近世代数复习

tip：此复习笔记为备考2026暑期夏令营所创. 按章进行, 每章内容分为书中全部定义与定理以及笔记内容. 重要程度用颜色分辨…

第一章 群

1.2 什么是群

引理 1（合成运算满足结合律） 设 $f:A\to B$, $g:B\to C$, $h:C\to D$ 均是集合的映射，则

$$h\circ(g\circ f)=(h\circ g)\circ f.$$

引理 2 映射 $f:A\to B$ 是一一对应的充分必要条件是存在映射 $g:B\to A$，使得 $f\circ g=1_B$, $g\circ f=1_A$.

定义：**半群**：封闭；结合律 $((a\circ b)\circ c=a\circ(b\circ c))$

交换半群：又满足交换律

如：$(-\mathbb{N},+)$ 为半群，$(-\mathbb{N},\times)$ 不是半群

$(GL_n(\mathbb{R}),+)$ 不是半群，$(GL_n(\mathbb{R}),\times)$ 是半群.

$GL_n(\mathbb{R})$ 为 n 阶可逆矩阵，$SL_n(\mathbb{Z})=\{A\in M_n(\mathbb{Z})\mid \det A=\pm1\}$

群：半群 + 幺元 + 逆元

Abel群：对 $\forall a,b\in G$，$a\cdot b=b\cdot a$（交换群）

例 1 设 M 为非负整数全体，$(M,+)$ 是含幺交换半群，幺元素是数 0，但它不是群，因为，只有 0 对于加法在 M 中才可逆.

Z, **Q**, **R**, **C** 对于加法均是阿贝尔群，分别叫做整数加法群，有理数加法群等等.

设 $(M,\cdot)$ 是含幺半群，我们以 $U(M)$ 或者 M^* 表示半群 M 中可逆元素全体.

定理 若 $(M,\cdot)$ 是含幺半群，则 $(U(M),\cdot)$ 是群.

(a) 全体 n 阶可逆复方阵形成乘法群，叫做复数上的 **n 次一般线性群**，表示成 $GL(n,\mathbf{C})$. 同样有群 $GL(n,\mathbf{R})$, $GL(n,\mathbf{Q})$ 等.

(b) 设 A 为非空集合，A 到自身之上的所有一一对应对于合成运算形成群，叫做集合 A 上的**对称群**或**全置换群**，表示成 $S(A)$，其中元素（即 A 到 A 的一一对应）叫做集合 A 上的置换.

(c) 设 n 为正整数，a 为整数 a 的模 n 同余类. 则集合

$$Z_n^*=\{\bar a\mid (a,n)=1\}$$

对于乘法形成阿贝尔群. 这个群有 $\varphi(n)$ 个元素，其中 $\varphi(n)$ 是 1 到 n 中与 n 互素的整数个数（$\varphi(n)$ 叫欧拉函数）.

设 G 是群. 若集合 G 有限，称 G 为有限群，否则叫无限群. 若有限群 G 共有 n 个元素，则 G 叫 **n 阶群**或叫 n 元群，$n=|G|$ 叫有限群 G 的阶.

例：$f,g\in\Sigma(A)$. 若 $|A|=\infty$，$g\circ f=id\Rightarrow f$ 为单射 $\not\Rightarrow$ 为双射

若 $|A|<\infty$，$g\circ f=id\Rightarrow f$ 为双射

例：$(\mathbb{Z}/n\mathbb{Z},\times)$ 为含幺半群. m 可逆 $\Leftrightarrow \gcd(m,n)=1$

$(\mathbb{Z}/n\mathbb{Z},+)$ 为 Abel 群. $a\sim b$ 若 $a\equiv b \bmod n$

定义 5 设 $(G,\cdot)$ 和 $(G',\circ)$ 是两个群. 映射 $f:G\to G'$ 叫做群 G 到群 G' 的同态，是指对 $a,b\in G$，

$$f(a\cdot b)=f(a)\circ f(b)\quad(\text{简记成 } f(ab)=f(a)f(b)).$$

此外，若 f 又为单射或满射，则 f 分别叫**单同态**或**满同态**. 如果同态 f 是一一对应，则称 f 是群 G 到群 G' 的**同构**. 这时，称群 G 和 G' 是同构的，表示成 $G\cong G'$ 或者 $f:G\cong G'$.　　证单射：$\ker f=\{1\}$.

事实上，彼此同构的群具有完全相同的群结构，群论中同构的群被视为同一个群

例：1. $GL_n(\mathbb{R})\xrightarrow{\det}\mathbb{R}^*$ 为群同态. $\det(AB)=\det A\cdot\det B$

2. G 为群. $\Sigma(G)=\{f:G\to G \text{ 群同态}\}\Rightarrow$ 半群（含幺 (id)）

$Aut(G)=\{f:G\to G \text{ 群同构}\}\Rightarrow$ 群

1.3 子群与陪集分解

定义 1 设 $(G,\cdot)$ 为群. A 为 G 的子集. 如果 $(A,\cdot)$ 为群，则称 A 为 G 的子群，表示成 $A\leqslant G$. 此外，若 $A\neq G$，则称 A 为 G 的**真子群**，表示成 $A<G$.

验证子群：①幺元 ②逆元 ③封闭性　　若 $AA^{-1}=A$　A 为子群

例：G 的两平凡子群：$\{1_G\}$, G.　　$(\mathbb{Z},+)$ 的两平凡子群：$n\mathbb{Z}$, $n=0,1$

$\mathbb{Z}/2\mathbb{Z}$ 无非平凡子群.　　对 $\forall n\geq1$, $n\mathbb{Z}$ 为 $(\mathbb{Z},+)$ 的子群

引理 1 设 G 是群，$A\leqslant G$. 定义 G 上的关系为：对于 $g,h\in G$，$g\sim h\Leftrightarrow gh^{-1}\in A$. 则 $\sim$ 是 G 上的等价关系，并且元素 g 对此等价关系的等价类是 Ag.

定义：$G=\coprod_{g\in R}Ag$　R 右陪集代表元系. Ag 为右陪集. 右陪集个数为 $|R|=[G:A]$. 称子群 A 对 G 的指数

定理 1（拉格朗日(J. Lagrange)） 设 G 为有限群，$A\leqslant G$. 则

$$|G|=|A|\cdot[G:A],$$

特别地，G 的每个子群的阶都是 G 的阶的因子.　→ 素数阶群只有平凡子群.

例：$[O(n):SO(n)]=2$　　$[\mathbb{Z}_{10}:\mathbb{Z}_{60}]=6$

$[\mathbb{C}:\mathbb{R}]=\infty$.（平面：直线）　$[\mathbb{R}:\mathbb{Q}]=\infty$

定理 2 设 G 是有限群，则 G 中每个元素 g 的阶均是 $|G|$ 的因子.

证明 由上所述知 g 是有限阶元素. 设 g 的阶为 n，则 $1=g^0,g^1,\cdots,g^{n-1}$ 是 G 中 n 个不同的元素，而 $g^n=1$. 不难看出它们形成 G 的一个 n 阶子群 A，于是，由定理 1 即知 $n=|A|$ 为 $|G|$ 的因子. 证毕.

定理：素数阶群一定是 Abel 群

一定同构于 $\mathbb{Z}_p$

定理：最小的非 Abel 群是 6 阶群.

只需证 4 阶群为 Abel 群.

对 4 阶群：$g\neq1\in G$. g 的阶为 2 或 4.

若阶为 2：$\forall a\in G$, $a^2=1$ $(a=a^{-1})$. 要证 $ab=ba\Leftrightarrow aba^{-1}b^{-1}=1\Leftrightarrow abab=1\Leftrightarrow(ab)^2=1$ 成立.

若阶为 4：$\{1,g,g^2,g^3\}\cong\mathbb{Z}_4$. 故可交换

定理 3 设 g 和 h 为群 G 中元素.

(1) 若 g 是 n 阶元素，则对每个正整数 m，g^m 的阶是 $\dfrac{n}{(m,n)}$；

(2) 若 $gh=hg$，元素 g 和 h 的阶为 m 和 n，并且 $(m,n)=1$，则 gh 的阶为 nm.

(1) 设 g^m 的阶为 N. 有 $(g^m)^{\frac{n}{(m,n)}}=(g^n)^{\frac{m}{(m,n)}}=1$. 有 $N\mid\frac{n}{(m,n)}$

又 $(g^m)^N=1\Rightarrow n\mid mN$ 即 $\frac{n}{(n,m)}\mid\frac{m}{(n,m)}N$. 又 $\left(\frac{n}{(m,n)},\frac{m}{(m,n)}\right)=1\Rightarrow\frac{n}{(m,n)}\mid N$　} $N=\frac{n}{(m,n)}$

(2). 设 gh 的阶为 N，有 $(gh)^{mn}=(g^m)^n(h^n)^m=1\Rightarrow N\mid mn$.

又 $g^nh^n=g^n$ 由(1)知其阶为 $\frac{N}{(n,N)}$，有 $m=\frac{N}{(n,N)}$ 即 $m\mid N$，同理 $n\mid N\Rightarrow mn\mid N$　} $N=mn$

定理：$A\leq B\leq G$. 且 $[G:B]<+\infty$. $[B:A]<+\infty$. 则 $[G:A]<+\infty$ 且 $[G:A]=[G:B][B:A]$.

定理：若 $A,B\leq G$. 且 G 为有限群. 则 $|AB|\cdot|A\cap B|=|A|\cdot|B|$，其中 $AB=\{a\cdot b\mid a\in A, b\in B\}$

$AB=\coprod_{1\leq i\leq[AB:A]}Ab_i$　　$B=\coprod_{1\leq i\leq[B:A\cap B]}(A\cap B)b_i$

对 $Ab=Ab'\Leftrightarrow b'b^{-1}\in A\Leftrightarrow b'b^{-1}\in A\cap B\Leftrightarrow(A\cap B)b=(A\cap B)b'$ 于是两陪集分解个数相同. 证毕

有 $\frac{|G|}{|A\cdot B|}\cdot\frac{|G|}{|A\cap B|}=\frac{|G|}{|A|}\cdot\frac{|G|}{|B|}$ 则有

① $[G:A\cap B]\leq[G:A][G:B]$

② $G=A\cdot B\Leftrightarrow[G:A\cap B]=[G:A][G:B]$

③ 若 $[G:A]$ 与 $[G:B]$ 互素，则有 $G=A\cdot B$

例：$G=\mathbb{Z}_{30}$. $A=5\mathbb{Z}_{30}$　$B=6\mathbb{Z}_{30}$. $[G:A]=5$. $[G:B]=6$ 于是有 $G=A+B$.　← 因为是加法群. $A\cdot B$ 为 $A+B$.

定义 2 设 A 和 B 是群 G 的两个子集. 如果存在 $g\in G$ 使得 $g^{-1}Ag=B$，则称 A 和 B 共轭.

不难看出，群 G 的子集之间的共轭关系是等价关系. 每个等价类叫做**共轭类**. 易知 $|g^{-1}Ag|=|A|$，从而彼此共轭的集合有相同的势数. 又若 A 是 G 的子群，易知 $g^{-1}Ag$ 也是 G 的子群，叫做 A 的**共轭子群**. 从而 G 的所有子群也分成一些共轭类. 元素 $g^{-1}ag$ 叫做 a 的共轭元素.

定义：若 $M\leq G$. $N_G(M)=\{g\in G\mid g^{-1}Mg=M\}$. 有 $N_G(M)\leq G$. 称为 M 的正规化子.（← 对 M 共轭的元素集合）

定理 5 设 M 是群 G 的子集，则与 M 共轭的子集个数等于 $[G:N_G(M)]$.

定义：若 $M\leq G$. $C_G(M)=\{g\in G\mid g^{-1}mg=m,\ \forall m\in M\}$. 称为 M 的中心化子（← 与 M 中每个元素交换的元素集合）　有 $C_G(M)\leq N_G(M)$.

$C(G)=\{g\in G\mid\forall h\in G, gh=hg\}$ 称为 G 的中心 ← 与固有集合中每个元素交换的元素集合

若 $G=C(G)$ 则 G 为 Abel 群；$C(G)$ 为 Abel 群　　$\forall g\in G$. $C_G(g)=N_G(g)$

有 $g\in C(G)$: $gx=xg$

系 设 $a\in G$，则与 a 共轭的元素个数等于 $[G:C_G(a)]$.

定理 6 设 p 为素数，$n\geqslant1$，G 为 p^n 阶群. 则 $|C(G)|>1$，即 G 有非平凡（即不为 1）的中心元素.

$g\in G$：$|C_G(g)|=\dfrac{|G|}{|g\text{ 的共轭类}|}$

定理 7 对每个素数 p，p^2 阶群 G 均是阿贝尔群.

对子群 H　$\dfrac{N_G(H)}{C_G(H)}\cong Aut(H)$

M 为 G 子集：$|N_G(M)|=\dfrac{|G|}{|M\text{ 的共轭子集}|}$

1.4 循环群

如果群 G 自身由子集 S 生成，即 $G=\langle S\rangle$，则称 S 是 G 的一个**生成元系**，如果 $G=\langle S\rangle$ 并且 S 是有限集，称 G 是**有限生成群**. 特别若群 G 由一个元素 a 生成，即 $G=\langle a\rangle$，称 G 是**循环群**. 循环群是一类最简单的群，本节研究这种群的性质(子群特性，生成元特性以及确定它们的自同构群).

定理 1 无限循环群同构于整数加法群 $\mathbb{Z}$，n 阶有限循环群同构于 $\mathbb{Z}_n$. 从而同阶循环群彼此同构(不同阶循环群当然不同构).

定理 2 循环群的子群均是循环群. 详言之，设 $G=\langle a\rangle$ 是循环群.

(1) 若 G 是无限循环群，则对每个正整数 m，G 恰有一个指数为 m 的子群 $G_m=\langle a^m\rangle$，并且它们和 $\{1\}$ 是 G 的全部子群；

(2) 若 G 是 n 阶有限循环群，则对 n 的每个正因子 m，G 恰有一个指数为 m 的 $\frac{n}{m}$ 阶子群 $G_m=\langle a^m\rangle$，并且它们是 G 的全部子群.

定理 3 设 $G=\langle a\rangle$ 是循环群.

(1) 若 G 为无限循环群，则 G 的生成元只有 a 和 a^{-1}；

(2) 若 G 为 n 阶有限循环群，则 G 的生成元共有 $\varphi(n)$ 个，它们是 a^k $(1\leqslant k\leqslant n,(k,n)=1)$.

定理：若 G 为有限群，则 $g\in G$ 均为有限阶元素

$A_g=\{1, g, g^2\cdots; g^{-1}, g^{-2}\cdots\}$ A_g 为 G 的子群. $\begin{cases} g\text{的阶数为}n \Leftrightarrow A_g\cong \mathbb{Z}_n \\ g\text{的阶数为}\infty \Leftrightarrow A_g\cong\mathbb{Z}\end{cases}$

对于阶数为 ∞: $\mathbb{Z}\cong G$
① $m\mathbb{Z}, m\in\mathbb{N}^+$ $\langle g^m\rangle$
② 生成元: ±1 (1个) g, g^{-1}
③ $Aut(\mathbb{Z})=\{\pm id\}$ $Aut G=\{id, 取逆\}$

对于阶数为 n: $\mathbb{Z}\cong G$
① $m\mathbb{Z}$ 要求 $m|n$ $\langle g^m\rangle$ 要求 $m|n$
② 生成元: $\bar{k}$ $(k,n)=1$ g^k, 要求 $(k,n)=1$
③ $|Aut\,\mathbb{Z}_n|=\varphi(n)$ $|Aut\,G|=\varphi(n)$
$Aut\,\mathbb{Z}_n=\mathbb{Z}_n^*=\{\bar{k}\mid(k,n)=1\}$ $Aut\,G=\langle g^k\rangle$ $(k,n)=1$

1.5 正规子群、商群与同态定理

定义 群 G 的子群 N 叫做 G 的**正规子群**，是指对每个 $g\in G$，$g^{-1}Ng=N$. 如果 N 是 G 的正规子群，则表示成 $N\lhd G$.

引理 1 设 N 是 G 的子群. 则下列条件彼此等价：

(1) $N\lhd G$；

(2) 对于每个 $g\in G$，$gN=Ng$；

(3) $N_G(N)=G$；

(4) G 对于 N 的每个左陪集均是右陪集.

定义：商群: $G/N=\{gN=Ng\mid g\in G\}$, $|G/N|=[G:N]$
可表示为 $\bar{g}=gN=Ng$ ← N一定为G正规子群, G/N元素为N的陪集

若 G 为 Abel 群, 任意子群为正规子群

定理:(同构基本定理) 若 $f: G\to G'$ 为群同态. 则 $G/Ker f\cong Im f$
∵ 同构. ∴ $\cong G'$

例: $GL_n(\mathbb{R})\xrightarrow{det}\mathbb{R}^*$
$Ker(det)=SL_n(\mathbb{R})$. 则 $GL_n(\mathbb{R})/SL_n(\mathbb{R})\cong\mathbb{R}^*$
$SL_n(\mathbb{R})\lhd GL_n(\mathbb{R})$. 即若 $det A=1$. 有 $det BAB^{-1}=1$

例: $\mathbb{Z}\xrightarrow{g}\mathbb{Z}_m$ $g(a)=\bar{a}$ $Ker g=m\mathbb{Z}$ $\mathbb{Z}/m\mathbb{Z}\cong\mathbb{Z}_m$

定理: 设 $N\lhd G$. 则 $\{M\mid N\leq M\leq G\}\xleftrightarrow{1:1}\{\bar{M}\mid\bar{M}\leq G/N\}$

定理: 设 $N\lhd G$, $M\lhd G$, $N\leq M$. 则 $G/M\cong\frac{G/N}{M/N}$ 构造 $G/N\to G/M$

定理: 设 $N\lhd G$. $H\leq G$. 则 $(H\cap N)\lhd H$. $N\lhd NH\leq G$. $NH/N\simeq H/H\cap N$
由 $N\lhd G$: 对 $\forall h\in H$. $Nh=hN$ 即 $NH=HN$.
$(NH)(NH)^{-1}=(NH)(H^{-1}N^{-1})=NHHN=NHN=NNH=NH\Rightarrow NH\leq G$ ← 证子群方法: $AA^{-1}=A$
由 $N\lhd G$, $N\subset NH\subset G$: $N\lhd NH$
构造映射 $f: H\to NH/N$. 即对 $h\in H$. $h\mapsto Nh$ 满同态
有 $h\in Ker f\Leftrightarrow f(h)=Nh=N\Leftrightarrow h\in N\Leftrightarrow h\in N\cap H$
于是 $Ker f=N\cap H\Rightarrow H/N\cap H\simeq NH/N$. 证毕

问题: $N\lhd G$, $N'\lhd G'$. $G/N\simeq G'/N'$. 是否 $G\simeq G'$?
否: 对 $G=\mathbb{Z}_4$ $G'=\mathbb{Z}_2\times\mathbb{Z}_2$ 且 $G/N\simeq\mathbb{Z}_2$ 而 $\mathbb{Z}_4$ 中有2个4阶元 $\bar{1},\bar{3}$, 1个2阶元 $\bar{2}$
$N=2\mathbb{Z}_4\simeq\mathbb{Z}_2$ $N'=\mathbb{Z}_2\times\{0\}$ $G'/N'\simeq\mathbb{Z}_2$ $\mathbb{Z}_2\times\mathbb{Z}_2$ 中 3个2阶元 $(\bar{0},\bar{1})(\bar{1},\bar{0})(\bar{1},\bar{1})$
$N\lhd M$. $M\lhd G$. 是否 $N\lhd G$?
否: $\mathbb{Z}_2\lhd K_4\lhd S_4$. 但 $\mathbb{Z}_2 \ntriangleleft S_4$

1.6 置换群

对于集合 $\Sigma=\{a_1,\cdots,a_n\}$. $|\Sigma|=n$. $S(\Sigma)=\{\Sigma$ 到 Σ 的双射$\}$, $|S(\Sigma)|=n!$
S_n 称为对称群, S_n 的子群为置换群

定义: 轮换: $a_1a_2\cdots a_k\mapsto a_ka_1\cdots a_{k-1}$ 简写为 $(a_1a_2\cdots a_n)$ 对换: 长度为2的轮换
每个置换都能表示为一些轮换的乘积. 也能表示成一些对换的乘积
置换 σ 的阶是所有轮换长度的最小公倍数

$S_n\xrightarrow{f}\{\pm1,\times\}$ 有 $Ker f=A_n$ 交错群. $|A_n|=\frac{n!}{2}$
σ 群同态 1 偶置换 $A_n\lhd S_n$. $[S_n:A_n]=2$
-1 奇置换

定理 1 将 S_n 看作是 $\{1,2,\cdots,n\}$ 上的对称群，则 $n\geqslant2$ 时，$(12),(13),\cdots,(1n)$ 是 S_n 的一个生成元系.

证明 由于每个置换均是有限个对换之积，而当 $i\neq j$，$i\neq1$，$j\neq1$ 时，$(ij)=(1i)(1j)(1i)$. 证毕.

定理 2 当 $n\geqslant3$ 时，全体长为 3 的轮换形成 A_n 的一个生成元系.

证明 设 $\sigma\neq1$ 是偶置换，则 σ 是偶数个对换之积. 从而只需证任意两个对换之积可用长为 3 的轮换表示即可. 对于 $\tau=(ij)(rs)(i\neq j,r\neq s)$. 如果 $(ij)=(rs)$，则 $\tau=1$. 如果 $j=r$，$i\neq s$，则 $\tau=(jsi)$. 如果 i,j,r,s 两两不等，则 $\tau=(ris)(ijr)$. 证毕.

现在研究 S_n 中元素的共轭分类. 设 $\sigma\in S_n$，设将 σ(唯一地)表示成没有公共元素的轮换之积. 如果其中长为 r 的轮换共有 λ_r 个 $(1\leqslant r\leqslant n)$，则称置换 σ 的**型**为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$. 例如 S_7 中的置换 $\sigma=(123)(45)$ 的型为 $1^2 2^1 3^1 4^0 5^0 6^0 7^0$. 当 $\lambda_i=0$ 时(即 σ 中没有长为 i 的轮换)，$i^{\lambda_i}=i^0$ 可略去. 例如前面 σ 的型为 $1^2 2^1 3^1$.

定理 3 对称群 S_n 中两个置换共轭的充要条件是它们有相同的型.

定义: σ 可以写为长度为 i 的轮换的 λ_i 次乘积, 称 σ 的型, 记为 $1^{\lambda_1}2^{\lambda_2}\cdots n^{\lambda_n}$, 有 $\sum_{i=1}^{n}i\lambda_i=n$.

定义 群 G 称为**单群**，如果 $G\neq\{1\}$，并且 G 的正规子群只有 $\{1\}$ 和 G 本身.

例如：素数阶群 $\mathbb{Z}_p$ 是循环群，它只有平凡子群 $\{1\}$ 和 $\mathbb{Z}_p$，从而是单群. 由 1.4 节定理 2 知，阿贝尔群是单群的充要条件是它为素数阶(循环)群. 所以除了素数阶(循环)群之外，其他单群均是非阿贝尔群. 决定全部有限非阿贝尔单群的问题具有漫长而有趣的历史. 这个著名群论问题最终于 1981 年才完全解决. 可是人们很早就发现：

定理 4 当 $n\geqslant5$ 时，交错群 A_n 是单群.

S_3: 1 1^3 id
3 $1^1 2^1$ (12) (13) (23)
2 3^1 (123) $(132)=(123)^2$

S_3 的正规子群? 对 $N\lhd S_3$
$|N|=2$, 或 3 (由 Lagrange 定理)
若有 (12) 类. 对 $g=(123)$. $g(12)g^{-1}\neq(12)$. 同理均不是. 于是 $N=\{id,(123),(132)\}$. $[S_3:N]=2$
事实上正规子群若包含 (12) 类, 则一定包含全部 (12) (23) (13) 则含 (12) 的正规子群 N 有 $|N|=4$. 矛盾!
$\nearrow A_3$

S_3 的子群? 对 $A\leq S_3$. $|A|=2$ 或 3 (非平凡)
A 为循环群. $|A|=2$ $\{1,(12)\}$ $\{1,(13)\}$ $\{1,(23)\}$
$|A|=3$ $\{1,(123),(132)\}$

S_4: 1 1^4 id
6 $1^2 2^1$ (12) (13) ⋯ (34)
8 $1^1 3^1$ (123) ⋯ (234)
3 2^2 (12)(34), (13)(24), (14)(23)
6 4^1 (1234) (1243) (1324) (1342) (1423) (1432)

S_4 的正规子群? 对 $N\lhd S_4$
$|N|=2, 3, 4, 6, 8, 12$ → A_4
对 $|N|=4$. $K=\{1,(12)(34),(13)(24),(14)(23)\}$

定理: $n\geq5$ 时 A_n 为 S_n 唯一非平凡正规子群

1.7 群在集合上的作用

设 Σ 是一个集合，$S(\Sigma)$ 是 Σ 上的对称群，群 G 到 $S(\Sigma)$ 的每个同态 $f: G\to S(\Sigma)$ 都叫做**群 G 在集合 Σ 上的一个置换表示**. 如果 f 是单同态，则称 f 是**忠实表示**. 这时，对于 G 中不同的元素 g，$f(g)$ 是 Σ 上不同的置换. 群 G 借助于置换表示 f 作用在集合 Σ 之上，也就是说，元素 $g\in G$ 在集合 Σ 上的作用看成是置换 $f(g)$，对于每个 $a\in\Sigma$，定义 $ga=f(g)a$.

设 $\pi: G\to S(\Sigma)$ 是一个置换表示. 在 Σ 上定义如下的关系：对于 $a,b\in\Sigma$，$a\sim b\Leftrightarrow$ 有 $g\in G$，使得 $ga=b$. 容易验证这是一个等价关系.

对于上述等价关系，Σ 中元素 a 所在的等价类是 $[a]=Ga=\{ga\mid g\in G\}$. 每个等价类叫一个 **G-轨道**，或简称**轨道**. 于是集合 Σ 分拆成一些轨道，在同一轨道中，可以通过某个 $g\in G$ 的作用将其一个元素变为另一个元素，而不同轨道中的两个元素不可以这样做. 如果 G 在 Σ 上的作用只有一个轨道，则称 G 在 Σ 上是**传递**的. 显然，如果将 G 看成它在某一个 G-轨道上的作用，则 G 显然是传递的.

定义: 左正则表示指 $\rho: G\to S(G)$ $\rho(g)a=ga$ =看成单同态, 即均忠实
右正则表示指 $\rho: G\to S(G)$ $\rho(g)a=ag^{-1}$

定理 1(凯莱(Cayley)) 每个群均同构于某个置换群.

例: $G\to S(\Sigma)$ Σ 为所有 $\{1,2,3,4\}$ 构成的二元子集合. $|\Sigma|=6$.
设 $G=S_4$: 有 $(12)\mapsto(24)(35)$ (计算后)
计算: $\Sigma=\{(12),(13),(14),(23),(24),(34)\}$ 即 $\sigma(12)=(24)(35)$
$\{(21),(23),(24),(13),(14),(34)\}$

例: $A\leq G$. $\Sigma=\{hA\mid h\in G\}$. $|\Sigma|=[G:A]$ $\rho: G\to S(\Sigma)$ $g\mapsto\rho(g):\Sigma\to\Sigma$ 为置换
$hA\mapsto g(hA)$
对 $g\in Ker\rho$. $\rho(g)=id$. → $Ker\rho$: $hA=ghA\Rightarrow A=h^{-1}ghA\Rightarrow g\in hAh^{-1}$ $\forall h\in G$ 即 $Ker\rho=\bigcap_{h\in G}hAh^{-1}$

例: $A\leq G$. $\Sigma=\{hAh^{-1}\mid h\in G\}$. $\rho: G\to S(\Sigma)$ $g\mapsto\rho(g):\Sigma\to\Sigma$
$hAh^{-1}\mapsto ghAh^{-1}g^{-1}$
$Ker\rho$: $hAh^{-1}=ghAh^{-1}g^{-1}\Rightarrow A=h^{-1}ghA(h^{-1}gh)^{-1}\Rightarrow h^{-1}gh\in N_G(A)$. $g\in hN_G(A)h^{-1}$. $Ker\rho=\bigcap_{h\in G}hN_G(A)h^{-1}$

设群 G 作用于集合 Σ 之上，则对每个元素 $a\in\Sigma$，$G_a=\{g\in G\mid ga=a\}$ 是 G 的一个子群，叫做元素 a 的**固定子群**.

定理 2(轨道公式) 设有限群 G 作用于集合 Σ 上，$a\in\Sigma$，则
$$|G|=|G_a|\,|[a]|.$$
若 $x,y\in[x]$. $|G_x|=|G_y|$

系 设有限群 G 作用在有限集 Σ 上是传递的，则对于每个 $a\in\Sigma$，

$$|G|=|G_a||\Sigma|.$$

注意：(1) 当 G 是无限群时，如果 $[G:G_a]$ 有限，则 $|[a]|=[G:G_a]$ 也是正确的.

(2) 利用例 3 的共轭表示和定理 2，我们重新得到前面所证的：设 A 为群 G 的子集，则 A 的共轭子集个数等于 $[G:N_G(A)]$.

引理 1 设 G 是 $2n$ 阶群，$2\nmid n$，则 G 必有指数为 2 的正规子群.

证明 考虑 G 的左正则表示 $\rho: G\to S(G)=S_{2n}$. 由于 ρ 是忠实表示，$G\cong\rho(G)$，因此只需对置换群 $\rho(G)$ 证明该引理. 注意群 G 中必有 2 阶元素 $g, g\neq 1, g^2=1$. 由于 $\rho(g)a\neq a$，$\rho(g)^2a=a$，$\forall a\in G$，置换 $\rho(g)$ 是一些对换 $(a, \rho(g)a)$ 之积. G 共有 $2n$ 个元素，从而 $\rho(g)$ 是 n 个对换之积. 由假设 n 是奇数，$\rho(g)$ 为奇置换. 我们证明了群 $\rho(G)$ 中含有奇置换，从而 $\rho(G)$ 中的偶置换构成了 $\rho(G)$ 的指数为 2 的子群，指数为 2 的子群必是正规的，证毕.

例： 设 $A\le G$, $[G:A]=n$. 则 G 中必存在正规子群 $N\lhd G$ 且 $N\le A$. 使得 $[G:N]\mid n!$

证明：$\Sigma=\{hA\mid h\in G\}$, $|\Sigma|=[G:A]$. $G\xrightarrow{\rho_A}S(\Sigma)=S_n$. 取 $N=\operatorname{Ker}\rho_A\le A$

有 $G/\operatorname{Ker}\rho_A=\operatorname{Im}\rho_A\le S_n\Rightarrow[G:N]\mid n!$ 成立

引理： 设 $A\le G$, $[G:A]=p$, p 为 $|G|$ 最小素因子. 则 $A\lhd G$.（G 为有限群）

$G\xrightarrow{\rho_A}S_p$ $\operatorname{Ker}\rho_A\le A$. $[G:\operatorname{Ker}\rho_A]\mid p!\Rightarrow[G:\operatorname{Ker}\rho_A]=p.\Rightarrow A=\operatorname{Ker}\rho_A$

1.8 西罗定理

有若 $A\le G$, $|A|\mid|G|$. 问题：① 是否对 $\forall m\mid|G|$, 是否一定存在 A, $|A|=m$? 否. 如：$A_n(n\ge5)$ 不存在半大小的子群

② ⋯ $m=p^r\mid|G|$. ⋯ ⋯ ⋯？是

定理 1 设 G 是有限群，p 为素数，r 是正整数，p^r 是 $|G|$ 的因子. 用 $N(p^r)$ 表示 G 的 p^r 阶子群的个数. 则 $N(p^r)\equiv1(\mathrm{mod}\ p)$. 特别地，若 $p^r\mid|G|$，则 G 至少存在一个 p^r 阶子群.

定义： 设 $p^m\mid|G|$. $p^{m+1}\nmid|G|$. 则 G 的每个 p^m 阶子群称为 G 的西罗 p-子群

定理： 设 $A\le G$. 且 $|A|=p^r\mid|G|$, 则存在 $g\in G$ 与 G 的某个西罗 p-子群 P s.t. $g^{-1}Ag\le P$

Sylow 定理： 设 $p\mid|G|$. ① 则西罗 p-子群存在且个数 $\equiv1\ \mathrm{mod}\ p$

② 西罗 p-子群彼此共轭

③ 若 P 为 G 的某个西罗 p-子群，则 G 的西罗 p-子群的个数为 $[G:N_G(P)]$ ☆

唯一的西罗子群必定正规的.

系 1 设素数 p 是 $|G|$ 的因子，则群 G 的每个 p 方幂阶的子群 B 均包含在 G 的某个西罗 p-子群内.

证明 仍以 Σ 表示 G 的全部西罗 p-子群，由定理 2 可知 $|\Sigma|\equiv1(\mathrm{mod}\ p)$. 将 B 共轭作用在 Σ 上，每个 B-轨道的长度是 $|B|$ 的因子，从而为 p 的方幂. 由 $|\Sigma|\equiv1(\mathrm{mod}\ p)$ 可知必有长为 1 的 B-轨道 $\{P\}$. 与证明定理 2 的 (2) 一样可由此推出 $BP=P$，于是 $B\le P$，即 B 包含在西罗 p-子群 P 内. 证毕.

系 2 设 P 是 G 的西罗 p-子群，$A\le G$，且 $N_G(P)\le A$，则 $N_G(A)=A$.

证明 设 $g\in N_G(A)$，则 $g^{-1}Ag=A$，从而 $g^{-1}Pg\le g^{-1}Ag=A$，由于 $P\le N_G(P)\le A\le G$，从而 P 为 A 的西罗 p-子群. 再由 $g^{-1}Pg\le A$，$|P|=|g^{-1}Pg|$，知 $g^{-1}Pg$ 也是 A 的西罗 p-子群. 由定理 2 即知存在 $a\in A$，使得 $a^{-1}(g^{-1}Pg)a=P$，即 $ga\in N_G(P)\le A$. 于是 $g\in A$. 证毕.

系 3（弗拉梯尼 (Fratini)） $M\lhd G$，P 为 M 的西罗 p-子群，则

$$G=MN_G(P).$$

证明 对每个 $g\in G$，$g^{-1}Pg\le g^{-1}Mg=M$. 于是由定理 2 知有 $k\in M$ 使得 $k^{-1}(g^{-1}Pg)k=P$，即 $gk\in N_G(P)$. 从而 $g=(gk)k^{-1}\in N_G(P)M=MN_G(P)$. 证毕.

推论： 设 $p\mid|G|$. 则 G 中一定有 p 阶元素

定理： 若 p, q 为素数. 则 pq 阶群非单群.

若 $p=q\Rightarrow p^2$ 阶群为 Abel 群. 有 p 阶子群. 正规.

若 $p\neq q$. 设 $p>q\Rightarrow N(p)=np+1\mid q\Rightarrow n=0$. 有 1 个西罗-$p$ 子群. 正规, 又 $|P|=p$ 不平凡.

定理： 若 p, q 为素数. 则 p^2q 阶群非单群（证明类似）

证明 若 $p=q$，已证过 p^3 阶群 G 必有非平凡的中心 $C(G)$，且 $C(G)$ 有 p 阶子群 N，显然 $N\lhd G$. 因此 G 不是单群.

如果 $p>q$，则 $N(p^2)=np+1\mid q$，$q<p$，于是 $n=0$. G 有正规的 p^2 阶西罗子群，G 不是单群.

最后设 $p<q$. 则 $N(q)=nq+1\mid p^2$. 如果 $N(q)=1$，则 G 有正规 q 阶子群，G 不是单群. 由于 $p<q$，$N(q)$ 不能为 p. 最后若 $N(q)=p^2$，即 G 有 p^2 个 q 阶子群，它们共占据 G 的 $p^2(q-1)+1$ 个元素，余下 p^2-1 个元素和 1_G 便构成 G 的唯一的 p^2 阶西罗子群 P，$P\lhd G$. 所以 G 也不是单群. 证毕.

例 1 148 阶群不是单群.

证明 取 $p=37\mid148$，则 $N(37)\equiv1(\mathrm{mod}37)$. 从而 $N(37)=37l+1$. 由于 148 阶群 G 的全部西罗 37-子群形成一个共轭类，其总数应当是 $|G|=148$ 的因子，即 $N(37)=37l+1\mid148$. 于是 $37l+1\mid4$，这只能 $l=0$，即 $N(37)=1$. 因此 G 只有一个 37 阶子群，从而必然是正规子群，G 不是单群.

例 2 56 阶群 G 不是单群.

证明 与前例一样，$N(7)=7n+1\mid56$，从而 $7n+1\mid8$，于是 $N(7)=1$ 或 8. 如果 $N(7)=1$，则 7 阶西罗子群是正规的；如果 $N(7)=8$，令 $P_1, P_2, \cdots, P_8$ 是 G 的 8 个不同的 7 阶子群，它们中的任意两个只有公共元素 1_G，合起来共占了 $7\times8-7=49$ 个元素，余下 $56-49=7$ 个元素加上 1_G 必然形成 G 的 8 阶西罗 2-子群，从而 G 的西罗 2-子群只有一个，必为正规子群. G 不是单群.

命题： 6 阶非 Abel 群只有 S_3.

证明：$|G|=6=2\times3$. 西罗 2 子群的个数 $=2l+1\mid3$ 有一 Sylow 3-子群 N.

① $l=1$. 有唯一 Sylow 2-子群 H. $H\lhd G$. $N\cap H=\{e\}$. 又 $|N|\cdot|H|=|G|$. $N\lhd G$, 有 $G=N\rtimes H$

又 $H\lhd G$. $G=N\times H\cong\mathbb{Z}_3\times\mathbb{Z}_2\cong\mathbb{Z}_6$ 为循环群. 故 G 为 Abel 群

② $l=2$. 有 3 个 Sylow 2-子群. 记为 H_1, H_2, H_3. 构造 $\rho: G\to S_3$ 在 G 左陪集集合上作用. 有 $\operatorname{Ker}\rho=\bigcap_{g\in G}gHg^{-1}=H_1\cap H_2\cap H_3=\{e\}$. 因为 $[G:H]=3$

为单同态. 又 $|G|=|S_3|=6$. 有限群上单同态一定同构. 则 $G\cong S_3$. 非 Abel 群.

定理： 非 Abel 单群的最小阶数是 60.

我们已经有的结论：① p^n (p 素, $n\ge2$) 阶群有非平凡中心. 故有非平凡正规子群.

② pq. p^2q (p, q 素) 阶群均非单群

③ $2m$ (m 奇数) 阶群不是单群

④ p 阶循环群为 Abel 群

于是只需考虑 24. 36. 40. 48. 56 阶群. 又已证 56 阶群非单群. 易知 40 阶群有唯一的西罗-5 子群

下证 48 阶群非单群：有 $48=2^4\times3$ 则西罗 2 子群的个数为 1 或 3. 若为 1. 显然非单群

若为 3. 设三西罗-2 子群为 P_1, P_2, P_3. 诱导自然同态 $\rho: G\to S_3$. 有 $|G|>|S_3|$ 于是非单同态. 则 $\operatorname{Ker}\rho\neq\{1_G\}$

不为 G → 又若 $\operatorname{Ker}\rho=G\Rightarrow$ 对 $\forall g\in G$. $gP_ig^{-1}=P_i\Rightarrow P_1, P_2, P_3$ 均为 G 的正规子群.

但 P_1, P_2, P_3 是共轭的 $\Rightarrow P_1=P_2=P_3$ 与三个西罗-2 子群相矛盾！→ 若正规子群共轭，它们一定相等

于是有 $\operatorname{Ker}\rho\lhd G$ 为 G 的非平凡正规子群. 24 阶群类似可证 ($\forall g\in G$. $gHg^{-1}=H$. 又 $\exists g_1\in G$. $g_1Hg_1^{-1}=K\Rightarrow K=H$)

下证 36 阶群非单群：有 $36=2^2\times3^2$ 则西罗-3 子群有 1 或 4 个. 若为 1. 显然非单群

若为 4. 同上方法可证

1.9 自由群与群的表现（只需看直积部分）

自由群： 无任何约束的，最一般的群. 除逆元存在外. 无 $xy=yx$ 或 $x^2=1$ 等关系.

例： $S=\{a, b\}$. S 生成的自由群：$\{1, a, b, a^2, ab, ba, b^2, a^{-1}b, \cdots\}$ 两个或以上生成元的自由群一定是非 Abel 的

有限集生成的自由群称为有限生成自由群. 元素为 S 与 S^{-1} 的无限乘积.

定理： 任意（有限生成）群均为（有限生成）自由群的商群

定义 1 设 S 为任意集合，表现为

$$F=\langle S\mid ba=ab,\ \forall a, b\in S\rangle$$

的群叫做以 S 为基（或在 S 上）的自由阿贝尔群（除了交换性条件之外不再有任何关系）.

定义 2 设 $G_1, \cdots, G_n$ 是群，在集合的直积

$$G=G_1\times\cdots\times G_n=\{(g_1, \cdots, g_n)\mid g_i\in G_i, 1\le i\le n\}$$

中定义运算

$$(g_1, \cdots, g_n)(g_1', \cdots, g_n')=(g_1g_1', \cdots, g_ng_n').$$

定理 2 设 $G_1, \cdots, G_n\lhd G$, $n\ge2$. 则以下三个条件是彼此等价的：

(1) $G=G_1\times\cdots\times G_n$；

(2) G 中每个元素可以唯一表示成 $g=g_1\cdots g_n$，其中 $g_i\in G_i$；

(3) $G=G_1\cdots G_n$，且对每个 $m(1<m\le n)$，有 $(G_1G_2\cdots G_{m-1})\cap G_m=\{1\}$.

特别地，$G=H\times N\Leftrightarrow$ ① $G=HN=\{hn\mid h\in H, n\in N\}$ 即证 $\forall g$, $\exists h, n$. $g=hn$. 且 $hn=e\Leftrightarrow h=e, n=e$

② $H\cap N=\{e\}$.

③ $H, N\lhd G$.

如果 $G\cong Z^r$，则 r 叫做有限生成自由阿贝尔群 G 的**秩**，记为 $\operatorname{rank}(G)$. 综合上述，我们证明了下面的结构定理：

定理 3 有限生成自由阿贝尔群 G 同构于有限个无限循环群的直积，$G\cong Z^r$，$r=\operatorname{rank}(G)\ge1$. 两个这样的群 G 和 G' 同构 $\Leftrightarrow\operatorname{rank}(G)=\operatorname{rank}(G')$.

系 设 S 和 S' 是有限生成自由阿贝尔群 G 的两组基，则 $|S|=|S'|$.

1.10 有限生成 Abel 群的结构.

定理 1 有限生成自由阿贝尔群 F 的每个子群 $G(G\neq\{0\})$ 仍是有限生成自由阿贝尔群，且 $\operatorname{rank}(G)\le\operatorname{rank}(F)$. 更确切地说，令 $n=\operatorname{rank}(F)$，则存在 F 的一组基 $\{x_1, \cdots, x_n\}$，一个整数 $r(1\le r\le n)$ 和一组正整数 $d_1, \cdots, d_r$，使得 $d_1\mid d_2\mid\cdots\mid d_r$，并且 G 是以 $\{d_1x_1, \cdots, d_rx_r\}$ 为基的自由阿贝尔群.

定理 2 每个有限生成阿贝尔群 A 均同构于 $Z^r\oplus Z_{m_1}\oplus\cdots\oplus Z_{m_t}$，其中 $r, t\ge0$，$1<m_1\le\cdots\le m_t$ 且 $m_1\mid m_2\mid\cdots\mid m_t$.

定义： 设 A 为 Abel 群. $A_t=\{a\in A\mid\exists m\in\mathbb{Z}, ma=0\}$ 有 $A_t\le A$. 为扭子群.

tip：若 A 为有限生成 Abel 群. 则 A_t 为有限群；A 为无限群时不成立. 如 $A=\mathbb{Z}_1\oplus\mathbb{Z}_2\oplus\cdots$ $A=A_t$

定理 3 设 A 和 B 是有限生成阿贝尔群.

(1) 存在 A 的有限生成自由阿贝尔子群 A_f，使得 $A=A_f\oplus A_t$.

(2) 如果 $A=A_f\oplus A_t$，$B=B_f\oplus B_t$，其中 A_f 和 B_f 分别为 A 和 B 的有限生成自由阿贝尔子群，则

$$A\cong B\Leftrightarrow\operatorname{rank}(A_f)=\operatorname{rank}(B_f)\text{ 且 }A_t\cong B_t.$$

定理 4 设 A 为有限阿贝尔群，$A\neq\{0\}$.

(1) 存在 $1<m_1\mid m_2\mid\cdots\mid m_t(t\ge1)$，使得 $A\cong Z_{m_1}\oplus\cdots\oplus Z_{m_t}$，$(m_1, \cdots, m_t)$ 由 A 唯一确定.

(2) 存在一组正整数 $\{p_1^{s_1}, p_2^{s_2}, \cdots, p_k^{s_k}\}$，其中 $p_1, \cdots, p_k$ 为（不必不同的）素数，$s_1, \cdots, s_k$ 为正整数，使得 $A\cong Z_{p_1^{s_1}}\oplus\cdots\oplus Z_{p_k^{s_k}}$，且集合 $\{p_1^{s_1}, \cdots, p_k^{s_k}\}$ 由群 A 唯一确定.

定理 4 中的 $\{m_1, \cdots, m_t\}$ 叫做 A 的**不变因子**，$\{p_1^{s_1}, \cdots, p_k^{s_k}\}$ 叫做 A 的**初等因子**. 对于有限生成阿贝尔群 A，A_t 的不变因子和初等因子也分别叫做 A 的不变因子和初等因子. 综合上述我们完成了有限生成阿贝尔群的结构定理：

定理 5 两个有限生成阿贝尔群同构 $\Leftrightarrow$ 它们有相同的秩和初等因子 $\Leftrightarrow$ 它们有相同的秩和不变因子. 特别地，两个有限阿贝尔群同构 $\Leftrightarrow$ 它们有相同的初等因子 $\Leftrightarrow$ 它们有相同的不变因子.

例 1500 阶阿贝尔群的分类. 设 A 为阿贝尔群，$|A|=1500=2^2\times3\times5^3$. 于是 A 的西罗子群的阶分别为 $|A_2|=2^2$，$|A_3|=3$，$|A_5|=5^3$. A 的初等因子共有以下六种可能：$\{2,2,3,5,5,5\}$，$\{2,2,3,5,25\}$，$\{2,2,3,125\}$，$\{4,3,5,5,5\}$，$\{4,3,5,25\}$，$\{4,3,125\}$. 所以 1500 阶阿贝尔群共有六个：$Z_2^2\oplus Z_3\oplus Z_5^3$，$Z_2^2\oplus Z_3\oplus Z_5\oplus Z_{25}$，$Z_2^2\oplus Z_3\oplus Z_{125}$，$Z_4\oplus Z_3\oplus Z_5^3$，$Z_4\oplus Z_3\oplus Z_5\oplus Z_{25}$，$Z_4\oplus Z_3\oplus Z_{125}$.

将初等因子 $\{2,2,3,5,5,5\}$ 化为不变因子则为 $t=3$，$m_3=2\times3\times5$，$m_2=2\times5$，$m_1=5$，即不变因子为 $\{5,10,30\}$，于是 $Z_2^2\oplus Z_3\oplus Z_5^3\cong Z_5\oplus Z_{10}\oplus Z_{30}$. 另外五个群的不变因子分别依次为 $\{10,150\}$，$\{2,750\}$，$\{5,5,60\}$，$\{5,300\}$ 和 $\{1500\}$.

期中复习：

1. p, p^2 阶群为Abel群.

2. 证明如：$\frac{|AB|}{|A|}=\frac{|B|}{|A\cap B|}$. 证陪集数一样多. 即 $Ab\to Ab^{-1} \Leftrightarrow (A\cap B)b \to (A\cap B)b^{-1}$.

3. 与M共轭的子群数为 $[G:N_G(M)]$

与a共轭的元素数为 $[G:C_G(a)]$

4. p^n阶群有非平凡中心 $(|C(G)|>1)$

$|G|=|C(G)|+\sum_i [G:C_G(g_i)]$ g_i为非中心共轭类的代表元.

$\equiv 0 \bmod p$ ↓ $\equiv 0 \bmod p$ → 一定 $\equiv 0 \bmod p$.

5. 有限循环群生成元有 $\varphi(n)$ 个. 为 a^k $((k,n)=1)$

6. $N\lhd G$. 则 $N_G(N)=G$

7. 正明同态即为单同态. 单同态 $\Leftrightarrow \ker f=\{1\}$. 即 $\forall a$ 满足 $f(a)=1_{G'}$ 有 $a=1_G$

8. $f: G\to G'$. 证 $G/\ker f\cong G'$ 时要证f是满同态. (此时 $\operatorname{Im} f=G'$)

9. $N\lhd G$. $N'\lhd G'$. 若 $N\cong N'$. $G/N\cong G'/N' \not\Rightarrow G\cong G'$ (如 $K_4/\langle a\rangle \cong Z_4/\langle g^2\rangle$. $\langle a\rangle \lhd K_4$. $\langle g^2\rangle\lhd Z_4$. $\langle a\rangle\cong\langle g^2\rangle$ 但 $K_4\not\cong Z_4$)

10. 说明映射的良定性：如 $f: G/N\to G/M$, $gN\mapsto gM$ 要证每个元素的像在映射后一定相等.

即如此例：若 $gN=g'N$. 则 $g'g^{-1}\in N\subset M \Rightarrow gM=g'M$ 于是良定的

11. 全体3-轮换构成 A_n 的生成元.

12. 两置换共轭 $\Leftrightarrow$ 型相同

13. $n\geq 5$ 时 A_n 为单群. 于是 A_n 为 S_n 唯一非平凡正规子群

14. 对"轨道"的理解：如 $E=\{a,\cdots,a^{n-1},b,\cdots,b^{n-1},c,\cdots,1\}$

G作用后：$\{ga,\cdots ga^{n-1}, gb,\cdots gb^{n-1}, \cdots g\}$

一个轨道 一个轨道.

注意不是相乘！是置换

如 $g(12)(3)=g$

对 a.b.c作用. 则 a.b为一个轨道.

c为一个轨道.

15. $|G|=|[a]|\,|G_a|$ 若作用在为 $|[a]|=|H|$ 而不是 $|[a]|=|G|$

16. $|G|\equiv 2 \bmod 4$ $|G|>6$ 则G非单群. pq, p^2q 阶群非单群.

17. 对 $\forall p^r \mid |G|$. 有 $N(p^r)\equiv 1 \bmod p$. (不一定要 $p^{r+1}\nmid |G|$ 才可)

18. Sylow-p子群相互共轭. 数量为 $[G:N_G(P)]$

表 1 阶数≤15 的群

$\lvert G\rvert$	G	
	阿贝尔群	非阿贝尔群
1	{1}	
2	Z_2	
3	Z_3	
4	Z_2^2, Z_4	
5	Z_5	
6	Z_6	$S_3=D_3$
7	Z_7	
8	$Z_2^3, Z_2\oplus Z_4, Z_8$	D_4, Q_8
9	Z_3^2, Z_9	
10	Z_{10}	D_5
11	Z_{11}	
12	$Z_2^2\oplus Z_3, Z_{12}$	D_6, A_4, T
13	Z_{13}	
14	Z_{14}	D_7
15	Z_{15}	

第二章 环和域

2.1 基本概念

定义 1 环是一个集合 R 和 R 上两个二元运算(通常表示成加法 + 和乘法 ·)组成的代数结构 $(R,+,\cdot)$，并且满足以下三个条件：

(1) $(R,+)$ 是阿贝尔群. 这个加法群的幺元素表示成 0_R(或者简记为 0)，叫做环 R 的零元素.

(2) $(R,\cdot)$ 是半群. 这意味着 R 中乘法运算满足结合律.

(3) 加法和乘法满足分配律. 即对任意的 $a,b,c\in R$，有

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca.$$

} 环

注记 如果只是前两个条件，那么 R 不过是具有阿贝尔群 $(R,+)$ 和乘法半群 $(R,\cdot)$ 两个彼此孤立的代数结构. 正是条件(3)将两个运算用分配律联系在一起，从而形成新的代数结构——环.

如果环 R 还满足条件：

(4) 对所有 $a, b\in R$，$ab=ba$，

则称 R 为交换环. 因此，这里"交换"二字是表明 R 中乘法满足交换律(因为环中加法永远规定有交换律). 另一方面，如果半群 $(R,\cdot)$ 具有幺元素，即如果

(5) 存在元素 $1_R\in R$，使得对每个元素 $a\in R$，$1_R a=a1_R=a$. 则 R 叫含幺环. 元素 1_R(或者简写为 1)叫做环 R 的幺元素.

注记 环 R 中的零元素是唯一的，如果环 R 有幺元素，则它也是唯一的.

定理 1 设 R 为环. 则

(1) 对每个 $a\in R$，$0a=a0=0$；

(2) 对每个 $a,b\in R$，

$$(-a)b=a(-b)=-(ab),\quad (-a)(-b)=ab;$$

(3) 对于 $a_i, b_j\in R$，

$$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j;$$

(4) 对于 $n\in Z$，$a, b\in R$，有

$$(na)b=a(nb)=n(ab).$$

定义 2 环 R 中非零元素 a 叫做环 R 的**左零因子**，是指存在非零元素 $b\in R$，使得 $ab=0$. 类似地若 $ba=0$，则 a 叫环 R 的**右零因子**. 如果 a 同时是左零因子和右零因子，则 a 叫做环 R 的**零因子**.

若 R 为交换环，易知 R 中每个左(或右)零因子均是零因子，从而左零因子、右零因子和零因子这三者是一回事.

定义 3 设 R 是含幺环. R 中元素 a 叫做**左可逆**的，是指存在 $c\in R$ 使得 $ca=1$. 这时 c 叫做元素 a 的**左逆**. 类似地可以定义**右可逆**和**右逆**. 如果 a 同时左可逆和右可逆，则 a 是乘法含幺半群 $(R,\cdot)$ 中的可逆元素，从而 a 具有唯一的乘法逆元素 a^{-1}. 环 R 中的可逆元素 a 通常叫做环 R 中的**单位**(unit). 含幺环 R 中的全体单位形成乘法群(第 1 章 1.2 节定理)，叫做环 R 的**单位群**，表示成 $U(R)$.

若 R 是含幺交换环，则左可逆、右可逆和可逆这三个概念是一致的.

定义：设 R 为含幺环. 若 $U(R)=R\setminus\{0\}$, 则 R 称为体. 若体交换, 则称域

(i) 整环. 体. 域至少有 0.1　　整环为无零因子的含幺交换环 ← 前提!!!

(ii) 域一定是整环

若 R 为含幺交换环. 则 $R[x]$ 也是含幺交换环

定义：$S\subseteq R$ 为环. S 对 $(+,\cdot)$ 也是环. 则 S 称为 R 的子环　→ 难定. $a-b$. ab 封闭.

如 $mZ\subseteq Z\subseteq Q\subseteq R\subseteq C$. $R\subseteq R[x_1]\subseteq R[x_1,x_2]\subseteq\cdots$　　子环一定是加法子群

例 7 偶整数环 $2Z$ 是整数环 Z 的子环. 而 Z 又是有理整数域 Q 的子环. $M_n(Q)$ 是 $M_n(R)$ 的子环. Q 是环 $Q[x]$ 的子域. $Z[\sqrt{-1}]$ 是域 $Q[\sqrt{-1}]$ 的子环. 每个环 R 均是多项式环 $R[x]$ 的子环.

例 8 设 $S_i(i\in I)$ 均是环 R 的子环，则它们的交 $\bigcap_{i\in I}S_i$ 也是 R 的子环.

例 9 设 S 是整数环 Z 的子环，则 S 必然是 Z 的加法子群. 由群论知 $S=nZ(n\geq 0)$，而易知每个 nZ 均是子环，从而 Z 的全部子环为 $\{nZ \mid n\geq 0\}$.

例 10 每个环均有两个平凡子环：零环(0)和环 R 自身.

定义：R.S 为环. $f: R\to S$ 为环同态. 若 $f(a+b)=f(a)+f(b)$. $f(ab)=f(a)f(b)$. 若双射. f 为同构.

R 到自身的同态称自同态. 自同构构成群 $\operatorname{Aut}(R)$

例 15 设环 R 没有幺元素. Z 为整数环. 考虑集合 $S=R\times Z$，并且如下定义：

$$(r_1,k_1)+(r_2,k_2)=(r_1+r_2,k_1+k_2),$$

$$(r_1,k_1)(r_2,k_2)=(r_1r_2+k_2r_1+k_1r_2,k_1k_2).$$

请读者直接验证：S 对于如此定义的加法和乘法是含幺环. 幺元素为 $1_S=(0,1)$. 作映射

$$f: R\to S,\qquad r\mapsto(r,0).$$

不难证明这是环的嵌入. 这个例子表明：任何不含幺元素的环均可嵌到含幺环中.

例 16 现在确定一些环或域的自同构群. 设 $f: Z\to Z$ 为环的自同构. 则必然有 $f(0)=0$，$f(1)=1$，从而对每个正整数 n，

$$f(n)=f(1+1+\cdots+1)=f(1)+f(1)+\cdots+f(1)$$
$$=nf(1)=n\cdot 1=n.$$

于是 $f(-n)=-f(n)=-n$. 这就表明：环 Z 只有恒等自同构，即 $\operatorname{Aut}(Z)=\{1\}$.

类似地，设 φ 是域 Q 的自同构，则上面的推理表明 $\varphi(n)=n$(对每个 $n\in Z$). 但是域同构有性质 $\varphi(m^{-1})=\varphi(m)^{-1}$(对于 $0\neq m\in Z$). 从而对于每个有理数 $n/m(m\neq 0, m,n\in Z)$，$\varphi(n/m)=\varphi(n)\varphi(m^{-1})=\varphi(n)\varphi(m)^{-1}=n/m$. 于是有理数域 Q 也只有恒等自同构.

实数域 R 的自同构也只有一个(习题)，但是复数域的自同构有(不可数地)无穷多个. 例如"复共轭"$a+b\sqrt{-1}\mapsto a-b\sqrt{-1}(a,b\in R)$便是 C 的一个非恒等自同构.

2.2 环的同构定理

定义：理想：子环 I 称为 R 的理想. 若 ① $\forall a,b\in I$. $a\pm b\in I$ ② $\forall a\in I$. $r\in R$. $ra, ar\in I$

定义：商环：$R/I=\{a+I \mid a\in R\}$ $\bar{a}$ 为等价类. 等价关系：$a\sim b \Leftrightarrow a-b\in I$

验证：$\bar{a}+\bar{b}=\overline{a+b}$　：若 $a\sim a'$, $b\sim b'$

$\bar{a}\cdot\bar{b}=\overline{ab}$

① $a-a'+b-b'\in I$ 即 $a+b\sim a'+b'$

① $ab-a'b=(a-a')b\in I \Rightarrow ab\sim a'b$ 同理 $a'b\sim a'b'$ 于是 $ab\sim a'b'$

定义 2 设 X 是环 R 的一个子集合，环 R 中包含 X 的最小理想称作由集合 X 生成的理想，并且表示成 (X).

若 I.J 为 R 的理想. 则 $I\cap J$. $I+J=\{a+b \mid a\in I, b\in J\}$ $I\cdot J=\{\sum_i a_ib_i \mid a_i\in I, b_i\in J\}$ 均为理想

例：Z 的理想一定是 mZ. 若 $I=nZ$. $J=mZ$. 则 $I\cap J=[m,n]Z$. $I\cup J=(m,n)Z$. $I\cdot J=mnZ$

Q 的理想只有 $\{0\}$ 和 Q

体或域只有平凡理想. (设 R 为体. $I\subseteq R$. $0\neq a\in I$ $a^{-1}\in I \Rightarrow 1\in I \Rightarrow \forall r\in R$. $r\in I \Rightarrow I=R$)

定义：若 R 只有平凡理想. 则称 R 为单环

体. 域均为单环. 含幺交换环 R 为单环 $\Leftrightarrow$ R 为域. 若 R 非域. $\exists a\in R$. $0\neq a$ 无逆元. 则 $I=\langle a\rangle\neq R$.

定义 3 由一个元素 $x \in R$ 生成的理想 (x) 叫做环 R 的主理想. 如果 R 是整环(即没有零因子的含幺交换环),并且 R 的每个理想都是主理想 $(x) = xR$,则 R 叫做**主理想整环**,简记作 PID(Principal Ideal Domain). PID

$\mathbb{Z}$ 与 $\mathbb{C}[x]$ 均为PID. $\mathbb{Z}[x]$, $\mathbb{C}[x_1,x_2]$ 不是PID.

定理 1(第一同构定理) 如果 $f: R \to S$ 是环的同态,则 $\mathrm{Ker} f$ 为环 R 的理想,并且映射

$$\bar{f}: R/\mathrm{Ker} f \to S, \qquad \bar{r} = f(r) \quad (r \in R)$$

是环的单同态(嵌入),其中 $\bar{r}$ 表示商环 $R/\mathrm{Ker} f$ 中的元素 $r + \mathrm{Ker} f$. 特别地,我们有环的同构:

$$\bar{f}: R/\mathrm{Ker} f \cong \mathrm{Im} f.$$

例 6 设 m 和 n 是两个正整数,$m \mid n$. 则 $m\mathbb{Z} \supseteq n\mathbb{Z}$. 并且由定理 2 可知有环同构

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

例 4 设 $a \in \mathbb{R}$(实数域),作映射

$$\varphi: \mathbb{R}[x] \to \mathbb{R}, \qquad f(x) \mapsto f(a).$$

不难验证 φ 是环的满同态. 另一方面,从中学代数就知道:实数 a 是多项式 $f(x) \in \mathbb{R}[x]$ 的根 $\Leftrightarrow f(x)$ 可被 $x - a$ 整除. 因此

$$\begin{aligned}\mathrm{Ker}\,\varphi &= \{f(x) \in \mathbb{R}[x] \mid f(a) = 0\} \\ &= \{f(x) \in \mathbb{R}[x] \mid (x-a) \mid f(x)\} \\ &= (x - a) \quad (\text{表示由 } x - a \text{ 生成的主理想}).\end{aligned}$$

于是由定理 1 可知我们有环的同构 $\mathbb{R} \cong \mathbb{R}[x]/(x - a)$ (对每个实数 a).

定理 2 设 I 和 J 是环 R 的理想,则

(1)(第二同构定理)

$$I/(I \cap J) \cong (I + J)/J \quad (\text{环的同构}).$$

(2)(第三同构定理) 如果 $I \subset J$,则

$$\frac{(R/I)}{(J/I)} \cong \frac{R}{J} \quad (\text{环的同构}).$$

定理 3 设 I 是环 R 的理想,以 N 表示商环 R/I 的所有理想构成的集合,M 表示环 R 中包含 I 的所有理想构成的集合. 则映射

$$f: M \to N, \qquad J \mapsto J/I$$

是从 M 到 N 之上的一一对应.

2.3 同态的应用

① 环的特征

定义 1 设 R 为环. 如果存在正整数 m,使得对每个 $r \in R$ 均有 $mr = 0$,我们把满足此条件的最小正整数 m 叫做环 R 的**特征**. 如果不存在这样的正整数 m,便称环 R 的**特征是零**. 环 R 的特征记为 $\mathrm{char}\, R$.

若 $\mathrm{char} R = 0$. 存在子环 P. $P \simeq \mathbb{Z}$
若 $\mathrm{char} R = m$. 存在子环 P. $P \simeq \mathbb{Z}_m$
→ 称为含幺环 R 的素子环

R 为整环 ⇒ 若 R 的特征为 $m>0$. 则 m 为素数.

域的特征为 0 ($\mathbb{Q}$) 或 p ($\mathbb{Z}_p$) (括号内为最小域)

定理 1 设 R 为交换环,$\mathrm{char}\, R = p$ 为素数,则对 $x, y \in R$,有 $(x+y)^p = x^p + y^p$.

系 1 设 R 是特征 p 的交换环,p 为素数,则 $f: R \to R$, $r \mapsto r^p$ 是环 R 的自同态.

② 整环的商域

定理(整环的分式域存在性与唯一性)

设 D 是整环(无零因子的含幺交换环),记 $D^* = D \setminus \{0\}$。在集合 $D \times D^* = \{(r,s) \mid r \in D, s \in D^*\}$ 上定义等价关系:

$(r,s) \sim (r',s') \iff sr' = s'r$

以 r/s 表示 (r,s) 所在的等价类,记所有等价类的集合为 K。在 K 上定义加法与乘法运算:

$\frac{r}{s} + \frac{r'}{s'} = \frac{rs' + r's}{ss'}$, $\quad \frac{r}{s} \cdot \frac{r'}{s'} = \frac{rr'}{ss'}$

(由 $s, s' \in D^*$ 且 D 是整环,故 $ss' \in D^*$,运算良定义)。则:

1. K 关于上述加法和乘法构成一个域; 称为 D 的商域
2. 映射 $f: D \to K$, $a \mapsto \frac{a}{1}$ 是环的单同态(嵌入),因此可将 D 视为 K 的子环;
3. K 是包含 D 的最小域:对任意域 M,若 $g: D \to M$ 是环的单同态(嵌入),则存在唯一的域的单同态(嵌入)$g': K \to M$,使得对任意 $a \in D$,有 $g'\left(\frac{a}{1}\right) = g(a)$ (即 g' 是 g 在 K 上的扩张)。

③ 环的直积

R_1 与 R_2 为环. $R_1 \times R_2$: $(a_1,a_2) \times (b_1,b_2) = (a_1b_1, a_2b_2)$ ⇒ 乘法幺元为 $(1_{R_1}, 1_{R_2})$ (若 R_1, R_2 为含幺环)
$(a_1,a_2) + (b_1,b_2) = (a_1+b_1, a_2+b_2)$ ⇒ 加法幺元为 $(0,0)$

定理 3(中国剩余定理) 设 R 是含幺环,$I_1, \cdots, I_n$ 为环 R 的理想. 并且当 $i \neq j$ 时,$I_i + I_j = R$. 则有环同构 $R/(I_1 \cap \cdots \cap I_n) \cong \prod_{i=1}^{n} (R/I_i)$.

系 2 设 $m_1, \cdots, m_n$ 是两两互素的正整数. 则有环同构

$$f: \mathbb{Z}/m_1 \cdots m_n \mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}.$$

系 3 设 $m_1, \cdots, m_n$ 是两两互素的正整数,则

(1) 对于任意 n 个整数 $a_1, \cdots, a_n \in \mathbb{Z}$,同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ \cdots, \\ x \equiv a_n \pmod{m_n} \end{cases}$$

有整数解;

(2) 设 $x_0 \in \mathbb{Z}$ 是上述同余方程组的一个解. 则它的全部整数解恰好是一个陪集 $x_0 + m_1 \cdots m_n \mathbb{Z}$.

④ 素理想与极大理想

定义 3 环 R 的理想 P 叫做**素理想**,是指

(1) $P \neq R$;

(2) 对于环 R 的任意两个理想 A 和 B. 如果 $AB \subseteq P$,则 $A \subseteq P$ 或者 $B \subseteq P$.

定理 4 设 R 是含幺交换环,P 是 R 的真理想(即 $P \neq R$,或者等价地,$1 \notin P$),则以下三个条件彼此等价:

(1) P 是素理想;

(2) 对于 $a, b \in R$,如果 $ab \in P$,则 $a \in P$ 或者 $b \in P$;

(3) R/P 为整环.

注记 特别若 R 是含幺交换环,则 R 为整环的充分必要条件是零理想为素理想.

例 2 整数环 $\mathbb{Z}$ 的理想均有形式 $n\mathbb{Z}(n \geq 0)$. 由于 $\mathbb{Z}$ 是整环,从而零理想 (0) 为素理想. 而当 $n \geq 2$ 时,$n\mathbb{Z}$ 为素理想 $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ 为整环 $\Leftrightarrow n$ 为素数,这就表明整数环 $\mathbb{Z}$ 的全部素理想是 $p\mathbb{Z}$(p 为素数)以及零理想 (0). 即素理想和素数概念基本上是一致的.

定义 4 环 R 中理想 M 叫做 R 的**极大理想**,是指

(1) $M \neq R$;

(2) 对于 R 的每个理想 N,如果 $M \subseteq N \subseteq R$,则必然 $N = M$ 或者 $N = R$.

定理 5 设 R 为含幺交换环,M 为 R 的理想. 则 M 是 R 的极大理想 $\Leftrightarrow R/M$ 为域. 特别地,含幺交换环 R 为域的充要条件是零理想 (0) 为 R 的极大理想.

tip: 域为整环. 故 M 为 R 极大理想 ⇒ M 为 R 素理想 即极大理想一定是素理想
特别地. PID 中极大理想 ⇔ 素理想

例 3 仍以整数环 $\mathbb{Z}$ 为例. 我们已知道 $\mathbb{Z}$ 的全部素理想是 $p\mathbb{Z}$(p 为素数)和 (0). 由于 $\mathbb{Z}$ 不是域,所以 (0) 不是极大理想. 由于 $\mathbb{Z}/p\mathbb{Z}$ 为域,从而 $\mathbb{Z}$ 的全部极大理想为 $p\mathbb{Z}$(p 为素数).

例 4 设 $R = \mathbb{Z}[x]$. 作映射

$$\varphi: \mathbb{Z}[x] \to \mathbb{Z}, \qquad g(x) \mapsto g(0),$$

这是环的满同态,并且 $\mathrm{Ker}\,\varphi = (x)$,因此 $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$. 从而 (x) 是 $\mathbb{Z}(x)$ 的素理想但不是极大理想,因为 $\mathbb{Z}$ 是整环但不是域. 而 $(x,2)$ 是 $\mathbb{Z}[x]$ 的极大理想,因为不难证明 $\mathbb{Z}[x]/(x,2) \cong \mathbb{Z}/2\mathbb{Z}$,而 $\mathbb{Z}/2\mathbb{Z}$ 为域.

↳ $\mathbb{Z}[x]/(x,2) \cong \frac{\mathbb{Z}[x]/(x)}{(x,2)/(x)} \cong \mathbb{Z}/(2) = \mathbb{Z}/2\mathbb{Z}$

2.4 交换环中的因子分解

定义 1 设 R 为交换环. $a, b \in R$, $a \neq 0$ 如果存在元素 $x \in R$ 使得 $ax = b$,则称 a **整除** b(或者称 b **被** a **整除**),并且表示成 $a \mid b$. 这时,a 叫 b 的**因子**,而 b 叫 a 的**倍元**. 如果不存在 $x \in R$ 使得 $ax = b$,称 a 不能整除 b(或者称 b 不能被 a 整除)表示成 $a \nmid b$.

如果 $a \mid b$ 和 $b \mid a$ 同时成立(其中 $a \neq 0$, $b \neq 0$),则称元素 a 和 b **相伴**,表示成 $a \sim b$.

若 R 是含幺交换环. 如果 $a = bc$,并且 b 和 c 均不是 R 中单位,则称 b(和 c)为 a 的**真因子**.

下面定理将上述概念用主理想的语言表达出来.

定理 1 设 R 是含幺交换环,$a, b, u \in R - \{0\}$,$U(R)$ 为 R 的单位群. 则

(1) $a \mid b \Leftrightarrow (b) \subseteq (a)$, $\quad a \sim b \Leftrightarrow (a) = (b)$;

(2) $u \in U(R) \Leftrightarrow u \sim 1 \Leftrightarrow (u) = R \Leftrightarrow u \mid r$ (对每个 $r \in R$);

(3) $a = bu$, $u \in U(R) \Rightarrow a \sim b$,如果 R 为整环,则反过来也成立;

(4) 若 R 是整环,则 a 为 b 的真因子 $\Leftrightarrow (b) \subseteq (a)$ 但是 $(b) \neq (a)$.

定义 2 含幺交换环 R 中元素 $a \neq 0$ 叫做**不可约元**,是指:

(1) $a \notin U(R)$;

(2) a 没有真因子.

而 $p \neq 0$ 叫做**素元**,是指:

(1) $p \notin U(R)$;

(2) $a, b \in R$. 若 $p \mid ab$,则 $p \mid a$ 或者 $p \mid b$.

例 1 $R = \mathbb{Z}_6$. 则 $\bar{2}$ 是素元(读者自证),但不是不可约元,因为 $\bar{2} = \bar{2} \cdot \bar{4}$,从而 $\bar{4}$ 是 $\bar{2}$ 的真因子.

例 2 $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. 其中 3 是不可约元(详见后面例 4). 但是 3 不是素元,因为:

$$3 \mid 9 = (2 + \sqrt{-5})(2 - \sqrt{-5}), \quad \text{且在 } R \text{ 中 } 3 \nmid (2 \pm \sqrt{-5}).$$

定理 2 设 R 为整环,$p, c \in R - \{0\}$. 以 S 表示 R 的全部非平凡主理想组成的集合,即 $S = \{(a) \mid a \in R, a \neq 0, a \neq U(R)\}$. 则

(1) p 为素元 $\Leftrightarrow (p)$ 为非零素理想;

(2) c 为不可约元 $\Leftrightarrow$ 主理想 (c) 为集合 S 中的极大元;

(3) R 中素元必是不可约元;

(4) 若 R 为主理想整环(PID),则不可约元必是素元.

(i) ⇒) p 素元 ⇒ $p \notin U(R)$. $(p) \neq R$. 若 $ab \in (p) \Rightarrow p \mid ab$ 则 $p \mid a$ 或 $p \mid b$ 则 $a \in (p)$ 或 $b \in (p)$. 于是 (p) 为素理想.
⇐) (p) 素理想. $(p) \neq R \Rightarrow p \notin U(R)$ 若 $p \mid ab$ 则 $(a)(b) = (ab) \subseteq (p)$. $(a) \subseteq (p)$ 或 $(b) \subseteq (p)$ 即 $p \mid a$ 或 $p \mid b$. 证毕

(ii) ⇒) c 不可约 ⇒ $c \notin U(R)$. $(c) \in S$. 若 $(c) \subseteq (d)$ $d \in R$. 则 $c = dx$ 又 c 不可约: $d \in U(R)$ ($(d) \notin S$) 或 $x \in U(R)$ ($(c) = (d)$). 矛盾! 于是 (c) 是极大的
⇐) (c) 在 S 中极大. $(c) \in S$ 则 $c \notin U(R)$. 若 $c = ab$. $a, b \in R$. 则 $(c) \subseteq (a)$ 由 (c) 极大性: $(a) = (c)$ ($b \in U(R)$) 或 $(a) = R$ ($a \in U(R)$). 故 c 不可约

(iii) p 素 ⇒ $p = ab$ 则 $p \mid a$ 或 $p \mid b$. 若 $p \mid a$. $px = a$ $x \in R$ 则 $abx = px = a$ 又 $a \neq 0$. R 整环: $bx = 1$ 则 $b \in U(R)$
同理若 $p \mid b$. $a \in U(R)$ 于是 p 不可约

证素元: $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$. 素理想: $ab \in (p)$. 则 $a \in (p)$ 或 $b \in (p)$ / $R/(p)$ 为整环 整环中三者等价

证不可约元: $c = ab \Rightarrow a$ 或 $b \in U(R)$. 极大主理想: $(c) \subseteq (d)$. 则 $(d) = R$ 或 $(d) = (c)$ / $R/(c)$ 为域 整环中三者等价

含幺交换: 极大理想一定为素理想. 素元一定是不可约元. ← 不是极大理想!
↓ 在PID中均等价

定义 3 整环 R 叫做唯一因子分解整环(Uniquely Factorial Domain,今后简记作 UFD),是指: UFD

(1)(分解的存在性) 每个非零非单位元素 $a\in R$ 均可写成 $a=c_1c_2\cdots c_n$,其中 c_i 均为不可约元;

(2)(分解的唯一性) 如果 $a=c_1c_2\cdots c_n=d_1d_2\cdots d_m$ 是 a 的任意两个上述分解式,其中 c_i,d_j 均为 R 中不可约元,则 $n=m$,并且存在集合 $\{1,2,\cdots,n\}$ 的一个置换 σ,使得 $c_i\sim d_{\sigma(i)}$ $(1\leqslant i\leqslant n)$.

例 4 考虑环 $R=\mathbb{Z}[\sqrt{-5}]$.这是含幺交换环,并且是复数域的子环,所以 R 是整环.我们先决定 $U(R)$,为此作映射

$$N:R\to\{0,1,2,\cdots,n,\cdots\},$$

$$N(a+b\sqrt{-5})=(a+b\sqrt{-5})(a-b\sqrt{-5})=a^2+5b^2\quad(a,b\in\mathbb{Z}).$$

对于 $a\in R$,元素 $N(a)$是非负整数,叫做 a 的范数.它是复数 a 通常绝对值的平方.由……

环	ED?	PID?	UFD?	备注
$\mathbb{Z}$	✅	✅	✅	整数环，带余除法
$F[x]$	✅	✅	✅	域上一元多项式环
$\mathbb{Z}[i]$	✅	✅	✅	高斯整数环
$\mathbb{Z}[\omega]$	✅	✅	✅	艾森斯坦整数环
$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$	❌	✅	✅	非ED的PID
F (域)	✅	✅	✅	特殊情况
$\mathbb{Z}[x]$	❌	❌	✅	典型UFD但非PID
$\mathbb{Q}[x,y]$	❌	❌	✅	多元多项式环UFD
$\mathbb{Z}[\sqrt{-5}]$	❌	❌	❌	经典非UFD反例

(…… 现在让 …… 由于 …… $=\{\pm1\}$. 现 …… 的乘积.如果 a 不 …… 和 $N(c)$ 均是大 …… ,否则又要写成 …… 1)作有限步之后 …… 现 …… 中的不可约元. …… >1,但是 $N(a)$ …… $=2$ 没有整数解 …… 地,再由 x^2+5 …… 有两种分解方式:)

$$6=2\cdot3=(1+\sqrt{-5})(1-\sqrt{-5}).$$

而 2 和 $1\pm\sqrt{-5}$ 均不相伴,从而破坏了分解的唯一性.因而整环 $\mathbb{Z}[\sqrt{-5}]$不是 UFD.

UFD中不可约元⟺素元

例: $\mathbb{Z}$为UFD. PID是UFD. 若R为UFD. 则R[x]为UFD.

性质: (i) R中不存在无限序列 $a_1,a_2,\cdots$ 使得 a_{i+1} 为 a_i 的真因子

(ii) 不可约元一定是素元

$p_1^{c_1}\cdots p_k^{c_k}q_1^{a_1}\cdots q_t^{a_t}=ad$

证明: 设a为不可约元. $a|bc$. 则∃d. $bc=ad$ a一定是 $p_1,\cdots,p_k,q_1,\cdots,q_t$ 中某一个 ⇒ $a|b$ 或 $a|c$ ⇒ a为素元

(iii) ∀a.b∈R a.b≠0. 则a.b的最大公因子存在

定义 4 设 R 是整环,$a,b\in R-\{0\}$.元素 d 叫做是 a 和 b 的最大公因子,是指:

若d=(a.b) 则与d相伴的元素均为(a.b),构成等价类

(1) d 是 a 和 b 的公因子,即 $d|a,d|b$;

(2) 若 d' 也是 a 和 b 的公因子,则 $d'|d$.元素 a 和 b 的最大公因子记为(a,b).

Tip: (i) 最大公因子不一定存在

(ii) 若存在.在差一个单位的意义下唯一

若d,d'均为a.b的最大公因子 ⇒ $d|d'$, $d'|d$ ⇒ $d=ud'$, $d'=vd$ ⇒ $d=uvd$ 则 $uv=1$. 则u.v为单位 在差一个单位意义下唯一

引理 设 R 为整环,$a,b,c\in R-\{0\}$,则

(1) $c(a,b)\sim(ca,cb)$;

(2) $(a,b)\sim1,(a,c)\sim1$,则$(a,bc)\sim1$.

定理: 若R为整环.下三条等价:(i) R为UFD (ii) R满足性质1和3 (iii) R满足性质1和2

定理 7 每个 PID(主理想整环)都是 UFD.

证明 根据定理 6,我们只需证明每个主理想整环 R 都有性质 1′(它等价于性质 1)和性质 3.设 $a_1,a_2,\cdots,a_n,\cdots$是 R 中元素的无限序列,并且 $a_{i+1}|a_i$ $(i=1,2,3,\cdots)$.化成主理想的语言,则为$(a_1)\subseteq(a_2)\subseteq\cdots\subseteq(a_n)\subseteq\cdots$.令 $I=\bigcup_{n=1}^{\infty}(a_n)$,这是 R 的理想(2.2 节习题 11).由于 R 为主理想整环,从而 $I=(a)$,$a\in R$.由于 $a\in I$,从而 a 必然属于某个(a_k).由此推出$(a)\subseteq(a_k)\subseteq(a_{k+1})\subseteq\cdots\subseteq I=(a)$.于是$(a_k)=(a_{k+1})=\cdots$,即 $a_k\sim a_{k+1}\sim\cdots$.这就证明了性质(1′).

再证性质 3 设 $a,b\in R-\{0\}$.令 I 为理想$(a)+(b)$.由于 R 是主理想整环,从而 $I=(d)$,$d\in R$.现在证明 d 为 a 和 b 的一个最大公因子.由于 $a=a+0\in(a)+(b)=(d)$,从而 $d|a$.同样 $d|b$,即 d 是 a 和 b 的公因子.如果 d'也是 a 和 b 的公因子,则 $d'|a$,$d'|b$,于是 $a\in(d')$,$b\in(d')$,从而$(d)=(a)+(b)\subseteq(d')$,于是 $d'|d$,这就表明 d 是 a 和 b 的最大公因子.证毕.

定义 5 设 N 是非负整数集合.整环 R 叫做欧氏整环(简写为 ED),是指我们能定义一个映射 $\varphi:R\to\mathbb{N}$ 具有以下性质(叫做欧氏性质):

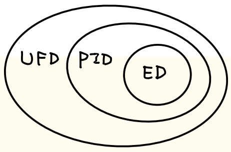
(1) $\varphi(x)=0\Leftrightarrow x=0$;

(2) 对于 $a,b\in R$,$b\neq0$,均有 $q,r\in R$,使得 $a=bq+r$,并且 $\varphi(r)<\varphi(b)$.

例 5 整数环 Z 取 $\varphi(n)=|n|$,则上述欧氏性质即为通常的欧氏除法算式.从而 Z 为 ED.

例 6 对于每个域 F,令 $\varphi(0)=0$,而当 $x\in F-\{0\}$时,$\varphi(x)=1$.易知 φ 满足欧氏性质,从而每个域都是 ED.

定理 8 每个 ED 必为 PID(从而为 UFD).



2.5 多项式环

$R[x]=\{f(x)=a_nx^n+\cdots+a_0 \mid a_i\in R\}$

设 $f(x)=\sum_{i=0}^{m}a_ix^i$ $g(x)=\sum_{j=0}^{n}b_jx^j$ 则 $f(x)+g(x)=\sum_{k=0}^{\max\{n,m\}}c_kx^k$ $c_k=\sum_{i+j=k}a_ib_j$

定理: R为整环⟺R[x]为整环 ← 两非零多项式相乘一定非零.

R为交换环⟺R[x]为交换环 若R不交换,对 $h(x)=f(x)g(x)\in R[x]$,一般无 $h(a)=f(a)g(a)$

定理 2 设 R 为环,$f(x),g(x)\in R[x]$.则

(1) $\deg(f+g)\leqslant\max\{\deg f,\deg g\}$;

(2) $\deg fg\leqslant\deg f+\deg g$;

(3) 如果 f 或者 g 的首项系数不是 R 中零因子,则

$$\deg fg=\deg f+\deg g.$$

定理 3 若 R 为整环,则 $U(R[x])=U(R)$.

定理 4(欧氏除法算式) 设 R 为含幺环,$f(x),g(x)\in R[x]$,并且 $g(x)$的首项系数是 R 中单位.则存在唯一的 $q(x),r(x)\in R[x]$.使得 $f(x)=q(x)g(x)+r(x)$,并且 $\deg r<\deg g$.

系 1 若 F 为域,则 $F[x]$为欧氏整环,从而也为 PID 和 UFD.

系 2(余数定理) 设 R 为含幺环,$f(x)\in R[x]$.则对于每个元素 $c\in R$,均有唯一的多项式 $q(x)\in R[x]$,使得 $f(x)=q(x)(x-c)+f(c)$.

定理 5 设 R 是含幺交换环.$f(x)\in R[x]$,$c\in R$.则 c 为 $f(x)$的根 $\Leftrightarrow(x-c)|f(x)$.

定理 6 设 D 和 E 均为整环,$D\subseteq E$ 则对于每个多项式 $f(x)\in D[x]$ ($\deg f=n$),它在 E 中至多有 n 个不同的根,

定理 7 设 D 为 UFD,F 为 D 的商域,$f(x)=\sum_{i=0}^{n}a_ix^i\in D[x]$.设 $u=c/d\in F$ 是$f(x)$在 F 中的一个根,其中 $c,d\in D$,$c\neq0$,$d\neq0$,$(c,d)=1$,则在 D 中 $c|a_0$,$d|a_n$. 用Vieta定理记忆

例: $f(x)=3x^4+6x^3-21x^2-4$ 的有理根只能是 $\begin{cases}c=\pm1,\pm2,\pm4\\ d=\pm1,\pm3\end{cases}$ 分别验证,只有4为其有理根

定义 2 设 D 为整环,$c\in D$,$f(x)\in D[x]$,如果$(x-c)^m\,\|\,f(x)$(即$(x-c)^m|f(x)$但是$(x-c)^{m+1}\nmid f(x)$),$m\geqslant2$,则称 c 是$f(x)$的重根并且重数为 m.若 $m=1$,则称 c 为$f(x)$的单根.

定理 8 设 D 和 E 为整环,$D\subseteq E$,$f(x)\in D[x]$,$c\in E$,则

(1) c 为$f(x)$的重根$\Leftrightarrow f(c)=f'(c)=0$;

(2) 如果 D 为域,并且在 $D[x]$中$(f,f')=1$,则$f(x)$在 E 中没有重根.

裴蜀定理: PID中∃k.l s.t. $ak+bl=(a.b)$

定义 3 设 D 是 UFD.$0\neq f(x)=\sum_{i=0}^{n}a_ix^i\in D[x]$,我们把$f(x)$诸系数(在 D 中)的最大公因子$(a_0,a_1,\cdots,a_n)$叫做$f(x)$的容量(Content,这是高斯本人起的名称),并且表示成 $c(f)$.作为 D 中一些元素的最大公因子,可知 $c(f)$是一个相伴元素的等价类.如果 $c(f)\sim1$,则称 $f(x)$是 $D[x]$中本原多项式.

$f(x)=c(f)\cdot g(x)$ $g(x)$为D[x]中本原多项式.

高斯引理 设 D 为 UFD,$f(x),g(x)\in D[x]$,则 $c(fg)=c(f)\cdot c(g)$,特别地,$D[x]$中两个本原多项式的乘积仍是本原多项式.

高斯定理 如果 D 为 UFD,则 $D[x]$(从而 $D[x_1,\cdots,x_n]$)也是 UFD.

定理 9 设 D 为 UFD,$F(x)=\sum_{i=0}^{n}a_ix^i$ 为$D[x]$中本原多项式,$\deg f\geqslant1$.如果 p 是D 中不可约元,使得

$$p\nmid a_n,\quad p|a_i(0\leqslant i\leqslant n-1),\quad p^2\nmid a_0,$$

则 $f(x)$为 $D[x]$中不可约多项式.

Eisenstein判别法.用于判断多项式不可约.

例: $f(x)=2x^5-6x^3+9x^2-15\in\mathbb{Z}[x]$ 不可约

① 3为$\mathbb{Z}$中不可约元, ② $\mathbb{Z}[x]$为UFD. ③ $f(x)$为$\mathbb{Z}[x]$中本原多项式. ④ $3\nmid2$. $3|6.9.15$. $3^2\nmid15$.

则由Eisenstein判别法知f在$\mathbb{Z}[x]$中不可约

例: $f(x,y)=y^3+x^2y+x^3y+x\in D[x,y]=(D[x])[y]$ D为UFD.

x为D中不可约元. $x\nmid1$. $x|x^2.x^3.x$. $x^2\nmid x$.

例: $f(x)=x^{p-1}+x^{p-2}+\cdots+1\in\mathbb{Z}[x]$ 则f(x)在$\mathbb{Z}[x]$不可约

$f(x)=\frac{x^p-1}{x-1}$ 设 $g(x)=f(x+1)$本原 $=\frac{(x+1)^p-1}{x}=x^{p-1}+\binom{p}{1}x^{p-2}+\cdots+\binom{p}{p-1}$,…,记得

2.6 域的扩张

定义: K⊆F为F的子域,则F称为K的域扩张.记这一对域为F/K

u∈F K[u] 为包含K与u的最小子环

K(u) 为包含K与u的最小子域

S⊆F K[S] 为包含K与S的最小子环

K(S) 为包含K与S的最小子域

特别地.称K(S)为S在K上生成的域

若|S|<∞.称K(S)为有限生成域扩张.

若 S={u}.域K(u)称为K的单扩张

如果 L 和 M 都是域F 的子域,则 $L(M)=M(L)$.我们将它叫做域 L 和M 的合成域,表示成 $LM(=ML)$,它是 F 中包含 $L\cup M$ 的最小子域.

定理 1 设 F/K 为域的扩张,$u,u_i\in F$,$S\subseteq F$,x,x_i 为彼此不同的文字,$K[x],K[x_1,\cdots,x_n]$为多项式环.则

(1) $K[u]=\{f(u)\mid f(x)\in K[x]\}$,

$K[u_1,\cdots,u_n]=\{f(u_1,\cdots,u_n)\mid f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n]\}$,

$K[S]=\{f(u_1,\cdots,u_n)\mid f(x_1,\cdots,x_n)\in K[x_1,\cdots,x_n],$
$u_1,\cdots,u_n\in S,n\geqslant1\}$.

(2) $K(u)=\{f(u)/g(u)\mid f(x),g(x)\in K[x],g(u)\neq0\}$,

$K(u_1,\cdots,u_n)=\{f(u_1,\cdots,u_n)/g(u_1,\cdots,u_n)\mid$
$f,g\in K[x_1,\cdots,x_n],g(u_1,\cdots,u_n)\neq0\}$,

$K(S)=\{f(u_1,\cdots,u_n)/g(u_1,\cdots,u_n)\mid f,g\in K[x_1,\cdots,x_n],$
$u_1,\cdots,u_n\in S,\ g(u_1,\cdots,u_n)\neq0,n\geqslant1\}$.

(3) 对每个 $v\in K[S]$(域 $K(S)$),均存在 S 的有限子集 S',使得 $v\in K[S']$(或 $K(S')$).

定义 2 设 F/K 是域的扩张. 元素 $u\in F$ 叫做 K 上的**代数元素**(或叫**在 K 上代数**), 如果 u 是 $K[x]$ 中某个非零多项式的根; 反之, 如果 u 不是 $K[x]$ 中任何非零多项式的根, 则称 u 是 K 上**超越元素**(或称 u **在 K 上超越**). 如果 F 中每个元素在 K 上均代数, 则称 F 是 K 的**代数扩张**; 反之, 如果 F 中至少有一个元素在 K 上超越, 则称 F 是 K 的**超越扩张**.

例 1 K 中每个元素 u 均在 K 上代数, 因为它是多项式 $x-u\in K[x]$ 的根.

例 2 设 $u\in F$ 在 K 的某个子域 K' 上代数, 则由定义易知 u 在 K 上代数.

例 3 $\sqrt{-1},\sqrt[n]{2},\mathrm{e}^{\frac{2\pi i}{n}}$ (n 为正整数)均是 $\mathbf{Q}$ 上代数元素, 它们分别是 $\mathbf{Q}[x]$ 中多项式 x^2+1, x^3-2 和 x^n-1 的根. 另一方面, 可以证明 π 和 $\mathrm{e}\left(=\sum_{n=0}^{\infty}\frac{1}{n!}\right)$ 均是 $\mathbf{Q}$ 上超越元素. 研究哪些实数或复数是有理数域上的超越元素, 是数论的一个分支——超越数论的主要研究课题.

定义 3 设 F/K 为域的扩张, 则 F 是域 K 上的**向量空间**. 我们以 $[F:K]$ 表示向量空间 F 在 K 上的维数, 并且今后将它叫做是扩张 F/K 的**次数**. 当 $[F:K]$ 有限时, 称 F/K 为**有限(次)扩张**. 而当 $[F:K]$ 无限时, 称 F/K 为**无限(次)扩张**.

定理 2 设 $F/E, E/K$ 为域的扩张, 则

(1) $[F:K]=[F:E][E:K]$;

(2) F/K 为有限扩张 $\Leftrightarrow F/E$ 和 E/K 均是有限扩张.

定理 3 设 F/K 为域的扩张, $u\in F$, 并且 u 为 K 上超越元素, 则

(1) 存在着域同构 $\sigma: K(x)\xrightarrow{\sim} K(u)$, 并且 σ 在 K 上是恒等自同构;

(2) $K(u)/K$ 是无限(超越)扩张.

证明 (1) 作映射 $\sigma: K[x]\to K(u)$, $f(x)\mapsto f(u)$. 易知这是环的同态, 由 u 在 K 上超越可知 σ 是单射. 从而 σ 是环的嵌入. 根据 2.3 节便知 σ 可扩充到 $K[x]$ 的商域 $K(x)$ 上, 即存在域的嵌入

$$\sigma: K(x)\to K(u),\qquad \frac{f(x)}{g(x)}\mapsto\frac{f(u)}{g(u)}.$$

其中 $f(x), g(x)\in K[x], g(x)\neq 0$(从而 $g(u)\neq 0$). 由定理 1 中对于 $K(u)$ 的刻画可知 σ 是满射, 于是, σ 事实上是域 $K(x)$ 和 $K(u)$ 的同构, 并且对于 $a\in K$, 显然 $\sigma(a)=a$.

(2) 只需证明 $\{1,u,u^2,\cdots u^n,\cdots\}$ 是 K-线性无关的. 用反证法: 如果它们在 K 上线性相关, 则存在 $n\geqslant 0$ 和不全为零的元素 $c_0,c_1,\cdots,c_n\in K$, 使得 $c_0+c_1u+\cdots+c_nu^n=0$. 这相当于说 u 是 $K[x]$ 中非零多项式 $c_0+c_1x+\cdots+c_nx^n$ 的根, 与 u 在 K 上超越矛盾. 因此 $K(u)/K$ 为无限扩张. 由于 u 在 K 上超越元素, 所以 $K(u)/K$ 是超越扩张. 证毕.

定理 4 设 F 是 K 的扩域, $u\in F$, 并且 u 在 K 上代数. 则

(1) $K(u)=K[u]$;

(2) 存在唯一的不可约首 1 多项式 $f(x)\in K[x]$, $\deg f\geqslant 1$, 使得 $f(u)=0$, 并且 $K(u)\cong K[x]/(f(x))$;

(3) $[K(u):K]=n$, 其中 $n=\deg f$, 从而 $K(u)/K$ 为有限扩张, 并且 $\{1,u,u^2,\cdots,u^{n-1}\}$ 是向量空间 $K(u)$ 的一组 K-基;

(4) $K(u)/K$ 为(有限)代数扩张.

证明 (1)和(2)考虑环的同态

$$\sigma: K[x]\to K[u],\qquad g(x)\mapsto g(u),$$

这是环的满同态. 由于 u 在 K 上代数, 从而存在 $0\neq g(x)\in K[x]$, 使得 $g(u)=0$. 因此 $g(x)\in\mathrm{Ker}\,\sigma$. 从而 $\mathrm{Ker}\,\sigma\neq(0)$. 但是 $\mathrm{Ker}\,\sigma$ 是 $K[x]$ 的非零理想, 而 $K[x]$ 是主理想整环. 因此存在 $0\neq f(x)\in K[x]$, 使得 $\mathrm{Ker}\,\sigma=(f(x))$, 并且如果假定 $f(x)$ 为首 1 多项式, 那么多项式 $f(x)$ 就是唯一决定的. 由于 $\sigma(1)=1\neq 0$, 即 $1\notin\mathrm{Ker}\,\sigma$, 从而 $(f(x))$ 是 $K[x]$ 的真理想, 即 $\deg f\geqslant 1$. 由同构定理可知 $K[x]/(f(x))\cong K[u]$. 由于 $K[u]$ 为整环(它是域 F 的子环), 从而 $K[x]/(f(x))$ 为整环, 于是 $(f(x))$ 为 $K[x]$ 的素理想, 从而 $f(x)$ 为 $K[x]$ 中不可约元. 这又推出 $(f(x))$ 是 $K[x]$ 的极大理想, 因此 $K[x]/(f(x))$ 是域. 从而 $K[u]$ 是域. 由于 $K[u]$ 是整环 $K[u]$ 的商域, 从而 $K[u]=K(u)$.

定义 4 定理 4 中不可约首 1 多项式 $f(x)$ 是由 K 上代数的元素 u 所唯一确定的. 将 $f(x)$ 叫做是 u 在 K 上的**极小多项式**. 它可以刻画为

(1) $f(x)$ 为 $K[x]$ 中首 1 多项式, 并且 $f(u)=0$;

(2) 如果 $g(x)\in K[x]$ 并且 $g(u)=0$, 则 $f(x)\mid g(x)$.

定义 5 设 u 为 K 上代数元素, $f(x)$ 是 u 在 K 上的极小多项式, $\deg f=n(\geqslant 1)$. 则 u 也叫做 K 上的 n 次**代数元素**.

例 5 $f(x)=x^3-3x-1$ 是 $\mathbf{Q}[x]$ 中不可约多项式. 设 u 是 $f(x)$ 的一个实根(实系数奇次多项式必有实根). 由于 $f(x)$ 为 $\mathbf{Q}[x]$ 上不可约的首 1 多项式, 并且 $f(u)=0$, 从而 $f(x)$ 也就是 u 在 $\mathbf{Q}$ 上的极小多项式(为什么?). 于是 u 为 $\mathbf{Q}$ 上 3 次数代数. 而 $\{1,u,u^2\}$ 是 $\mathbf{Q}(u)$ 在 $\mathbf{Q}$上的一组基. 比如说, 为了将 $u^4+2u^3+3\in\mathbf{Q}(u)$ 表示成 $1,u,u^2$ 的 $\mathbf{Q}$-线性组合, 我们用除法算式:

$$x^4+2x^3+3=(x+2)(x^3-3x-1)+(3x^2+7x+5),$$

从而 $u^4+2u^3+3=3u^2+7u+5$. 又如, $(3u^2+7u+5)^{-1}$ 也是域 $\mathbf{Q}(u)$ 中元素, 从而也应当有

$$(3u^2+7u+5)^{-1}=a_0+a_1u+a_2u^2\quad(a_i\in\mathbf{Q}).$$

于是

$$\begin{aligned}1&=(a_2u^2+a_1u+a_0)(3u^2+7u+5)\\&=3a_2u^4+(3a_1+7a_2)u^3+(3a_0+7a_1+5a_2)u^2\\&\quad+(7a_0+5a_1)u+5a_0\\&=(3a_0+7a_1+14a_2)u^2+(7a_0+14a_1+24a_2)u\\&\quad+(5a_0+3a_1+7a_2),\end{aligned}$$

从而

$$\begin{cases}5a_0+3a_1+7a_2=1,\\7a_0+14a_1+24a_2=0,\\3a_0+7a_1+14a_2=0.\end{cases}$$

由此解出 $(a_0,a_1,a_2)=(28/111,-26/111,7/111)$. 从而

$$(3u^2+7u+5)^{-1}=\frac{28}{111}-\frac{26}{111}u+\frac{7}{111}u^2.$$

定理 5 (1) 域的有限扩域必是有限生成代数扩张;

(2) 设 $K(u_1,\cdots,u_n)/K$ 是有限生成扩张, 其中 $u_i(1\leqslant i\leqslant n)$ 在 K 的某个扩域中, 并且均是 K 上代数元素, 则 $K(u_1,\cdots,u_n)/K$ 是有限扩张(从而是代数扩张);

(3) 若 u 是域 F 上的代数元素, F/K 为代数扩张, 则 u 在 K 上也是代数元素;

(4) 设 F/E 和 E/K 为域的扩张. 则 F/K 为代数扩张 $\Leftrightarrow F/E$ 和 E/K 均是代数扩张.

定理 6 设 $\sigma: K\xrightarrow{\sim} L$ 是域的同构, u 和 v 分别属于 K 和 L 的某个扩域. 如果

(1) u 和 v 分别是 K 和 L 上的超越元素; 或者

(2) u 在 K 上代数, 并且 u 在 K 上的极小多项式为 $f(x)=\sum r_nx^n\in K[x]$, 而 v 是多项式 $\sum\sigma(r_n)x^n\in L[x]$ 的根. 则 σ 可扩充成域的同构 $K(u)\cong L(v)$, 并且它将 u 映成 v.

系 设 E 和 F 均是 K 的扩域, $u\in E, v\in F$, 并且 u 和 v 均是 K 上代数元素, 则下列两个条件等价:

(1) u 和 v 在 K 上有相同的极小多项式;

(2) 存在域的同构 $\varphi: K(u)\xrightarrow{\sim} K(v)$, 使得 $\varphi(u)=v$, 并且 φ 在 K 上的限制是 K 的恒等自同构.

定理 7 设 K 为域, $f(x)\in K[x]$, $\deg f=n\geqslant 1$, 则存在 K 的单扩张 $F=K(u)$, 使得

(1) $u\in F$ 是 $f(x)$ 的根;

(2) $[K(u):K]\leqslant n$, 并且 $[K(u):K]=n\Leftrightarrow f(x)$ 在 $K[x]$ 中不可约;

(3) 如果 $f(x)$ 在 $K[x]$ 中不可约, 则域 $F=K(u)$ 不计同构是唯一确定的.

定义 6 设 K 为域. 如果 u 是 K 的某扩域中元素, 并且 u 在 K 上代数, 则必然 $u\in K$, 就称 K 是**代数封闭域**.

设 F/K 为域的扩张. 如果 F 是代数封闭域, 并且 F/K 为代数扩张, 则称 F 是 K 的**代数闭包**.