后文中将用记号 $\mathbb{F}_p$ 代替 $\mathbb{Z}_p$（事实上，容易证明所有的 p 元域均同构），这说明 F 为 $\mathbb{F}_p$ 的一个扩域，并且 F 的有限性说明这是一个有限扩张，若设 $[F:F_p]=r$，则存在 $v_1,\cdots,v_r \in F$ 张成整个 F，简单计数可得 $|F|=p^r$.

命题 4.4

有限域 F 的元素个数必为素数的幂次.

我们很自然会考虑，反过来是否成立？即是否对任意素幂都有 p^r 元域？考虑如下定理.

定理 4.4

设 $\mathbb{F}_p$ 的代数闭包为 Ω_p，$q=p^r$，则

1. $\mathbb{F}_q=\{x\in\Omega_p : x^q=x\}$ 为包含 $\mathbb{F}_p$ 的 q 元域，并且是 Ω_p 中唯一的 q 元域，进一步有
$$\Omega_p=\bigcup_{n\geqslant 1}\mathbb{F}_{p^n}. \tag{4.18}$$
2. $\mathbb{F}_q^*$ 为循环群，若记 $\mathbb{F}_q^*=\langle\alpha\rangle$，则 $\mathbb{F}_q=\mathbb{F}_p(\alpha)$，
3. 若 K 为 q 元域，则 $K\cong\mathbb{F}_q$.
4. 若考虑 $\mathrm{Aut}(\mathbb{F}_q)$，则 $\sigma_p: a\mapsto a^p\in\mathrm{Aut}(\mathbb{F}_q)$，并且 $\mathrm{Aut}(\mathbb{F}_q)=\langle\sigma_p\rangle$ 为 r 阶循环群.

证明

1. 由于多项式 x^q-x 在 Ω_p 中无重根，故 $\mathbb{F}_q$ 恰好包含其 $q=p^r$ 个根，并且显然 $\mathbb{F}_p\subset\mathbb{F}_q$. 下证该集合为域，即证明其为交换幺环且非零元可逆，显然 $1,0\in\mathbb{F}_q$，对任意 $a,b\in\mathbb{F}_q$ 有
$$(a+b)^q=a^q+b^q=a+b,\quad (ab)^q=a^qb^q=ab, \tag{4.19}$$
故对加法、乘法封闭，$a\in\mathbb{F}_p$ 非零，则
$$(a^{-1})^q=(a^q)^{-1}=a^{-1}, \tag{4.20}$$
说明 $a^{-1}\in\mathbb{F}_q$，故 $\mathbb{F}_q$ 为包含 $\mathbb{F}_p$ 的 q 元域. 假设 F 也为 Ω_p 的 q 元域，则其中元素必然是多项式 x^q-x 的根，故 $F=\mathbb{F}_q$. 由于 $\Omega_p/\mathbb{F}_q,\mathbb{F}_q/\mathbb{F}_p$ 均为代数扩张，故 $\Omega_p/\mathbb{F}_p$ 为代数扩张，对任意 $a\in\Omega_p$，设 a 在 $\mathbb{F}_p$ 中的次数为 n，则 $\mathbb{F}_p(a)/\mathbb{F}_p$ 为 n 次扩张，因此 $\mathbb{F}_p(a)=\mathbb{F}_{p^n}$，故
$$\Omega_p=\bigcup_{n\geqslant 1}\mathbb{F}_{p^n}. \tag{4.21}$$
2. $|\mathbb{F}_q^*|=p^r-1=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ 且为 Abel 群，设有分解
$$\mathbb{F}_q^*=G_1\times\cdots\times G_s, \tag{4.22}$$
这里 G_i 为 $p_i^{\alpha_i}$ 阶群（也就是素因子 p_i 的不变因子分解的直和），也即对任意 $g\in G_i$ 有 $g^{p_i^{\alpha_i}}=1$，但是 $\mathbb{F}_q^*$ 中方程 $x^{p_i^{\alpha_i-1}}=1$ 至多有 $p_i^{\alpha_i-1}$ 个根，因此 G_i 中必有 $p_i^{\alpha_i}$ 阶元，故 $G_i\cong\mathbb{Z}_{p_i^{\alpha_i}}$，同理可证其余 G 也为循环群，并且 $G_1,\cdots,G_s$ 阶两两互素，因此 $\mathbb{F}_q^*$ 为循环群. 若设 $\mathbb{F}_q^*=\langle\alpha\rangle$，则
$$\mathbb{F}_q=\{0,1,\alpha,\alpha^2,\cdots,\alpha^{p^r-1}\}, \tag{4.23}$$
故 $\mathbb{F}_q=\mathbb{F}_p(\alpha)$.
3. 设 K 也为 q 元域，考虑其代数闭包 Ω'，则 K 也为 Ω' 中的唯一的，包含 $\mathbb{F}_p$ 的 q 元域，设 x^q-x 在 Ω' 中的根为 β，则 $\mathbb{F}_p(\beta)$ 是一个 Ω' 中的 q 元域，故 $K=\mathbb{F}_p(\beta)$，即有同构
$$K\cong\mathbb{F}_p[x]/(x^q-x)\cong\mathbb{F}_q, \tag{4.24}$$
得证.

4.1.2 分裂域

定义 4.8 (分裂域)

设 E/F 为扩域，$f(x)\in F[x]$，若 f 在 E 中的不可约因子均为一次多项式，则称 $f(x)$ 在 E 中分裂；若 $f(x)$ 在任何 E,F 的中间域中都不能分裂，则称 E 为 f 的分裂域.

定理 4.5

设 F 为域，$f(x)\in F[x]$ 为非常值多项式，则 f 存在分裂域，并且它们在同构意义下唯一.

证明 存在性：对 f 的次数归纳，$\deg f=1$ 的情形是平凡的. 设命题对所有 $\deg f<d$ 的 f 成立，则对 $\deg f=d$，存在域 B 使得 f 在 B 中有根 α_1，即 f 在 B 有分解 $f(x)=(x-\alpha_1)g(x)$，这里 $\deg g=d-1$，根据归纳假设，g（关于 B）存在分裂域 E_1，且在 E_1 中有分解

$$g(x)=(x-\alpha_2)\cdots(x-\alpha_k), \tag{4.25}$$

即 f 在 $B(\alpha_2,\cdots,\alpha_k)$ 中分裂，并且不能在更小的域中分裂（否则与 E_1 的极小性矛盾），故

$$B(\alpha_2,\cdots,\alpha_k)=F(\alpha_1,\cdots,\alpha_k) \tag{4.26}$$

为 f 的分裂域，得证.

在证明唯一性之前，先考虑一些分裂域的性质.

推论 4.4

设 E 为 $f(x)\in F[x]$ 的分裂域，则 E/F 为有限扩张，从而是代数扩张.

推论 4.5

设 $f(x)\in F[x]$ 为非常值多项式，E 为其分裂域，$\deg f=d$，则 $d|[E:F]$ 且 $[E:F]\leqslant d!$.

为了证明唯一性，需要考虑一些同构的延拓.

引理 4.1

设 $\sigma_0:F_1\to F_2$ 为一个域同构，$f_1(x)\in F_1[x]$ 不可约，$f_2(x)=\sigma_0(f(x))\in F_2[x]$，且 $E_i=F_i(\alpha_i),f(\alpha_i)=0$，则 σ_0 可以延拓为（或者说唯一诱导出）域同构 $\sigma:E_1\to E_2$ 的域同构，使得 $\sigma(\alpha_1)=\alpha_2$.

推论 4.6

设 $f(x)\in F[x]$ 不可约，α_1,α_2 为 f 的两个根，$E_i=F(\alpha_i)$，则存在唯一同构 $\sigma:E_1\to E_2$ 使得 $\sigma(\alpha_1)=\alpha_2,\sigma|_F=\mathrm{Id}$.

定理 4.6

设 $\sigma_0:F_1\to F_2$ 为一个域同构，$f_1(x)\in F_1[x]$ 不可约，$f_2(x)=\sigma_0(f(x))\in F_2[x]$，$E_1,E_2$ 分别为 f_1,f_2 的分裂域，则 σ_0 可以延拓为域同构 $\sigma:E_1\to E_2$.

证明 设 f_1 在 $F_1[x]$ 中分解为 k 个不可约因子之积，令 $d_F(f_1)=\deg f_1-k$，，当 $d_F(f_1)=0$ 时结论显然成立（这时 $E_i=F_i,\sigma=\sigma_0$），若 $d_F(f_1)>0$，则其存在次数大于 1 的不可约因子 $g_1(x)$，设 α_1,α_2 分别为 g_1,g_2 在 E_1,E_2 中的根，则根据延拓定理，σ_0 可以先延拓为域同构

$$\sigma_1:F_1(\alpha_1)\to F_2(\alpha_2),\sigma_1(\alpha_1)=\alpha_2, \tag{4.27}$$

设 $B_i=F_i(\alpha_i)$，则 $f_1(x)\in F[x]\subset B[x]$，这时 $d_B(f_1)<d_F(f_1)$，E_i 可以看作 $B_i[x]$ 上 f 的分裂域，因此由归纳假设，σ_1 可以延拓为域同构 $\sigma:E_1\to E_2$，得证.

推论 4.7

设 $f(x)\in F[x]$，则 f 的任何分裂域均相互同构.

4.2 正规、可分、Galois 扩张

定义 4.9 (正规扩张)

称代数扩张 E/F 为正规扩张，若任何在 E 中有根的多项式 $f(x)\in F[x]$ 都在 E 中分裂.

注 容易验证正规扩张的另一个等价定义：任意 $\alpha\in E$ 在 F 中的极小多项式 $m_\alpha(x)$ 在 E 中分裂.

定义 4.10 (可分性)

1. 称 $f(x)\in F[x]$ 为可分多项式，若其任意不可约因子都没有重根.
2. 设 E/F 为代数扩张，称 $\alpha\in E$ 为可分元，若其在 F 中的极小多项式 $m_\alpha(x)$ 可分.
3. 称代数扩张 E/F 为可分扩张，若任何 $\alpha\in E$ 都是可分元.

下面定义 Galois 理论的重要概念：Galois 群与固定子域.

定义 4.11 (Galois 群)

设 E/F 为代数扩张，定义该扩张的 Galois 群为

$$\mathrm{Gal}(E/F)=\{\sigma\in\mathrm{Aut}(E):\sigma|_F=\mathrm{Id}\}. \tag{4.28}$$

注 有时 $\mathrm{Gal}(E/F)$ 也记作 $\mathrm{Aut}_F(E)$，表示固定 F 中元素的 E 上的自同构.

定义 4.12 (固定子域)

设 E 为域，$G\leqslant\mathrm{Aut}(E)$，则定义该子群的固定子域为

$$\mathrm{Fix}(G)=\{u\in E:\sigma(u)=u,\forall\sigma\in G\}. \tag{4.29}$$

注 事实上，当 G 仅为 E 的子集时，作相同定义得到的 $\mathrm{Fix}(G)$ 也是一个域.

容易验证，Galois 群确实是一个子群，固定子域也确实是域. 另外由定义可以看出，Galois 群与固定子域存在互逆关系，它们有如下性质

命题 4.5

设 $F,F_1,F_2\leqslant E,G,G_1,G_2\leqslant\mathrm{Aut}(E)$，则

1. 若 $G_1\leqslant G_2$ 则 $\mathrm{Fix}(G_1)\geqslant\mathrm{Fix}(G_2)$；若 $F_1\leqslant F_2$ 则 $\mathrm{Gal}(E/F_1)\geqslant\mathrm{Gal}(E/F_2)$.
2. $F\leqslant\mathrm{Fix}(\mathrm{Gal}(E/F))$，$G\leqslant\mathrm{Gal}(E/\mathrm{Fix}(G))$.
3. $\mathrm{Gal}(E/\mathrm{Fix}(\mathrm{Gal}(E/F)))=\mathrm{Gal}(E/F)$，$\mathrm{Fix}(\mathrm{Gal}(E/\mathrm{Fix}(E/F)))=\mathrm{Fix}(E/F)$.

证明

1. 这是显然的.
2. 这是显然的.
3. 令 $G=\mathrm{Gal}(E/F)$，由 2 直接得到

$$\mathrm{Gal}(E/F)\leqslant\mathrm{Gal}(E/\mathrm{Fix}(\mathrm{Gal}(E/F))), \tag{4.30}$$

另一方面

$$F\leqslant\mathrm{Fix}(\mathrm{Gal}(E/F))\Rightarrow\mathrm{Gal}(E/F)\geqslant\mathrm{Gal}(E/\mathrm{Fix}(\mathrm{Gal}(E/F))), \tag{4.31}$$

故 $\mathrm{Gal}(E/\mathrm{Fix}(\mathrm{Gal}(E/F)))=\mathrm{Gal}(E/F)$，另一个同理.

当上面的不等式取等时，则称该扩张为 Galois 扩张.

定义 4.13 (Galois 扩张)

设 E/F 为代数扩张，若 $\mathrm{Fix}(\mathrm{Gal}(E/F)) = F$，则称 E 为 F 的 Galois 扩张. ♣

下面的目标是证明 Galois 基本定理（FTGT），它建立了扩张 E/F 中间域与 $G = \mathrm{Gal}(E/F)$ 的子群间的对应，架起了域论与群论之间的桥梁.

定义 4.14 (Galois 共轭集)

设 E/F 为代数扩张，$\alpha \in E$，则 $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(E/F)\}$ 称为 α 的 (Galois) 共轭集，其中元素称为 (Galois) 共轭元. ♣

引理 4.2

设 E/F 为代数扩张，$H = \{\sigma \in \mathrm{Gal}(E/F) : \sigma(\alpha) = \alpha\}$，则 $H \leqslant G = \mathrm{Gal}(E/F)$ 且 α 的共轭元的个数为 $[G : H]$. ♡

证明 显然 $H \leqslant G$，令 G 作用于 α 的共轭集上，则 H 恰好为 α 的稳定子群，且每个轨道对应一个共轭元，而轨道个数 $|O_\alpha| = [G : G_\alpha] = [G : H]$，得证.

引理 4.3

设 E/F 为 Galois 扩张，$\alpha \in E$，则 α 在 E 中共轭元个数有限，若设为 $\alpha = \alpha_1, \cdots, \alpha_r$，则 $m_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_r)$. ♡

证明 由于 $m_\alpha \in F[x]$，并且对任意 $\sigma \in \mathrm{Gal}(E/F)$，$\sigma(\alpha)$ 也为 m_α 的根，因此 α 的共轭元个数有限，并且 σ 实际上作了这些共轭元的一个置换. 设

$$n_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_r), \tag{4.32}$$

则 $\sigma(n_\alpha(x)) = n_\alpha(x)$，也即 σ 固定了 n_α 的每个系数，σ 的任意性说明 $\mathrm{Gal}(E/F)$ 固定 n_α 的系数，而 $\mathrm{Fix}(\mathrm{Gal}(E/F)) = F$ 说明 $n_\alpha(x) \in F[x]$. 并且每个 α_i 也都是 m_α 的根，因此 $x - \alpha_i | m_\alpha$，故 $n_\alpha | m_\alpha$，根据 m_α 的极小性可知 $n_\alpha = m_\alpha$，得证.

推论 4.8

设 E/F 为 Galois 扩张，$\alpha \in E$，则 $[F(\alpha) : F]$ 等于 α 在 E 中的共轭元个数. ♡

证明 注意到 $[F(\alpha) : F] = \deg m_\alpha$，根据上一条引理即得.

下面的定理给出了有限扩张情形下的重要结论.

定理 4.7

设 E/F 为有限扩张，则下述命题等价：

1. E/F 为 Galois 扩张.
2. E/F 为正规可分扩张.
3. E 为某个可分多项式 $f(x) \in F[x]$ 的分裂域.

♡

证明 $1 \Rightarrow 2$：对任意 $\alpha \in E$，根据前述引理有 $m_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_r)$，这里 $\alpha_1, \cdots, \alpha_r$ 为 α 的共轭元，因此 m_α 分裂且无重根，即 E/F 为正规可分扩张.

$2 \Rightarrow 3$：设 $E = F(\beta_1, \cdots, \beta_m)$，$f(x) = m_{\beta_1}(x) \cdots m_{\beta_m}(x)$，则 f 可分（其任何不可约因子都是某个 m_{β_k} 的因子，由扩张的可分性即得），并且 E 恰好为 f 的分裂域（f 分裂当且仅当每个 m_{β_k} 分裂），得证.

$3 \Rightarrow 1$：对 $[E : F]$ 归纳，当 $[E : F] = 1$ 时 $E = F, \mathrm{Gal}(E/F) = \{\mathrm{Id}\}$，$E/F$ 显然为 Galois 扩张. 设 $[E : F] < n$

的扩张均为 Galois 扩张，考虑 $[E:F]=n$ 的情形. 设 E 为可分多项式 $f(x)\in F[x]$ 的分裂域，作不可约分解

$$f(x)=f_1(x)\cdots f_k(x), f_i(x)\in F[x], \tag{4.33}$$

并不妨设 $\deg f_1>1$，$\alpha=\alpha_1$ 为 f_1（在 E 中）的一个根，则 $f_1(x)\in F[x]$ 为 α 的极小多项式（因为不可约），f 的可分性保证 f_1 的根 $\alpha_1,\cdots,\alpha_r$ 两两不同，并且 f_1 同时为每一个 α_i 的极小多项式，根据延拓定理，对每个 α_i，Id_F 可以延拓为同构

$$\sigma_i:F(\alpha_1)\to F(\alpha_i),\quad \sigma(\alpha_1)=\alpha_i, \tag{4.34}$$

而 E 可以看作每个 $F(\alpha_i)$ 的代数扩张，因此 σ_i 可以进一步延拓为 E 的自同构，仍记为 σ_i，则 $\sigma_i\in\mathrm{Gal}(E/F)$. 注意到 $[E:F(\alpha)]<[E:F]$，根据归纳假设，$E/F(\alpha)$ 为 Galois 扩张，即

$$F(\alpha)=\mathrm{Fix}(\mathrm{Gal}(E/F(\alpha)))\Rightarrow B=\mathrm{Fix}(\mathrm{Gal}(E/F))\leqslant\mathrm{Fix}(\mathrm{Gal}(E/F(\alpha)))=F(\alpha), \tag{4.35}$$

下证 $B=F$，根据固定子域的性质可知 $F\leqslant B$，而 $B\leqslant F(\alpha)$ 说明 $B(\alpha)=F(\alpha)$. 设 $\tilde{m}_\alpha(x)\in B[x]$ 为 α 在 B 中的极小多项式，则 $\tilde{m}_\alpha|m_\alpha=(x-\alpha_1)\cdots(x-\alpha_r)$，前面得到的 $\sigma_i\in\mathrm{Gal}(E/F)$ 满足 $\sigma_i(\alpha)=\alpha_i$，根据固定子域的定义有

$$\sigma_i|_B=\mathrm{Id}_B\Rightarrow\sigma_i\in\mathrm{Gal}(E/B)\Rightarrow\tilde{m}_\alpha(\alpha_i)=\sigma_i(\tilde{m}_\alpha(\alpha))=0, \tag{4.36}$$

即 $x-\alpha_i|\tilde{m}_\alpha(x)$，因此 $m_\alpha|\tilde{m}_\alpha$，即 $m_\alpha=\tilde{m}_\alpha$，这说明

$$[F(\alpha):F]=\deg m_\alpha=\deg\tilde{m}_\alpha=[B(\alpha):B]=[F(\alpha):B], \tag{4.37}$$

故 $F=B$，得证.

4.3 Galois 基本定理

本节将证明首个重要定理：Galois 基本定理，首先作一些准备工作.

定义 4.15 (特征标 (character))

群 G 到域 F 的乘群中的同态 $\sigma:G\to F^*$ 称为 G 在 F 中的特征标.

♣

注 特别当 $G=F^*$ 时，F^* 在 F 上的特征标包括了 F 的自同态.

定义 4.16 (相关性)

称一组特征标 $\sigma_1,\cdots,\sigma_n$ 线性相关，若存在不全为零的 $a_1,\cdots,a_n\in F$ 使得 $a_1\sigma_1+\cdots+a_n\sigma_n=0$（这里的 0 表示将所有 $g\in G$ 映为 $0\in F$ 的映射，注意它不是 G 的一个特征标），反之称其无关.

♣

定理 4.8 (Dirichlet)

设 $\sigma_1,\cdots,\sigma_n$ 为 G 在 F 中两两不同的特征标，则它们线性无关.

♡

证明 对 n 归纳，当 $n=1$ 时命题显然成立，设命题对小于 n 的情形均成立，考虑 n 的情形，设 $a_1\sigma_1+\cdots+a_n\sigma_n=0$，只需证明每个 a_i 均为 0，若不然，不妨设 $a_1\neq0$，由于这些 σ_i 两两不同，因此存在 $x\in G$ 使得 $\sigma_1(x)\neq\sigma_n(x)$，而对任意 $y\in G$ 有

$$a_1\sigma_1(y)+\cdots+a_n\sigma_n(y)=0, \tag{4.38}$$

$$a_1\sigma_1(xy)+\cdots+a_n\sigma_n(xy)=a_1\sigma_1(x)\sigma_1(y)+\cdots+a_n\sigma_n(x)\sigma_n(y) \tag{4.39}$$

$$=0, \tag{4.40}$$

对上式乘 $\sigma_n(x)$，与下式相减即得

$$a_1(\sigma_1(x)-\sigma_n(x))\sigma_1(y)+\cdots+a_{n-1}(\sigma_{n-1}(x)-\sigma_n(x))\sigma_{n-1}(y)=0, \tag{4.41}$$

根据归纳假设，$\sigma_1,\cdots,\sigma_{n-1}$ 线性无关，因此上面的系数均为 0，即得 $a_1(\sigma_1(x)-\sigma_n(x))=0$，矛盾，故 $\sigma_1,\cdots,\sigma_n$ 线性无关.

定理 4.9

设 $\Sigma=\{\sigma_1,\cdots,\sigma_n\}$ 为由域 E 的自同构构成的有限群，令 $F=\mathrm{Fix}(\Sigma)$，则 $[E:F]=n$，也即 $[E:\mathrm{Fix}(\Sigma)]=|\Sigma|$.

证明 设 $r=[E:F]$，我们将分别证明 $n\leqslant r$ 和 $n\geqslant r$.

Step 1. 若 $r<n$，则取 E/F 的基 $e_1,\cdots,e_r$，此时线性方程组

$$\begin{cases}a_1\sigma_1(e_1)+\cdots+a_n\sigma_n(e_1)=0\\ \cdots\\ a_1\sigma_1(e_r)+\cdots+a_n\sigma_n(e_r)=0\end{cases}\tag{4.42}$$

有非零解 $(a_1,\cdots,a_n)$，对任意 $e=\sum_{k=1}^r b_ke_k\in E$（$b_k\in F$）有

$$\sum_{i=1}^n a_i\sigma_i(e)=\sum_{i=1}^n a_i\sum_{k=1}^r b_k\sigma_i(e_k)\tag{4.43}$$

$$=\sum_{k=1}^r b_k\sum_{i=1}^n a_i\sigma_i(e_k)\tag{4.44}$$

$$=0,\tag{4.45}$$

故 $a_1\sigma_1+\cdots+a_n\sigma_n=0$，与 Dirichlet 定理矛盾，故 $n\leqslant r$.

Step 2. 若 $r>n$，由于 Σ 为群，故不妨设 $\sigma_1=\mathrm{Id}_E$，取 E 中的 F-线性无关组 $e_1,\cdots,e_{n+1}$，则方程

$$\begin{cases}a_1\sigma_1(e_1)+\cdots+a_{n+1}\sigma_1(e_{n+1})=0\\ \cdots\\ a_1\sigma_n(e_1)+\cdots+a_{n+1}\sigma_n(e_{n+1})=0\end{cases}\tag{4.46}$$

有非零解，设 $(a_1,\cdots,a_{n+1})$ 为所有非零解中具有最少非零元者，不妨设其中仅 $a_1,\cdots,a_s$ 不为 0，再不妨设 $a_s=1$，这里 a_i 并不全在 F 中（否则 $e_1,\cdots,e_n$ 线性相关，与前面 $n+1$ 元组的无关性矛盾），因此不妨设 $a_1\notin F$，则有

$$a_1\sigma_i(e_1)+\cdots+\sigma_i(e_s)=0,\quad\forall 1\leqslant i\leqslant n,\tag{4.47}$$

$a_1\notin F=\mathrm{Fix}(\Sigma)$ 说明存在 $\sigma_k\in\Sigma$ 使得 $\sigma_k(a_1)\neq a_1$，而 Σ 群的性质说明存在 σ_j 使得 $\sigma_j=\sigma_k\circ\sigma_i$，因此用 σ_k 作用上式可得

$$\sigma_k(a_1)\sigma_j(e_1)+\cdots+\sigma_j(e_s)=0,\quad\forall 1\leqslant j\leqslant n,\tag{4.48}$$

将上面两组等式中下标对应的等式相减即得

$$(a_1-\sigma_k(a_1))\sigma_i(e_1)+\cdots+(a_{s-1}-\sigma_k(a_{s-1}))\sigma_i(e_{s-1})=0,\quad\forall 1\leqslant i\leqslant n,\tag{4.49}$$

若设 $b_i=a_i-\sigma_k(a_i)$，则 $(b_1,b_2,\cdots,b_{s-1},0,\cdots,0)$ 为前面方程的非零解，且具有更少的非零元，矛盾.

推论 4.9

1. 若有限群 $G\leqslant\mathrm{Aut}(E)$，则 $\mathrm{Gal}(E/\mathrm{Fix}(G))=G$.
2. 设 $G_1,G_2\leqslant\mathrm{Aut}(E)$ 且不相同，则 $\mathrm{Fix}(G_1),\mathrm{Fix}(G_2)$ 也不相同.

证明

1. 根据定义显然有 $G\leqslant\mathrm{Gal}(E/\mathrm{Fix}(G))$，反之假设存在 $\sigma\in\mathrm{Gal}(E/\mathrm{Fix}(G)),\sigma\notin G$，则根据前面的定理（以及其前一半结论）可得

$$n=|G|=[E:\mathrm{Fix}(G)]\geqslant[E:\mathrm{Fix}(G\cup\{\sigma\})]\geqslant|G\cup\{\sigma\}|=n+1,\tag{4.50}$$

矛盾.

2. 注意到 $G_i = \mathrm{Gal}(E/\mathrm{Fix}(G_i))$，则

$$\mathrm{Fix}(G_1) = \mathrm{Fix}(G_2) \Leftrightarrow \mathrm{Gal}(E/\mathrm{Fix}(G_1)) = \mathrm{Gal}(E/\mathrm{Fix}(G_2)) \Leftrightarrow G_1 = G_2, \tag{4.51}$$

即得.

引理 4.4

设 $H \leqslant G \leqslant \mathrm{Aut}(E)$，$\sigma \in G$，则 $\sigma(\mathrm{Fix}(H)) = \mathrm{Fix}(\sigma H \sigma^{-1})$.

♡

证明 显然 $\sigma(\mathrm{Fix}(H)) \leqslant \mathrm{Fix}(\sigma H \sigma^{-1})$，而对任意 $a \in \mathrm{Fix}(\sigma H \sigma^{-1}), h \in H$，都有

$$\sigma h \sigma^{-1}(a) = a \Leftrightarrow h(\sigma^{-1}(a)) = \sigma^{-1}(a) \tag{4.52}$$

故 $\sigma^{-1}(a) \in \mathrm{Fix}(H), a \in \sigma(\mathrm{Fix}(H))$，即得 $\mathrm{Fix}(\sigma H \sigma^{-1}) \subset \sigma(\mathrm{Fix}(H))$，得证.

定理 4.10 (Galois 基本定理 (FTGT))

设 E/F 为有限 Galois 扩张，$G = \mathrm{Gal}(E/F)$，则

1. E/F 的中间域 B 与 G 的子群 G_B 之间存在一一对应：$B = \mathrm{Fix}(G_B), G_B = \mathrm{Gal}(E/B)$.
2. 设 $E \supset B \supset F$，则 B/F 为正规扩张当且仅当 $G_B \triangleleft G$，并且此时 B/F 为 Galois 扩张，$\mathrm{Gal}(B/F) \cong G/G_B = \mathrm{Gal}(E/F)/\mathrm{Gal}(E/B)$.
3. 对每个中间域 B，$[B:F] = [G:G_B]$ 且 $[E:B] = |G_B|$.

♡

证明

1. 对任意 $H \leqslant G$，Fix 给出了一个映射

$$\Gamma : \{G\text{的子群}\} \longrightarrow \{E/F\text{中间域}\}, \tag{4.53}$$

前面证明过 $\mathrm{Fix}(H_1) = \mathrm{Fix}(H_2)$ 当且仅当 $H_1 = H_2$，因此 Γ 为单射，另外对任意中间域 B，$\mathrm{Gal}(E/B) \leqslant G$，而 E/F 为 Galois 扩张说明 E/B 为 Galois 扩张，因此 $B = \mathrm{Fix}(\mathrm{Gal}(E/B))$，故 Γ 为满射. 综上所述，即建立了子群与中间域的一一对应.

2. 若 $G_B \triangleleft G$，则根据上一条引理，对任意 $\sigma \in G$ 有

$$\sigma(B) = \mathrm{Fix}(\sigma G_B \sigma^{-1}) = \mathrm{Fix}(G_B) = B, \tag{4.54}$$

因此对任意 $\alpha \in B, m_\alpha(x) \in F[x]$，$\sigma(\alpha) \in B$，$E/F$ 的正规性说明 m_α 的根 $\alpha = \alpha_1, \cdots, \alpha_r \in E$，根据延拓定理，对每个 α_i，Id_F 可以延拓为同构

$$\sigma_i : F(\alpha_1) \to F(\alpha_i), \quad \sigma_i(\alpha_1) = \alpha_i, \tag{4.55}$$

因此 $\alpha_i = \sigma_i(\alpha_1) \in B$，故这 r 个根均在 B 中，即 B/F 为正规扩张.

进一步，$\sigma(B) = B$ 实际上诱导出了一个良定的群同态

$$\mathcal{R} : \mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(B/F) \tag{4.56}$$

$$\sigma \longmapsto \sigma|_B \tag{4.57}$$

显然 $\mathcal{R}$ 为满射，并且

$$\mathrm{Ker}\,\mathcal{R} = \{\sigma : \sigma|_B = \mathrm{Id}_B\} = \mathrm{Gal}(E/B) = G_B, \tag{4.58}$$

因此根据同态基本定理可得

$$G/G_B = \mathrm{Gal}(E/F)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/F). \tag{4.59}$$

反之若 B/F 为 Galois 扩张，则 B 必然为某个可分多项式 $f(x) \in F[x]$ 的分裂域，设 $\beta_1, \cdots, \beta_r$ 为 f 的根，则 $B = F(\beta_1, \cdots, \beta_r)$.$f \in F[x]$ 说明对任意 $\sigma \in G$ 有 $\sigma(f(x)) = f(x)$，因此 σ 作了这 r 个根的置换，这也说明了 $\sigma(B) = B$，根据上一条引理有 $\mathrm{Fix}(\sigma G_B \sigma^{-1}) = \mathrm{Fix}(G_B)$，因此 $G_B = \sigma G_B \sigma^{-1}$，即 $G_B \triangleleft G$.

3. E/F 为 Galois 扩张说明 E/B 为 Galois 扩张，因此

$$B = \mathrm{Fix}(\mathrm{Gal}(E/B)) \Rightarrow [E:B] = |\mathrm{Gal}(E/B)| = |G_B|, \tag{4.60}$$

而另一方面 $[E:F] = [E:B][B:F], |G| = |G_B|[G:G_B]$，因此 $[B:F] = [G:G_B]$.

对于两个中间域，可以定义共轭的概念，并且这种概念很好的反映到了群的共轭上.

定义 4.17 (共轭)

设 E/F 为代数扩张，则称两个中间域 B_1, B_2 共轭，若存在 $\sigma \in \mathrm{Gal}(E/F)$ 使得 $\sigma(B_1) = B_2$.

命题 4.6

设 E/F 为有限 Galois 扩张，则两个中间域 B_1, B_2 共轭当且仅当 G_{B_1}, G_{B_2} 共轭，特别的，B 的共轭类仅有一个元素当且仅当 $G_B \triangleleft G$.

下面延续 FTGT，讨论一些结论.

定义 4.18

设 E/F 为 Galois 扩张，B 为中间域，设 $Q_B = \{\sigma : B \to B' \text{为同构} : E/B'/F, \sigma|_F = \mathrm{Id}_F\}$，由于任意 $\sigma_0 \in Q_B$ 可以延拓为 $\sigma \in \mathrm{Gal}(E/F)$，因此可以定义映射

$$\Lambda : Q_B \longrightarrow \{\sigma G_B : \sigma \in G\} \tag{4.61}$$

$$\sigma_0 \longmapsto [\sigma] = \sigma G_B \tag{4.62}$$

命题 4.7

1. 上面定义的映射 Λ 为良定的双射.
2. $\mathrm{Gal}(B/F) = Q_B$ 当且仅当 $G_B \triangleleft G$，或者说 B/F 为 Galois 扩张，这时 $\Lambda : Q_B \to G/G_B$ 为群同构.

证明

1. 首先证明良定性，设 σ_0 有两种延拓 σ, σ'，则它们在 B 上的限制均为恒同映射，也即 $\sigma^{-1} \circ \sigma'|_B = \mathrm{Id}_B$，因此 $\sigma^{-1} \circ \sigma' \in G_B$，也即 $[\sigma] = [\sigma']$，得证.

   再证明 Λ 为双射，$\Lambda(\sigma_0) = \Lambda(\tau_0)$ 当且仅当 $\tau^{-1}\sigma \in G_B$，即

$$\tau^{-1} \circ \sigma|_B = \mathrm{Id}_B \Rightarrow \sigma|_B = \tau|_B \Rightarrow \sigma_0 = \tau_0, \tag{4.63}$$

   故 Λ 为单射，对任意 $\sigma \in G$，$\sigma_0 = \sigma|_B$ 都为同构，因此 $\Lambda(\sigma_0) = [\sigma]$，即 Λ 为满射，得证.
2. $\mathrm{Gal}(B/F) = Q_B$ 当且仅当对任意 $\sigma_0 \in Q_B$，$\sigma_0(B) = B$，即 $G_B \triangleleft G$，这当然也等价于 B/F 为 Galois 扩张.G_B 的正规性说明

$$\Lambda(\tau\sigma) = \tau\sigma G_B = (\tau G_B)(\sigma G_B) = \Lambda(\tau)\Lambda(\sigma), \tag{4.64}$$

   即 Λ 为同构.

命题 4.8

设 E/F 为 Galois 扩张，B_1, B_2 为中间域，则

1. $B_1B_2 = \mathrm{Fix}(G_{B_1} \cap G_{B_2})$.
2. $B_1 \cap B_2 = \mathrm{Fix}(\langle G_{B_1}, G_{B_2} \rangle)$.

证明

1. $\sigma \in G_{B_1} \cap G_{B_2}$ 说明 $\sigma|_{B_1} = \mathrm{Id}_{B_1}, \sigma|_{B_2} = \mathrm{Id}_{B_2}$，因此 $\sigma|_{B_1B_2} = \mathrm{Id}|_{B_1B_2}$；反之若 σ 固定 B_1B_2，则它显然固定 B_1, B_2，即 $\sigma \in G_{B_1} \cap G_{B_2}$，因此

$$\mathrm{Gal}(E/(B_1B_2)) = G_{B_1} \cap G_{B_2} \Rightarrow B_1B_2 = \mathrm{Fix}(G_{B_1} \cap G_{B_2}). \tag{4.65}$$

2. 对任意 $\beta \in B_1 \cap B_2$，它必然被所有 $\sigma \in G_{B_1} \cup G_{B_2}$ 固定，因此 $\beta \in \mathrm{Fix}(\langle G_{B_1}, G_{B_2}\rangle)$；另一方面对任意 $\beta \in \mathrm{Fix}(\langle G_{B_1}, G_{B_2}\rangle)$，它必然被 G_{B_1}, G_{B_2} 固定，因此

$$\beta \in \mathrm{Fix}(G_{B_1}) \cap \mathrm{Fix}(G_{B_2}) = B_1 \cap B_2. \tag{4.66}$$

得证.

命题 4.9

设 E/F 为 Galois 扩张，则 E 是某个可分多项式 $f(x) \in F[x]$ 的分裂域，而 $G = \mathrm{Gal}(E/F)$ 同构于 $f(x)$ 的根的一个置换群. 特别当 f 不可约时，G 同构于 $f(x)$ 根的一个可迁置换群.

♠

注 称 G 在集合 S 上的作用是可迁的，若对任意 $s_i, s_j \in S$，存在 $\sigma \in G$ 使得 $\sigma(s_i) = s_j$，或者说 S 中所有元素均在同一轨道上.

证明 设 $\alpha_1, \cdots, \alpha_d \in E$ 为 f 的根，则对任意 $\sigma \in \mathrm{Gal}(E/F)$，$\sigma(\alpha_i)$ 也为 f 的根，故 $\mathrm{Gal}(E/F)$ 实际上置换了这些根. 若 f 不可约，则每个 $\alpha_i \notin F$，因此同构 $\sigma_0 : F(\alpha_i) \to F(\alpha_j), \sigma_0(\alpha_i) = \alpha_j, \sigma_0|_F = \mathrm{Id}_F$ 可以延拓为 E 的自同构 $\sigma \in \mathrm{Gal}(E/F)$，故作用是可迁的.

推论 4.10

设 E 为可分多项式 $f(x) \in F[x]$ 的分裂域，其不可约分解为 $f(x) = f_1(x)^{e_1} \cdots f_k(x)^{e_k}$，设 $\deg f_i = d_i$，则 $\mathrm{Gal}(E/F)$ 同构于 $S_{d_1} \times \cdots \times S_{d_k}$ 的某个子群. 特别地若设 $\deg f = d$，则 $\mathrm{Gal}(E/F)$ 同构于 S_d 的某个子群.

♡

定理 4.11

设 E/F 为 d 次 Galois 扩张，则 $G = \mathrm{Gal}(E/F)$ 同构于 S_d 的某个可迁子群，并且 G 有子群 H 使得 $[G : H] = d$.

♡

证明 这里先使用后面将证明的结论：有限可分扩张必为单扩张，则存在 $\alpha \in E$ 使得 $E = F(\alpha)$，并且 E 为不可约多项式 $m_\alpha(x)$ 的分裂域，而 $d = [E : F] = [F(\alpha) : F] = \deg m_\alpha(x)$，故 $\mathrm{Gal}(E/F)$ 同构于 S_d 的某个可迁子群.

4.4 Galois 理论的应用

4.4.1 对称函数与对称群

设 D 为域，则 $E = D(x_1, \cdots, x_d)$ 表示其上的 d 元有理函数域，而其中在 S_d 作用下不变的元素构成对称函数域.

定义 4.19 (对称函数域)

E 在 S_d 作用下的固定子域称为 d 元对称函数域，即

$$F = \mathrm{Fix}(S_d) = \{f(x_1, \cdots, x_d) \in E : f(x_{\sigma(1)}, \cdots, x_{\sigma(d)}) = f(x_1, \cdots, x_d), \forall \sigma \in S_d\}. \tag{4.67}$$

F 中的多项式称为对称多项式.

♣

根据定义 $F = \mathrm{Fix}(S_d)$，而 $S_d \leqslant \mathrm{Aut}(E)$ 说明 $\mathrm{Gal}(E/\mathrm{Fix}(S_d)) = S_d$，因此 $F = \mathrm{Fix}(\mathrm{Gal}(E/F))$，$E/F$ 为 Galois 扩张，借助这一观察可以给出如下命题.

引理 4.5

1. 设 G 为有限群，则存在 Galois 扩张 E/B 使得 $\mathrm{Gal}(E/B) \cong G$.
2. 存在 Galois 扩张 E/B 使得 $\mathrm{Gal}(E/B) \cong G$，这里 E, B 为 $\mathbb{C}$ 的子域.

♡

证明

1. 设 $|G|=d$, 根据 Caylay 定理, G 同构于某个置换群(即 S_d 的子群), 因此取 $E=D(x_1,\cdots,x_d)$, $B=\mathrm{Fix}(G)$, 则 E/B 为 Galois 扩张且 $\mathrm{Gal}(E/B)\cong G$.
2. 设 $D=\mathbb{Q}$, $t_1,\cdots,t_d$ 为 $\mathbb{C}$ 中线性无关的超越元, 则 $\mathbb{Q}(x_1,\cdots,x_d)\cong\mathbb{Q}(t_1,\cdots,t_d)$, 令 $E=\mathbb{Q}(t_1,\cdots,t_d)$, $B=\mathrm{Fix}(G)$ 可得 E/B 正规以及 $\mathrm{Gal}(E/B)\cong G$.

定义 4.20 (基本对称多项式)

基本对称多项式 $s_1,\cdots,s_d\in D(x_1,\cdots,x_d)$ 定义为

$$s_k=\sum_{1\leqslant i_1<\cdots<i_k\leqslant d}x_{i_1}\cdots x_{i_k},\quad k=1,2,\cdots,d. \tag{4.68}$$

♣

例 4.2 当 $d=4$ 时

$$s_1=x_1+x_2+x_3+x_4, \tag{4.69}$$

$$s_2=x_1x_2+x_1x_3+x_2x_3+x_2x_4+x_3x_4, \tag{4.70}$$

$$s_3=x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4, \tag{4.71}$$

$$s_4=x_1x_2x_3x_4. \tag{4.72}$$

可以证明, 任何对称函数都能由对称多项式表示, 即

引理 4.6

d 元对称函数域 $F=D(s_1,\cdots,s_d)$.

♡

证明 设 $B=D(s_1,\cdots,s_d)\subset F$, 由于每个 s_i 都被 S_d 固定, 由于 $[E:F]=|S_d|=d!$, 故 $[E:B]\geqslant d!$, 由于 E 为可分 d 次多项式

$$f(x)=(x-x_1)\cdots(x-x_d), \tag{4.73}$$

的分裂域, 因此 $[E:B]=|\mathrm{Gal}(E/B)|\leqslant d!$, 即得 $[E:B]=d!, F=B$.

引理 4.7

设单项式 $y=x_2^1x_3^2\cdots x_d^{d-1}$, 则 $E=F(y)$.

♡

证明 由于 S_d 中固定 $F(y)$ 的只有恒同映射, 因此 $|\mathrm{Gal}(E/F(Y))|=1$, 由 FTGT 可得

$$[F(y):F]=[S_d:\mathrm{Gal}(E/F(Y))]=d!=[E:F], \tag{4.74}$$

因此 $E=F(Y)$.

推论 4.11

任何 $f(x_1,\cdots,x_d)\in E$ 可以唯一表示为

$$f(x_1,\cdots,x_d)=\sum_{i=0}^{d!-1}g_i(s_1,\cdots,s_d)y^i, \tag{4.75}$$

其中 $y=x_2^1x_3^2\cdots x_d^{d-1}$, $g_i(s_1,\cdots,s_d)$ 为关于 $s_1,\cdots,s_d$ 的有理函数.

♡

引理 4.8

设单项式 $y=x_2^1x_3^2\cdots x_d^{d-1}$, 并定义 $y_\sigma=x_{\sigma(2)}^1\cdots x_{\sigma(d)}^{d-1}$, 则 $\{y_\sigma:\sigma\in S_d\}$ 为 E/F 的一组基.

♡

证明 由于这一组元素有 $d!$ 个, 因此只需证明其线性无关. 对 d 归纳, $d=1$ 时命题显然成立, 假设对 $d-1$ 成立,

考虑 d 的情形，设

$$\sum_{\sigma\in S_d} c_\sigma(x_1,\cdots,x_d)y_\sigma = 0, \tag{4.76}$$

其中 $c_\sigma(x_1,\cdots,x_d)\in F$，通过去分母，可以设每个 c_σ 均为多项式且无公因子. 设

$$H_i = \{\sigma\in S_d : \sigma(i)=i\}, i=1,2,\cdots,d, \tag{4.77}$$

记前面的和为 S，则有分解 $S = S_1+\cdots+S_d$，其中

$$S_i = \sum_{\sigma\in H_i} c_\sigma(x_1,\cdots,x_d)y_\sigma, \tag{4.78}$$

而每个 $S_i = S_i' + S_i''$，记 $H_i' = \{\sigma\in H_i : x_i\nmid c_\sigma\}, H_i'' = \{\sigma\in H_i : x_i | c_\sigma\}$ 则

$$S_i' = \sum_{\sigma\in H_i'} c_\sigma(x_1,\cdots,x_d)y_\sigma,\quad S_i'' = \sum_{\sigma\in H_i''} c_\sigma(x_1,\cdots,x_d)y_\sigma, \tag{4.79}$$

考虑 S 中 x_1 的次数，除 S_1 外，每项中 x_1 的次数至少为 1，因此

$$S_1' = \sum_{\sigma\in H_1'} c_\sigma(x_1,\cdots,x_d)y_\sigma = 0, \tag{4.80}$$

而上面的每个求和项都不含 x_1，因此可令 $x_1=0$ 得到

$$0 = \sum_{\substack{\sigma\in H_1\\ x_1\nmid c_\sigma}} c_\sigma(0,x_2,\cdots,x_d)y_\sigma \tag{4.81}$$

$$= \left(\sum_{\substack{\sigma\in H_1\\ x_1\nmid c_\sigma}} c_\sigma(0,x_2,\cdots,x_d)x_{\sigma(3)}\cdots x_{\sigma(d)}^{d-2}\right) x_{\sigma(2)}\cdots x_{\sigma(d)}, \tag{4.82}$$

根据归纳假设，$\{x_{\sigma(3)}\cdots x_{\sigma(d)}^{d-2}\}$ 为 $D(x_2,\cdots,x_d)/\tilde{F}$ 的一组基，因此这里的每个 $c_\sigma(0,x_2,\cdots,x_d)=0$，而它们赋值前都不含 x_1 因子，因此 $c_\sigma(x_1,\cdots,x_d)=0$，也即 $H_1'=\emptyset, H_1''=H_1$，类似可得 $H_i'=\emptyset, H_i''=H_i$.

考虑和 S_1''，其中每个 c_σ 都被 x_1 整除，而它为对称多项式，因此也被 $x_2,\cdots,x_d$ 整除，也即它们都整除 $x_1,\cdots,x_d$，这对 $S_2'',\cdots,S_d''$ 亦然，这说明所有的 c_σ 有公因子 $x_1\cdots x_d$，这与一开始的选取矛盾，得证.

由于 $F = D(s_1,\cdots,s_d)$，并且 E 中元素可被 $\{y_\sigma\}$ 线性表示，因此可得推论

推论 4.12

任何 $f(x_1,\cdots,x_d)\in E$ 可唯一表示为

$$f(x_1,\cdots,x_d) = \sum_{\sigma\in S_d} h_\sigma(s_1,\cdots,s_d)y_\sigma, \tag{4.83}$$

其中 $y_\sigma = x_{\sigma(2)}^1\cdots x_{\sigma(d)}^{d-1}$，$h_\sigma\in D(s_1,\cdots,s_d)$.

♡

我们已经证明了 $F = D(s_1,\cdots,s_d)$，因此 F 中的元素可以被基本对称多项式表示，事实上这种表示是唯一且“直接”的.

定理 4.12

对任意 $f(x_1,\cdots,x_d)\in F$，存在唯一 $e(s_1,\cdots,s_d)\in D(s_1,\cdots,s_d)$ 使得 $f(x_1,\cdots,x_d)=e(s_1,\cdots,s_d)$.

♡

注 这一命题在已有结论 $F = D(s_1,\cdots,s_d)$ 下并不是平凡的，因为还没有证明 $s_1,\cdots,s_d$ 是线性无关的.

证明

上面的结论可以加强

定理 4.13

对任意多项式 $f(x_1,\cdots,x_d)\in F$，存在唯一 $e(s_1,\cdots,s_d)\in D[s_1,\cdots,s_d]$ 使得 $f(x_1,\cdots,x_d) = e(s_1,\cdots,s_d)$.

♡

证明

最后以 Newton 公式结尾：

定理 4.14 (Newton 恒等式)

设 $s_1,\cdots,s_d$ 为基本对称多项式，$t_i=x_1^i+\cdots+x_d^i$，则对任意 $k=1,2,\cdots$ 有

$$t_k-s_1t_{k-1}+s_2t_{k-2}+\cdots+(-1)^{k-1}s_{k-1}t_1+(-1)^k ks_k=0. \tag{4.84}$$

♡

4.4.2 可分扩张

本小节继续讨论可分扩张，首先是关于多项式单根的一些命题.

引理 4.9

设 E/F 为域扩张，$\alpha\in E$ 为代数元，$f(x)\in F[x]$ 非零且 $f(\alpha)=0$，则 α 为 f 的单根当且仅当 $f(\alpha)=0,f'(\alpha)\neq 0$.

♡

证明 设 $f(x)=(x-\alpha)g(x)$，则 $f'(x)=(x-\alpha)g'(x)+g(x)$，即 $f'(\alpha)=g(\alpha)$，因此若 α 为 f 的单根，则 $f'(\alpha)=g(\alpha)\neq 0$；反之若 $f'(\alpha)\neq 0$ 则 $g(\alpha)\neq 0$，因此 $x-\alpha\nmid g(x)$，即 α 为 f 的单根.

命题 4.10

设 $f(x)\in F[x]$ 不可约，若 $f'(x)\neq 0$，则 $f(x)$ 可分. 进一步有

1. 若 $\operatorname{char}F=0,f(x)\in F[x]$ 不可约且 $f'(x)\neq 0$，则 f 可分.
2. 若 $\operatorname{char}F=p,f(x)\in F[x]$ 不可约，则 f 可分（$f'(x)\neq 0$）或存在 $g(x)\in F[x]$ 使得 $f(x)=g(x^p)$.

♠

证明 设 E 为 f 的分裂域，$\alpha\in E$ 为 f 的根，则 f 不可约说明 $f(x)=m_\alpha(x)$，并且 $f'(\alpha)\neq 0$（否则与极小性矛盾），故 α 为 f 的单根，因此 f 可分.$\operatorname{char}F=p$ 的情形也是显然的.

回忆定义，称 E/F 称为**可分扩张**，若对任意 $\alpha\in E$，$m_\alpha(x)\in F[x]$ 均可分，借助上面的命题可得

推论 4.13

若 $\operatorname{char}F=0$，则 F 的任何代数扩张均可分.

♡

证明 设 E/F 为代数扩张，则对任意 $\alpha\in E$，$m_\alpha(x)\in F[x]$ 无重根，因此 E/F 可分.

定义 4.21 (完全域 (perfect field))

称域 F 为完全域，若其任何代数扩张均为可分扩张.

♣

前面的推论说明，任何零特征域均为完全域，下面给出一个 p 特征域的完全性判别法，首先考虑一个引理.

引理 4.10

设 $\operatorname{char}F=p$，$a\in F,a\notin F^p$，则对任意 $t\geqslant 1$，$f(x)=x^{p^t}-a\in F[x]$ 不可约.

♡

证明 作不可约分解 $f(x)=g_1(x)\cdots g_k(x)\in F[x]$，设 $g_1(\alpha)=0,E=F(\alpha)$，则 $g_1(x)=m_\alpha(x)$，进一步

$$f(x)=x^{p^t}-a=(x-\alpha)^{p^t}\in E[x], \tag{4.85}$$

由于每个 $g_i(x)|f(x)$，因此 g_i 均为 $x-\alpha$ 的幂，故 $g_1|g_i$，将上面的讨论对 $g_2,\cdots,g_k$ 进行，则可知 $g_1=\cdots=g_k=g$，即 $f(x)=g(x)^k$，因此

$$f(x)=(x-\alpha)^{p^t}=(x-\alpha)^{jk}, \tag{4.86}$$

设 $j=p^s,k=p^{t-s}$，若 $t-s\neq 0$ 则

$$g(x)=(x-\alpha)^{p^s}\in F[x]\Rightarrow g(x)^{p^{t-s-1}}=(x-\alpha)^{p^{t-1}}=x^{p^{t-1}}-\alpha^{p^{t-1}}\in F[x], \tag{4.87}$$

因此 $b=\alpha^{p^{t-1}}\in F$，此时 $b^p=\alpha^{p^t}=a$，与 $a\notin F^p$ 矛盾，因此 $t=s,k=1$，即 $f=g$ 不可约.

定理 4.15

F 为完全域当且仅当 $\operatorname{char}F=0$ 或 $\operatorname{char}F=p$ 且 $F=F^p=\{a^p:a\in F\}$.

证明 设 E/F 为代数扩张，若 $\operatorname{char}F=p,F=F^p$，则对任意 $\alpha\in E,m_\alpha(x)\in F[x]$，若 $m'_\alpha\neq 0$，则 m_α 可分；若 $m'_\alpha=0$ 则设 $m_\alpha(x)=\sum_{i=0}^k c_ix^{ip}$，由于 $F=F^p$，存在 $d_i^p=c_i$，即

$$m_\alpha(x)=\sum_{i=0}^k c_ix^{ip}=\sum_{i=0}^k(d_ix^i)^p=\left(\sum_{i=0}^k d_ix^i\right)^p, \tag{4.88}$$

这与 m_α 的不可约性矛盾，故 E/F 可分.

反之设 F 为完全域，$\operatorname{char}F=p$，假设存在 $a\in F,a\notin F^p$，则考虑多项式 $f(x)=x^p-a\in F[x]$，由引理可得 $f(x)$ 不可约，设 α 为 f 的根，则 $f(x)=(x-\alpha)^n$，它有重根，与 $F(\alpha)/F$ 的可分性矛盾.

推论 4.14

任何有限域都是完全域.

证明 设 F 为有限域，$\operatorname{char}F=p$，考虑 Frobenius 自同态 $\Phi:F\to F,\Phi(a)=a^p$，则 $\operatorname{Im}\Phi=F^p\leqslant F$，对任意 $a,b\in F$，$a\neq b$ 说明 $\Phi(a)-\Phi(b)=\Phi(a-b)\neq 0$，故 Φ 为单射，即 $|\operatorname{Im}\Phi|=|F|,F^p=F$，即 F 为完全域.

4.4.3 有限域

本小节将借助 FTGT 讨论有限域的结构，一个非常有用的工具是 Frobenius 自同态.

定理 4.16

设 p 为素数，r 为正整数，则

1. 存在 p^r 阶域 F_{p^r}，并且在同构意义下唯一.
2. 设 $s|r$，则 F_{p^r} 包含唯一的 p^s 阶子域；若 $s\nmid r$ 则 F_{p^r} 中不存在 p^s 阶子域.
3. 设 $E=F_{p^r},F=F_{p^s},s|r$，则 $\operatorname{Gal}(E/F)\cong\mathbb{Z}_{r/s}$，由 $\Psi=\Phi^s$ 生成，这里 Φ 为 Frobenius 同构；特别的，若 $s=1$，则 $\operatorname{Gal}(E/F)$ 为 r 阶循环群，由 Φ 生成.

证明

1. 设 $q=p^r,f(x)=x^q-x\in F_p[x]$，再设 F 为 $f(x)$ 的分裂域，令 $g(x)=x^{q-1}-1$，则 $f'(x)=-1$ 说明 f 无重根，$\deg f=q=p^r$ 说明 F 中至少有 q 个元素，令 $D=\{a\in F:a^q=a\}$，则容易验证 $D\subset F$ 为域，并且 f 在 D 中分裂，故 $F=D=F_q$. 另一方面，若 B 也为 q 元域，则 $|B^*|=q-1$，因此 B^* 中元素均为 $f(x)$ 的根，即 B 也为 f 的分裂域，而分裂域在同构意义下唯一，故 F_q 也是唯一的.
2. f 无重根说明 f 为可分多项式，而 F_q 为该可分多项式的分裂域，因此 F_q/F_p 为 Galois 扩张，可计算出

$$|\operatorname{Gal}(F_q/F_p)|=[F_q:F_p]=r, \tag{4.89}$$

考虑 Frobenius 同态 $\Phi\in\operatorname{Aut}(F_q)$，由 Fermat 小定理可知 $\Phi|_{F_p}=\operatorname{Id}_{F_p}$，因此 $\Phi\in\operatorname{Gal}(F_q/F_p)$，注意到 $\Phi^r=\operatorname{Id}_{\mathbb{F}_q}$，并且对任意 $s<r$ 有 $\Phi^s\neq\operatorname{Id}_{\mathbb{F}_q}$（否则 F_q 中元素均为 $x^{p^s}-x$ 的根，显然矛盾），因此 $\operatorname{Gal}(F_q/F_p)$ 为由 Φ 生成的 r 阶循环群，再借助 FTGT，其余结论是易得的.

推论 4.15

设 $F=F_{p^s}$，$f(x)\in F[x]$ 为 n 次不可约多项式，$r=ns$，则 $E=F_{p^r}$ 为 f 的分裂域，并且 $\operatorname{Gal}(E/F)=\mathbb{Z}_n=\langle\Psi\rangle=\langle\Phi^s\rangle$.

证明 设 α 为 f 的根，$E_0=F(\alpha)$，则 $[E_0:F]=\deg f=n$，即得 $E_0=F_{p^{ns}}=F_{p^r}$，设 $E\supset E_0$ 为 f 的分裂域，下证 $E=E_0$. 由于 E_0/F 为 Galois 扩张，因此它是一个正规可分扩张，$f(x)\in F[x]$ 在 E_0 有根，故在 E_0 分裂，

即得 $E=E_0$.

上面的结果也可以直接得到，显然 $\mathrm{Gal}(E_0/F)=\langle\Psi\rangle$，因此 α 为 f 的根说明 $\Psi(\alpha),\cdots,\Psi^{n-1}(\alpha)$ 也是 f 的根，因此 f 在 E_0 中分裂.

推论 4.16

1. 对任意 p,s,n，存在 n 次不可约多项式 $f(x)\in F_{p^s}[x]$.
2. 设
$$k(p^s,n)=|\mathcal{K}|=\#\left\{1\leqslant k\leqslant p^{ns}-1:\frac{p^{ns}-1}{\gcd(k,p^{ns}-1)}\text{不整除}p^{ms-1},\forall m|n,m\neq n\right\},\tag{4.90}$$
则 $F_{p^s}[x]$ 中的 n 次不可约多项式共有 $k(p^s,n)/n$ 个.

♡

证明

1. 取 $F_{p^{ns}}^*$ 的生成元 α_0，则 $F_{p^{ns}}=F_{p^s}(\alpha_0)$，因此 $f(x)=m_{\alpha_0}(x)\in F_{p^s}[x]$ 为 n 次不可约多项式.
2. 断言
$$k(p^s,n)=|\mathcal{K}'|=\#\{\alpha\in F_{p^{ns}}:\alpha\notin E,\forall E\subsetneq F_{p^{ns}},E\not\supset F_{p^s}\},\tag{4.91}$$
任取 $\alpha=\alpha_0^k\in F_{p^{ns}}^*$，则 $\operatorname{ord}\alpha|p^{ns}-1$，而 $F_{p^{ns}}$ 的包含 F_{p^s} 的子域为 $F_{p^{ms}}$，这里 $m|n.\alpha\in F_{p^{ms}}$ 当且仅当
$$\operatorname{ord}\alpha=\frac{p^{ns}-1}{\gcd(k,p^{ns}-1)}\Big|p^{ms}-1\Rightarrow\mathcal{K}'=\{\alpha_0^k:k\in\mathcal{K}\},\tag{4.92}$$
故断言得证. 由于
$$F_{p^s}(\alpha)=F_{p^{ns}}\Leftrightarrow\alpha\in\mathcal{K}'\Leftrightarrow\deg m_\alpha=n,\tag{4.93}$$
此时 $f(x)=m_\alpha(x)$ 就是一个满足条件的多项式（并且容易验证所有满足条件的多项式都有这种形式），进一步，每个 $f(x)|x^{ns}-x$，故无重根；两两 f_1,f_2 均为极小多项式故无相同根，上面已知 $k(p^s,n)$ 表示这些根的个数，因此 $k(p^s,n)/n$ 就表示这些多项式的个数.

最后再讨论一下 $k(p^s,n)$.

引理 4.11

1. $k(p^s,n)\geqslant\varphi(p^{ns}-1)$，这里 φ 为 Euler 函数.
2. 若 n 为素数，则 $k(p^s,n)=p^{ns}-p^s$.
3. 对任意 $n\in\mathbb{N}$ 有
$$k(p^s,n)=\sum_{d|n}\mu(n/d)p^{sd},\tag{4.94}$$
这里 μ 为 Mobius 函数.

♡

证明

1. $\varphi(n)$ 表示小于 n 的与 n 互素的整数，而满足这一条件的数必然在 $\mathcal{K}$ 中，因此 $k(p^s,n)\geqslant\varphi(p^{ns}-1)$.
2. 若 n 为素数，则 $F_{p^{ns}}/F_{p^s}$ 无非平凡中间域，因此 $\mathcal{K}'=F_{p^{ns}}\backslash F_{p^s}$，即 $k(p^s,n)=p^{ns}-p^s$.
3. 设 $f(p^s,n)=p^{ns}=|F_{p^{ns}}|$，则
$$f(p^s,n)=\sum_{d|n}k(p^s,d),\tag{4.95}$$
这是因为任何 $\alpha\in F_{p^{ns}}$ 都能生成某个 $F_{p^{ds}}$，这里的 d 恰好满足对任意 $c|d,c\neq d$ 有 $\alpha\notin F_{p^{cs}}$，因此由 Mobius 反演公式可得
$$k(p^s,n)=\sum_{d|n}\mu(n/d)f(p^s,d)=\sum_{d|n}\mu(n/d)p^{sd}.\tag{4.96}$$

4.4.4 无交扩张

本节中所有域都是 A 的子域.

定义 4.22 (无交扩张) 设 B_1, B_2 为 F 的扩域，若 $B_1 \cap B_2 = F$，则称 B_1, B_2 为无交扩张. ♣

注 显然 B_1, B_2 都是 $B_1 \cap B_2$ 的无交扩张.

引理 4.12 设 B_1, B_2 为 F 的有限扩张，$d_i = [B_i : F]$，若 $\gcd(d_1, d_2) = 1$，则 B_1, B_2 为无交扩张，且 $[B_1B_2 : F] = d_1d_2$. ♡

证明 设 $B_0 = B_1 \cap B_2, d_0 = [B_0 : F]$，由于 $[B_i : F] = [B_i : B_0][B_0 : F]$，因此 $d_0 | d_i$，$\gcd(d_1, d_2) = 1$ 说明 $d_0 = 1, B_0 = F$. 再令 $d = [B_1B_2 : F] = [B_1B_2 : B_i][B_i : F]$ 可得 $d_i | d$，因此 $d_1d_2 | d$，但是 $d \leqslant d_1d_2$，因此 $d = d_1d_2$.

定理 4.17 设 $B_2/(B_1 \cap B_2)$ 为有限 Galois 扩张，则 B_1B_2 为 B_2 的有限 Galois 扩张，且有 $\mathrm{Gal}(B_1B_2/B_1) \cong \mathrm{Gal}(B_2/B_1 \cap B_2)$. ♡

证明 设 $B_0 = B_1 \cap B_2$，则 B_2/B_0 为某个可分多项式 $f(x) \in B_0[x]$ 的分裂域，设其根为 $\alpha_1, \cdots, \alpha_k$，则

$$B_2 = B_0(\alpha_1, \cdots, \alpha_k) \Rightarrow B_1B_2 = B_1(\alpha_1, \cdots, \alpha_k), \tag{4.97}$$

故 B_1B_2/B_1 为有限 Galois 扩张，对任意 $\sigma \in \mathrm{Gal}(B_1B_2/B_1)$，$\sigma|_{B_1} = \mathrm{Id}$，因此 $\sigma|_{B_0} = \mathrm{Id}$，并且 $\sigma(f(x)) = f(x)$，它给出了根的置换

$$\sigma(B_2) = B_0(\sigma(\alpha_1), \cdots, \sigma(\alpha_k)) = B_0(\alpha_1', \cdots, \alpha_k') = B_2, \tag{4.98}$$

这时 $\sigma|_{B_2} \in \mathrm{Gal}(B_2/B_0)$，断言 $\sigma \mapsto \sigma|_{B_2}$ 即为所求同构. 显然这是单射，对任意 $\tau \in \mathrm{Gal}(B_2/B_0)$，由于 $B_1B_2 = B_1(\alpha_1, \cdots, \alpha_k)$ 是 $f(x) \in B_1[x]$ 的分裂域，因此由延拓定理，τ 可以延拓为自同构 $\sigma : B_1B_2 \to B_1B_2$，即 $\sigma|_{B_2} = \tau$，故为满射.

推论 4.17 设 $B_2/(B_1 \cap B_2)$ 为有限 Galois 扩张，则

$$[B_1B_2 : B_1] = [B_2 : B_1 \cap B_2], \quad [B_1B_2 : B_2] = [B_1 : B_1 \cap B_2], \tag{4.99}$$

$$[B_1B_2 : B_1 \cap B_2] = [B_1 : B_1 \cap B_2][B_2 : B_1 \cap B_2]. \tag{4.100}$$

♡

证明 根据 Galois 群的同构关系可得前者，直接计算

$$[B_1B_2 : B_1 \cap B_2] = [B_1B_2 : B_2][B_2 : B_1 \cap B_2] = [B_1 : B_1 \cap B_2][B_2 : B_1 \cap B_2]. \tag{4.101}$$

推论 4.18 设 B_1, B_2 为 F 的有限扩张，且 B_2/F 为 Galois 扩张，则 $[B_1B_2 : F] = [B_1 : F][B_2 : F]$ 当且仅当 B_1, B_2 为 F 的无交扩张. ♡

证明 由于

$$[B_1 : F][B_2 : F] = [B_1 : B_1 \cap B_2][B_1 \cap B_2 : F][B_2 : B_1 \cap B_2][B_1 \cap B_2 : F] \tag{4.102}$$

$$= [B_1B_2 : B_1 \cap B_2][B_1 \cap B_2 : F]^2 \tag{4.103}$$

$$= [B_1B_2 : F][B_1 \cap B_2 : F] \tag{4.104}$$

得证.

推论 4.19 (Theorem on Natural Irrationalities) 设 $f(x)\in F[x]$ 为可分多项式，E 为 f 的分裂域，$B\supset F$，则 BE 为 f 在 B 上的分裂域，$\mathrm{Gal}(BE/B)\cong \mathrm{Gal}(E/E\cap B)\leqslant \mathrm{Gal}(E/F)$.

证明 设 f 的根为 $\alpha_1,\cdots,\alpha_k$，则

$$E=F(\alpha_1,\cdots,\alpha_k),\quad BE=B(\alpha_1,\cdots,\alpha_k), \tag{4.105}$$

故 BE 为 f 在 B 上的分裂域. 由于 $F\subset B\cap E\subset E=(B\cap E)(\alpha_1,\cdots,\alpha_k)$，即 $E/(B\cap E)$ 为有限 Galois 扩张，根据前述定理得证.

定理 4.18

1. 设 B_1,B_2 为 F 的无交 Galois 扩张，则 $E=B_1B_2$ 为 F 的 Galois 扩张，且 $\mathrm{Gal}(E/F)=\mathrm{Gal}(B_1/F)\times \mathrm{Gal}(B_2/F)$.
2. 设 E 为 F 的 Galois 扩张，$\mathrm{Gal}(E/F)=G_1\times G_2$，若令 $B_i=\mathrm{Fix}(G_i)$，则 B_1,B_2 为 F 的无交 Galois 扩张且 $E=B_1B_2$.

证明

1. 根据前述定理可得同构 $\mathrm{Gal}(E/B_i)\cong \mathrm{Gal}(B_j/F)$，即对任意 $\sigma_j\in\mathrm{Gal}(B_j/F)$，存在唯一扩张 $\tilde\sigma_j\in\mathrm{Gal}(E/B_i)$，对任意 $e=\sum b_i^1b_i^2\in E$ 有

$$\begin{aligned}\tilde\sigma_1\tilde\sigma_2(e)&=\sum\tilde\sigma_1\tilde\sigma_2(b_i^1b_i^2) &(4.106)\\ &=\sum\tilde\sigma_1\tilde\sigma_2(b_i^1)\tilde\sigma_1\tilde\sigma_2(b_i^2) &(4.107)\\ &=\sum\tilde\sigma_1(b_i^1)\tilde\sigma_2(b_i^2) &(4.108)\\ &=\sum\tilde\sigma_2\tilde\sigma_1(b_i^1)\tilde\sigma_1\tilde\sigma_2(b_i^2) &(4.109)\\ &=\tilde\sigma_2\tilde\sigma_1(e), &(4.110)\end{aligned}$$

   故 $\tilde\sigma_1,\tilde\sigma_2$ 可交换，考虑映射

$$\begin{aligned}\mathrm{Gal}(B_1/F)\times\mathrm{Gal}(B_2/F)&\longrightarrow\mathrm{Gal}(E/F) &(4.111)\\ (\sigma_1,\sigma_2)&\longmapsto\tilde\sigma_1\tilde\sigma_2, &(4.112)\end{aligned}$$

   显然该映射为单射，另一方面

$$\begin{aligned}|\mathrm{Gal}(E/F)|&\geqslant|\mathrm{Gal}(B_1/F)\times\mathrm{Gal}(B_2/F)| &(4.113)\\ &=|\mathrm{Gal}(B_1/F)|\,|\mathrm{Gal}(B_2/F)| &(4.114)\\ &=[B_1:F][B_2:F] &(4.115)\\ &=[E:F], &(4.116)\end{aligned}$$

   而 $|\mathrm{Gal}(E/F)|=[E:\mathrm{Fix}(\mathrm{Gal}(E/F))]\leqslant[E:F]$，故 $|\mathrm{Gal}(E/F)|=[E:F]$，即上面的映射为满射.
2. 此时

$$B_1B_2=\mathrm{Fix}(G_1\cap G_2)=E,\quad B_1\cap B_2=\mathrm{Fix}(\langle G_1,G_2\rangle)=\mathrm{Fix}(\mathrm{Gal}(E/F))=F. \tag{4.117}$$

推论 4.20 设 B_1,B_2 为 F 的有限 Galois 扩张，$E=B_1B_2,B_0=B_1\cap B_2$，则 E/F 为 Galois 扩张，并且 $\mathrm{Gal}(E/F)\cong\{(\sigma_1,\sigma_2)\in\mathrm{Gal}(B_1/F)\times\mathrm{Gal}(B_2/F):\sigma_1|_{B_0}=\sigma_2|_{B_0}\}$.

证明 $B_1/F,B_2/F$ 均为有限 Galois 扩张，因此存在可分多项式 $f_1(x),f_2(x)\in F[x]$ 使得 B_1,B_2 分别为 f_1,f_2 的

分裂域，而 $E=B_1B_2$ 恰好是可分多项式 $f(x)=f_1(x)f_2(x)$ 的分裂域，故 E/F 为 Galois 扩张.

注意到对任意 $\sigma\in\mathrm{Gal}(E/F)$ 有 $\sigma(B_i)=B_i$（因为 B_i 为 $F[x]$ 中某个可分多项式的分裂域，而该多项式在 σ 下不变），因此有单同态（注意到 $E=B_1B_2$）

$$\mathrm{Gal}(E/F)\longrightarrow \mathrm{Gal}(B_1/F)\times\mathrm{Gal}(B_2/F) \tag{4.118}$$

$$\sigma\longmapsto(\sigma_1,\sigma_2)=(\sigma|_{B_1},\sigma|_{B_2}) \tag{4.119}$$

显然 $\sigma\in\mathrm{Gal}(E/F)$ 的像满足 $\sigma_1|_{B_0}=\sigma_2|_{B_0}$，而

$$[E:F]=[E:B_2][B_2:B_0][B_0:F]=[B_1:B_0][B_2:B_0][B_0:F]=[B_1:F][B_2:F]/[B_0:F] \tag{4.120}$$

这恰好是两个群的阶（考虑延拓定理），故同构得证.

推论 4.21

设 B,E 为 F 的无交扩张，E/F 为 Galois 扩张，设 $r:\mathrm{Gal}(EB/B)\to\mathrm{Gal}(E/F)$ 为限制映射 $r(\sigma)=\sigma|_E$，设 $H\leqslant\mathrm{Gal}(BE/B)$，则

$$\mathrm{Fix}(H)=B\mathrm{Fix}(r(H)). \tag{4.121}$$

♡

证明 这里的 r 实际上是一个同构，令 $K=r(H),D=\mathrm{Fix}(K)$，则显然 $\mathrm{Fix}(H)\supset BD$.Galois 群的同构说明 $[BE:B]=[E:F]$，因此

$$[BE:BD][BD:B]=[E:D][D:F]. \tag{4.122}$$

但由于 $[BE:BD]\leqslant[E:D],[BD:B]\leqslant[D:F]$，因此这里都能取等. 根据 $H\cong K$ 以及固定子域的扩张次数可得

$$[BE:\mathrm{Fix}(H)]=|H|=|K|=[E:\mathrm{Fix}(K)]=[E:D]=[BE:BD] \tag{4.123}$$

即 $\mathrm{Fix}(H)=BD$.

定理 4.19

设 B,E 为 F 的无交扩张，则

1. 设 B,E 均为 F 的有限 Galois 扩张，$N_1=\mathrm{Gal}(BE/B),N_2=\mathrm{Gal}(BE/E)$，则 BE/F 为 Galois 扩张，并且 $N_1,N_2\triangleleft\mathrm{Gal}(BE/F)$. 更精确地，$\mathrm{Gal}(BE/F)=N_1\times N_2$.
2. 设 E/F 为有限 Galois 扩张，$H=\mathrm{Gal}(BE/B),N=\mathrm{Gal}(BE/E)$，则 BE/F 为 Galois 扩张且 $N\triangleleft\mathrm{Gal}(BE/F)$. 更精确地，$G=N\rtimes H$（即 NH 的子群 N,H 的半直积）.

♡

注 半直积定义如下：设 $H\leqslant G,N\triangleleft G$，若 $H\cong G/N$ 且同构为典范映射 $\pi|_H:h\mapsto hN$，则称 G 为 H,N 的半直积，记为 $G=N\rtimes H$.

证明

1. 由于 B,E 的共轭类仅有自身（$\sigma\in\mathrm{Gal}(BE/F)$ 为二者的自同构），因此对应的 Galois 群为正规子群，其余部分由已有结论可得.
2. 同理 BE/F 为 Galois 扩张，$N\triangleleft\mathrm{Gal}(BE/F)$，商群为 $H_0=\mathrm{Gal}(E/F)$，它可以看作 $H=\mathrm{Gal}(BE/B)$ 在典范映射下的同构像（实际上限制映射的像一一对应了陪集），故 $G=HN$.

引理 4.13

设 $\alpha\in A$ 为可分元，$m_\alpha(x)\in F[x]$（为可分多项式），E 为 m_α 分裂域，若 B 也为 F 的扩张且 B,E 为无交扩张，则 m_α 在 $B[x]$ 中不可约.

♡

证明 设 $\tilde{m}_\alpha(x)\in B[x]$ 为 α 的极小多项式，显然其在 $B[x]$ 中不可约. 设 $\alpha_1,\cdots,\alpha_d\in E$ 为 m_α 的根，则 E/F 为 Galois 扩张，并且 $\mathrm{Gal}(E/F)$ 可迁地作用在 $\{\alpha_1,\cdots,\alpha_d\}$ 上，而任何 $\sigma_0\in\mathrm{Gal}(E/F)$ 可以延拓为 $\sigma\in\mathrm{Gal}(EB/B)$，因此 $\mathrm{Gal}(EB/B)$ 也可迁作用在根的集合上，因此 $\tilde{m}_\alpha(x)=(x-\alpha_1)\cdots(x-\alpha_d)=m_\alpha(x)$，得证.

引理 4.14

设 $\alpha \in A$ 为可分元，$m_\alpha(x) \in F[x]$，若 $E = F(\alpha)$ 为 m_α 的分裂域，B/F 为扩张且 m_α 在 $B[x]$ 中不可约，则 B, E 为 F 的无交扩张.

证明 m_α 的不可约性说明它同时是 α 在 $F[x], B[x]$ 中的极小多项式，因此

$$[B(\alpha) : B] = \deg \tilde{m}_\alpha = \deg m_\alpha = [F(\alpha) : F] = [E : F], \tag{4.124}$$

另一方面

$$[B(\alpha) : B] = [BF(\alpha) : B] = [BE : B] = [E : B \cap E], \tag{4.125}$$

故 $B \cap E = F$，得证.

4.4.5 单扩张

定义 4.23 (单扩张)

设 E/F 为代数扩张且存在 $\alpha \in E$ 使得 $E = F(\alpha)$，则称 E 为 F 的单扩张.

定理 4.20

设 E/F 为有限扩张，则 E/F 为单扩张当且仅当存在有限多个中间域 $F \subset B \subset E$.

证明 若 F 为有限域，则 E/F 为有限扩张说明 E 为有限域，因此其中间域个数也是有限的，E^* 为循环群，因此存在 $\alpha \in E$ 使得 $E = F(\alpha)$.

对于 F 无限的情况，若 $E = F(\alpha)$ 为单扩张，考虑 $m_\alpha(x) \in F[x]$，对任意中间域 $F \subset B \subset E$，可以考虑 $\tilde{m}_\alpha(x) \in B[x]$，则显然有

$$E = B(\alpha), \quad \deg \tilde{m}_\alpha = [E : B], \tag{4.126}$$

设在 F 中添加 $\tilde{m}_\alpha$ 的系数得到的域为 D，则 $F \subset D \subset B, E = D(\alpha), \tilde{m}_\alpha(x) \in D[x]$，此时 $\tilde{m}_\alpha$ 必然为 α 在 D 中的极小多项式，因此 $[E : D] = \deg \tilde{m}_\alpha = [E : B]$，这说明 $B = D$，也即中间域 B 与极小多项式 $\tilde{m}_\alpha$ 一一对应，这样的极小多项式只有有限个，故中间域也只有有限多个.

反之设 E/F 的中间域仅有限多个，只需证明对任意 $\alpha, \beta \in E$，存在 $\gamma_1 \in E$ 使得 $F(\alpha, \beta) = F(\gamma_1)$. 对于 $a \in F$，考虑扩域 $F(\alpha + a\beta)$，由于中间域仅有限多个，因此必然存在 $a_1 \neq a_2 \in F$ 使得 $F(\alpha + a_1\beta) = F(\alpha + a_2\beta)$，令 $\gamma_i = \alpha + a_i\beta$，则 $F(\gamma_1) = F(\gamma_2)$，即 $\gamma_1, \gamma_2 \in F(\gamma_1)$，$\gamma_2 - \gamma_1 = (a_2 - a_1)\beta \in F(\gamma_1)$，这说明

$$F(\gamma_1) \subset F(\alpha, \beta) \subset F(\gamma_1), \tag{4.127}$$

即 $F(\gamma_1) = F(\alpha, \beta)$，得证.

推论 4.22

若 E/F 为有限可分扩张，则 E/F 为单扩张.

证明 设 $E = F(\alpha_1, \cdots, \alpha_k)$，则根据定义，每个极小多项式 $m_{\alpha_i}(x) \in F[x]$ 都是可分多项式（不可约因子无重根），因此 $f(x) = m_{\alpha_1}(x) \cdots m_{\alpha_k}(x)$ 也是可分多项式，设 $E' \supset E$ 为 f 的分裂域，则 E'/F 为 Galois 扩张，根据 FTGT，E'/F 只有有限多个中间域（每个中间域对应了 $\mathrm{Gal}(E'/F)$ 的子群），因此 E/F 也只有有限多个中间域，即 E/F 为单扩张.

引理 4.15

设 E/F 为有限 Galois 扩张，$\alpha \in E$，则 $E = F(\alpha)$ 当且仅当对任意 $\sigma \in \mathrm{Gal}(E/F), \sigma \neq \mathrm{Id}$ 有 $\sigma(\alpha) \neq \alpha$.

证明 证法 1：设

$$d=[F(\alpha):F]=|\mathrm{Gal}(E/F)|,\quad n=[E:F]=\deg m_\alpha(x), \tag{4.128}$$

则 $E=F(\alpha)$ 当且仅当 $n=d$，设 $m_\alpha(x)=(x-\alpha_1)\cdots(x-\alpha_d)$，这里的根为 α 的 Galois 共轭元，$\alpha_1=\alpha$，故 $E=F(\alpha)$ 当且仅当 α 有 n 个共轭元，即每个 $\sigma\in\mathrm{Gal}(E/F)$ 对应了一个共轭元（Id 对应自身）.

证法 2：设 $B=F(\alpha)$，则由 FTGT，存在 $H\leqslant\mathrm{Gal}(E/F)$ 使得 $B=\mathrm{Fix}(H)$，事实上这里

$$H=\{\sigma\in\mathrm{Gal}(E/F):\sigma|_B=\mathrm{Id}\}=\{\sigma\in\mathrm{Gal}(E/F):\sigma(\alpha)=\alpha\}, \tag{4.129}$$

因此 $B=E$ 当且仅当 $E=\mathrm{Fix}(H)$，即 $H=\{\mathrm{Id}\}$，得证.

命题 4.11

设 F 特征为 0，B_1,B_2 为 F 的有限无交 Galois 扩张，设 $B=B_1B_2$，$B_1=F(\alpha_1),B_2=F(\alpha_2)$，则 $B=F(\alpha)$，这里 $\alpha=\alpha_1+\alpha_2$.

证明 根据上一节可知 B/F 为 Galois 扩张，因此只需证明对任意 $\sigma\in\mathrm{Gal}(B/F),\sigma\neq\mathrm{Id}$ 有 $\sigma(\alpha)\neq\alpha$. 由于 $\mathrm{Gal}(E/F)=\mathrm{Gal}(B_1/F)\times\mathrm{Gal}(B_2/F)$，因此设 $\sigma=(\sigma_1,\sigma_2)$，若

$$\alpha_1+\alpha_2=\alpha=\sigma(\alpha)=\sigma_1(\alpha_1)+\sigma_2(\alpha_2), \tag{4.130}$$

则 $\sigma_1(\alpha_1)-\alpha_1=\sigma_2(\alpha_2)-\alpha_2\in B_1\cap B_2=F$，即 $\sigma_1(\alpha)=\alpha+a$，$\sigma_1^k(\alpha)=\alpha+ka$，但是 σ 的阶有限，$\mathrm{char}\,F=0$，因此 $a=0$，即 $\sigma_i(\alpha_i)=\alpha_i$，$\sigma=\mathrm{Id}$.

4.4.6 正规基定理

定义 4.24 (Normal basis)

设 E/F 为 Galois 扩张，则 E/F 的基 $\{\alpha_i:i=1,\cdots,n\}$ 称为正规基，若存在 $\alpha\in E$ 使得 $\{\alpha_i\}=\{\sigma_i(\alpha)\}$，这里 $\sigma_i\in\mathrm{Gal}(E/F)$.

注 换句话说，一组基是正规基当且仅当它是（$\mathrm{Gal}(E/F)$ 作用于）某个 $\alpha\in E$ 的轨道.

定理 4.21

设 E/F 为 n 次 Galois 扩张，若 $\mathrm{Gal}(E/F)$ 为循环群，则 E 有正规基.

证明 设 $\mathrm{Gal}(E/F)$ 由 σ 生成，考虑线性映射 $T:E\to E,T(\alpha)=\sigma(\alpha)$，断言 $m_T(x)=x^n-1$. 显然 $m_T(x)|x^n-1$，设 $m_T(x)=\sum_{i=0}^d a_ix^i,d<n$，也即

$$a_0\mathrm{Id}+\cdots+a_{d-1}\sigma^{d-1}=0, \tag{4.131}$$

但是 $\{\mathrm{Id},\sigma,\cdots,\sigma^{d-1}\}$ 是 E^* 的不同特征标，因此是无关的，即每个 $a_i=0$，矛盾. 故存在 $\alpha\in E$ 使得 $\mathrm{Ann}(\alpha)=(m_T(x))$（即 $\alpha\in E$ 的零化子由 m_T 生成），而 $\deg m_T=n$，因此 $\{\alpha,T(\alpha),\cdots,T^{n-1}(\alpha)\}=\{\alpha,\sigma(\alpha),\cdots,\sigma^{n-1}(\alpha)\}$ 就是一组正规基.

引理 4.16

设 E/F 为 n 次 Galois 扩张，$\sigma_1,\cdots,\sigma_n\in\mathrm{Gal}(E/F)$，$\alpha_1,\cdots,\alpha_n\in E$，则 $\{\alpha_1,\cdots,\alpha_n\}$ 是 E/F 的一组基当且仅当矩阵 $A=(\sigma_i(\alpha_j))_{n\times n}$ 是非奇异的.

证明 显然.

引理 4.17

设 F 为无限域，E 为 F 扩域，$f(x_1,\cdots,x_k)\in E[x_1,\cdots,x_k]$ 为多项式，若对任意 $(a_1,\cdots,a_k)\in F^k$ 有 $f(a_1,\cdots,a_k)=0$，则 f 为零多项式.

证明 归纳，$k=1$ 显然，对于一般情况有

$$f(x_1,\cdots,x_k)=\sum_{i=0}^{n} g_i(x_1,\cdots,x_{k-1})x_k^i, \tag{4.132}$$

对任意固定的 $a_1,\cdots,a_{k-1}\in F$，考虑 $\tilde{f}(x_k)=f(a_1,\cdots,a_{k-1},x_k)$，它有多于 $\deg\tilde{f}$ 个根，根据 $k=1$ 的情形可知每个 g_i 都为零多项式，由归纳假设得证.

定理 4.22

设 F 为无限域，$\mathrm{Gal}(E/F)=\{\sigma_1,\cdots,\sigma_n\}$，则 $\sigma_1,\cdots,\sigma_n$ 为代数无关的，即对于 $f(x_1,\cdots,x_n)\in E[x_1,\cdots,x_n]$，若对任意 $\alpha\in E$ 有 $f(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))=0$，则 f 为零多项式. ♡

证明 设 $\{\alpha_1,\cdots,\alpha_n\}$ 为 E/F 的一组基，则 $A=(\sigma_i(\alpha_j))$ 可逆，对任意 $\alpha=\sum_{j=1}^n c_j\alpha_j\in E/F$ 有

$$(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))^T=A(c_1,\cdots,c_n)^T, \tag{4.133}$$

设 $f(x_1,\cdots,x_n)\in E[x_1,\cdots,x_n]$ 使得对任意 $\alpha\in E$ 有 $f(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))=0$，则这相当于对任意 $(c_1,\cdots,c_n)\in F^n$ 有（这里不区分 n 元组与列向量，不会引起混淆）

$$0=f(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))=f(A(c_1,\cdots,c_n)^T), \tag{4.134}$$

若令 $g(x_1,\cdots,x_n)=f(A(x_1,\cdots,x_n)^T)\in E[x_1,\cdots,x_n]$，则由引理，$g$ 为零多项式，根据 A 的可逆性可知对任意 $A^{-1}(b_1,\cdots,b_n)^T$ 有 $f(b_1,\cdots,b_n)=0$，故 f 也为零多项式.

定理 4.23

设 E/F 为有限 Galois 扩张，则 E 有正规基. ♡

证明 若 F 为有限域，则 E/F 为循环扩张（$\mathrm{Gal}(E/F)$ 为循环群），故有正规基.

若 F 为无限域，设 $\mathrm{Gal}(E/F)=\{\sigma_1,\cdots,\sigma_n\}$，考虑多项矩阵 $B(x_1,\cdots,x_n)=(b_{ij}(x_1,\cdots,x_n))$，其中 $b_{ij}=x_k$，这里 k 满足 $\sigma_i\sigma_j=\sigma_k$，行列式 $\det B=d(x_1,\cdots,x_n)$. 如果不妨设 $\sigma_1=\mathrm{Id}$，则容易验证 $d(1,0,\cdots,0)=\pm1$，即 d 不是零多项式，根据引理，存在 $\alpha\in E$ 满足 $d(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))\neq0$，令

$$\alpha_j=\sigma_j(\alpha),\quad A=B(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))=(a_{ij}) \tag{4.135}$$

容易发现 $a_{ij}=\sigma_k(\alpha),\sigma_k(\alpha)=\sigma_i\sigma_j(\alpha)=\sigma_i(\alpha_j)$，因此 $A=(\sigma_i(\alpha_j))$，由于 $\det A=d(\sigma_1(\alpha),\cdots,\sigma_n(\alpha))\neq0$，故 A 可逆，$\{\sigma_1,\cdots,\sigma_n\}=\{\sigma_1(\alpha),\cdots,\sigma_n(\alpha)\}$ 为 E/F 的正规基.

4.4.7 Abel 扩张与 Kummer 域

定义 4.25 (Abel 扩张)

设 E/F 为 Galois 扩张，若 $\mathrm{Gal}(E/F)$ 为 Abel 群，则称之为 Abel 扩张. ♣

定义 4.26 (primitive root)

称 $\zeta\in F$ 为 n 次本原单位根，若 $\zeta^n=1$ 且对任意 $0<m<n$ 有 $\zeta^m\neq1$. ♣

引理 4.18

1. 设 F 有 n 次本原单位根，则 $\mathrm{char}\,F=0$ 或 $\mathrm{char}\,F=n$（此时 n 为素数）.
2. F 有 n 次本原单位根当且仅当 F 有 n 个不同的 n 次单位根. ♡

证明

1. 设 $\zeta\in F$ 为 n 次本原单位根，若 $\mathrm{char}\,F\neq0$，设 $\mathrm{char}\,F=p|n$（带余除法可得），则 ζ 为 $x^n-1=(x^{n/p})^p-1=(x^{n/p}-1)^p$ 的根说明其也为 $x^{n/p}-1$ 的根，与本原性矛盾，故 $\mathrm{char}\,F=p=n$.

2. 若 $\zeta \in F$ 为 n 次本原单位根，则 $1, \zeta, \cdots, \zeta^{n-1}$ 为 n 个不同的 n 次单位根. 反之若 F 有 n 个 n 次单位根，则它们构成一个 n 阶循环群，这个循环群的生成元就是一个 n 次本原单位根.

对于域 F，后面用 F_0 表示它的素域 (prime field)，它是 F 的最小子域，容易验证任何域都有唯一素域，并且 $\operatorname{char} F = 0$ 时 $F_0 \cong \mathbb{Q}$；$\operatorname{char} F = p$ 时 $F_0 \cong F_p$.

引理 4.19

设 $\zeta_n = e^{2\pi i/n}$（即 $\mathbb{C}$ 的 n 次本原单位根），则 $F_0(\zeta_n)/F_0$ 是一个 Galois 扩张，并且 $\operatorname{Gal}(F_0(\zeta_n)/F_0)$ 同构于 $\mathbb{Z}_n^*$ 的一个子群，特别地是一个 Abel 群.

♡

证明 $F_0(\zeta_n)$ 是 $x^n - 1 \in F_0[x]$ 的分裂域，故 $F_0(\zeta_n)/F_0$ 为 Galois 扩张. 对任意 $\sigma_1 \in \operatorname{Gal}(F_0(\zeta_n)/F_0)$，$\sigma_1(\zeta_n)$ 也是 n 次本原单位根，故 $\sigma_1(\zeta_n) = \zeta_n^{k_1}$，这里 $\gcd(k_1, n) = 1$. 出于这种观察，可以得到一个单同态 $\operatorname{Gal}(F_0(\zeta_n)/F_0) \to \mathbb{Z}_n^*, \sigma_i \mapsto k_i$，而 $|\operatorname{Gal}(F_0(\zeta)/F_0)| = [F_0(\zeta_n) : F_0] = n$，得证.

定义 4.27 (n-powerless)

设 $\alpha \in F$，称 α 为 n-非幂的，若对任意 $m|n, m > 1$，α 不是某个元素的 m 次幂.

♣

命题 4.12

设 $F \supset F_0(\zeta_n)$，设 E 为 $x^n - a \in F[x]$ 的分裂域，则 $\operatorname{Gal}(E/F)$ 同构于 $\mathbb{Z}_n$ 的一个子群，特别地是一个循环群. 进一步，如下陈述等价：

1. $a \in F$ 为 n-非幂的.
2. $\operatorname{Gal}(E/F) \cong \mathbb{Z}_n$.
3. $x^n - a \in F[x]$ 不可约.

♠

证明 设 α 为 $x^n - a$ 的根，则 $x^n - a = \prod_{i=0}^{n-1}(x - \zeta_n^i \alpha), E = F(\alpha)$，$m_\alpha | x^n - a$ 说明 $m_\alpha(x) = \prod_{k=0}^{m-1}(x - \zeta_n^{i_k}\alpha)$，这里 $\{i_0, \cdots, i_{m-1}\}$ 是 $\{0, \cdots, n-1\}$ 的一个子集.

根据延拓定理，Id_F 可以延拓为域同构 $F(\alpha) \to F(\zeta_n^{i_k}\alpha), \alpha \mapsto \zeta_n^{i_k}\alpha$，而它可以进一步延拓为 $\sigma_k \in \operatorname{Gal}(E/F)$，并且延拓的结果是唯一的. 进一步，对 σ_k, σ_l 有

$$\sigma_k \sigma_l(\alpha) = \zeta_n^{i_k + i_l}\alpha, \tag{4.136}$$

这便给出了同态 $\operatorname{Gal}(E/F) \cong \{i_k : 0 \leqslant k \leqslant m-1\} \to \mathbb{Z}_n$（省略一些细节），得证.

进一步，由于 $|\operatorname{Gal}(E/F)| = [E : F] = [F(\alpha) : F] = \deg m_\alpha$，因此

$$\operatorname{Gal}(E/F) \cong \mathbb{Z}_n \Leftrightarrow \deg m_\alpha = |\operatorname{Gal}(E/F)| = n \Leftrightarrow m_\alpha(x) = x^n - a \Leftrightarrow x^n - a \in F[x] \text{不可约}. \tag{4.137}$$

这说明 $2 \Leftrightarrow 3$，下证 $1 \Leftrightarrow 3$. 若 1 不成立，设存在 $b \in F$ 使得 $a = b^m, n = jm$，则 $x^n - a = x^{jm} - b^m$，它有真因子 $x^j - b$，与不可约性矛盾；反之若 $x^n - a \in F[x]$ 可约，则 $x^n - a = \prod_{i=0}^{n-1}(x - \zeta_n^i \alpha), E = F(\alpha)$，$\{i_0, \cdots, i_{m-1}\}$ 是 $\mathbb{Z}_n$ 的一个 m 阶子群，因此 $m_\alpha(x) = x^m - \alpha^m = x^m - b \in F[x]$，若设 $n = mj$，则 $a = \alpha^n = b^j$，即 $a\alpha$ 不是 n-非幂的，由此即得 $1 \Leftrightarrow 3$.

反过来，可以考虑如下命题.

命题 4.13

设 $F \supset F_0(\zeta_n)$，E 为 F 的一个扩张，则下述等价：

1. 存在某个 n-非幂的 $a \in F$，使得 E 为 $x^n - a \in F[x]$ 的分裂域.
2. E/F 为 Galois 扩张且 $\operatorname{Gal}(E/F) \cong \mathbb{Z}_n$.

♠

证明 根据前述定理可知 $1 \Rightarrow 2$，假设 2 成立，设 σ 为 $\operatorname{Gal}(E/F)$ 的生成元，则存在 $\alpha \in E$，使得 E 有一组正规基 $\{\alpha, \sigma(\alpha), \cdots, \sigma^{n-1}(\alpha)\}$，设

$$\beta = \alpha + \zeta_n^{-1}\sigma(\alpha) + \cdots + \zeta_n^{-(n-1)}\sigma^{n-1}(\alpha), \tag{4.138}$$

则 $\beta\neq 0$，并且容易验证 $\sigma(\beta)=\zeta_n\beta$，即得 $\sigma^i(\beta)=\zeta_n^i\beta$，因此对除恒同映射外的任意 $\tau\in \mathrm{Gal}(E/F)$ 都有 $\tau(\beta)\neq\beta$，故 $E=F(\beta)$（根据单扩张的某个定理）. 进一步

$$m_\beta(x)=\prod_{i=0}^{n-1}(x-\zeta_n^i\beta)=x^n-\beta^n\in F[x], \tag{4.139}$$

令 $a=\beta^n\in F$，则 E 为 $x^n-a\in F[x]$ 的分裂域，同上一条定理的证明可知 a 是 n-非幂的.

定义 4.28 (Kummer 域)

设 $F\supset F_0(\zeta_n)$，称 E 为 Kummer 域，若其为形如

$$f(x)=(x^n-a_1)\cdots(x^n-a_t),a_i\in F \tag{4.140}$$

的多项式的分裂域.

♣

定理 4.24

设 $F\supset F_0(\zeta_n)$，则 E/F 的 Kummer 域当且仅当同时有

1. E/F 为 Galois 扩张.
2. E/F 为 Abel 扩张（即 $\mathrm{Gal}(E/F)$ 为 Abel 群）.
3. $\mathrm{Gal}(E/F)$ 的指数整除 n.

♡

注 这里群 G 的指数定义为最小的，使得对任意 $g\in G$ 有 $g^e=1$ 的 $e\in\mathbb{N}$，易知 $e||G|$

证明 首先设 E/F 为 Kummer 域，即 $f(x)=(x^n-a_1)\cdots(x^n-a_t)$ 的分裂域，设 $\alpha_i\in E,\alpha_i^n=a_i$，则

$$x^n-a_i=\prod_{j=1}^{n}(x-\zeta_n^j\alpha_i), \tag{4.141}$$

故每个 x^n-a_i 都是可分多项式，即 $f\in F[x]$ 为可分多项式，E/F 为 Galois 扩张.

对 t 归纳，当 $t=1$ 时 E/F 显然 2,3 成立，假设 $t-1$ 的情形 2,3 成立，设 $B_1\subset E$ 为 $f_1(x)=(x^n-a_1)\cdots(x^n-a_{t-1})$ 的分裂域，$B_2\subset E$ 为 $f_2(x)=x^n-a_t$ 的分裂域，则 $E=B_1B_2$，此时（根据无交扩张部分的某个推论）

$$\mathrm{Gal}(E/F)\leqslant \mathrm{Gal}(B_1/F)\times\mathrm{Gal}(B_2/F), \tag{4.142}$$

而 $\mathrm{Gal}(B_1/F),\mathrm{Gal}(B_2/F)$ 均为 Abel 群（归纳假设 + 显然），故 $\mathrm{Gal}(E/F)$ 也为 Abel 群，同时它的指数显然整除 $\mathrm{Gal}(B_1/F)\times\mathrm{Gal}(B_2/F)$ 的指数，即 n，得证.

反之若 E/F 为 Abel 扩张且 $G=\mathrm{Gal}(E/F)$ 的指数整除 n，则设

$$G=H_1\oplus\cdots\oplus H_s, \tag{4.143}$$

其中每个 H_i 都是指数整除 n 的循环群. 对 s 归纳，当 $s=1$ 时命题显然成立，假设命题对 $s-1$ 成立，考虑 s 的情形，令

$$B_1=\mathrm{Fix}(H_1\oplus\cdots\oplus H_{s-1}),\quad B_2=\mathrm{Fix}(H_s), \tag{4.144}$$

则 B_1 是某个 $g_1(x)=(x^n-a_1)\cdots(x^n-a_r)\in F[x]$ 的分裂域，B_2 是某个 $g_2(x)=x^n-a_{r+1}\in F[x]$ 的分裂域，而

$$B_1B_2=\mathrm{Fix}((H_1\oplus\cdots\oplus H_{s-1})\cap H_s)=\mathrm{Fix}(\{1\})=E, \tag{4.145}$$

故 $E=B_1B_2$ 是 $g_1(x)g_2(x)$ 的分裂域，即 E 为 Kummer 域.

下面更细致讨论一下 Kummer 扩张的 Galois 群. 设

$$(F^*)^n=\{a^n:a\in F^*\}. \tag{4.146}$$

定理 4.25

设 $F\supset F_0(\zeta_n)$，E 为 $f(x)=(x^n-a_1)\cdots(x^n-a_t)$ 的分裂域，每个 $a_i\neq 0$，则 $\mathrm{Gal}(E/F)\cong\langle a_1,\cdots,a_t\rangle\leqslant F^*/(F^*)^n$.

♡

证明 设 $\alpha_i \in E^*, \alpha_i^n = a_i$，$G = \langle \alpha_1, \cdots, \alpha_t \rangle \leqslant E^*/(F^*)^n, G' = \langle a_1, \cdots, a_t \rangle \leqslant F^*/(F^*)^n$，满同态

$$\phi : G \longrightarrow G' \tag{4.147}$$

$$\alpha \longmapsto \alpha^n, \tag{4.148}$$

下证 ϕ 为同构，即证 ϕ 为单射. 设 $\phi(\alpha) = \alpha^n = 1$，由于 $\alpha^n \in (F^*)^n$，因此存在 $f \in F^*$ 使得 $\alpha^n = f^n$，这说明存在 k 使得 $\alpha = \zeta_n^k f \in F^*$（注意 $\zeta_n \in F^*$）. 设 $G = H_1 \oplus \cdots \oplus H_s$，每个 H_i 的生成元为 $\beta_i \in E$，阶为 m_i，则 $\beta_i^{m_i} \in F$ 为 m_i-非幂的.

下面对 s 归纳，证明 $\mathrm{Gal}(E/F) = \langle \eta_1, \cdots, \eta_s \rangle$，这里 $\eta_i(\beta_i) = \zeta_{m_i}\beta_i, \eta_i(\beta_j) = \beta_j$. 当 $s = 1$ 时显然成立，假设对 $s-1$ 的情形成立，设 $B = F(\beta_1, \cdots, \beta_{s-1}), D = F(\beta_s)$，则只需证明 B, D 为 F 的无交扩张且 $BD = E$，则有

$$\mathrm{Gal}(E/F) = \mathrm{Gal}(B/F) \times \mathrm{Gal}(D/F), \tag{4.149}$$

根据归纳法即得.

首先 $E = F(\alpha_1, \cdots, \alpha_t)$，$\langle \alpha_1, \cdots, \alpha_t \rangle = \langle \beta_1, \cdots, \beta_s \rangle \subset E^*$，故 $E = BD$. 设 $B_0 = B \cap D$，则存在 $K \leqslant \mathrm{Gal}(B/F)$ 使得 $B_0 = \mathrm{Fix}(K)$（FTGT），故 $D_0 = F((\beta_s)^{m'}) = F(\sqrt[m]{b_s})$，这里 $m_s = mm'$，下证 $m = 1$. 设 $\beta = \sqrt[m]{b_s} = (\beta_s)^{m'} \in B \cap D \subset B$，根据归纳假设有

$$\beta = (\beta_s)^{m'} = \sum_{i_1, \cdots, i_{s-1}} c_{i_1, \cdots, i_{s-1}} \beta_1^{i_1} \cdots \beta_{s-1}^{i_{s-1}}, \tag{4.150}$$

这里 $i_j = 0, \cdots, m_j - 1; j = 1, \cdots, s-1; c_{i_1, \cdots, i_{s-1}} \in F$.

设 $\sigma \in \mathrm{Gal}(B/F)$，则存在单位根 ζ 使得 $\sigma(\beta) = \zeta\beta$，同理，存在单位根 ζ' 使得 $\sigma(\beta_1^{i_1} \cdots \beta_{s-1}^{i_{s-1}}) = \zeta'\beta_1^{i_1} \cdots \beta_{s-1}^{i_{s-1}}$，并且对 $c_{i_1, \cdots, i_{s-1}} \neq 0$ 的项有 $\zeta' = \zeta$，但根据归纳假设，存在 σ 使得 $\sigma(\beta_j) = \zeta_{m_j}\beta_j$，若上面和式有多于一项的非零项，则必然有两项在 σ 作用下所乘的单位根不同，矛盾，故

$$\beta = (\beta_s)^{m'} = c_{i_1, \cdots, i_{s-1}} \beta_1^{i_1} \cdots, \beta_{s-1}^{i_{s-1}} \in H_1 \oplus \cdots \oplus H_{s-1}, \tag{4.151}$$

由于 $(H_1 \oplus \cdots \oplus H_{s-1}) \cap H_s = \{1\}$，因此 $m' = m_s$，得证.

推论 4.23

延续上一条定理的记号，同构 $\bigoplus_{i=1}^s \mathbb{Z}_{m_i} \to \mathrm{Gal}(E/F)$ 为

$$(j_1, \cdots, j_s) \mapsto \sigma, \quad \sigma(\beta_i) = \zeta_n^{j_i n/m_i}\beta_i (= \zeta_{m_i}^{j_i}\beta_i). \tag{4.152}$$

♡

4.4.8 范数与迹

定义 4.29 (Galois 扩张的范数/迹)

设 E/F 为有限 Galois 扩张，$G = \mathrm{Gal}(E/F)$，对于 $\alpha \in E$，定义（E/F 的）范数

$$\mathrm{N}_{E/F}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha), \tag{4.153}$$

以及（E/F 的）迹

$$\mathrm{Tr}_{E/F}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha). \tag{4.154}$$

♣

引理 4.20

对任意 $\alpha \in E$，$\mathrm{N}_{E/F}(\alpha), \mathrm{Tr}_{E/F}(\alpha) \in F$.

♡

证明 显然它们在 G 下不变，因此 $\mathrm{N}_{E/F}(\alpha), \mathrm{Tr}_{E/F}(\alpha) \in \mathrm{Fix}(\mathrm{Gal}(E/F)) = F$.

引理 4.21

设 $\alpha\in E,\deg m_\alpha=r$，若 $m_\alpha(x)=\sum_{i=0}^r c_ix^i$，$[E:F]=n$，则

$$\mathrm{N}_{E/F}(\alpha)=(-1)^nc_0^{n/r},\quad \mathrm{Tr}_{E/F}(\alpha)=-(n/r)c_{r-1}. \tag{4.155}$$

♡

证明 设 α 不同的共轭元为 $\alpha_1=\alpha,\alpha_2,\cdots,\alpha_r$，则 $m_\alpha(x)=\prod_{i=1}^r(x-\alpha_i)$，因此

$$c_0=(-1)^r\alpha_1\cdots\alpha_r,\quad c_{r-1}=-(\alpha_1+\cdots+\alpha_r), \tag{4.156}$$

实际上 $r|n$，$\mathrm{Gal}(E/F)$ 中将 α 映为 α_k 的均有 n/r 个，因此

$$\mathrm{N}_{E/F}(\alpha)=\prod_{\sigma\in G}\sigma(\alpha)=(\alpha_1\cdots\alpha_r)^{n/r}=(-1)^nc_0^{n/r} \tag{4.157}$$

$$\mathrm{Tr}_{E/F}(\alpha)=\sum_{\sigma\in G}\sigma(\alpha)=(n/r)(\alpha_1+\cdots+\alpha_r)=-(n/r)c_{r-1}. \tag{4.158}$$

引理 4.22

设 $\alpha\in E$，设 $T_\alpha:E\to E,T_\alpha(\beta)=\alpha\beta$ 为 F-线性映射，则

$$\mathrm{N}_{E/F}(\alpha)=\det(T_\alpha),\quad \mathrm{Tr}_{E/F}(\alpha)=\mathrm{tr}(T_\alpha). \tag{4.159}$$

♡

证明 设 $B=F(\alpha),r=\deg m_\alpha$，则 B 有一组基 $\{1,\alpha,\cdots,\alpha^{r-1}\}$. 设 $[E:F]=n,[E:B]=n/r$，取 E/B 的一组基 $\{1=\epsilon_1,\cdots,\epsilon_{n/r}\}$，则

$$C=\{1,\alpha,\cdots,\alpha^{r-1},\cdots,\epsilon_{n/r},\epsilon_{n/r}\alpha,\cdots,\epsilon_{n/r}\alpha^{r-1}\} \tag{4.160}$$

是 E/F 的一组基. 显然的，T_α 在 C 下的矩阵为分块对角阵，共 n/r 个分块，每个分块都是 $m_\alpha(x)$ 的友方阵，而其友方阵的行列式为 $(-1)^ra_0$，迹为 $-a_{n-1}$，得证.

定理 4.26

设 E/F 为 n 次 Galois 扩张，设 B 为中间域（故 E/F 为 Galois 扩张）且 B/F 为 Galois 扩张，则对任意 $a\in F,\alpha,\beta\in E$ 有

1. $\mathrm{N}_{E/F}(a)=a^n$，$\mathrm{Tr}_{E/F}=na$.
2. $\mathrm{N}_{E/F}(\alpha\beta)=\mathrm{N}_{E/F}(\alpha)\mathrm{N}_{E/F}(\beta)$，$\mathrm{Tr}_{E/F}(\alpha+\beta)=\mathrm{Tr}_{E/F}(\alpha)+\mathrm{Tr}_{E/F}(\beta)$.
3. $\mathrm{N}_{E/F}(\alpha)=\mathrm{N}_{B/F}(\mathrm{N}_{E/B}(\alpha))$，$\mathrm{Tr}_{E/F}(\alpha)=\mathrm{Tr}_{B/F}(\mathrm{Tr}_{E/B}(\alpha))$

♡

引理 4.23

存在 $\alpha\in E$ 使得 $\mathrm{Tr}_{E/F}(\alpha)\neq 0$.

♡

证明 若 $\mathrm{char}\,F=0$ 或 $[E:F]$ 与 $\mathrm{char}\,F\neq 0$ 互素，则 $\alpha=1$ 满足条件. 因此只需考虑 $\mathrm{char}\,F=p$，对任意 $\sigma\in\mathrm{Gal}(E/F)$，$\sigma:E^*\to E^*$ 是一个特征标，由 Dirichlet 定理可知不同特征标线性无关，故它们的和不为零映射，即存在某个 α 满足条件.

定理 4.27 (Hilbert's Theorem 90)

设 E/F 为 n 次循环扩张，σ 为 $G=\mathrm{Gal}(E/F)$ 的生成元，则

1. 设 $\beta\in E,\mathrm{N}_{E/F}(\beta)=1$，则存在 $\alpha\in E$ 使得 $\beta=\alpha/\sigma(\alpha)$.
2. 若 $\beta\in E,\mathrm{Tr}_{E/F}(\beta)=0$，则存在 $\alpha\in E$ 使得 $\beta=\alpha-\sigma(\alpha)$.

♡

证明

1. 由于 $\mathrm{N}_{E/F}(\beta)=\beta\sigma(\beta)\cdots\sigma^{n-1}(\beta)=1$，需要找到 $\alpha\in E$ 使得 $\alpha=\beta\sigma^1(\alpha)$，令 $\epsilon_0=1$，

$$\epsilon_i=\beta\sigma^1(\beta)\cdots\sigma^{i-1}(\beta),\quad i=1,\cdots,n-1, \tag{4.161}$$

则 $\beta\sigma(\epsilon_i) = \epsilon_{i+1}, i = 0, 1, \cdots, n-2$，$\beta(\sigma(\epsilon_{n-1})) = 1 = \epsilon_0$. 根据特征标的无关性，存在 $\delta \in E$ 使得 $\alpha = \sum_{i=0}^{n-1} \epsilon_i \sigma^i(\delta) \neq 0$，这里的 α 即满足条件.

2. 类似地，令 $\epsilon_0 = 0$，

$$\epsilon_i = \beta + \sigma(\beta) + \cdots + \sigma^{i-1}(\beta), \quad i = 0, \cdots, n-1, \tag{4.162}$$

则 $\beta + \sigma(\epsilon_i) = \epsilon_{i+1}, i = 0, \cdots, n-2$，$\beta + \sigma(\epsilon_{n-1}) = 0$. 根据特征标的无关性，存在 $\gamma \in E$ 使得 $\delta = \sum_{i=0}^{n-1} \epsilon_i \sigma^i(\gamma) \neq 0$，计算可得

$$\delta - \sigma(\delta) = \sum_{i=0}^{n-1} \epsilon_i \sigma^i(\gamma) - \sum_{i=0}^{n-1} \sigma(\epsilon_i)\sigma^{i+1}(\gamma) \tag{4.163}$$

$$= \sum_{i=0}^{n-1} \epsilon_i \sigma^i(\gamma) - \sum_{i=0}^{n-2} (\epsilon_{i+1} - \beta)\sigma^{i+1}(\gamma) \tag{4.164}$$

$$= \beta \sum_{i=0}^{n-1} \sigma^{i+1}(\gamma) = \beta \sum_{i=0}^{n-1} \sigma^i(\gamma) \tag{4.165}$$

$$= \beta \mathrm{Tr}_{E/F}(\gamma), \tag{4.166}$$

因此令 $\alpha = \delta / \mathrm{Tr}_{E/F}(\gamma)$，则有 $\beta = \alpha - \sigma(\alpha)$.

定义 4.30 (可分扩张的范数/迹)

设 E/F 为有限可分扩张，则定义

$$\mathrm{N}_{E/F} = \mathrm{N}_{D/F}, \quad \mathrm{Tr}_{E/F} = \mathrm{Tr}_{D/F}, \tag{4.167}$$

这里 D 为 E 的任意正规闭包.

♣

注 关于正规闭包的讨论见后文.

定义 4.31 (一般扩张的范数/迹)

设 E/F 为有限扩张，则定义

$$\mathrm{N}_{E/F} = (\mathrm{N}_{D/F})^d, \quad \mathrm{Tr}_{E/F} = d\mathrm{Tr}_{D/F}, \tag{4.168}$$

这里 D 为 E 的任意正规闭包，$d = [Fix(\mathrm{Gal}(D/F)) : F]$.

♣

注 若 $\mathrm{char}\, F = p$ 且 E/F 不是可分扩张，则 d 为 p 的幂，此时 $\mathrm{Tr}_{E/F} \equiv 0$.

4.5 有理数域上的扩张

本节讨论对象默认为零特征域.

4.5.1 分圆域

定义 4.32 (分圆多项式)

称 $\Phi_n(x) = \prod_{(n,k)=1} (x - \zeta_n^k)$ 为 n 次分圆多项式.

♣

注 Φ_n 实际上是所有 n 次本原单位根的一次式的乘积，而 ζ_n^k 为本原根当且仅当 $\gcd(n, k) = 1$，这实际上也说明 $\deg \Phi_n = \varphi(n)$，这里 φ 为 Euler 函数.

命题 4.14

1. $\Phi_n(x) \in \mathbb{Q}[x]$.
2. 若 $n_1 \neq n_2$，则 Φ_{n_1}, Φ_{n_2} 互素.
3. $x^n - 1 \prod_{d|n} \Phi_d(x)$.
4. $\Phi_n(x) \in \mathbb{Z}[x]$.

♠

证明 只证明 1，设 $E = \mathbb{Q}(\zeta_n)$，则 E 为可分多项式 $x^n - 1$ 的分裂域，$E/\mathbb{Q}$ 为 Galois 扩张.ζ_n 为本原单位根，因此对任意 $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$，$\sigma(\zeta_n)$ 也是一个本原根，故 Φ_n 在 $\mathrm{Gal}(E/\mathbb{Q})$ 下不变，即 $\Phi_n \in \mathbb{Q}[x]$.

定理 4.28

任何分圆多项式在 $\mathbb{Q}[x]$ 中都是不可约的.

♡

证明 只需证明 $\Phi_n(x) \in \mathbb{Q}[x]$ 是 ζ_n 的极小多项式，由于 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 为 Galois 扩张（因为它是可分多项式 $x^n - 1$ 的分裂域），因此

$$\deg m_{\zeta_n} = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n) = \deg \Phi_n, \tag{4.169}$$

而显然 $m_{\zeta_n} | \Phi_n$，故得证.

推论 4.24

1. $m_{\zeta_n}(x) = \Phi_n(x)$，$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.
2. $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \mathbb{Z}_n^*$，特别地，$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ 为 Abel 群.

♡

推论 4.25

设 $m, n \in \mathbb{N}, d = \gcd(m, n), l = \mathrm{lcm}(m, n)$，则 $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_l)$，$\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_d)$.

♡

证明 由于 $\zeta_m = \zeta_l^{l/m}, \zeta_n = \zeta_l^{l/n}$，因此 $\mathbb{Q}(\zeta_l) \supset \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$，设 $s, t \in \mathbb{Z}$ 满足 $s(l/m) + t(l/n) = 1$，则 $\zeta_l = \zeta_m^s \zeta_n^t$，故 $\mathbb{Q}(\zeta_l) \subset \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$，第一部分得证.

由于 $\zeta_d = \zeta_m^{m/d} = \zeta_n^{n/d} \in \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)$，故 $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) \supset \mathbb{Q}(\zeta_d)$. 另一方面

$$[\mathbb{Q}(\zeta_n) : (\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))] = [\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_m)] \tag{4.170}$$

$$= \varphi(l)/\varphi(m), \tag{4.171}$$

$$[\mathbb{Q}(\zeta_n) : (\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n))] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_d)]/[(\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)) : \mathbb{Q}(\zeta_d)] \tag{4.172}$$

$$= \varphi(n)/\varphi(d)[(\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)) : \mathbb{Q}(\zeta_d)], \tag{4.173}$$

由此可得

$$[(\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n)) : \mathbb{Q}(\zeta_d)] = \frac{\varphi(l)\varphi(d)}{\varphi(n)\varphi(m)} = 1, \tag{4.174}$$

第二部分得证.

命题 4.15

对任意 n，n 次分圆多项式为

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}, \tag{4.175}$$

这里 μ 为 Mobius 函数.

♠

证明 由于 $x^n - 1 = \prod_{d|n} \Phi_d(x)$，根据乘积形式的 Mobius 反演公式

$$g(n) = \prod_{d|n} f(d) \Longleftrightarrow f(n) = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)} \tag{4.176}$$

即得.

4.5.2 可解扩张与可解群

定义 4.33 (radical polynomial/radical extension/radical sovable)

1. 称形如 $f(x)=x^n-a\in F[x]$ 的多项式为 $F[x]$ 中的根式多项式.
2. 称 E/F 为根式扩张，若 $E=F(\alpha)$，这里 α 是某个根式多项式的根.
3. 设 $f(x)\in F[x]$，对于方程 $f(x)=0$，称其根式可解，若存在扩张序列

$$F=E_0\subset E_1\subset\cdots\subset E_k, \tag{4.177}$$

这里每个 E_i 都是某个根式多项式 $f_{i-1}(x)\in E_{i-1}[x]$ 的分裂域，并且 E_k 为 $f(x)\in F[x]$ 的分裂域. ♣

引理 4.24

设 $f(x)=x^n-a\in F[x]$，E 为 $f(x)$ 的分裂域，则 $G=\mathrm{Gal}(E/F)$ 为可解群. ♡

证明 $E=F(\zeta_n,\sqrt[n]{a})$，设 $B=F(\zeta_n)$ 为二者的中间域，$G_1=\mathrm{Gal}(E/B)$，则 $E/B,B/F$ 为 Galois 扩张，特别地 G_1 为循环群且 $G_1\triangleleft G$，并且 $G/G_1\cong\mathrm{Gal}(B/F)$ 也为 Abel 群，因此 G 有可解列，是可解群.

推论 4.26

设 $f(x)=\prod_{j=1}^t(x^{n_j}-a_j),a_j\in F$，$E$ 为 $f(x)$ 分裂域，则 $G=\mathrm{Gal}(E/F)$ 为可解群. ♡

证明 考虑一列域

$$F=D_0\subset\cdots\subset D_t=E, \tag{4.178}$$

这里 D_j 为 $x^{n_j-a_j}\in D_{j-1}[x]$ 的分裂域，设 $G_j=\mathrm{Gal}(D_{t-j}/D_0)$，则

$$G=G_0\geqslant\cdots\geqslant G_t=\{1\}, \tag{4.179}$$

并且 $G_{j-1}/G_j=\mathrm{Gal}(D_{t-j+1}/D_{t-j})$，根据上一条引理可知这是可解群，故 G 是可解的（这里的序列可以 refinement 为一个可解列）.

定理 4.29

设 $f(x)\in F[x]$，E 为 $f(x)$ 分裂域，则 $f(x)=0$ 根式可解当且仅当 $G=\mathrm{Gal}(E/F)$ 为可解群. ♡

证明 首先假设 G 可解，$\deg f=m,n=m!$.

Case 1. 若 $F\supset\mathbb{Q}(\zeta_n)$，设次正规列

$$G=G_0\triangleright\cdots\triangleright G_k=\{1\}, \tag{4.180}$$

这里每个 G_i/G_{i+1} 为循环群，记其阶为 m_i，则 $m_i\leqslant m$，设 $B_i=\mathrm{Fix}(G_i)$，则 B_i/B_{i-1} 为 m_i 次循环扩张，而 $B_{i-1}\supset\mathbb{Q}(\zeta_n)\supset\mathbb{Q}(\zeta_{m_i})$，因此 B_i 实际上是某个 $x^{m_i}-a_i\in B_{i-1}[x]$ 的分裂域，即 $f(x)=0$ 根式可解，得证.

Case 2. 设 $B=F(\zeta_n)$，E_B 为 $f(x)\in B[x]$ 的分裂域，则 $\mathrm{Gal}(E_B/B)$ 与 $\mathrm{Gal}(E/F)$ 的某个子群同构，而可解群的子群依然可解，故 $\mathrm{Gal}(E_B/B)$ 可解，仿照 Case 1 可证.

反之假设 $f(x)=0$ 根式可解，则存在扩张列

$$F=B_0\subset B_1\subset\cdots\subset B_k=E, \tag{4.181}$$

这里 B_i 为某个 $x^{m_i}-a_i\in B_{i-1}[x]$ 的分裂域，因此 $\mathrm{Gal}(B_i/B_{i-1})$ 为可解群（引理）. 当 $k=2$ 时，$\mathrm{Gal}(B_2/B_1)$ 均为可解群，$B_2/B_1,B_1/B_0$ 均为 Galois 扩张，只需证明 B_2/B_0 为 Galois 扩张，则 G 为可解群. 下面归纳证明.

当 $B_0'=B_0=F,B_1'=B_1$ 时，B_1'/F 为 Galois 扩张. 假设 B_{i-1}'/F 为 Galois 扩张，B_i' 为

$$\prod_{\sigma\in\mathrm{Gal}(B_{i-1}'/B_0')}(x^{m_i}-\sigma(a_i))\in B_{i-1}'[x] \tag{4.182}$$

的分裂域，而该多项式在 $\mathrm{Gal}(B'_{i-1}/B'_0)$ 下不变，因此它实际上属于 $B'_0[x]=F[x]$，而 B'_i 实际上就是这个 $F[x]$ 中可分多项式的分裂域，即 B'_i/F 为 Galois 扩张，由此即得扩张列

$$F=B'_0\subset B'_1\subset\cdots\subset B'_k, \tag{4.183}$$

这里每个 B'_i/F 都是 Galois 扩张且 $B'_k\supset B_k\supset E$. 设 $G=\mathrm{Gal}(B'_k/F), G_i=\mathrm{Gal}(B'_{k-i}/B'_0), i=0,\cdots,k$，则

$$G=G_0\supset\cdots\supset G_k=\{1\}, \tag{4.184}$$

并且 $G_{i-1}/G_i=\mathrm{Gal}(B'_{k-i}/B'_0)$，根据引理可知 G_{i-1}/G_i 可解，因此 $G=\mathrm{Gal}(B'_k/F)$ 可解. 而 $F\subset E\subset B'_k$，E/F 为 Galois 扩张，因此 $\mathrm{Gal}(E/F)=\mathrm{Gal}(B'_k/F)/\mathrm{Gal}(B'_k/E)$ 也是可解的（可解群的商群），得证.

推论 4.27 (Abel)

次数大于等于 5 的方程不都是根式可解的.

♡

证明 取 $f_n(x)\in F[x]$，E 为 f_n 的分裂域，使得 $\mathrm{Gal}(E/F)=S_n$，则由于 $n\geqslant 5$ 时 S_n 不可解，得证.

定理 4.30 (Galois)

设 $f(x)\in F[x]$ 为素数 p 次不可约多项式，则 $f(x)=0$ 根式可解当且仅当其所有根都是其它任何两个根的有理函数.

♡

证明 $f(x)=0$ 根式可解当且仅当 $G=\mathrm{Gal}(E/F)$ 为可解群，这里 E 为 f 的分裂域.f 不可约说明 G 可迁作用于 f 的根上.

首先假设 $f(x)=0$ 的所有根都是其它任何两个根的有理函数，设 G 为 S_p 子群，它作用在 f 的根上，则对任意 $\sigma\in G$，若 $\alpha_1\neq\alpha_2$，则对任意 $\epsilon\in E$，$\sigma(\epsilon)$ 由 $\sigma(\alpha_1),\sigma(\alpha_2)$ 唯一确定（因为是有理函数）. 而 $\sigma(\alpha_1),\sigma(\alpha_2)$ 的选择至多有 $p(p-1)$ 种，因此 $|G|\leqslant p(p-1)$，即 G 可解（还是附录的结论）.

反之设 G 可解，设 α_1,α_2 为 f 的两个不同的根，$B=F(\alpha_1,\alpha_2)\subset E$，下证 $B=E$. 根据 FTGT，$G'=\mathrm{Gal}(E/B)\subset G$ 与 $\mathrm{Fix}(\mathrm{Gal}(E/B))=\{\sigma\in G:\sigma(\beta)=\beta,\forall\beta\in B\}$ 对应，因此 $B=E$ 当且仅当 $G'=\{\mathrm{Id}\}$.

设 $\sigma\in G$，则 $\sigma\in G'$ 当且仅当 $\sigma(\alpha_1)=\alpha_1,\sigma(\alpha_2)=\alpha_2$，根据附录结论，可以将 G 在 f 根的作用视为 G_H（$H\leqslant F_p^*$）在集合 T 上的作用，这里

$$G_H=\left\{\begin{pmatrix}h & n\\ 0 & 1\end{pmatrix}:h\in H,n\in F_p\right\},\quad T=\left\{\begin{pmatrix}i\\ 1\end{pmatrix}:i\in F_p\right\}, \tag{4.185}$$

设 α_1,α_2 分别对应 $\begin{pmatrix}i_1\\1\end{pmatrix},\begin{pmatrix}i_2\\1\end{pmatrix}$，则通过简单的线性代数计算可知 σ 对应 G_H 中的“单位阵”，即 $h=1,n=0$，得证.

推论 4.28

设 $F\subset\mathbb{R}$，$f(x)\in F[x]$ 为素数 p 阶不可约多项式，有 $1<k<p$ 个实根，则 $f(x)=0$ 根式不可解.

♡

证明 设 α_1,α_2,β 分别是 f 的不同的两个实根和一个复根，则根据 Galois 定理可知 f 根式不可解.

4.5.3 尺规作图

定理 4.31

$z\in\mathbb{C}$ 可被尺规构造当且仅当 z 为 $\mathbb{Q}$ 中的代数数，并且存在扩张序列

$$F_0=\mathbb{Q}\subset F_1\subset\cdots\subset F_k, \tag{4.186}$$

这里 $\mathbb{Q}(z)\subset F_k$，$[F_i:F_{i-1}]=2$.

♡

证明 首先显然 $\mathbb{Q}$ 都是可构造的，设 $[F:F_0]=2$，则存在 $\alpha_1\in\mathbb{C}$ 使得 $F=F_0(\alpha_1)$，这里 $\alpha_1=\sqrt{a_1},a_1\in\mathbb{Q}$，因此 α_1 可构造，则 F_1 可构造，归纳即得存在上述扩张序列的数必然可构造.

反之设 $z\in\mathbb{C}$ 可被尺规构造，则它只能由如下三种方法得到

1. 两条直线相交.
2. 直线与圆相交.
3. 两圆相交.

并且对应直线/圆方程的系数均在 $\mathbb{Q}$ 中，因此简单的解析几何计算可知这样的序列是存在的.

推论 4.29

如下三个问题不可被尺规构造解决：

1. 三等分角：将任意角三等分.
2. 倍立方：给定一个立方体，构造一个新立方体，使之体积是原来的两倍.
3. 化圆为方：给定一个圆，构造一个与之面积相等的正方形.

♡

证明

1. 只需举出反例，由于
$$\cos 3\theta=4\cos^4\theta-3\cos\theta, \tag{4.187}$$
取 $\theta=\pi/3$，则 $x_0=\cos(\theta/3)$ 是 $f(x)=8x^3-6x-1=0$ 的根，而该多项式不可约，因此 $[\mathbb{Q}(x_0):\mathbb{Q}]=3$，故不可构造.
2. 这实际上是要作出 $\sqrt[3]{2}$，但这是不可构造的（扩张次数为 3）.
3. 这实际上要构造 $\sqrt{\pi}$，这不是代数数.

引理 4.25

对于 $z\in\mathbb{C}$，如下陈述等价：

1. 存在扩张序列 $F_0=\mathbb{Q}\subset F_1\subset\cdots\subset F_k$，满足 $\mathbb{Q}(z)\subset F_k,[F_i:F_{i-1}]=2$.
2. 若 E 为 $m_z(x)\in\mathbb{Q}(x)$ 的分裂域，则 $[E:\mathbb{Q}]$ 为 2 的幂.

♡

证明 $2\Rightarrow1$：此时设 $G=\mathrm{Gal}(E/\mathbb{Q})$ 的阶为 2^k，则存在子群序列
$$G=G_0\supset G_1\supset\cdots\supset G_k=\{1\}, \tag{4.188}$$
满足 $[G:G_i]=2^i$（实际上是 Sylow 定理的推论），取 $F_i=\mathrm{Fix}(G_i)$ 即得满足要求的扩张序列.

$1\Rightarrow2$：对 k 归纳，$k=0,1$ 是平凡的，设 $[F_k:F_{k-1}]=2$，则存在 $\alpha_k\in F_k$ 使得 $F_k=F_{k-1}(\alpha_k),\deg m_{\alpha_k}=2$. 并且对任意 $E_{k-1}\supset F_{k-1}$，$[E_{k-1}(\alpha):E_{k-1}]=1$或2.

设 $E_0=F_0,E_1=F_1$，从 α_1 开始，若 $\alpha_k\in E_{k-1}$，则 $E_k=E_{k-1}$；若不然，则设 $G=\mathrm{Gal}(E_{k-1}/E_0)$ 以及
$$f(x)=\prod_{\sigma\in G}\sigma(m_{\alpha_k}(x)), \tag{4.189}$$
则 f 在 G 下不变，即 $f(x)\in E_0[x]$，设 E_k 为 $f(x)$ 的分裂域（显然包含 F_k），$f(x)$ 根为 $\beta_1=\alpha_k,\cdots,\beta_m$，$\deg m_{\alpha_k}=2$ 说明 $\deg\sigma(m_{\alpha_k}(x))=2$，故 $[E_{k-1}(\beta_i):E_{k-1}]=2$，进一步
$$E_{k-1}\subset E_{k-1}(\beta_1)\subset\cdots\subset E_{k-1}(\beta_1,\cdots,\beta_m)=E_k, \tag{4.190}$$
若设 $E'_{k-1}=E_{k-1}(\beta_1,\cdots,\beta_{i-1})$，则 $E_{k-1}(\beta_1,\cdots,\beta_i)=E'_{k-1}(\beta_i)=E'_{k-1}E_{k-1}(\beta_i)$，因此
$$\begin{aligned}[E_{k-1}(\beta_1,\cdots,\beta_i):E_{k-1}(\beta_1,\cdots,\beta_{i-1})]&=[E'_{k-1}(\beta_i):E'_{k-1}] &(4.191)\\ &\leqslant[E_{k-1}(\beta_i):E_{k-1}] &(4.192)\\ &=2, &(4.193)\end{aligned}$$
故 $[E_k:E_{k-1}]=2^m$，说明 $[E_k:\mathbb{Q}]$ 为 2 的幂，E_k 同时是分裂域说明 $E_k/\mathbb{Q}$ 为 Galois 扩张，因此对任意 $z\in E_k$，m_z 在 E_k 中分裂，其分裂域 $E\subset E_k$，故 $[E:\mathbb{Q}]$ 也为 2 的幂.

定理 4.32 (Gauss)

正 n 边形可用尺规构造当且仅当 $n=2^k p_1\cdots p_j$，这里 $\{p_i\}$ 为不同的 Fermat 数. ♡

注 Fermat 数定义为 $F_k=2^{2^k}+1$.

证明 只需考虑单位圆的内接正 n 边形，它可构造当且仅当 $\zeta_n=e^{2\pi i/n}$ 可构造，这又当且仅当 $\deg m_{\zeta_n}=\varphi(n)=2^k$，设唯一分解 $n=2^a p_1^{u_1}\cdots p_t^{u_t}$，则

$$\varphi(n)=2^{a-1}\prod_{i=1}^{t}(p_i-1)p_i^{u_i-1}, \tag{4.194}$$

故 $\varphi(n)=2^k$ 当且仅当 $u_1=\cdots=u_t=1$，且 $p_i=2^{v_i}+1$，p 为素数必有 $v_i=2^{s_i}$（否则能被 3 整除），即 p_i 为 Fermat 数.

由于 $2=2^{2^1}+1, 17=2^{2^2}+1$ 是 Fermat 数，因此正五边形，正十七边形都是可尺规作出的.

例 4.3 尺规作正五边形 设 $a=\zeta_5+\zeta_5^{-1}$，则 a,ζ_5 分别满足方程

$$x^2-x-1=0,\quad x^2-ax+1=0, \tag{4.195}$$

由此可解得 ζ_5，事实上这里考虑了扩张 $\mathbb{Q}\subset\mathbb{Q}(\zeta_5+\zeta_5^{-1})\subset\mathbb{Q}(\zeta_5)$.

例 4.4 尺规作正十七边形 设 $\zeta=\zeta_{17}, G=G_0=\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$，则 $G\cong\mathbb{Z}_{16}$，为了找到想要的扩张序列

$$\mathbb{Q}\subset F_1\subset F_2\subset F_3\subset\mathbb{Q}(\zeta), \tag{4.196}$$

根据 FTGT，只需找到对应的群序列

$$G\supset G_1\supset G_2\supset G_3\supset\{1\}, \tag{4.197}$$

这里 $[F_i:\mathbb{Q}]=[G:G_i]$ 说明 $|G_i|=2^{4-i}$. 设 $\sigma\in G, \sigma(\zeta)=\zeta^3$ 生成 G，则 $G_i=\langle\sigma^{2^i}\rangle$ 恰好满足条件，$F_i=\mathrm{Fix}(G_i)=\mathrm{Fix}(\{\sigma^{2^i}\})$，断言

$$F_1=\mathbb{Q}(\zeta+\zeta^2+\zeta^4+\zeta^8+\zeta^{-8}+\zeta^{-4}+\zeta^{-2}+\zeta^{-1})=\mathbb{Q}(\alpha_1), \tag{4.198}$$

$$F_2=\mathbb{Q}(\zeta+\zeta^4+\zeta^{-4}+\zeta^{-1})=\mathbb{Q}(\alpha_2), \tag{4.199}$$

$$F_3=\mathbb{Q}(\zeta+\zeta^{-1})=\mathbb{Q}(\alpha_3), \tag{4.200}$$

满足条件，借助原根计算可证断言，最后来计算 ζ 满足的方程，这实际上是在依次计算极小多项式（并且每个都是二次的），而 α 的极小多项式的根都是对应的 Galois 共轭元，因此

1. 对于 $\mathbb{Q}(\zeta)/F_3$，$m_\zeta\in F_3[x]$，$\mathrm{Gal}(\mathbb{Q}(\zeta)/F_3)=G_3=\{\mathrm{Id},\sigma^8\}$，故

$$m_\zeta(x)=(x-\zeta)(x-\sigma^8(\zeta))=(x-\zeta)(x-\zeta^{-1}) \tag{4.201}$$

$$=x^2-(\zeta+\zeta^{-1})x+1 \tag{4.202}$$

$$=x^2-\alpha_3x+1. \tag{4.203}$$

2. 对于 F_3/F_2，$m_{\alpha_3}\in F_2[x]$，$\mathrm{Gal}(F_3/F_2)=G_2/G_3=\{G_3,\sigma^4G_3\}$，故

$$m_{\alpha_3}(x)=(x-\alpha_3)(x-\sigma^4(\alpha_3)) \tag{4.204}$$

$$=(x-(\zeta+\zeta^{-1}))(x-(\zeta^4+\zeta^{-4})) \tag{4.205}$$

$$=x^2-\alpha_2x+\sigma(\alpha_2), \tag{4.206}$$

3. 对于 F_2/F_1，$m_{\alpha_2}\in F_1[x]$，$\mathrm{Gal}(F_2/F_1)=G_1/G_2=\{G_2,\sigma^2G_2\}$，故

$$m_{\alpha_2}(x)=(x-\alpha_2)(x-\sigma^2(\alpha_2)) \tag{4.207}$$

$$=x^2-\alpha_1x-1, \tag{4.208}$$

4. 对于 $F_1/\mathbb{Q}$，$m_{\alpha_1}\in\mathbb{Q}[x]$，$\mathrm{Gal}(F_1/\mathbb{Q})=G/G_1=\{G_1,\sigma G_2\}$，故

$$m_{\alpha_1}(x)=(x-\alpha_1)(x-\sigma(\alpha_1)) \tag{4.209}$$

$$=x^2+x-4, \tag{4.210}$$

根据对称性，$\sigma(\alpha_2)$ 是 $\sigma(m_{\alpha_2}(x))=x^2-\sigma(\alpha_1)x-1=0$ 的根. 综上，计算 ζ 的过程可以总结为如下几步：

1. 解方程 $x^2+x-4=0$，得到 $\alpha_1>0$.
2. 解方程 $x^2-\alpha_1 x-1=0, x^2-\sigma(\alpha_1)x-1=0$，分别取两个方程的正根 $\alpha_2,\sigma(\alpha_2)>0$.
3. 解方程 $x^2-\alpha_2 x+\sigma(\alpha_2)=0$，得到 $\alpha_3,\sigma^4(\alpha_3)$（注意 $\alpha_3>\sigma^4(\alpha_3)$）.

实际上并不需要解 $x^2-\alpha_3 x+1=0$，因为得到 $\alpha_3=\zeta+\zeta^{-1}=\cos(2\pi/17)$ 后足以尺规作出正十七边形. 计算可得

$$\cos\frac{2\pi}{17}=\frac{1}{4}(\alpha_2+\sqrt{\alpha_2^2-4\sigma(\alpha_2)}) \tag{4.211}$$

$$=\frac{1}{16}\left(\sqrt{17}-1+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}+\sqrt{170-26\sqrt{17}}-4\sqrt{34+2\sqrt{17}}}\right). \tag{4.212}$$

4.5.4 $\mathbb{Q}$ 上的二次扩张

对于素数 p，F_p^* 为循环群，它的生成元被称为模 p 的**原根**. 根据初等数论有关结论，模 p 的原根总是存在的. 进一步，$G=F_p^*$ 为 $\varphi(p)=p-1$ 阶循环群，因此它有唯一的 p 阶子群 H，设 $\pi:G\to G/H\cong\mathbb{Z}_2$ 为商映射，则对任意 $k\in G$，定义 $\chi_p(k)=(-1)^{\pi(k)}$ 为模 p 的二次剩余特征.

根据二次剩余理论，模素数 p 的二次剩余与非二次剩余恰好各有 $(p-1)/2$ 个，因此上面的群 H 恰好是所有二次剩余构成的群，即当 k 为模 p 的二次剩余时 $\chi_p(k)=1$，反之 $\chi_p(k)=-1$. 这个记号有时也会用 Legendre 符号表示.

命题 4.16

设 $\chi=\chi_p$ 为二次剩余特征，则它有如下性质：

1. $\chi(jk)=\chi(j)\chi(k)$（即 $\chi:F_p^*\to\{\pm1\}$ 为一个群同态）.
2. $\sum_{k=1}^{p-1}\chi(k)=0$（毕竟二次剩余与非剩余数量相同）.
3. $\chi(-1)=(-1)^{(p-1)/2}$.

♠

定理 4.33

设 E 为 $\mathbb{Q}$ 上的一个二次扩张，则 E 为 $\mathbb{Q}$ 和某个分圆域的中间域. 特别地

1. $\mathbb{Q}(\sqrt{-1})=\mathbb{Q}(\zeta_4)$.
2. $\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\zeta_8),\mathbb{Q}(\sqrt{-2})\subset\mathbb{Q}(\zeta_8)$.
3. 若素数 $p\equiv1(\bmod 4)$，则 $\mathbb{Q}(\sqrt{p})\subset\mathbb{Q}(\zeta_p)$.
4. 若素数 $p\equiv3(\bmod 4)$，则 $\mathbb{Q}(\sqrt{-p})\subset\mathbb{Q}(\zeta_p)$.

♡

证明 事实上，若 $\mathbb{Q}(\sqrt{a})\subset\mathbb{Q}(\zeta_m),\mathbb{Q}(\sqrt{b})\subset\mathbb{Q}(\zeta_n)$，则

$$\mathbb{Q}(\sqrt{ab})\subset\mathbb{Q}(\sqrt{a},\sqrt{b})\subset\mathbb{Q}(\zeta_m,\zeta_n)\subset\mathbb{Q}(\zeta_{mn}), \tag{4.213}$$

因此只需证明上面的 1,2,3,4，而 1,2 是显然的，下面直接证明 3,4. 设

$$S_p=\sum_{k=1}^{p-1}\chi(k)\zeta_p^k, \tag{4.214}$$

则

$$S_p^2=\sum_{k=1}^{p-1}\sum_{j=1}^{p-1}\chi(k)\zeta_p^k\chi(j)\zeta_p^j=\sum_{k=1}^{p-1}\sum_{j=1}^{p-1}\chi(kj)\zeta_p^{k+j}, \tag{4.215}$$

设 $j\equiv km(\bmod p)$，则 $\chi(kj)=\chi(m)$，故

$$S_p^2=\sum_{k=1}^{p-1}\sum_{j=1}^{p-1}\chi(m)\zeta_p^{k(1+m)}=\sum_{m=1}^{p-1}\chi(m)\sum_{k=1}^{p-1}(\zeta_p^{1+m})^k \tag{4.216}$$

$$= (p-1)\chi(-1) - \sum_{m=1}^{p-2} \chi(m) \tag{4.217}$$

$$= p\chi(-1) \tag{4.218}$$

这里用到了 $1+\zeta_p+\cdots+\zeta_p^{p-1}=0$ 以及 $\sum_{m=1}^{p-1}\chi(m)=0$. 因此有 $S_p=\sqrt{p}\in\mathbb{Q}(\zeta_p)$ 或 $S_p=\sqrt{-p}\in\mathbb{Q}(\zeta_p)$.

证明 证法 2: 设 $G=\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, 其由 σ_0 生成, $\sigma_0(\zeta_p)=\zeta_p^r$, 这里 r 为模 p 的原根. 注意到任何满足 $\sigma_0(\alpha)=\alpha$ 的 $\alpha\in\mathbb{Q}(\zeta_p)$ 实际上在 $\mathbb{Q}$ 中. 而 $[\mathbb{Q}(\zeta_p):\mathbb{Q}]=p-1$ 且 $\mathbb{Q}(\zeta_p)$ 的一组基为 $\zeta_p,\cdots,\zeta_p^{p-1}$, 因此设 $\alpha=\sum_{i=1}^{p-1}a_i\zeta_p^i$, 则必有 $a_1=\cdots=a_{p-1}=a\in\mathbb{Q}$, 也即 $\alpha=-a$.

设

$$\alpha_0=\sum_{i=1}^{(p-1)/2}\zeta_p^{r^{2i-2}},\quad \alpha_1=\sum_{i=1}^{(p-1)/2}\zeta_p^{r^{2i-1}}, \tag{4.219}$$

则 $\alpha_0+\alpha_1=\zeta_p+\cdots+\zeta_p^{p-1}=-1$ 且 $\sigma_0(\alpha_0)=\alpha_1,\sigma_0(\alpha_1)=\alpha_0$, 因此 $b=\alpha_0\alpha_1\in\mathbb{Q}$. 下面具体计算 b. 展开后的和式共有 $(p-1)^2/4$ 项, 每项形如 $\zeta_p^j\zeta_p^k$, 其中 j,k 分别为二次剩余与二次非剩余, 因此分两种情况讨论.

若 $p\equiv 1(\mathrm{mod}\,4)$, 则 $\chi(-j)=\chi(j)$, 这就说明每一项均不为 1, 将每一项按照 $\zeta_p^1,\cdots,\zeta_p^{p-1}$ 归并, 易得 $b=-(p-1)/4$.

若 $p\equiv 3(\mathrm{mod}\,4)$, 则 $\chi(-j)=-\chi(j)$, 因此可设 $b=(p-1)/2+b'$, 这里 b' 为剩余 (为配对) $(p-1)(p-3)/4$ 项和, 仿照上面的思路可知 $b'=-(p-3)/4$, 即 $b=(p+1)/4$.

综上可知 $(x-\alpha_0)(x-\alpha_1)=x^2+x+b\in\mathbb{Q}[x]$, 根据 p 模 4 的不同情形, 由求根公式直接得到

$$\{\alpha_0,\alpha_1\}=\{(-1\pm\sqrt{p})/2\},\quad p\equiv 1(\mathrm{mod}\,4), \tag{4.220}$$

$$\{\alpha_0,\alpha_1\}=\{(-1\pm\sqrt{-p})/2\},\quad p\equiv 3(\mathrm{mod}\,4), \tag{4.221}$$

$$\tag{4.222}$$

得证.

推论 4.30

设 p 为奇素数, 则 $\mathbb{Q}(\sqrt{\chi_p(-1)p})$ 为 $\mathbb{Q},\mathbb{Q}(\zeta_p)$ 的唯一二次中间域.

证明 $G=\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})\cong\mathbb{Z}_{p-1}^*$ 包含唯一子群 H 使得 $[G:H]=2$.

4.5.5 根多项式

4.5.6 $\mathbb{Q}$ 上的 Galois 扩张

定理 4.34

对任何有限 Galois 群 H, 存在对应的域扩张 $E/\mathbb{Q}$.

证明 设循环群分解 $H=H_1\oplus\cdots\oplus H_s$, 其中 $|H_i|=m_i$, 取不同的素数 $p_1,\cdots,p_s$ 使得 $p_i\equiv 1(\mathrm{mod}\,m_i)$, 再令 $n_0=1,n_i=p_1\cdots p_i$, 则 $\mathbb{Q}(\zeta_{n_{i-1}})$ 与 $\mathbb{Q}(\zeta_{p_i})$ 为无交扩张, 因此 $G=\mathrm{Gal}(\mathbb{Q}(\zeta_{n_s})/\mathbb{Q})=G_1\oplus\cdots\oplus G_s$, 这里 $G_i\cong\mathbb{Z}_{p_i-1}$. 因此 H 可以视为 G 的一个商群, 根据 FTGT 存在 $\mathbb{Q}(\zeta_{n_s})/\mathbb{Q}$ 的中间域 E 使得 $\mathrm{Gal}(E/\mathbb{Q})=H$.

上面的结论可以回答: 何时 Galois 扩张 $E/\mathbb{Q}$ 是分圆域的子域? $E/\mathbb{Q}$ 为 Abel 扩张就是一个合适的条件, 而这是一个著名定理

定理 4.35 (Kronecker-Weber)

$\mathbb{Q}$ 的任何 Abel 扩域都是某个分圆域的子域.

证明略.

定理 4.36

设 $f(x)\in\mathbb{Q}[x]$ 为素数 p 次不可约多项式，且有 $p-2$ 个实根.E 为 $f(x)$ 的分裂域，则 $\mathrm{Gal}(E/\mathbb{Q})=S_p$.

证明 显然 f 的剩下两个复根相互共轭，设其根 $\alpha_1,\cdots,\alpha_p$（前两个为共轭复根），设 τ 为复共轭映射，则 $\tau(\alpha_1)=\alpha_2,\tau(\alpha_2)=\alpha_1$，对其余有 $\tau(\alpha_i)=\alpha_i$.

推论 4.31

对任意有限群 G，存在 $\mathbb{Q}$ 的扩域 E 使得存在子域 B，满足 $\mathrm{Gal}(E/B)\cong G$.

4.5.7 判别式

定义 4.34 (判别式)

设 $f(x)\in F[x]$ 为 n 次多项式，根为 $\alpha_1,\cdots,\alpha_n$（在分裂域中），设

$$\delta=\prod_{i<j}(\alpha_i-\alpha_j),\quad \Delta=\Delta(f(x))=\delta^2, \tag{4.223}$$

则称 Δ 为 f 的判别式.

注

1. δ 依赖根的顺序，但 Δ 不依赖，仅与 f 有关.
2. 若 f 无重根则 $\Delta(f(x))\neq 0$.
3. Δ 是关于 f 根的对称多项式，因此它是关于 f 系数的多项式，故 $\Delta\in F$，与分裂域 E 的选择无关.
4. Δ 必定为 E 中的平方数，但不一定是 F 中的平方数.

引理 4.26

设 $f(x)\in F[x]$ 不可约，分裂域为 E，Galois 群 $G=\mathrm{Gal}(E/F)$，Δ 为 f 的判别式，则

1. 若 Δ 是 F 中的平方数，也即 $\delta\in F$，则 $G\subset A_n$.
2. 若 Δ 不是 F 中的平方数，业界 $\delta\notin F$，则 $G\not\subset A_n$.

证明 若 $\delta\in F$，则对任意 $\sigma\in G$，$\mathrm{sign}(\sigma)\delta=\sigma(\delta)=\delta$，因此 $\mathrm{sign}(\sigma)=1$，故 $G\subset A_n$，反之同理.

推论 4.32

设 $f(x)\in F[x]$ 为三次不可约多项式，$G=\mathrm{Gal}(E/F)$，若 $\Delta(f(x))\notin F$，则 $G=S_3$；若 $\Delta(f(x))\in F$，则 $G=A_3\cong\mathbb{Z}_3$.

命题 4.17

设 $f(x)\in F[x]$，$\Delta=\Delta(f(x))$.

1. 若 $f(x)=x^2+ax+b$，则 $\Delta=a^2-4b$.
2. 若 $f(x)=x^3+bx+c$，则 $\Delta=-4b^3-27c^2$.
3. 若 $f(x)=x^3+ax^2+bx+c$，则 $\Delta=-4a^3c+a^2b^2+18abc-4b^3-27c^2$.

证明

1. 此时 $a=-s_1=-(\alpha_1+\alpha_2),b=s_2=\alpha_1\alpha_2$，故

$$\begin{aligned}\Delta&=(\alpha_1-\alpha_2)^2 &(4.224)\\ &=(\alpha_1+\alpha_2)^2-4\alpha_1\alpha_2 &(4.225)\\ &=a^2-4b. &(4.226)\end{aligned}$$

2. 此时 $b = s_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1, c = -s_3 = -\alpha_1\alpha_2\alpha_3$. 注意到 Δ 为关于 s_1, s_2, s_3 的六次齐次多项式，或者说关于 b, c 的六次齐次多项式，故设 $\Delta = sb^3 + tc^2$，考虑 $f(x) = x^3 - x, g(x) = x^3 - 1$ 可知 $s = -4, t = -27$.
3. 换元显然.