2009级近世代数课堂笔记整理

January 18, 2012

目　录

第 1 章　群论(上)

1.1　代数方程发展史

这部分是对近世代数的发展的历史介绍, 我省略整理这一部分, 有兴趣的话可以自己记录.

1.2 群的概念与例子

定义1.2.1

设 X 为非空集, 对 $x,y\in X$, 有唯一的元素 $x\circ y$, 且运算 $\circ$ 满足结合律

$$(x\circ y)\circ z=x\circ(y\circ z)$$

则说 X 按运算 $\circ$ 构成**半群**.
设 X 按 $\circ$ 构成半群, 如果 X 有个特殊元 e, 使

$$a\circ e=a,e\circ a=a\quad(\forall a\in X)$$

则称 e 为半群 X 的**单位元**（幺元）.有单位元的半群叫**幺半群**.

对于幺半群 M, 如果有两个单位元, e_1,e_2, 则

$$e_1=e_1\circ e_2=e_2$$

即幺半群的单位元是**唯一**的.

对幺半群 M 中的元素 a, 如果有 $b\in M$, 使得

$$e=a\circ b=b\circ a$$

则称 b 为 a 的**逆元**.

如果 b,c 均为 a 的逆元, 则

$$b=b\circ e=b\circ(a\circ c)=(b\circ a)\circ c=e\circ c=c$$

即 a 可逆时, a 的**逆元唯一**, 记为 a^{-1}, 也就是

$$a\circ a^{-1}=e=a^{-1}\circ a$$

如果 a,b 可逆, 则 ab 可逆, 且 $(ab)^{-1}=b^{-1}a^{-1}$.
因为

$$(ab)(b^{-1}a^{-1})=a\big(b(b^{-1}a^{-1})\big)=a\big((bb^{-1})a^{-1}\big)=e;$$
$$(b^{-1}a^{-1})(ab)=b^{-1}\big(a^{-1}(ab)\big)=b^{-1}\big((a^{-1}a)b\big)=e$$

(为了表示方便, 在不引起歧义的情况下, 我们记 $a\circ b$ 为 ab.)

例1.2.1

正整数群 $\mathbb{Z}^+=\{1,2,3\ldots\}$ 按照乘法构成幺半群（单位元 1 ）;
自然数群 $\mathbb{N}=\{0,1,2\ldots\}$ 按加法构成幺半群（单位元 0 ）.

例1.2.2

记 $i=\sqrt{-1}$, 那么 $\mathbb{Z}[i]=\{a+bi;a,b\in\mathbb{Z}\}$ 按照乘法构成幺半群；
记 $\omega=\frac{-1+\sqrt{3}i}{2}$, 那么 $\mathbb{Z}[\omega]=\{a+b\omega;a,b\in\mathbb{Z}\}$ 按照乘法构成幺半群.($\omega^3=1$)

例1.2.3

任给整数 m,

$$R_m=\{\frac{a}{b}:a,b\in\mathbb{Z},b\neq 0,(b,m)=1\}$$

按照乘法构成幺半群.其中 $R_0=\mathbb{Z}$, $R_1=\mathbb{Q}$.

例1.2.4

设 $d\in\mathbb{Z}$, $M_d=\{x^2+dy^2:x,y\in\mathbb{Z}\}$ 按乘法构成幺半群. 因为

$$\begin{aligned}(x_1^2+dy_1^2)(x_2^2+dy_2^2)&=(x_1x_2)^2+d^2(y_1y_2)^2+d(x_1^2y_2^2+x_2^2y_1^2)\\&=(x_1x_2+dy_1y_2)^2+d(x_1y_2-x_2y_1)^2\end{aligned}$$

例1.2.5

设 X 为集合,

$$\mathcal{P}(X)=\{A:A\subseteq X\}$$

按并运算 $\cup$ (或交运算 $\cap$)构成幺半群.因为：

$$\begin{matrix}A\subseteq X\\B\subseteq X\end{matrix}\implies\begin{matrix}A\cup B\subseteq X\\A\cap B\subseteq X\end{matrix}$$

又

$$\begin{gathered}(A\cup B)\cup C=A\cup(B\cup C)\\(A\cap B)\cap C=A\cap(B\cap C)\end{gathered}$$

此外：

$$\begin{aligned}A\cup\emptyset=\emptyset\cup A=A&\quad\emptyset\text{为并运算的单位元}\\A\cap X=X\cap A=A&\quad X\text{为交运算的单位元}\end{aligned}$$

例1.2.6

给定“字母表” S, 由 S 中字母构成的有序字串叫做基于字母表 S 的字, 对于两个这种字 w_1,w_2 定义：

$$w_1\circ w_2:w_2\text{紧接}w_1\text{后得到的字}$$

叫做字的毗连运算.
全体基于 S 的字构成的集合（包括空字 Λ ）, 依 $\circ$ 构成幺半群, 其中 Λ 为单位元.

例1.2.7

记 $M_n(\mathbb{R})=\{n$阶实方阵$\}$, 则 $M_n(\mathbb{R})$ 按矩阵乘法构成幺半群.

单位元为n×n矩阵 $\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$

例1.2.8

$f:\mathbb{Z}\to\mathbb{Z}$, 叫 $\mathbb{Z}$ 上的变换, $M_{\mathbb{Z}}=\{\mathbb{Z}$上变换$\}$ 按映射的复合构成幺半群.
其中, 恒等映射 $I_X: x\mapsto x$ 为单位元, 因为:

$$I_X\circ f(x)=I_X\big(f(x)\big)=f(x)\quad f\circ I_X=f\big(I_X(x)\big)=f(x)$$

定理1.2.1

设 M 为半群, 对于 $a_1,\dots,a_n\in M$, 依此顺序做成的乘积与括号的添加方式无关.

证明 对 n 进行归纳, $n=1,2$ 时显然成立.
设 $n>2$ 且对小于 n 的数结论正确,

$$\begin{aligned}(a_1\dots a_m)(a_{m+1}\dots a_n)&=\big(a_1(a_2\dots a_m)\big)(a_{m+1}\dots a_n)\\&=a_1\big((a_2\dots a_m)(a_{m+1}\dots a_n)\big)\\&=a_1(a_2\dots a_n)\quad\square\end{aligned}$$

对于半群 M 中元素 a, 定义 $a^n=\overbrace{a\cdots a}^{n个}$, 当 $m,n\in\mathbb{Z}^+$ 时, 有:

$$a^ma^n=a^{m+n},\quad (a^m)^n=a^{mn}$$

如果 M 有单位元 e, 定义 $a^0=e$, 当 $m,n\in\mathbb{N}$ 时, 有:

$$a^ma^n=a^{m+n}$$

a 可逆时, 定义 $a^{-n}=(a^{-1})^n$, 则可知:

$$\begin{aligned}a^na^{-n}&=a^{n-1}a\,a^{-1}a^{-(n-1)}=a^{n-1}\,e\,a^{-(n-1)}\\&=a^{n-1}a^{-(n-1)}=a\,a^{-1}\\&=e\end{aligned}$$

类似可证

$$a^{-n}a^n=e,\quad a^{-n}=(a^n)^{-1},\quad a^ma^n=a^{m+n},\quad (a^m)^n=a^{mn}$$

定义1.2.2

如果半群 M 中运算 $\circ$ 满足交换律:

$$\forall a, b \in M, ab = ba$$

则称 M 为**交换半群**(或**可换半群**).

定理1.2.2

对于交换半群 M 中 n 个元 $a_1, \ldots, a_n$, 对乘积 $a_1 \cdots\ a_n$ 任意颠倒因子顺序, 结果不变.

证明 对 n 归纳, $n = 1, 2$ 时显然成立.

设 $n > 2$ 且对更小的 n 结论正确. 任给 $1, \ldots, n$ 的全排列 $i_1, \ldots, i_n$ 设 $i_m = n$,

$$\begin{aligned} a_{i_1} \cdots\ a_{i_n} &= (a_{i_1} \cdots a_{i_{m-1}})\big(a_n(a_{i_{m+1}} \cdots a_{i_n})\big) \\ &= (a_{i_1} \cdots a_{i_{m-1}})(a_{i_{m+1}} \cdots a_{i_n})a_n \\ &= (a_1 \cdots a_{n-1})a_n(\text{由归纳假设得到}) \end{aligned}$$

与排列顺序 $i_1, \ldots, i_n$ 无关. □

定义1.2.3

设 G 为按 $\circ$ 构成的半群, G 至少有一个“左单位元” e, 即对 $\forall a \in G$, 有 $ea = a$, 且对每个 $a \in G$ 至少有一个“左逆元” a^{-1}, 即对 $\forall a \in G$, 有 $a^{-1}a = e$, 则称 G 按运算 $\circ$ 构成一个**群**.

定理1.2.3

设 G 为群, 则 G 中左单位元也是右单位元, 从而是单位元, 每个 $a \in G$ 的左逆元也是右逆元, 从而为 a 的逆元.

证明　设 e 是 G 的左单位元, $\forall a \in G$ 有左逆元 a^{-1}. $a^{-1}a = e$.

$$a^{-1} = ea^{-1} = (a^{-1}a)a^{-1} = a^{-1}aa^{-1}$$

设 a^{-1} 的左逆元为 $b = (a^{-1})^{-1}$
则

$$e = ba^{-1} = b\big(a^{-1}(aa^{-1})\big) = (ba^{-1})(aa^{-1}) = e(aa^{-1}) = aa^{-1}$$

$$ae = a(a^{-1}a) = (aa^{-1})a = ea = a$$

因此 e 为群 G 单位元, 由于 $a^{-1}a = e = aa^{-1}$, a^{-1} 为a 在群 G 中逆元. □

定理1.2.4

设 G 为群, 对于 $a \in G$ 有

$$a^{m+n} = a^m a^n,\ (a^m)^n = a^{mn} \quad (m, n \in \mathbb{Z})$$

定理1.2.5

半群 G 构成群等价于它具有下列可除性条件:

$$\text{对任何}a, b \in G, \begin{cases} ax = b \\ ya = b \end{cases} \text{在}G\text{中有解.}$$

证明　"$\Rightarrow$" : G 为群时,

$$a(a^{-1}b) = (aa^{-1})b = eb = b \quad \Rightarrow \quad ax = b\text{在}G\text{中有解.}$$
$$(ba^{-1})a = b(a^{-1}a) = be = b \quad \Rightarrow \quad ya = b\text{在}G\text{中有解.}$$

"$\Leftarrow$" : 任取 $a \in G$, $ya = a$ 在 G 中有解 e, 则 $ea = a$.
任给 $b \in G$, 有 $x \in G$, 使得 $ax = b$, 于是

$$eb = eax = (ea)x = ax = b$$

可见 e 为 G 的左单位元; 又 $yb = e$ 在 G 中有解, 那么 y 为 b 的左逆元.
于是 G 为群. □

推论1.2.1

(1) 设 G 为群, 则 G 中有消去律：

$$\begin{aligned} ax = ay &\Rightarrow x = y \\ xa = ya &\Rightarrow x = y \end{aligned}$$

(2) 具有消去律的有限半群必为群.

证明 (1)

$$\begin{aligned} ax = ay &\Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow ex = ey \Rightarrow x = y \\ xa = ya &\Rightarrow (xa)a^{-1} = (ya)a^{-1} \Rightarrow xe = ye \Rightarrow x = y \end{aligned}$$

(2) 设 $G = \{a_1, a_2, \ldots, a_n\}$ 是个半群且满足消去律
对于 $a \in G$, 让 $aG = \{ax : x \in G\} = \{aa_1, aa_2, \ldots, aa_n\}$,
由消去律, $aa_1, aa_2, \ldots, aa_n$ 两两不等, 共有n个元素从而
$G = \{aa_1, aa_2, \ldots, aa_n\}$.
那么, 任给 $b \in G$, 有 i 使得 $aa_i = b$, 故 $ax = b$ 有解. 类似地, 因为
$a_1a, a_2a, \ldots, a_na$ 两两不等, 同上可证 $ya = b$ 也可解.
由定理1.2.5知, G 为群. □

P.S：半群 G 无限时有反例：例1.2.10

例1.2.10

$\mathbb{Z}^+ = \{1, 2, 3 \ldots\}$ 按乘法构成幺半群, 也有消去律, 但 $\mathbb{Z}^+$ 不是群.
$\mathbb{N} = \{0, 1, 2 \ldots\}$ 按加法构成幺半群, 有消去律, 但不是群.

定义1.2.4

如果群 G 中只有有限个元素, 则称 G 为**有限群**, 如果 $|G| = n$ （n为正整数）, 则说 G 为 n **阶群**.
如果群 G 满足交换律 $\forall a \in G \forall b \in G\,(ab = ba)$, 则称 G 为**Abel群**.（或**交换群**）

例1.2.11

$\mathbb{Q}^* = \{$非零有理数$\}$ 按乘法构成Abel群.
$\mathbb{R}^* = \{$非零实数$\}$, $\mathbb{C}^* = \{$非零复数$\}$ 按乘法构成Abel群.

例1.2.12

复数域 $\mathbb{C}$ 中全体 n 次单位根依乘法构成 n 阶Abel群.

$$C_n = \{z \in \mathbb{C} : z^n = 1\} \quad (z_1)^n = 1,\, (z_2)^n = 1 \Rightarrow (z_1 z_2)^n = 1$$

$$1 \in C_n,\, z^n = 1 \Rightarrow (z^{-1})^n = 1$$

$$C_n = \{e^{2\pi i \frac{k}{n}} : k = 0, 1, 2, \ldots, n-1\}$$

$$C_1 = \{1\}, C_2 = \{1, -1\}, C_3 = \{1, \omega, \omega^2\}\ [1], C_4 = \{\pm 1, \pm i\}$$

例1.2.13

设 m 为正整数, $m\mathbb{Z} = \{mx : x \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\}$ 按加法构成 Abel 群, 0为其加法单位元（一般把加法单位元叫零元）.
mx 的加法逆元（也叫负元）为 $-mx = m(-x)$
$\mathbb{Z} = 1\mathbb{Z}$ 按照加法构成 Abel 群, 它叫整数加群.

对 $a, b \in \mathbb{Z}$, 如果 $a - b \in m\mathbb{Z}$, 则说 a 与 b 模 m 同余, 记为 $a \equiv b \pmod m$, $m \mid a - b$.

$$\begin{aligned} \overline{a} &= \{x \in \mathbb{Z} : x \equiv a \pmod m\} \\ &= \{a + mq : q \in \mathbb{Z}\} \\ &= a + m\mathbb{Z} \\ &= a \pmod m \end{aligned}$$

叫做 a 所在的模 m 的剩余类（或同余类）.

对于正整数 m, 记 $\mathbb{Z}/m\mathbb{Z} = \{\overline{a} = a + m\mathbb{Z} : a \in \mathbb{Z}\} = \mathbb{Z}_m$

在 $\mathbb{Z}_m$ 上定义加法、乘法如下

$$\overline{a} + \overline{b} = \overline{a + b} \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

如果 $\overline{a} = \overline{c}$, $\overline{b} = \overline{d}$, 则 $\overline{a + b} = \overline{c + d}$, $\overline{ab} = \overline{cd}$, 从而定义合理.

因为：

(1) $\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a} \quad (\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$；

(2) $\overline{0} = 0 + m\mathbb{Z} = m\mathbb{Z}$ 为加法单位元, 因为 $\overline{a} + \overline{0} = \overline{a + 0} = \overline{a}$；

(3) $\overline{-a}$ 为 $\overline{a}$ 的加法逆元 $-\overline{a}$.

所以 $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ 按加法构成 m 阶Abel群.（$\overline{i}$ 的逆元为 $\overline{m-i}$, $1 \leqslant i \leqslant m-1$）

[1] $\omega = \frac{-1+\sqrt{3}i}{2}$.

此外, $\overline{a}\overline{b} = \overline{b}\overline{a}$　$(\overline{a}\cdot\overline{b})\overline{c} = \overline{a}(\overline{b}\cdot\overline{c})$, $\overline{1}\overline{a} = \overline{1a} = \overline{a}$.

$\mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z} = \{\overline{0},\overline{1}\}$, 那么 $0+2\mathbb{Z} = 2\mathbb{Z}$, $\overline{1} = 1+2\mathbb{Z}$, $\overline{0}+\overline{1} = \overline{1}$, $\overline{1}+\overline{1} = \overline{2} = \overline{0}$,
即奇+奇=偶.

$\mathbb{Z}_4 = \{\overline{0},\overline{1},\overline{2},\overline{3}\}$, 例如 $\overline{2}+\overline{3} = \overline{5} = \overline{1}$, $\overline{2}\cdot\overline{3} = \overline{6} = \overline{2}$, $\overline{2}+\overline{2} = \overline{4} = \overline{0}$

$U_m = \{\overline{a}\in\mathbb{Z}_m : (a,m) = 1\}$, 则

$$\overline{a}\in U_m \quad \overline{b}\in U_m \Rightarrow \overline{a}\overline{b} = \overline{ab}\in U_m$$

U_m 为乘法幺半群, 则 $|U_m| = |\{1\leqslant a\leqslant m : (a,m) = 1\}| = \varphi(m)$, 其中 $\varphi(m)$ 为 Euler 函数.因为:

设

$$\overline{a},\overline{x},\overline{y}\in U_m$$

则

$$\begin{aligned}\overline{a}\,\overline{x} = \overline{a}\,\overline{y} &\Rightarrow \overline{ax} = \overline{ay}\\ &\Rightarrow m|ax-ay\\ &\Rightarrow m\mid a(x-y)\\ &\Rightarrow m\,|x-y\ ((a,m)=1)\\ &\Rightarrow \overline{x} = \overline{y}\end{aligned}$$

所以 U_m 是满足消去律的有限半群, 故 U_m 为 $\varphi(m)$ 阶 Abel 群.

定理1.2.6

设 G 为 n 阶 Abel 群, 则 $a\in G$ 时, $a^n = e$.

证明　设 $a = \{a_1,\ldots,a_n\}$, $a\in G$ 时, $aa_1,\ldots,aa_n$ 两两不同, 从而 $G = \{aa_1,\ldots,aa_n\}$. 于是:

$$\prod_{i=1}^{n}(aa_i) = \prod_{x\in G} x = a_1\cdots a_n$$

即

$$a^n a_1\cdots a_n = ea_1\ldots a_n$$

因为 G 是群, 具有消去律, 从而 $a^n = e$. □

推论1.2.2 (Euler 定理)

设 m 为正整数, $a\in\mathbb{Z}$ 与 m 互素, 则

$$a^{\varphi(m)}\equiv 1\pmod m$$

证明 $U_m=\{\overline{x}:(x,m)=1\}$ 为 $\varphi(m)$ 阶 Abel 群.
由于 $(a,m)=1,\overline{a}\in U_m$, 则

$$\overline{a}^{\varphi(m)}=\overline{1}=\overline{a^{\varphi(m)}}$$

故 $a^{\varphi(m)}\equiv 1 \pmod m$. □

特别地, m 是素数 p 时, $\varphi(m)=\varphi(p)=p-1, p\nmid a\Rightarrow a^{(p-1)}\equiv 1 \pmod p$, 此即为 Fermat 小定理.

例1.2.14
$GL_n(\mathbb{R})=\{n\text{阶实方阵}A:\det A\neq 0\}$ 按矩阵乘法构成群, 叫做一般线性群.
$SL_n(\mathbb{R})=\{n\text{阶实方阵}A:\det A=1\}$ 按矩阵乘法构成群, 叫做特殊线性群.

例1.2.15
区间上 I 全体连续函数按函数加法构成Abel群. 其中:

$$(f+g)(x)\triangleq f(x)+g(x)\quad \mathbf{0}(x)=0\quad f+\mathbf{0}=f$$

f 的加法逆元（负元）为 $(-f)(x)=-f(x), f+(-f)=\mathbf{0}$

例1.2.16
设 X 为非空集, X 到 X 的双射（一一对应）叫 X 的一个**置换**.
$S(X)=\{X\text{上置换}\}$, 当 $X=\{x_1,\ldots,x_n\}$ 时, $\sigma\in S(X)$ 可表成:

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n}\end{pmatrix}$$

其中 $i_1,i_2\ldots,i_n$为$1,2,3\ldots n$的一个排列.
$|X|=n$ 时, $|S(X)|=n!, X=\{1,2,\ldots,n\}$ 时, $S(X)$ 记为 S_n
$S(X)$ 按映射的复合构成群:

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

其中单位元为恒等映射:

$$I_X:x\mapsto x,\quad f\circ I_X=I_X\circ f=f$$

f 的逆元为它的逆映射 f^{-1}： $f\circ f^{-1}=f^{-1}\circ f=I_X$.

一些特例如下:

$$S_1=\left\{\begin{pmatrix}1\\1\end{pmatrix}\right\}\quad S_2=\left\{\begin{pmatrix}1&2\\1&2\end{pmatrix},\begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$$

$$S_3=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\right\}$$

记

$$I = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\lambda = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \lambda^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \xi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

则

$$\lambda\lambda^{-1} = I,\, \sigma^{-1} = \sigma,\, \tau^{-1} = \tau,\, \xi^{-1} = \xi$$

$$\sigma\tau = \lambda,\, \tau\sigma = \tau^{-1}\sigma^{-1} = (\sigma\tau)^{-1} = \lambda^{-1}$$

注意：S_3 不是 Abel 群.此外, 因为：

$$\sigma = \lambda^{-1}\xi = \xi^{-1}\lambda = \lambda\xi\lambda^{-1}$$

$$\tau = \sigma^{-1}\lambda = \lambda^{-1}\sigma = \lambda\xi$$

所以 $S_3 = \langle \xi, \lambda \rangle$ [2].

例1.2.17

复数 $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$, 设 $z = a + bi$ 满足：

$$z\overline{z} = a^2 + b^2 = |z|^2,\, z \cdot \frac{\overline{z}}{a^2 + b^2} = 1,\, z^{-1} = \frac{\overline{z}}{a^2 + b^2}$$

超复数：

(1)若几何形式为三维向量：$z = a + bi + cj, \overline{z} = a - bi - cj$, 满足：

$$|z|^2 = a^2 + b^2 + c^2, \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$$

但是, 由于 Gauss-Legendre 定理[3]知道,

$$\{a^2 + b^2 + c^2 : a, b, c \in \mathbb{Z}\}$$

对乘法不封闭.即

$$|z_1 z_2|^2 = |z_1|^2 |z_2|^2$$

不一定能成立.

(2)Hamilton 四元数：

$$\begin{aligned} z &= a + bi + cj + dk \\ \overline{z} &= a - bi - cj - dk \end{aligned} \qquad (a, b, c, d \in \mathbb{R})$$

规定：

$$ij = k,\, jk = i,\, ki = j,\, i^2 = j^2 = k^2 = ijk = -1$$

那么也容易得到 $ji = -k$, $kj = -i$, $ik = -j$.

$D = \{\pm 1, \pm i, \pm j, \pm k\}$ 构成群

[2] $S_3 = \langle \xi, \lambda \rangle$ 表示 S_3 的所有元素均可由 ξ, λ 或者它们的逆的乘积表示

[3] 整数 n 可表示成三个整数的平方和 $\Leftrightarrow n$ 是不形如 $4^k(8l + 7)$ 的数.

$z\overline{z}=a^2+b^2+c^2+d^2$, 且满足 $|z_1z_2|^2=|z_1|^2|z_2|^2$, 也可知道

$$\{a^2+b^2+c^2+d^2 : a,b,c,d\in\mathbb{Z}\}$$

对乘法封闭.

作业：

(1) 设 M 为幺半群, a 为 M 中可逆元, 证明对任何 $m,n\in\mathbb{Z}$, 有
$a^ma^n=a^{m+n}, (a^m)^n=a^{mn}$

(2) 让 $M=\big\{$实数列$\{a_n\}:n\geqslant 0\big\}$, 定义卷积运算 $*$ 如下:

$$\{a_n\}*\{b_n\}=\{c_n\}$$

这儿 $c_n=\sum_{k=0}^{n}a_kb_{n-k}$, 证明：$M$ 按 $*$ 构成幺半群, 并指出单位元.

(3) 设 G 为群, 如果对 $\forall a\in G$, 都有 $a^2=e$, 则 G 为 Abel 群.

(4) 设函数 $f_1,f_2,\ldots,f_6$ （定义在 $(0,1)$ 上）如下给出：

$$\begin{array}{lll} f_1(x)=x & f_2(x)=\frac{1}{1-x} & f_3(x)=\frac{x-1}{x} \\ f_4(x)=\frac{1}{x} & f_5(x)=1-x & f_6(x)=\frac{x}{x-1} \end{array}$$

证明：$G=\{f_1,f_2,\ldots,f_6\}$ 依函数复合构成群, 并作出乘法表.

(5) 设正整数 d 不是完全平方, 证明：

$$\overline{G_d}=\{x+\sqrt{d}y : x^2-dy^2=1, x,y\in Z\}$$

按乘法构成Abel群.

1.3　子群与陪集

定义1.3.1

设 G 按运算 $\circ$ 构成群, $\emptyset \neq H \subseteq G$. 如果 H 按 $\circ$ 在 H 上限制也构成群, 则说 H 为 G 的子群, 记为 $H \leqslant G$.

性质1.3.1

设 $H \leqslant G$, 则

(1) H 的单位元 e_H 必是 G 的单位元 e.
证明： $e_H e_H = e_H = e e_H$, 所以 $e_H = e$.

(2) $a \in H$ 在 H 中的逆元 a_H^{-1} 就是 a 在 G 中逆元 a^{-1}.
证明： $a a_H^{-1} = e_H = e = a a^{-1}$, 因为群具有消去律, 所以 $a_H^{-1} = a^{-1}$.

定理1.3.1 (子群判别定理)

设 H 为群 G 的非空子集, 则下列几条等价：

(1) $H \leqslant G$

(2) H 对乘法和求逆封闭

(3) H 对右除法封闭即对 $\forall a, b \in H$, 有 $ab^{-1} \in H$.

证明　(1) $\Rightarrow$ (2) 和 (2) $\Rightarrow$ (3) 是显然的.
(3) $\Rightarrow$ (1)：任取 $a \in H$, 可以得到

$$e = aa^{-1} \in H \quad a^{-1} = ea^{-1} \in H \text{（对求逆封闭）}$$

$h \in H$ 时, 有

$$ha = h(a^{-1})^{-1} \in H \text{（对乘法封闭）}$$

故 $H \leqslant G$. □

定义1.3.2

对群 G 的子集 X, Y,

$$X^{-1} = \{x^{-1} : x \in X\} \quad XY = \{xy : x \in X, y \in Y\}$$

性质1.3.2

(1) $(X^{-1})^{-1}=\{(x^{-1})^{-1}:x\in X\}=X$

(2) $(xy)z=x(yz)\longrightarrow(XY)Z=X(YZ)$

(3) $(XY)^{-1}=Y^{-1}X^{-1}$

性质1.3.3

设 $H\leqslant G$, 则

(1) $H^{-1}=H$, 因为:

$$\begin{aligned} a\in H\Rightarrow a^{-1}\in H \qquad & \text{故 } H^{-1}\subseteq H \\ a\in H\Rightarrow a^{-1}\in H\Rightarrow(a^{-1})^{-1}\in H^{-1} \qquad & \text{故 } H\subseteq H^{-1} \end{aligned}$$

(2) $HH=H$, 因为:

$$\begin{aligned} H\text{对乘法封闭}\Rightarrow \qquad & HH\subseteq H \\ h\in H\text{时},\ h=eh\in HH\Rightarrow \qquad & H\subseteq HH \end{aligned}$$

验证 G 的子集 H 为 G 的子群, 一般如下进行:

(1) 先说明 $e\in H$

(2) 验证 H 对右除法封闭（$a,b\in H\Rightarrow ab^{-1}\in H$）

定理1.3.2

群 G 的若干个子群 $H_i\,(i\in I)$ 的交 $\bigcap_{i\in I}H_i$ 仍为 G 的子群.

证明 设 $H=\bigcap_{i\in I}H_i$, 由于 $e\in H_i\,(\forall i\in I)$, 故 $e\in H$.
$a,b\in H$ 时, 对 $\forall i\in I$, 有:

$$a,b\in H_i\Rightarrow ab^{-1}\in H_i$$

故 $ab^{-1}\in H$, 所以 H 对右除法封闭, 即 $H\leqslant G$. □

定义1.3.3

设 X 为群 G 的非空子集（X 不一定是子群），则

$$\langle X\rangle = \bigcap_{X\subseteq H\leqslant G} H$$

为包含 X 的 G 的最小子群

可知 $\langle X\rangle = \{x_1^{m_1}x_2^{m_2}\cdots x_k^{m_k} : x_1,\cdots,x_k\in X, m_1,\cdots,m_k\in\mathbb{Z}\}$，叫由 X 生成的子群.

定义1.3.4

如果 $G=\langle X\rangle$, 则说 G 是由 X 生成的.
$X=\{a_1,\cdots,a_n\}$ 时, $\langle X\rangle$ 写为 $\langle a_1,\cdots,a_n\rangle$.
$\langle a\rangle = \{a^m : m\in\mathbb{Z}\}$ 叫做由 a 生成的子群.

子群的例子：$\mathbb{Q}^*\leqslant\mathbb{R}^*\leqslant\mathbb{C}^*$, $SL_n(\mathbb{R})\leqslant GL_n(\mathbb{R})$ [1].

定理1.3.3

设 H,K 为 G 的子群, 则

$$HK\leqslant G \Leftrightarrow HK=KH$$

证明　充分性：设 $HK\leqslant G$, 则 $(HK)^{-1}=HK$, 即 $K^{-1}H^{-1}=HK$, 故 $HK=KH$.
必要性：设 $HK=KH$, 则 $e=e_He_K\in HK$, 另外：

$$\begin{aligned}(HK)(HK)^{-1} &= (HK)K^{-1}H^{-1} = HKKH\\ &= HKH = HHK\\ &= HK\end{aligned}$$

即 HK 对右除法封闭, 故 $HK\leqslant G$. □

[1] $\mathbb{Q}^*,\mathbb{R}^*,\mathbb{C}^*$ 见例1.2.11, $SL_n(\mathbb{R}),GL_n(\mathbb{R})$ 见例1.2.14

定义1.3.5

设 $H \leqslant G, a^{-1}b \in H$ 时, 称 $a \sim_e b$ (左等价).

左等价是等价关系, 因为它满足:

(1) 自反性: $a \sim_e a$ （$a^{-1}a = e \in H$）

(2) 对称性: $a \sim_e b \Rightarrow b \sim_e a$
（$a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H$）

(3) 传递性: $a \sim_e b, b \sim_e c \Rightarrow a \sim_e c$
（$a^{-1}b \in H, b^{-1}c \in H \Rightarrow a^{-1}c \in H \Rightarrow a \sim_e c$）

定义1.3.6

$\sim_e$ 是 G 上的如上所述的等价关系, a 所在的等价类

$$\{b \in G : a^{-1}b \in H\} = \{ah : h \in H\} = \{a\}H \triangleq aH$$

叫做 H 的一个**左陪集**.

性质1.3.4

(1) $a = ae \in aH$

(2) $x \in aH \Leftrightarrow xH = aH \Leftrightarrow a \in xH$, 即等价的两元素构成的左陪集相等.

证明: 如果 $x \in aH$, 设 $x = ah$, 则

$$xH = ahH = aH \, (hH = H\,^{2})$$

如果 $aH = xH$, 则

$$x = xe \in xH = aH$$

(3) $aH \neq bH \Rightarrow aH \cap bH = \emptyset$, 即只要两个左陪集有交集必然恒等.
证明: 如果 $aH \cap bH \neq \emptyset$, 则存在 $x \in aH \cap bH$, 由(2)可知, $aH = xH, bH = xH$, 从而 $aH = bH$, 得出矛盾.

类似地, $Ha = \{ha : h \in H\}$ 叫 H 的一个**右陪集**, 同样可以得到:

[2]因为: $hH \subseteq HH = H$, $H = hh^{-1}H \leqslant hH$

性质1.3.5

(1) $a = ea \in aH$.

(2) $x \in Ha \Leftrightarrow Hx = Ha$.

(3) $Ha \neq Hb \Rightarrow Ha \cap Hb = \emptyset$.

定理1.3.4

设 $H \leqslant G$, 则 $a \in G$ 时,

$$aH \approx H \approx Ha$$

且 $\{aH : a \in G\} \approx \{Ha : a \in G\}$.

证明 (1) 做 $f : H \to aH$ 如下:

$$f(h) = ah \quad h \in H$$

则
(i) f 为满射, 这是非常显然的.
(ii) $h_1, h_2 \in H$ 时, $ah_1 = ah_2 \Rightarrow h_1 = h_2$, f 也是单射.
类似地, $h \to ha$ 也是 H 到 Ha 的双射, 故 $aH \approx H \approx Ha$.
(2) 让 $S = \{aH : a \in G\}$, $T = \{Ha : a \in G\} = \{H^{-1}x^{-1} : x \in G\}$
做 $f : S \to T$ 如下:

$$f(xH) = (xH)^{-1} = H^{-1}x^{-1} = Hx$$

易知, f 为双射, 故 $S \approx T$. □

定义1.3.7

设 $H \leqslant G$, 则称

$$|\{aH : a \in G\}| = |\{Ha : a \in G\}|$$

为子群 H 在 G 中**指标**, 记为 $[G : H]$.

定理1.3.5

设 $H \leqslant G$, 则

(1) G 可表成 $[G:H]$ 个两两不相交的 H 左（右）陪集的并, 称 G 按 H 进行左（右）陪集分解.

(2) $[G:H]|H| = |G|$ （无穷时也成立）

(3) (Lagrange 定理)若 $|G| < \infty$, 那么 $|H| \mid |G|$.（即子群的势可以整除原群的势）

证明 (1)

$$G = \bigcup_{x \in G} xH = x_1H \cup x_2H \cup \cdots = \bigcup_{i \in I} x_iH$$

其中 $x_iH(i \in I)$ 为所有不同的 H 的左陪集.

(2) 设 G 有左陪集分解:

$$G = \bigcup_{i \in I} x_iH \quad |I| = [G:H]$$

让 $X = \{x_i : i \in I\}$, 则 $|X| = [G:H]$.

定义 $f : X \times H$如下:

$$f : \langle x_i, h \rangle \mapsto x_ih$$

则可知 f 为满射.又

$$x_ih = x_jh' \Rightarrow x_i = x_jh'h^{-1} \in x_jH \Rightarrow x_iH = x_jH \Rightarrow i = j,\ h = h'$$

故 f 也为单射.所以

$$X \times H = G \Rightarrow |G| = |X \times H| = |X||H| = [G:H][H]$$

(3) 设 G 为有限群, 则 $|G|, |H|, [G:H] \in \mathbb{Z}^+$, 所以 $|H| \mid |G|$. □

例1.3.2

设群 G 恰有四个元素 e, a, b, c, 且 $a^2 = b^2 = c^2 = e$, 则有:

$$ab = ba = c \quad bc = cb = a \quad ac = ca = b$$

G 为四阶群, 称为Klein四元群.

$H=\{e,a\}$ 为 G 的2阶子群, 则可得

$$eH=\{eh:h\in H\}=H=aH=H$$
$$bH=\{be,ba\}=\{b,c\}=cH=\{ce,ca\}=\{c,b\}$$

那么 $[G:H]=2$.

定理1.3.6

设 G 为 n 阶群, 在对任何 $a\in G$, 有 $a^n=e$.

证明 让 $H=\langle a\rangle=\{a^m:m\in\mathbb{Z}\}\leqslant G$, 则子群 H 是Abel群, 且$|H|\mid|G|$, 所以, 对 $a\in H$

$$a^{|H|}=e\Rightarrow a^n=\left(a^{|H|}\right)^{\frac{n}{|H|}}=e$$ □

定理1.3.7

设 $H,K\leqslant G$, 那么

(1) HK 是 $[K:H\cap K]$ 个不同的 H 右陪集的并, 从而 $[K:H\cap K]\leqslant[G:H]$. ($HK$ 也是 $[H:K\cap H]$ 个不同的 K 左陪集的并.)

(2) (Poincare) $H,K\leqslant G\Rightarrow[G:H\cap K]\leqslant[G:H][G:K]$

(3) 如果 $K\leqslant H\leqslant G$, 那么 $[G:H][H:K]=[G:K]$

证明 (1) $HK=\bigcup_{k\in K}Hk$, 对于 $k_1,k_2\in K$

$$\begin{aligned}Hk_1=Hk_2&\Leftrightarrow Hk_1k_2^{-1}=H\\&\Leftrightarrow k_1k_2^{-1}\in H\\&\Leftrightarrow k_1k_2^{-1}\in H\cap K\\&\Leftrightarrow k_1\in(H\cap K)k_2\\&\Leftrightarrow(H\cap K)k_1=(H\cap K)k_2\end{aligned}$$

故

$$|\{Hk:k\in K\}|=|\{(H\cap K)k:k\in K\}|=[K:H\cap K]$$
$$[K:H\cap K]=|\{Hx:Hx\subseteq HK\}|\leqslant[G:H]$$

(2) 做映射 $f:\{x(H\cap K):x\in G\}\to\{xH:x\in G\}\times\{xK:x\in G\}$ 如下：

$$f\big(x(H\cap K)\big)=\langle xH,xK\rangle$$

那么

$$\begin{aligned}x(H\cap K)=y(H\cap K)&\Leftrightarrow H\cap K=x^{-1}yH\cap K\\&\Leftrightarrow x^{-1}y\in H\cap K\\&\Leftrightarrow x^{-1}y\in H \text{ 且 } x^{-1}y\in K\\&\Leftrightarrow y\in xH\quad y\in xK\\&\Leftrightarrow xH=yH\quad xK=yK\\&\Leftrightarrow \langle xH,xK\rangle=\langle yH,yK\rangle\end{aligned}$$

故 f 定义合理且为单射.所以

$$|\{x(H\cap K):x\in G\}|\leqslant|\{xH:x\in G\}||\{xK:x\in G\}|=[G:H][G:K]$$

(3) $K\leqslant H\leqslant G$ 时, G 可按 H 进行左陪集分解：

$$G=\bigcup_{i\in I}x_iH\quad |I|=[G:H]$$

H 可按 K 进行左陪集分解：

$$H=\bigcup_{j\in J}y_jK\quad |J|=[H:K]$$

那么

$$x_iH=\bigcup_{j\in J}x_iy_jK\Rightarrow G=\bigcup_{i\in I}\bigcup_{j\in J}x_iy_jK$$

这是 G 按 K 的一个左陪集分解,则 $[G:K]=|I||J|=[G:H][H:K]$ □

作业：

(1) 设 G 为群, $x\in G$, 证明：

$$\begin{aligned}C_G(x)&=\{g\in G:gx=xg\}\leqslant G\\Z(G)&=\bigcap_{x\in G}\{g\in G:\forall x\in G(gx=xg)\}\leqslant G\end{aligned}$$

其中, $C_G(x)$ 叫 x 的中心化子.

(2) 设 $H\leqslant G,x\in G$, 证明：

(i) $xHx^{-1}=\{xhx^{-1}:h\in H\}\leqslant G$

(ii) $|xHx^{-1}|=|H|$

(iii) $[G:xHx^{-1}]=[G:H]$

(3) 设 $H\leqslant G,[G:H]=2$, 证明：

$$x\in G\text{时}, xH=Hx$$

1.4　元素的阶与循环群

定义1.4.1

设 G 为群, $a \in G$, 由 a 生成的子群为: $\langle a \rangle = \{a^m : m \in \mathbb{Z}\}$.
如果 $a, a^2, a^3 \cdots$ 都不等于 e. 则说 a 的**阶** $o(a)$ 为 ∞.
如果有正整数 n, 使得 $a^n = e$, 而且 $0 < m < n$ 时, $a^m \neq e$, 则说 a 的阶为 n, 记为 $o(a) = n$.

性质1.4.1

(1) $o(a)=\infty$ 时:

(i) $\cdots,a^{-2},a^{-1},a^0,a^1,a^2\cdots$ 两两不同.因为:

$$a^k=a^l\Leftrightarrow a^{k-l}=e\Leftrightarrow a^{|k-l|}=e\Leftrightarrow |k-l|=0\Leftrightarrow k=l$$

(ii) $m\in\mathbb{Z}\backslash\{0\}$ 时, $o(a^m)=\infty$. 因为:

$$\begin{aligned}&\cdots,a^{-2},a^{-1},a^0,a^1,a^2\cdots \text{两两不同}\\ \Rightarrow&\cdots,a^{-2m},a^{-m},a^0,a^m,a^{2m}\cdots \text{两两不同}\end{aligned}$$

(2) $o(a)=n$ 时,

(i) $a^0,a^1,a^2,\cdots,a^{n-1}$ 两两不同, 否则设 $0\leqslant k<l<n$, 则:

$$a^k=a^l\Rightarrow a^{l-k}=e$$

因为 $0<l-k<n$, 与 n 的最小性矛盾.

(ii) 对 $k,l\in\mathbb{Z}$, $a^k=a^l\Leftrightarrow k\equiv l\pmod n$, 特别地

$$a^m=e\Leftrightarrow o(a)=n\mid m$$

因为:

$$a^{nq+r}=(a^n)^qa^r=a^r$$

即

$$a^{nq+r}=e\Leftrightarrow a^r=e\Leftrightarrow r=0$$

从而

$$a^m=e\Leftrightarrow o(a)=n\mid m$$

注意到

$$a^k=a^l\Leftrightarrow a^{k-l}=e\Leftrightarrow a^{|k-l|}=e\Leftrightarrow k\equiv l\pmod n$$

(iii)

$$\begin{aligned}\langle a\rangle&=\left\{a^{nq+r}:q\in\mathbb{Z},r\in\{0,1,\cdots,n-1\}\right\}\\&=\{a^r:r=0,1,\cdots,n-1\}\\&=\{a^0,a^1,\cdots,a^{n-1}\}\end{aligned}$$

定理1.4.1

(1) 设群 G 中的元 a 的阶为 n, 则 $m \in \mathbb{Z}$ 时, $o(a^m) = \frac{n}{(m,n)}$, 特别地, 若 $(m,n)=1$, $o(a^m)=n$.

(2) 设 $a,b \in G$ 满足 $ab=ba$, 如果 $m=o(a)$ 与 $n=o(b)$ 互素, 则

$$o(ab)=mn=o(a)o(b)$$

证明 (1)

$$(a^m)^d = e \Leftrightarrow a^{md}=e \Leftrightarrow n \,\big|\, md \Leftrightarrow \frac{n}{(m,n)} \,\Big|\, \frac{m}{(m,n)}d \Leftrightarrow \frac{n}{(m,n)} \,\Big|\, d$$

(2) 设 $o(ab)=d$, 因为：

$$(ab)^{mn}=a^{mn}b^{mn}=(a^m)^n(b^n)^m=e$$

故 $d \,\big|\, mn$, 因为 $(ab)^d=e$, 所以 $a^d=b^{-d}$. 故

$$a^{d\frac{m}{(d,m)}}=b^{-d\frac{m}{(d,m)}}$$

即 $(a^m)^{\frac{d}{(d,m)}}=e$, 所以 $n \,\big|\, d\frac{m}{(d,m)}$. 而 $(n,m)=1$, 故

$$n \,\big|\, d$$

类似可证 $m \,\big|\, d$, 所以 $[m,n]=mn \,\big|\, d$.
因此 $d=mn$. □

定义1.4.2

对于群 G, 如果有 $a \in G$, 使 $G=\langle a\rangle=\{a^m : m\in\mathbb{Z}\}$, 则说 G 为**循环群**（由 a 生成）, a 叫做**生成元**.

例1.4.1

$m\in\mathbb{Z}$ 时, $m\mathbb{Z}=\{mx : x\in\mathbb{Z}\}$ 是由 m 生成的（加法）循环群.特别地, $\mathbb{Z}$ 是 1 生成的循环群.

$C_n=\{z\in\mathbb{C} : z^n=1\}=\{e^{2\pi i\frac{r}{n}} : r=0,1,\cdots,n-1\}$ 是由 $e^{\frac{2\pi i}{n}}$ 生成的循环群.特别地：

$$C_2=\langle -1\rangle,\ C_3=\langle \omega\rangle,\ C_4=\langle i\rangle$$

引理1.4.1

循环群 G 的子群仍为循环群.

证明　设 a 是 G 的生成元, 任给 $H \leqslant G$.
如果 $H=\{e\}$, 则 $H=\langle e\rangle$ 为循环群.
下设 $H \neq \{e\}$, 则有 $n \in \mathbb{Z}^+$, 使 $a^n \in H$. 让 $d=\min\{n \in \mathbb{Z}^+ : a^n \in H\}$, 则

$$a^d \in H \quad \langle a^d\rangle \subseteq H$$

设 $a^m \in H$, 对 m 做带余除法：$m=dq+r$, 其中 $0 \leqslant r < d$. 则

$$a^r = a^m a^{-dq} = a^m (a^d)^{-q} \in H$$

所以 r 必为0, 否则与 d 的选取矛盾.
因此 $m=dq$, $a^m=(a^d)^q \in \langle a^d\rangle$, 所以 $H=\langle a^d\rangle$ 为循环群. □

定理1.4.2

设 $G=\langle a\rangle$ 为循环群,

(1) 如果 $o(a)=\infty$, 即 $|G|=\aleph_0$, 则 G 含有 $\aleph_0$ 个子群.它们是

$$H_n=\langle a^n\rangle\,(n=0,1,2\cdots)$$

H_n 为无穷循环群.

(2) 如果 $o(a)=n$, 即 $|G|=n$, 则 G 恰有 $|\{d \in \mathbb{Z}^+ : d \mid n\}|$ 个子群.它们是 $H_d=\langle a^{\frac{n}{d}}\rangle$, 其中 d 为 n 的任一个正因子.

证明　(1) $o(a)=\infty$ 时, $\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2\cdots$ 两两不同, 从而 $n>0$ 时,
$o(a^n)=\infty$, 则 $\cdots, a^{-2}, a^{-1}, a^0, a^1, a^2\cdots$ 两两不同, 从而 H_n 为无穷循环群.
任给 $H \leqslant G$, 由引理1.4.1（28页）知, H 为循环群, 设 $H=\langle a^m\rangle$, 令 $n=|m|$, 则

$$H=\langle a^n\rangle = H_n$$

$n>0$ 时, $H_n \neq H_0$, $0<n<n'$ 时, $H_n \neq H_{n'}$

(2) $o(a)=n$ 时, d 为正因子时

$$(a^{\frac{n}{d}})^m = e \Leftrightarrow a^{\frac{n}{d}m} = e \Leftrightarrow n \,\Big|\, \frac{n}{d}m \Leftrightarrow d \mid m$$

故 $o(a^{\frac{n}{d}})=d$, $H_d=\langle a^d\rangle$ 为 G 的 d 阶子群.
d 与 d' 为 n 不同正因子时, $H_d\neq H_{d'}$, 因为 $|H_d|=d\neq |H'_d|=d'$.
任给 $H\leqslant G$, 依引理1.4.1知 H 为循环群, 所以 $H=\langle a^m\rangle$, 让 $d=|H|\bigm| n$ [1], 则

$$(a^m)^d=e\Rightarrow n\bigm| md\Rightarrow \frac{n}{d}\bigm| m$$

所以 $H=\langle a^m\rangle\subseteq\langle a^{\frac{n}{d}}\rangle=H_d$, 注意到 $|H|=d=|H_d|$, 从而 $H=H_d$. □

作业：

(1) 对 G 中的元 x,y, 如果有 $g\in G$, 是 $gx=yg$, 即 $y=gxg^{-1}$, 则说 x 与 y 共轭, 记为 $x\sim y$, 证明：

  (i) 共轭关系 $\sim$ 是 G 上的等价关系（满足自反性, 对称性, 传递性）
  (ii) 如果 $x\sim y$, 那么 $o(x)=o(y)$. 从而可得当 $a,b\in G$ 时, $o(ab)=o(ba)$ [2].

(2) 设 G 为 p^α 阶群, p 为素数, $\alpha\in\mathbb{Z}^+$, 证明：G 有 p 阶元.（考虑 $a^{p^{\alpha-1}}$ ）

(3) 证明： p 阶群（ p 为素数）必为循环群.

[1] $|H|\bigm| n$ 由 Lagrange 定理（22页）得到.
[2]注意 $ab=b^{-1}(ba)b$.

1.5　正规子群与商群

定义1.5.1

设 $H \leqslant G$, 如果 $\forall g \in G\,(gH = Hg)$, 则说 H 在 G 中**正规**或 H 为 G 的**正规子群**, 记为 $H \trianglelefteq G$. (注意：正规并不能保证元素的可交换性.)

定理1.5.1

设 $H \leqslant G$, 则下列几条等价：

(1)　$H \trianglelefteq G$

(2)　H 的每个左陪集也是右陪集, 反之也成立.

(3)　与 H 共轭的子群只有 H, 即 $\forall g \in G\,(gHg^{-1} = H)$.

(4)　对 $g \in G, h \in H$, 有 $ghg^{-1} \in H$ （用的较多）

(5)　H 的任两个左陪集之积仍为 H 的左陪集

证明　(1) $1 \Rightarrow 5$：

$$(aH)(bH) = a(Hb)H = a(b)HH = abH$$

(2) $5 \Rightarrow 4$：设 $gHg^{-1}H = xH$, 则 $e = geg^{-1}e \in xH$, 所以 $xH = H$. 当 $h \in H$ 时

$$ghg^{-1} = ghg^{-1}e \in gHg^{-1}H = H$$

(3) $4 \Rightarrow 3$：任给 $g \in G$, 可得

$$gHg^{-1} \subseteq H \tag{1.1}$$
$$g^{-1}H(g^{-1})^{-1} \subseteq H \tag{1.2}$$

注意(1.2)即为 $g^{-1}Hg \subseteq H$, 即可得 $H \subseteq gHg^{-1}$. 由(1.1), (1.2)可知 $gHg^{-1} = H$.

(4) $3 \Rightarrow 2$

$$gHg^{-1} = H \Rightarrow gH = Hg$$

(5) $2 \Rightarrow 1$：设 $gH = Hx$, 则 $g \in gH = Hx$, 从而 $Hx = Hg$, 即 $gH = Hg$. □

性质1.5.1

(1) 对于群 G, 有 $G \trianglelefteq G, \{e\} \trianglelefteq G$ [1], 其中 G 为 G 最大的正规子群, $\{e\}$ 为 G 中最小的正规子群.

(2) G为 Abel 群时, $H \leqslant G \Rightarrow H \trianglelefteq G$.

(3) 如果 $H \trianglelefteq G, K \leqslant G$, 则 $HK = KH \leqslant G$ [2].

(4) $H \leqslant K \leqslant G, H \trianglelefteq G \Rightarrow H \trianglelefteq K$ [3].

(5) 如果诸 $H_i\,(i \in I)$ 为 G 的正规子群, 则 $H = \bigcap_{i\in I} H_i \trianglelefteq G$ [4].

例1.5.1

$SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$, 因为 $P \in GL_n(\mathbb{R}), A \in SL_n(\mathbb{R})$, 又 $|PAP^{-1}| = 1$, 所以 $PAP^{-1} \in SL_n(\mathbb{R})$.

定理1.5.2

设 $H \leqslant G$, 则

(1)
$$H_G = \bigcap_{g\in G} gHg^{-1}$$
是被包含在 H 中的 G 的最大正规子群, H_G 叫 H 在 G 中**正规核**.

(2)
$$N_G(H) = \{g \in G : gH = Hg\}$$
是使 H 在其中正规的 G 的最大子群, $N_G(H)$ 叫做 H 的**正规化子**.

证明 (1) 由于 $gHg^{-1} \leqslant G \quad eHe^{-1} = H$, 所以
$$H_G = \bigcap_{g\in G} gHg^{-1} \leqslant G \quad H_G \subseteq H$$

[1] $\forall g,h \in G \quad ghg^{-1} \in G$. $\forall g \in G \quad geg^{-1} = e \in \{e\}$

[2]
$$HK = \bigcup_{k\in K} Hk = \bigcup_{k\in K} kH = KH$$
由定理1.3.3(19页)知道, $HK \leqslant G$.

[3] $k \in K, h \in H$ 时, 注意到 $k \in G, H \trianglelefteq G$, 可知 $khk^{-1} \in H$.

[4] 任给 $g \in G, h \in H$, 对 $\forall i \in I, h \in H_i$, 而 $H_i \trianglelefteq G$, 所以 $ghg^{-1} \in H_i$, 故
$$ghg^{-1} \in \bigcap_{i\in I} H_i$$
即 $H \trianglelefteq G$.

任取 $g\in G, x\in H_G$, 要证 $H_G\trianglelefteq G$, 即证 $gxg^{-1}\in H_G$, 即对 $\forall a\in G$ 时, 要证 $gxg^{-1}\in aHa^{-1}$, 即 $a^{-1}gHg^{-1}a\in H$. 因为要证 $(a^{-1}g)x(a^{-1}g)^{-1}\in H$, 只需证 $x\in g^{-1}aH(g^{-1}a)^{-1}$ 即可.
注意到

$$x\in\bigcap_{y\in G}yHy^{-1}\quad\{g^{-1}a:\forall a\in G\}=G$$

所以 $x\in g^{-1}aH(g^{-1}a)^{-1}$ 对任意 $a\in G$ 均成立, 即 $H_G\trianglelefteq G$.
(2) 因为 $h\in H$ 时, $hH=H=Hh$, 所以 $h\in N_G(H)$, 即

$$H\subseteq N_G(H)=\{g\in G:gH=Hg\}$$

注意到 $gH=Hg\Rightarrow Hg^{-1}=g^{-1}H\Rightarrow g^{-1}\in N_G(H)$. 如果 $a,b\in N_G(H)$, 则

$$abH=a(bH)=a(Hb)=aHb=Hab$$

所以 $ab\in N_G(H)$, 从而 $N_G(H)\leqslant G$.
因为当 $g\in N_G(H)$ 时, $gH=Hg$, 故 $H\trianglelefteq N_G(H)$.
假如 $H\trianglelefteq K\leqslant G$, 则 $k\in K$ 时, $kH=Hk$, 从而 $k\in N_G(H)$, 即 $K\leqslant N_G(H)$. □

定理1.5.3

设 $H\trianglelefteq G$, 则

$$G/H=\{\bar a=aH:a\in G\}$$

按陪集乘法构成群.（它叫 G 按正规子群 H 做成的**商群**.）

证明　$aHbH=abHH=abH\Rightarrow\bar a\bar b=\overline{ab}$, 即 G/H 对乘法封闭.
$(\bar a\bar b)\bar c=\bar a\bar b\bar c=\bar a(\bar b\bar c)$
$\bar e\bar a=\bar a=\bar a\bar e\Rightarrow\bar e=eH=H$ 为单位元.
$\overline{a^{-1}}\bar a=\overline{a^{-1}a}=\bar e\quad\bar a^{-1}=\overline{a^{-1}}$, 所以 $\bar a$ 有乘法逆元 $\overline{a^{-1}}$.
因此 G/H 为群. □

例1.5.2

$\mathbb{Z}$ 按加法构成Abel群, $m\mathbb{Z}=\{mx:x\in\mathbb{Z}\}\trianglelefteq\mathbb{Z}$.
$\bar a=a+m\mathbb{Z}=\{a+mq:q\in\mathbb{Z}\}$ 是 a 模 m 的剩余类.
$\mathbb{Z}/m\mathbb{Z}=a\{\bar a=a+m\mathbb{Z}:a\in\mathbb{Z}\}$ 按剩余类加法构成群.

作业:

(1) 设 G 为群, 则 G 的中心

$$Z_G=\{x\in G:\forall g\in G\,(gx=xg)\}\trianglelefteq G$$

(2) 设 $H\trianglelefteq G, K\leqslant G$, 则 $H\trianglelefteq HK$, $H\cap K\trianglelefteq K$.

1.6　群的同态与同构

定义1.6.1

设 σ 是群 G 到群 $\bar{G}$ 的映射, 如果 $\forall a,b\in G\,(\sigma(ab)=\sigma(a)\sigma(b))$, 则说 σ 是群 G 到群 $\bar{G}$ 的一个**同态**.
$\mathrm{Im}(\sigma)=\{\sigma(a):a\in G\}=\sigma(G)$ 叫**同态象**. $\ker\sigma=\{a\in G:\sigma(a)=\bar{e}\}$ 叫**同态核**.
如果 σ 既是同态又是单射, 称 σ 为**单同态**；如果 σ 既是同态又是满射, 称 σ 为**满同态**. 如果 σ既是同态又是双射, 称 σ 为 G 到 $\overline{G}$ 的一个**同构**（同构映射）, 此时说群 G 同构于 $\overline{G}$, 记为 $G\cong\overline{G}$.

定理1.6.1

设 σ 是群 G 到 $\overline{G}$ 同态, 则

(1)　$\sigma(e)=\bar{e}$, $a\in G$ 时, $\sigma(a^{-1})=\sigma(a)^{-1}$

(2)　(同态基本定理) $\ker\sigma\trianglelefteq G$　$\mathrm{Im}(\sigma)\leqslant\overline{G}$, 而且 $G/\ker\sigma\cong\mathrm{Im}(\sigma)$.

证明　(1) $\bar{e}\sigma(e)=\sigma(e)=\sigma(ee)=\sigma(e)\sigma(e)$, 使用 $\bar{G}$ 中消去律有 $\sigma(e)=\bar{e}$.
$a\in G$ 时, $\sigma(a)\sigma(a^{-1})=\sigma(aa^{-1})=\sigma(e)=\bar{e}$, 所以 $\sigma(a^{-1})=\sigma(a)^{-1}$

(2) $e\in\ker\sigma$, 所以 $\ker\sigma$ 非空.如果 $a,b\in\ker\sigma$, 则
$\sigma(ab^{-1})=\sigma(a)\sigma(b^{-1})=\bar{e}\bar{e}^{-1}=\bar{e}$, 故 $ab^{-1}\in\ker\sigma$. （对右除法封闭）
$\bar{e}=\sigma(e)\in\mathrm{Im}\sigma$ 如果 $a,b\in G$, 则 $\sigma(a)\sigma(b)^{-1}=\sigma(a)\sigma(b^{-1})=\sigma(ab^{-1})\in\mathrm{Im}\sigma$.（对右除法封闭）
让 $H=\ker\sigma$, 设 $g\in G,h\in H$ 时,

$$\sigma(ghg^{-1})=\sigma(g)\sigma(h)\sigma(g)^{-1}=\sigma(g)\sigma(g)^{-1}=\bar{e}$$

故 $ghg^{-1}\in H$, 所以 $H\trianglelefteq G$.
做 $\bar{\sigma}:aH\in G/H\to\sigma(a)\in\mathrm{Im}\sigma$, 注意：

$$\begin{aligned}aH=bH\Leftrightarrow H=a^{-1}bH&\Leftrightarrow a^{-1}b\in H\\&\Leftrightarrow\sigma(a^{-1}b)=\bar{e}\Leftrightarrow\sigma(a^{-1})\sigma(b)=\bar{e}\\&\Leftrightarrow\sigma(a)=\sigma(b)\end{aligned}$$

所以 $\bar{\sigma}$ 为单射, 又 $\bar{\sigma}$ 显然为满射, 故 $\bar{\sigma}$ 为双射.同时

$$\bar{\sigma}(aHbH)=\bar{\sigma}(abH)=\sigma(ab)=\sigma(a)\sigma(b)=\bar{\sigma}(aH)\bar{\sigma}(bH)$$

故 $\bar{\sigma}$ 为同态, 所以 $\bar{\sigma}$ 为同构映射, 即 $G/\ker\sigma\cong\mathrm{Im}(\sigma)$. □

例1.6.1

(1) $x \mapsto |x|$ 是乘法群 $\mathbb{R}^* = \mathbb{R}/\{0\}$ 到 $\mathbb{R}^+ = \{x为正实数\}$ 的满同态.

$$\ker\sigma = \{1, -1\} \quad \mathbb{R}^*/\{\pm 1\} \cong \mathbb{R}^+$$

(2)定义 $\sigma : GL_n(\mathbb{R}) \to \mathbb{R}^* \quad \sigma(A) = \det A \in \mathbb{R}^*$, 则 σ 为同态, 且为满同态.

$$\ker\sigma = \{A \in GL_n(\mathbb{R}) : |A| = 1\} = SL_n(\mathbb{R})$$

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong \mathbb{R}^*$$

(3) $\sigma : x \mapsto \ln x \in \mathbb{R}$ 是乘法群 $\mathbb{R}^+$ 到加法群 $\mathbb{R}$ 的同态.

$$\sigma(xy) = \sigma(x) + \sigma(y)$$

σ 既是满射又是单射, 从而为同构, $\mathbb{R}^+ \cong \mathbb{R}$

(4) $H \trianglelefteq G$ 时, $\sigma : a \mapsto \bar{a} = aH \in G/H$ 是 G 到 G/H 的满同态.

$$\sigma(ab) = \bar{ab} = \bar{a}\bar{b} = \sigma(a)\sigma(b)$$

$$\ker\sigma = \{a \in G : \bar{a} = \bar{e}即aH = H即a \in H\} = H$$

例1.6.2

$D = \{\pm i, \pm i, \pm j, \pm k\}$ 为Hamilton群, 注意 D 不是Abel群.让 $K = \{e, a, b, c\}$ 为Klein四元群.定义 $\sigma : D \to K$ 如下：

$$\sigma\{\pm 1\} = e \quad \sigma\{\pm i\} = a \quad \sigma\{\pm j\} = b \quad \sigma\{\pm k\} = c$$

则 σ 为满同态, 且

$$\ker\sigma = \{\pm 1\} \quad D/\{\pm 1\} \cong K$$

自学代数学引论的自同构 P_{71}

作业：

(1) 任何无穷循环群同构整数加群 $\mathbb{Z}$；任何 n 阶循环群同构于 $\mathbb{Z}\backslash n\mathbb{Z}$.

第 2 章　群论(下)

2.1　群在集合上的作用

定义2.1.1

设 G 为群, X 为非空集合, 如果对每个 $g \in G$ 及 $x \in X$ 有个 X 中元 $g \circ x$ [1]与之对应, 而且 $\circ$ 满足下列性质：

(1)　$e \circ x = x$

(2)　$(g_1 g_2) \circ x = g_1 \circ (g_2 \circ x)$

则说群 G （左）**作用**在集合 X 上.

注：“右作用”可转化为“左作用”.设群 G 右作用在非空集 X 上, 即 $xe = x \quad x(g_1 g_2) = (x g_1) g_2$, 定义 $g \circ x = x g^{-1}$, 则

$$e \circ x = xe = x \quad (g_1 g_2) \circ x = g_1 \circ (g_2 \circ x)$$

定理2.1.1

设 G 为群, X 为非空集, 则

$$\{G在X上的作用\} \approx \{群G到S(X)的同态\} = \mathrm{Hom}(G, S(X))$$

证明　(1) 任给 $\sigma \in \mathrm{Hom}(G, S(X))$, 对 $g \in G$ 及 $x \in X$, 定义

$$g \circ_\sigma x = \sigma(g)(x)$$

[1]不在引起误会的情况 $g \circ x$ 下简记为 gx.

注意 $e\circ_\sigma x=\sigma(e)(x)=I(x)=x$, 且对 $g_1,g_2\in G, x\in X$ 时, 有:

$$\begin{aligned}(g_1g_2)\circ_\sigma x&=\sigma(g_1g_2)(x)\\&=\sigma(g_1)\sigma(g_2)(x)\\&=\sigma(g_1)(\sigma(g_2)(x))\\&=g_1\circ_\sigma(g_2\circ_\sigma x)\end{aligned}$$

因此 $\circ_\sigma$ 是 G 在 X 上的作用, 如果 $\sigma,\tau\in\mathrm{Hom}(G,S(x))$ 且 $\sigma\neq\tau$, 则有 $g\in G$ 使 $\sigma(g)\neq\tau(g)$, 又有 $x\in X$ 使 $\sigma(g)(x)\neq\tau(g)(x)$, 即 $g\circ_\sigma x\neq g\circ_\tau x$, 故 $\circ_\sigma\neq\circ_\tau$ [2].

(2) 设群 G 作用于 X, 对 $g\in G$, $\sigma_g: x\mapsto g\circ x$ 属于 $S(X)$, 因为

$$g\circ x=g\circ y\Rightarrow g^{-1}\circ(g\circ x)=g^{-1}\circ(g\circ y)\Rightarrow e\circ x=e\circ y\Rightarrow x=y$$

即 σ_g 为单射. 又 $y\in X$ 时, 让 $x=g^{-1}y$, 则 $g\circ x=y$, 所以 σ_g 为满射.综上, 可知 $\sigma_g\in S(X)$

下证 $\sigma: g\mapsto\sigma_g\in S(X)$ 是 G 到 $S(X)$ 的同态, 即要证 $\sigma(g_1g_2)=\sigma(g_1)\sigma(g_2)$, 即 $\sigma_{g_1g_2}=\sigma_{g_1}\sigma_{g_2}$, 又

$$\sigma_{g_1}\sigma_{g_2}(x)=\sigma_{g_1}(g_2\circ x)=g_1\circ(g_2\circ x)=(g_1g_2)\circ x=\sigma_{g_1g_2}(x)$$

故 σ 是 G 到 $S(X)$ 的同态.注意到:

$$g\circ_\sigma x=\sigma(g)(x)=\sigma_g(x)=g\circ x$$

故 $\circ$ 即为 $\circ_\sigma$, 这里 $\sigma\in\mathrm{Hom}(G,S(X))$ [3]. □

定义2.1.2

设群 G 作用于非空集 X 上, X 上关系 $\sim_G$ 如下:

$$x\sim_G y\Leftrightarrow\exists g\in G\,(g\circ x=y)$$

$\mathrm{O}_x=\{y\in X: x\sim_G y\}$ 叫作 x **所在轨道**.
$\mathrm{Stab}(x)=\{g\in G: g\circ x=x\}$ 叫作 x **的稳定化子**.
$\ker(X)=\bigcap_{x\in X}\mathrm{Stab}(x)=\{g\in G:\forall x\in X\,(g\circ x=x)\}$ 叫**作用核**.

[2] 这是为了证明映射 $f:\mathrm{Hom}(G,S(X))\to\{G\text{在}X\text{上的作用}\}\quad f(\sigma)=\circ_\sigma$ 为单射.
[3] 这是为了证明映射 $f:\mathrm{Hom}(G,S(X))\to\{G\text{在}X\text{上的作用}\}\quad f(\sigma)=\circ_\sigma$ 为满射.

定理2.1.2

设群 G 作用于非空集 X 上, 则

(1) $\sim_G$ 为 X 上等价关系, X 是若干个不相交轨道的并.

(2) $x \in X$ 时, $\mathrm{Stab}_G(x) \leqslant G$, 且 $[G : \mathrm{Stab}_G(x)] = |\mathrm{O}_x|$, 即元素稳定化子的指标数等于所在轨道之势.

(3) $\ker(X) \trianglelefteq G$, 且 $G/\ker(X)$ 可嵌入到 $S(X)$ 中, 即同构与 $S(X)$ 的一个子群.

证明 (1) 因为 $e \circ x = x$, 所以 $x \sim_G x$. 设 $x \sim_G y$, 即有 $g \in G$ 使 $g \circ x = y$, 则 $g^{-1} \circ y = g^{-1} \circ (g \circ x) = x$, 故 $y \sim_G x$. 设 $x \sim_G y, y \sim_G z$, 即有 $g_1, g_2 \in G$ 使 $g_1 \circ x = y$, $g_2 \circ y = z$, 于是 $z = g_2 \circ (g_1 \circ x) = (g_2 g_1) \circ x$, 所以 $x \sim_G z$. 故 $\sim_G$ 满足自反性, 对称性和传递性, 即为 X上的等价关系, O_x 为 x 所在的等价类.

(2) 因为 $e \circ x = x$, 所以 $e \in \mathrm{Stab}(x)$.
设 $g_1, g_2 \in \mathrm{Stab}(x)$, 则

$$g_1 g_2 \circ x = g_1 \circ (g_2 \circ x) = g_1 \circ x = x$$

故 $g_1 g_2 \in \mathrm{Stab}(x)$.
$g \in \mathrm{Stab}(x)$ 时, 因为 $g \circ x = x$, 所以

$$g^{-1} \circ (x) = g^{-1} \circ (g \circ x) = e \circ x = x$$

即 $g^{-1} \in \mathrm{Stab}(x)$.综上可得, $\mathrm{Stab}_G(x) \leqslant G$.
让 $H_x = \mathrm{Stab}(x)$, G/H_x 表示集合 $\{gH_x : g \in G\}$. 定义

$$f : gH_x \mapsto g \circ x \in \mathrm{O}_x$$

注意到

$$\begin{aligned} g_1 H_x = g_2 H_x &\Leftrightarrow H_x = g_1^{-1} g_2 H_x \\ &\Leftrightarrow g_1^{-1} g_2 \in H_x \\ &\Leftrightarrow g_1^{-1} g_2 \circ x = x \\ &\Leftrightarrow g_1 \circ x = g_2 \circ x \end{aligned}$$

故 f 定义合理且为单射.又 f 显然为满射.所以 $G/H_x \overset{f}{\approx} \mathrm{O}_x$. 即

$$|\mathrm{O}_x| = |\{gH_x : g \in G\}| = [G : \mathrm{Stab}_G(x)]$$

(3) 注意到 $\ker(X)=\bigcap_{x\in X}\mathrm{Stab}(x)$, 即 $\ker(X)$ 为子群之交, 所以 $\ker(X)\leqslant G$. 让 $H=\ker(X)$, 则任给 $g\in G$ 及 $h\in H$, 当 $x\in X$ 时,

$$ghg^{-1}\circ x=g\circ\left(h\circ\left(g^{-1}\circ x\right)\right)=g\circ(g^{-1}\circ x)=x$$

故 $ghg^{-1}\in H$. 即 $\ker(X)\trianglelefteq G$.
注意由定理2.1.1(35页)的证明中知: $g\in G$ 时, $\sigma_g:x\mapsto g\circ x$ 属于 $S(X)$. $\sigma:g\mapsto\sigma_g$ 属于 $\mathrm{Hom}(G,S(X))$. 因为

$$\begin{aligned}\ker\sigma&=\{g\in G:\sigma_g\text{为 } S(X)\text{ 单位元 } I\}\\&=\{g\in G:\forall x\in X\,(\sigma_g(x)=x)\}\\&=\{g\in G:\forall x\in X\,(g\circ x=x)\}\\&=\ker(X)\trianglelefteq G\end{aligned}$$

所以由同态基本定理(33页的定理1.6.1(3)) 知;

$$G/\ker X=G/\ker\sigma\cong\mathrm{Im}\sigma\leqslant S(X)$$ □

例2.1.1

设 $H\leqslant G$, 考虑 H 在 $X=G$ 上的作用; $h\in H,x\in X$ 时, 让 $h\circ x=hx$. 可知 $e\circ x=x$, $h_1,h_2\in H$ 时, $h_1h_2\circ x=h_1\circ(h_2\circ x)$. 故可得:
x 所在轨道 $\mathrm{O}_x=\{h\circ x:h\in H\}=Hx$, 且 X 是不相交轨道的并等价于 G 可按 H 进行右陪集分解.
x 的稳定化子 $\mathrm{Stab}(x)=\{e\}$, $[H:\mathrm{Stab}(x)]=[H:\{e\}]=|H|=|\mathrm{O}_x|=|H_x|$, 注意到 $\ker(X)=\{e\}$, 所以由定理2.1.2（37页）知, $H\cong H/\{e\}=H/\ker(X)$ 可嵌入到 $S(G)$ 中, 特别地, G 同构于 $S(G)$ 中.由此可以得到Cayley定理.

Cayley定理. *任何一个群同构于某个置换群.*

例2.1.2

设 G 为群, 让 $X=G$, 对 $g\in G,x\in X$, 定义; $g\circ x=gxg^{-1}\in G=X$ （共轭作用）.可知:

$$e\circ x=x\quad g_1g_2\circ x=(g_1g_2)x(g_1g_2)^{-1}=g_1\circ(g_2\circ x)$$

故 G 作用于 $X=G$ 上, gxg^{-1} 叫 x 的共轭元.
轨道 $C(x)=\{gxg^{-1}:g\in G\}$ 叫 x 所在的共轭类, 则 $G=X$ 是不相交共轭类的并.
$\mathrm{Stab}(x)=\{g\in G:gxg^{-1}=x\}=C_G(x)\leqslant G$. $C_G(x)$ 为中心化子.
$\ker(X)=\{g\in G:\forall x\in G\,(gx=xg)\}=\bigcap_{x\in G}C_G(x)=Z(G)\trianglelefteq G$.
$[G:C_G(x)]=|C(x)|$

例2.1.3

设 G 为群, $H\leqslant G$, $X=G/H=\{xH:x\in G\}$. 对 $g\in G$ 及 $xH\in X$, 定义

$$g\circ xH=\{g\circ y:y\in xH\}=gxH\in X$$

则

$$e \circ xH = xH \quad g_1g_2 \circ xH = g_1 \circ (g_2 \circ x)$$

注意到 $xH \sim yH$ 是指有 $g \in G$ 使 $g \circ x = yH$, 取 $g = yx^{-1}$ 即可知 $xH \sim yH$.
故 X 中任两个元素等价, 即 X 只有一个轨道: $\mathrm{O}_{xH} = X = G/H$.
此外

$$\begin{aligned}\mathrm{Stab}(xH) &= \{g \in G : g \circ xH = xH\} = \{g \in G : x^{-1}gxH = H\} \\ &= \{g \in G : x^{-1}gx \in H\} = \{g \in G : g \in xHx^{-1}\} \\ &= xHx^{-1} \leqslant G\end{aligned}$$

则由定理2.1.2(2)（37页）得 $\underline{[G : xHx^{-1}] = [G : \mathrm{Stab}(x)] = |\mathrm{O}_{xH}| = [G : H]}$.
因为 $\ker(X) = \bigcap_{x\in G} \mathrm{Stab}(xH) = \bigcap_{x\in G} xHx^{-1} = H_G \trianglelefteq G$ [4], 则可知 G/H_G 同构于 $S(X)$ 的一个子群.
设 $[G : H] < \infty$, 则 $|G/H_G| \mid |S(G/H)|$, 又因为 $H_G \trianglelefteq H \leqslant G$, 所以
$[G : H][H : H_G] = [G : H_G]$, 注意到 $|S(G/H)| = [G : H]!$, 所以
$|H/H_G| \mid ([G : H] - 1)!$.
特别地, 设 G 为有限群, $|G| > 1$, 且 $[G : H]$ 是 $|G|$ 的最小素因子 p, 则
$|H/H_G| \mid (p - 1)!$.
又因为 $((p - 1)!, |G|) = 1$, 于是 $(|H/H_G|, |G|) = 1$, 而

$$|H/H_G| \mid |H| \quad |H| \mid |G|$$

所以 $|H/H_G| = 1$, 即 $H = H_G \trianglelefteq G$.

例2.1.4

设 $H \leqslant G$, 让 $æ = \{aHa^{-1} : a \in G\}$, 对 $g \in G$ 及 $aHa^{-1} \in æ$, 定义

$$g \circ aHa^{-1} = \{gxg^{-1} : x \in aHa^{-1}\} = g(aHa^{-1})g^{-1} = (ga)H(ga)^{-1} \in æ$$

可知 $e \circ aHa^{-1} = aHa^{-1}$,

$$g_1g_2 \circ aHa^{-1} = g_1g_2aHa^{-1}g_2^{-1}g_1^{-1} = g_1 \circ (g_2 \circ aHa^{-1})$$

故 G 作用于 $æ$ 上.
对 $a, b \in G$, 有 $g = ba^{-1} \in G$ 使 $g \circ aHa^{-1} = bHb^{-1}$.故 $æ$ 只有一个轨道, 即
$\mathrm{O}_H = æ$.又$\mathrm{Stab}(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$[5], 所以

$$[G : N_G(H)] = |\mathrm{O}_H| = |æ|$$

定义2.1.3

设群 G 作用在 X 上, 对于 $g \in G$, 让 $\mathrm{Fix}(g) = \{x \in X : g \circ x = x\} \subseteq X$, 称 $\mathrm{Fix}(g)$ 为 g 的**不动点**.
让 $\mathrm{Fix}(G) = \bigcap_{g\in G} \mathrm{Fix}(g) = \{x \in X : \forall g \in G\,(g \circ x = x)\}$, 称为**不动点**.

[4] H_G 参照31页的定理1.5.2
[5] $N_G(H)$ 参照31页的定理1.5.2

定理2.1.3

设有限群 G 作用于有限非空集 X 共产生 N 个不同的轨道, 则

$$N = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|$$

证明　设这 N 个轨道为 $\mathrm{O}_{x_1},\mathrm{O}_{x_2}\cdots,\mathrm{O}_{x_N}$ 让 $S=\{\langle g,x\rangle\in G\times X : g\circ x=x\}$, 则可知

$$|S|=\sum_{x\in X}|\mathrm{Stab}(x)|=\sum_{g\in G}|\mathrm{Fix}(g)|$$ [6]

则利用定理2.1.2(2)（37页）可知,

$$|S|=\sum_{x\in X}\frac{|G|}{|\mathrm{O}_x|}=\sum_{i=1}^{N}\sum_{x\in \mathrm{O}_{x_i}}\frac{G}{|\mathrm{O}_{x_i}|}=N|G|$$

即证得结论. □

定理2.1.4

设有限群 G 作用于有限非空集 X 上, 则 X 中非不动点的个数可以表示成 $|G|$ 的一些大于 1 的因子（可重复）和.

证明　对于 $x\in X$,

$$|\mathrm{O}_x|=1\Leftrightarrow \forall g\in G(g\circ x=x)\Leftrightarrow x\text{为不动点}$$

故设至少有两个元素的轨道为 $\mathrm{O}_1,\mathrm{O}_2,\cdots,\mathrm{O}_k$, 并且 $x_i\in \mathrm{O}_i$, 则

$$X=(\bigcup_{x\in\mathrm{Fix}(G)}\{x\})\cup \mathrm{O}_1\cup\cdots\cup \mathrm{O}_k$$

于是

$$|X|=|\mathrm{Fix}(G)|+\sum_{i=1}^{k}|\mathrm{O}_i|$$

注意到 $|\mathrm{O}_i|=[G:\mathrm{Stab}(x_i)]>1\quad [G:\mathrm{Stab}(x_i)]\mid |G|$, 定理得证. □

作业:

(1) 代数学引论 P_{98} 的第30题, 第46题, 第47题

(2) 设群 G 作用于 X 上, $g\in G, x\in X$ 时, $\mathrm{Stab}(g\circ x)=g\mathrm{Stab}(x)g^{-1}$.

(3) 证明定理2.1.3(40页)

[6]这就像统计一个方阵人数时, 一个按行统计, 一个按列统计.

2.2　群作用在 p 群上应用

定义2.2.1

设 p 为素数, 对于 $n=0,1,2,\cdots,p^n$ 阶群叫 p 群.

定理2.2.1

设 p 群 G 作用于有限非空集 X 上, 则

$$|X| \equiv |\mathrm{Fix}(G)| \pmod p$$

特别地, $p \nmid |X|$ 时必有不动点.

证明　设 $|G|=p^n$, 则 $|G|$ 大于1的因子只有 $p,p^2,\cdots,p^n$, 它们均为 p 的倍数.应用定理2.1.4(40页)可知定理成立. □

定理2.2.2

设 G 为 p^n 阶群, 这里 p 为素数, $n\in\mathbb{Z}^+$, 则 G 的中心 $Z(G)$ 必含非单位元.

证明　考虑群 G 共轭作用于 $X=G$ 上, 即 $g\circ x=gxg^{-1}$. 因为

$$\mathrm{Fix}(g) = \{x\in X : gxg^{-1}=x\} = C_G(g)$$
$$\mathrm{Fix}(G) = \bigcap_{g\in G} \mathrm{Fix}(g) = Z(G)$$

由定理2.2.1知 $|X|\equiv \mathrm{Fix}(G) \pmod p$, 而 $|X|=|G|=p^n$, 所以 $p \,\big|\, |Z(G)|$. 又因为 $e\in Z(G)$, 所以 $|Z(G)|\geq p>1$. □

推论2.2.1

设 p 为素数, 则 p^2 阶群 G 必为 Abel 群.

证明　依定理2.2.2, $|Z(G)|>1$, 而 $|Z(G)|\mid|G|$, 故 $Z(G)=p$或p^2. 因为 $Z(G)\trianglelefteq G$, 所以 $G/Z(G)=\{\bar{x}=xZ(G):x\in G\}$ 为群.注意到

$$|G/Z(G)|=\frac{|G|}{|Z(G)|}=1\text{或}p$$

(1) $|Z(G)|=p^2$ 时, 由 $Z(G)$ 的定义知, $|G|$ 显然为Abel群.
(2) $|Z(G)|=p$ 时, $G/Z(G)$ 为素数阶群, 而素数阶群为循环群[1], 故 $G/Z(G)$ 是循环群. 设 $\bar{g}=gZ(G)$ 为 $G/Z(G)$ 的生成元, 对于 $x\in G$, 有 $m\in\mathbb{Z}$ 使 $\bar{x}=\bar{g}^m=\overline{g^m}$, 即 $x\in\overline{g^m}=g^mZ(G)$, 于是有 $w\in Z(G)$ 使 $x=g^mw$, 同理对于 $y\in G$, 也有 $n\in\mathbb{Z}$ 及 $z\in Z(G)$ 使 $y=g^nz$. 则

$$xy=(g^mw)(g^nz)=g^m(g^nw)z=g^{m+n}zw=g^n(g^mz)w=g^nzg^mw=yx \quad \square$$

定义2.2.2

如果 $|G|>1$, 且 G 的正规子群只有 $\{e\}$ 与 G, 则说 G 为**单群**.

作业:

(1) 证明：Abel单群只有素数阶循环群.

[1] 参照29页的作业3

2.3　Sylow 定理

定义2.3.1

如果 $p^\alpha \mid n$, 但是 $p^{\alpha+1} \nmid n$, 记为 $p^\alpha \parallel n$, $\mathrm{ord}_p(n) = \alpha$, 其中 $\mathrm{ord}_p(n)$ 称为 n **在 p 处的阶**[1].
例如: $\mathrm{ord}_2(72) = 3, \mathrm{ord}_3(72) = 3, \mathrm{ord}_5(72) = 0 \quad \mathrm{ord}_p(mn) = \mathrm{ord}_p(m) + \mathrm{ord}_p(n)$

定义2.3.2

设 G 为群, $|G| = n$, 且 $p \parallel n$, 则称 G 的 p^α 阶子群 H 为 G 的 Sylow p-子群, 且写 $|G| = p^\alpha m\,(p \nmid m)$, 则 $[G:H] = m \not\equiv 0 \pmod p$.

定理2.3.1 (Sylow 第一定理)

设 G 为有限群, p 为素数, $a = \mathrm{ord}_p(|G|)$, 则 G 必有 p^a 阶子群（即 Sylow p-子群）.

证明　设 $|G| = p^a m\,(p \nmid m)$, 令 $n = \{U \subseteq G : |U| = p^a\}$, 则

$$\begin{aligned}|n| &= \binom{p^a m}{p^a} \\ &= \frac{p^a m(p^a m - 1)\cdots(p^a m - p^a + 1)}{1 \times 2 \times \cdots \times (p^a - 1) \times (p^a)} \\ &= m \prod_{k=1}^{p^a - 1} \frac{p^a m - k}{k}\end{aligned}$$

$1 \leqslant k < p^a$ 时, 如果 $p^b \parallel k$, 则 $b < a$, 因为 $p^{b+1} \mid p^a$, 而 $p^{b+1} \nmid k$, 所以 $p^b \parallel p^a m - k$. 故 $|n|$ 可写成 $\frac{s}{t}\,(p \nmid s, p \nmid t)$, 又

$$t|n| = s \not\equiv 0 \pmod p$$

故 $p \nmid |n|$.
对 $g \in G, U \in n$, 让

$$g \circ U = gU = \{gu : u \in U\} \in n$$

[1] 若未特别指出, 则本节中 p 均表示素数.

显然 $e\circ U=U \quad g_1g_2\circ U=g_1\circ(g_2\circ U)$, 故 G 作用在 n 上.
设 n 上共有 k 个不同的轨道 $\mathrm{O}_1\cdots\mathrm{O}_k$, 则

$$|\bigcup_{i=1}^{k}\mathrm{O}_i|=|n|\not\equiv 0 \pmod p$$

故有 i 使 $|\mathrm{O}_i|\not\equiv 0 \pmod p$. 任取 $U\in\mathrm{O}_i$

$$H=\mathrm{Stab}(U)\leqslant G \quad [G:H]=|\mathrm{O}_i|\not\equiv 0 \pmod p$$

而 $p^a\parallel |G|$, 故 $p^a\mid |H|$, 即 $|H|\geqslant p^a$.
任取 $x\in U$, $h\in H=\mathrm{Stab}(U)$, 有

$$hU=U\Rightarrow hx\in hU=U\Rightarrow Hx\subseteq U$$

于是 $|H|=|Hx|\leqslant|U|=p^a$, 则 $|H|=p^a$. □

定理2.3.2 (Sylow 第二定理)

设 H 为有限群 G 的任一个 Sylow p-子群, 则

$$\{G\text{的 Sylow } p\text{-子群}\}=\{gHg^{-1}:g\in G\}$$

任给 G 的 p-子群 K, 则必有 $g\in G$ 使 $K\subseteq gHg^{-1}$.

证明　设 K 为 G 的 p-子群, 让 $G/H=\{xH:x\in G\}$, 对 $k\in K$ 及 $xH\in G/H$

$$k\circ xH=\{ky:y\in xH\}=kxH\in G/H$$

显然可得 $e\circ xH=xH \quad k_1k_2\circ xH=k_1\circ(k_2\circ xH)$, 故 p-子群 K 作用在 $X=G/H$ 上.又

$$|G/H|=[G:H]=\frac{|G|}{|H|}=\frac{p^am}{p^a}=m\not\equiv 0 \pmod p$$

由于 $p\nmid|X|$, 依定理2.2.1（41页）, $X=G/H$ 中必有不动点 gH.
$k\in K$ 时,

$$k\circ gH=gH\Rightarrow g^{-1}kgH=H\Rightarrow g^{-1}kg\in H\Rightarrow k\in gHg^{-1}$$

故 $k\subseteq gHg^{-1}$.
对任何 $g\in G$, $|gHg^{-1}|=|H|=p^a$, 所以 gHg^{-1} 也是 G 的 Sylow p-子群.
如果 K 是 G 的 Sylow p-子群, 由上可知存在$g\in G$, 使 $K\subseteq gHg^{-1}$, 而 $|K|=p^a \quad |gHg^{-1}|=|H|=p^a$, 故 $K=gHg^{-1}$. □

推论2.3.1

设 P 为有限群 G 的 Sylow p-子群, 则

$$P \trianglelefteq G \Leftrightarrow P \text{ 是 } G \text{ 唯一的 Sylow } p\text{-子群}$$

例2.3.1

设 H 是群 G 的有限正规子群, P 为 H 的 Sylow p-子群, 则

$$|G| = HN_G(P)$$

证明　任给 $g \in G$, 则 $gPg^{-1} \leqslant gHg^{-1} = H$　$|gPg^{-1}| = |P|$, 故 gPg^{-1} 也是 H 的 Sylow p-子群.由 Sylow 第二定理（44页）知, 有 $h \in H$ 使 $gPg^{-1} = hPh^{-1}$, 于是

$$h^{-1}gP = Ph^{-1}g \Rightarrow h^{-1}g \in N_G(P)$$

所以 $g \in hN_G(P) \subseteq HN_G(P)$, 故 $G \leqslant HN_G(P)$, 注意 $HN_G(P) \leqslant G$, 则 $G = HN_G(P)$. □

例2.3.2

设 P 为有限群 G 的 Sylow p-子群, 如果 $N_G(P) \leqslant H \leqslant G$, 则 $N_G(H) = H$.

证明　因为 $P \trianglelefteq N_G(P) \leqslant H \leqslant G$, 所以 $[G:P] = [G:H][H:P]$, 又 $p \nmid [G:P]$, 从而 $p \nmid [H:P]$, 故 P 也为 H 的 Sylow p-子群.因为 $H \trianglelefteq k = N_G(H)$, 由例2.3.1知

$$K = HN_K(P) \subseteq HN_G(P) \subseteq HH = H$$

所以 $N_G(H) = H$. □

定理2.3.3 (Sylow 第三定理)

设 G 为群, $|G| = p^a m\,(p \nmid m)$, 让 n_p 表示 G 的 Sylow p-子群个数, 则对 G 的任一个 Sylow p-子群 H

(1)　$n_p = [G : N_G(H)]$

(2)　$n_p \mid m$, 且 $n_p \equiv 1 \pmod p$

证明 由 Sylow 第二定理(44页)知

$$n_p = |\{G\text{的 Sylow } p\text{-子群}\}| = |\{gHg^{-1} : g \in G\}| = [G : N_G(H)]$$ [2]

因为 $H \trianglelefteq N_G(H) \leqslant G$, 而 $[G:H] = [G:N_G(H)][N_G(H):H]$, 则

$$[G:N_G(H)] \mid [G:H] = \frac{|G|}{|H|} = m,\ n_p = [G:N_G(H)] \mid m$$

让 $æ = \{gHg^{-1} : g \in G\}$, 对 $h \in H$ 及 $gHg^{-1} \in æ$ 定义:

$$h \circ gHg^{-1} = hgHg^{-1}h^{-1} = (hg)H(hg)^{-1} \in æ$$

可验证 H 作用于 $æ$ 上.注意到

$$\begin{aligned}
gHg^{-1}\text{为不动点} &\Leftrightarrow \forall h \in H\,(hgHg^{-1}h^{-1} = gHg^{-1}) \\
&\Leftrightarrow \forall h \in H\,(g^{-1}hgH = Hg^{-1}hg) \\
&\Leftrightarrow \forall h \in H\,(g^{-1}hg \in N_G(H)) \\
&\Leftrightarrow g^{-1}Hg \leqslant N_G(H) \\
&\Leftrightarrow gHg^{-1}\text{为 } N_G(H)\text{的 Sylow } p\text{-子群}
\end{aligned}$$

由于 $H \leqslant N_G(H) \leqslant G$, 又 H 为 G 的 Sylow p-子群, 所以 H 也为 $N_G(H)$ 的 Sylow p-子群.而 $H \trianglelefteq N_G(H)$, 故由推论2.3.1（45页）知 H 为 $N_G(H)$ 的唯一的 Sylow p-子群. p 群 H 作用于 $æ$ 上, 由定理2.2.1（41页）知,

$$n_p = |æ| \equiv |\mathrm{Fix}(G)| \pmod p$$

□

例2.3.3

设 G 为 $p^\alpha q$ 阶群, 其中 p, q 为不同的素数, 且 $a > 0$, $q \not\equiv 1 \pmod p$, 则 G 必有正规的 Sylow p-子群, 从而 G 不是单群.

证明 由推论2.3.1（45页）知, 只要证 $n_p = 1$ 即可, 由 Sylow 第三定理（45页）知

$$n_p \mid q \quad n_p \equiv 1 \pmod p$$

由条件 $q \not\equiv 1 \pmod p$, 知 $n_p \neq q$, 从而 $n_p = 1$. □

例2.3.4

设 p, q 为不同素数, 且 $p \not\equiv 1 \pmod q$, $q \not\equiv 1 \pmod p$, 则 pq 阶群 G 必循环.

[2] 39页的例2.1.4

证明　由例2.3.3知 G 有正规的 Sylow p-子群 P, 也有正规的 Sylow q-子群 Q. 因为 $P\cap Q\leqslant P \quad P\cap Q\leqslant Q$, 所以

$$|P\cap Q|\,\big|\,|P| \qquad |P\cap Q|\,\big|\,|Q|$$

从而 $P\cap Q=\{e\}$.
注意到素数阶群必为循环群, 故有 p 阶元 x, 使 $P=\langle x\rangle$, q 阶元 y, 使 $Q=\langle y\rangle$.
因为 $P\trianglelefteq G$, 所以

$$(yx)^{-1}xy=x^{-1}y^{-1}xy=x^{-1}(y^{-1}xy)\in P$$

类似地因为 $Q\trianglelefteq G$, 所以

$$(yx)^{-1}xy=x^{-1}y^{-1}xy=(x^{-1}y^{-1}x)y\in Q$$

故 $(yx)^{-1}xy\in P\cap Q$, 从而 $(yx)^{-1}xy=e$, 即 $yx=xy$.
设 $o(xy)=n$, 则 $(xy)^n=e$, 因为 $yx=xy$, 所以 $x^ny^n=e$, 即
$x^n=y^{-n}\in P\cap Q=\{e\}$. 因此

$$p\,\big|\,n \quad q\,\big|\,n$$

从而 $o(xy)=pq$, 则 $G=\langle xy\rangle$. □

例2.3.5
设 G 为 p^2q 阶群, 其中 p,q 为不同的素数, 则 G 必有正规的 Sylow p-子群或正规的 Sylow q-子群, 从而 G 不是单群. [3]

证明　假设 n_q 大于1, 则依 Sylow 第三定理（45页）知道

$$n_p\,\big|\,q \quad n_p\equiv 1 \pmod p$$

从而 $n_p=q\equiv 1 \pmod p$, 则 $p<q$.
如果 H 为 G 的 q 阶子群, 则 $x\in H\backslash\{e\}$ 的阶均为 q, 如果 $x\in G$, 则 $H=\langle x\rangle$ 为 q 阶子群.
设 $G_1,G_2,\cdots,G_{n_q}$ 为全部的 q 阶子群, 则 $G_i\backslash\{e\}\,(i=1,2,\cdots,n_q)$ 两两不相交.则

$$|\bigcup_{i=1}^{n_q}G_i\backslash\{e\}|=n_q(q-1)$$

(1)如果 $n_q=p^2$, 则 G 中非 q 阶元个数为 $p^2q-p^2(q-1)=p^2$, 注意 Sylow p-子群中元为全部非 q 阶元, 则此时 $n_p=1$.
(2)如果 $n_q=p$, 则有 $n_q\equiv 1 \pmod q$, 由上知 $p<q$, 从而 $n_q=1$ 与假设矛盾.故原命题成立. □

作业：

(1) 设 G 为有限群, A,B 为 G 的非空子集（注意不是子群）, 如果 $|A|+|B|>|G|$, 则 $AB=G$.（先证 $e\in AB$, 在用类似方法证明 $g\in G\,(g\in AB)$）

[3] 注意区分例2.3.3和例2.3.5的条件的区别, 例2.3.3, 例2.3.4, 例2.3.5都可以出判断题.

2.4 同构定理

定理2.4.1 (同构定理)

设 σ 是群 G 到群 $\overline{G}$ 的同态, 则

(1) $\{G$ 的包含 $\ker\sigma$ 的子群$\}$ 与 $\{\sigma(G)=\mathrm{Im}\sigma$ 的子群$\}$ 之间有一一对应

$$H\mapsto\sigma(H)=\{\sigma(h):h\in H\}$$

(2) 当 $\ker\sigma\leqslant H\leqslant G$ 时, $H\trianglelefteq G\Leftrightarrow\sigma(H)\trianglelefteq\sigma(G)$.

(3) 当 $\ker\sigma\leqslant H\trianglelefteq G$ 时, $\sigma(G)/\sigma(H)\cong G/H$.

证明 (1) $H\leqslant G$ 时, 令 $\sigma(H)=\mathrm{Im}(\sigma|_H)$ [1], 则 $\sigma|_H$ 是 H 到 $\mathrm{Im}(\sigma)=\sigma(G)$ 的同态.依同态基本定理（33页）有 $\sigma(H)\leqslant\sigma(G)$. 令 $K=\ker\sigma$, $K\leqslant H\leqslant G$ 时,

$$\begin{aligned}\sigma(a)\in\sigma(H)&\Leftrightarrow\exists h\in H,\ \text{使}\ \sigma(a)=\sigma(h)\\&\Leftrightarrow\exists h\in H,\ \text{使}\ \sigma(ah^{-1})=\bar{e}\\&\Leftrightarrow\exists h\in H,\ \text{使}\ ah^{-1}\in K=\ker\sigma\\&\Leftrightarrow\exists h\in H,\ \text{使}\ a\in KH\\&\Leftrightarrow a\in KH=H\end{aligned}$$

下面证明 σ 为双射.当 $K\leqslant H_1\leqslant G$, $K\leqslant H_2\leqslant G$ 时,

$$\begin{aligned}\sigma(H_1)=\sigma(H_2)&\Rightarrow\ \text{对}\ \forall a\in G,\ \sigma(a)\in\sigma(H_1)\ \text{当且仅当}\ \sigma(a)\in\sigma(H_2))\\&\Rightarrow\ \text{对}\ \forall a\in G,\ a\in H_1\ \text{当且仅当}\ a\in H_2\\&\Rightarrow H_1=H_2\end{aligned}$$

即 σ 为单射.
任给 $æ\leqslant\sigma(G)$, 让 $H=\{a\in G:\sigma(a)\in æ\}$.当 $a\in K$ 时, 因为 $\sigma(a)=\bar{e}\in æ$, 故 $K\subseteq H$.
$a,b\in H$ 时, $\sigma(ab^{-1})=\sigma(a)\sigma(b)^{-1}\in æ$, 从而 $ab^{-1}\in H$, 即 H 对右除法封闭, 因此 $K\leqslant H\leqslant G$.
因为

$$\sigma(a)\in æ\Leftrightarrow a\in H\Leftrightarrow\sigma(a)\in\sigma(H)$$

故 $æ=\sigma(H)$. 即 σ 为满射.

[1] $\sigma|_H$ 表示映射 σ 限制在 H 上.

(2)设 $K \leqslant H \leqslant G$, 则

$$\begin{aligned} H \trianglelefteq G \Leftrightarrow &\ \text{对 } \forall g \in G \forall h \in H, ghg^{-1} \in H \\ \Leftrightarrow &\ \text{对 } \forall g \in G \forall h \in H,\ \sigma(ghg^{-1}) \in \sigma(H) \\ \Leftrightarrow &\ \text{对 } \forall g \in G \forall h \in H,\ \sigma(g)\sigma(h)\sigma(g^{-1}) \in \sigma(H) \\ \Leftrightarrow &\ \sigma(H) \trianglelefteq \sigma(G) \end{aligned}$$

(3) 设 $K = \ker\sigma \leqslant H \trianglelefteq G$, 做映射 $\bar{\sigma} : G/H \to \sigma(G)/\sigma(H)$ 如下:

$$\bar{\sigma}(aH) = \sigma(a)\sigma(H) \in \sigma(G)/\sigma(H)$$

注意到

$$\begin{aligned} \bar{\sigma}(aH) = \bar{\sigma}(bH) &\Leftrightarrow \sigma(a)\sigma(H) = \sigma(b)\sigma(H) \\ &\Leftrightarrow \sigma(H) = \sigma(a^{-1})\sigma(b)\sigma(H) \\ &\Leftrightarrow \sigma(a^{-1}b) \in \sigma(H) \\ &\Leftrightarrow b \in aH \\ &\Leftrightarrow aH = bH \end{aligned}$$

故 $\bar{\sigma}$ 定义合理且为单射, 此外 $\bar{\sigma}$ 显然为满射.下证 $\bar{\sigma}$ 为同态.

$$\begin{aligned} \bar{\sigma}(aH \cdot bH) &= \bar{\sigma}(abH) \\ &= \sigma(a)\sigma(b)\sigma(H) \\ &= \sigma(a)\sigma(H) \cdot \sigma(b)\sigma(H) \text{ [2]} \\ &= \bar{\sigma}(aH)\bar{\sigma}(bH) \end{aligned}$$

所以 $\bar{\sigma}$ 为同构, 故 $\sigma(G)/\sigma(H) \cong G/H$. □

定理2.4.2 (第一同构定理)

设 $K \trianglelefteq G$, 则

(1) $\{G/K\text{的子群}\} = \{H/K : K \leqslant H \leqslant G\}$.

(2) $K \leqslant H \leqslant G$ 时, $H/K \trianglelefteq G/K \Leftrightarrow H \trianglelefteq G$.

(3) $K \leqslant H \trianglelefteq G$ 时, $G/K \Big/ H/K \cong G/H$.

证明 (1) 做 $\sigma : G \to G/K$ 如下

$$\sigma(a) = aK$$

则 σ 是自然同态.可知 $\ker\sigma = \{a \in G : aK = K\} = K$, 由定理2.4.1（48页的同构定理）的(2)知, $\sigma(G) = G/K$ 的子群形如 $\sigma(H) = H/K$, 其中 $K \leqslant H \leqslant G$.

(2) 当 $K \leqslant H \leqslant G$ 时, 由定理2.4.1(2)知

$$H \trianglelefteq G \Leftrightarrow \sigma(H) \trianglelefteq \sigma(G) \Leftrightarrow H/K \trianglelefteq G/K$$

(3) 当 $K \leqslant H \trianglelefteq G$ 时, 由定理2.4.1(3)知

$$G/H \cong \sigma(G)/\sigma(H) = G/K \Big/ H/K$$

□

定理2.4.3 (第二同构定理)

设 $H \trianglelefteq K$, $K \leqslant G$, 则

$$H \cap K \trianglelefteq K \quad HK \leqslant G \text{且} K/(H \cap K) \cong HK/H$$

证明 做 $\sigma : K \to G/H$ 如下

$$\sigma(k) = kH \in G/H$$

因为

$$\sigma(k_1k_2) = k_1k_2H = k_1Hk_2H = \sigma(k_1)\sigma(k_2)$$

所以 σ 为同态.又

$$\ker\sigma = \{k \in K : kH = H\} = \{k \in K : k \in H\} = H \cap K \trianglelefteq K$$

另外

$$\begin{aligned}
\mathrm{Im}\sigma &= \{kH : k \in K\} \\
&= \{khH : k \in K,\ h \in H\} \\
&= \{xH : x \in KH = HK\} \\
&= HK/H
\end{aligned}$$

由同态基本定理（33页）知, $K/\ker\sigma \cong \mathrm{Im}(\sigma)$, 注意到 $\ker\sigma = H \cap K$, $\mathrm{Im}\sigma = HK/H$, 结论即得证.

□

推论2.4.1

设 $\underline{H \trianglelefteq K,\ K \leqslant G}$, 如果 $[G:H] < \infty$, 则

$$[K : H \cap K] \mid [G : H]$$

证明 因为 $K/(H \cap K) \cong HK/K \leqslant G/H$, 由 Lagrange 定理（22页）知 $|HK/H| \mid |G/H|$, 从而

$$[K : H \cap K] = |HK/H| \mid |G/H| = [G : H]$$ □

引理2.4.1 (Dedekind 律)

设 $K \leqslant H \leqslant G$, $L \leqslant G$, 则 $H \cap KL = K(H \cap L)$

证明 $K(H \cap L) \subseteq KH \cap KL = H \cap KL$. 下证 $H \cap KL \subseteq K(H \cap L)$.
设 $h \in H \cap KL$, 则 $h \in H$, 且有 $k \in K$, $l \in L$, 使得 $h = kl$, 则
$k^{-1}h = l \in KH \cap L = H \cap L$, 从而 $h \in k(H \cap L) \subseteq K(H \cap L)$. □

引理2.4.2

设 $K \trianglelefteq H \leqslant G$, $L \leqslant G$ 则

(1) $K \cap L \trianglelefteq H \cap L$ 且 $(H \cap L)/(K \cap L) \cong K(H \cap L)/K$

(2) 设 $L \trianglelefteq G$, 则 $KL \trianglelefteq HL$, $K(H \cap L) \trianglelefteq H$, 且

$$HL/KL \cong H/K(H \cap L)$$

证明 (1) $K \cap L = K \cap H \cap L = (H \cap L) \cap K$, 注意到 $K \trianglelefteq H$, $H \cap L \leqslant H$, 由定理2.4.3（第二同构定理）知道

$$K \cap L \trianglelefteq H \cap L \quad (H \cap L)/(K \cap L) \cong K(H \cap L)/K$$

(2)因为 $K \trianglelefteq H$, $L \trianglelefteq G$, 所以

$$KL \cdot HL = KHLL = HKLL = HL \cdot KL$$

即 $KL \trianglelefteq HL$. 又因为 $H \leqslant HL$, $KL \trianglelefteq HL$, 故由第二同构定理知 $H \cap KL \trianglelefteq H$, 由引理2.4.1(Dedekind律)知, $H \cap KL = K(H \cap L)$, 即证得 $K(H \cap L) \trianglelefteq H$, 注意到 $KL \trianglelefteq HL$, $H \leqslant HL$, 故由第二同构定理知, $KL \cdot H/KL \cong H/(H \cap KL)$, 因为 $KL \cdot H = HL$, $H \cap KL = K(H \cap L)$, 即引理得证. □

定理2.4.4 (第三同构定理)

设 G 为群, $L_1 \trianglelefteq H_1 \leqslant G$, $L_2 \trianglelefteq H_2 \leqslant G$, 则

$$(H_1 \cap L_2)L_1 \trianglelefteq (H_1 \cap H_2)L_1 \quad (H_2 \cap L_1)L_2 \trianglelefteq (H_1 \cap H_2)L_2$$

且

$$(H_1 \cap H_2)L_1 \big/ (H_1 \cap L_2)L_1 \cong (H_1 \cap H_2)L_2 \big/ (H_2 \cap L_1)L_2$$

证明 令 $H = H_1 \cap H_2$, 由于 $L_2 \trianglelefteq H_2$, 由第二同构定理知

$$H_1 \cap L_2 = H_1 \cap (H_2 \cap L_2) = H \cap L_2 \trianglelefteq H$$

同理, 由于 $L_1 \trianglelefteq H_1$, 有

$$H_2 \cap L_1 = H \cap L_1 \trianglelefteq H$$

于是

$$K = (H_1 \cap L_2)(H_2 \cap L_1) \trianglelefteq H$$ [3]

由于 $L_1 \trianglelefteq H_1$, $H \cap L_1 \leqslant H_2 \cap L_1 \leqslant L_1$, 依引理2.4.2的(2)知

$$(H_1 \cap L_2)L_1 = (H_1 \cap L_2)(H \cap L_1)L_1 = KL_1 \trianglelefteq HL_1$$

且

$$HL_1/KL_1 \cong H/K(H \cap L_1) = H/K$$

同理可得

$$(H_2 \cap L_1)L_2 = KL_2 \trianglelefteq HL_2 \text{且 } HL_2/KL_2 \cong H/K(H \cap L_2) = H/K$$

因此

$$HL_1/KL_1 \cong H/K \cong HL_2/KL_2$$

即

$$(H_1 \cap H_2)L_1 \big/ (H_1 \cap L_2)L_1 \cong (H_1 \cap H_2)L_2 \big/ (H_2 \cap L_1)L_2$$ □

作业:

(1) 设 $H \trianglelefteq G$, $K \trianglelefteq G$, 证明 $HK \trianglelefteq G$

(2) 证明引理2.4.2的(2)(51页)

[3] 易证如果 $H \trianglelefteq G$, $K \trianglelefteq G$, 则 $HK \trianglelefteq G$

2.5　正规群列与合成群列

定义2.5.1

设 G 为群, 如果

$$G_0=\{e\}\lhd G_1\lhd G_2\cdots\lhd G_n=G$$

则称这为群 G 的一个**正规群列**（长度为 n ）, 相应的商群为

$$G_1/G_0,\ G_2/G_1\cdots G_n/G_{n-1}$$

对于群 G 的正规群列

$$G_0=\{e\}\lhd G_1\lhd G_2\cdots\lhd G_n=G \tag{2.1}$$
$$H_0=\{e\}\lhd H_1\lhd H_2\cdots\lhd H_m=G \tag{2.2}$$

如果(2.1)中的诸子群在(2.2)中出现, 则称(2.2)为(2.1)的一个**加细**.
如果(2.1)中没有异于自身的加细, 则称(2.1)为G的一个**合成群列**.
正规群列(2.1)与(2.2)等价是指 $m=n$ 并且存在 $\sigma\in S_n$, 使

$$G_{\sigma(i)}/G_{\sigma(i)-1}\cong H_i/H_{i-1}\,(i=1,2\ldots,n)$$

注意：正规群列 $G_0=\{e\}\lhd G_1\lhd G_2\cdots\lhd G_n=G$ 为 G 的合成群列
$\Longleftrightarrow i=1,2,\ldots,n$ 时, G_{i-1} 为 G_i 的极大正规子群[1].
$\Longleftrightarrow i=1,2,\ldots,n$ 时, G_i/G_{i-1} 仅有的正规子群为 G_i/G_{i-1} 与 G_{i-1}/G_{i-1}[2].
$\Longleftrightarrow i=1,2,\ldots,n$ 时, G_i/G_{i-1} 为单群[3].

定理2.5.1

群 G 的任两个正规群列有等价的加细.

证明　设 G 有两个正规群列

$$G_0=\{e\}\lhd G_1\lhd G_2\cdots\lhd G_n=G$$
$$H_0=\{e\}\lhd H_1\lhd H_2\cdots\lhd H_m=G$$

让 $G_{i,j}=G_{i-1}(G_i\cap H_j)$, $H_{j,i}=H_{j-1}(H_j\cap G_i)$, 则

$$G_{i-1}\leqslant G_{i,j}\leqslant G_i\quad H_{j-1}\leqslant H_{j,i}\leqslant H_j$$

[1] $H\trianglelefteq G$ 为 G 的极大正规子群是指 $H\leqslant K\trianglelefteq G\Leftarrow K=H$ 或 G.
[2] 由第一同构定理(49页)知 $H/G_{i-1}\trianglelefteq G_i/G_{i-1}\Leftrightarrow G_{i-1}\leqslant H\trianglelefteq G_i$.
[3] 单群定义参见42页的定义2.2.2.

可得

$$G_{i-1}=G_{i,0}\leqslant G_{i,0}\cdots\leqslant G_{i,m}=G_i$$

由于 $H_{j-1}\trianglelefteq H_j$, $G_{i-1}\trianglelefteq G_i$, 所以由第三同构定理(52页)知道

$$G_{i,j-1}=G_{i-1}(G_i\cap H_{j-1})\lhd G_{i-1}(G_i\cap H_j)=G_{i,j}$$
$$H_{j,i-1}=H_{j-1}(H_j\cap G_{i-1})\lhd H_{j-1}(H_J\cap G_i)=H_{j,i}$$

且

$$G_{i,j}/G_{i,j-1}\cong H_{j,i}/H_{j,i-1}$$

注意到 $G_{i-1,m}=G_{i-1}=G_{i,0}$, $H_{j-1,n}=H_{j-1}=H_{j,0}$, 所以由正规群列等价的定义知

$$G_{0,0}=\{e\}\lhd G_{0,1}\cdots\lhd G_{0,m}\lhd G_{1,1}\cdots\lhd G_{n,1}\cdots\lhd G_{n,m}=G$$
$$H_{0,0}=\{e\}\lhd H_{0,1}\cdots\lhd H_{0,n}\lhd H_{1,1}\cdots\lhd H_{m,1}\cdots\lhd H_{m,n}=G$$

为两个等价的加细. □

定理2.5.2

设 G 有合成群列, 则

(1) G 的每个正规群列可加细成一个合成群列.

(2) G 的任两个合成群列等价.

证明 (1) 设 G 有合成群列

$$G_0=\{e\}\lhd G_1\lhd G_2\cdots\lhd G_n=G \tag{2.3}$$

任给 G 的一个正规群列

$$H_0=\{e\}\lhd H_1\lhd H_2\cdots\lhd H_m=G \tag{2.4}$$

由定理2.5.1知二者有等价加细, 因为(1)的加细为自身, 故(2.4)有个加细与(2.3)等价.因为(2.3)的商群列均为单群[4], 所以与(2.3)等价的正规群列商群列中也只有单群, 故与合成群列(2.3)等价的正规群列也是合成群列, 即(2.4)有加细为合成群列.

(2) 不妨设(2.3),(2.4)为 G 的合成群列, 由定理2.5.1知(2.3)与(2.4)有等价加细, 而(2.3),(2.4)的加细为自身, 故(2.3),(2.4)等价. □

[4]单群定义参见42页的定义2.2.2.

定义2.5.2

群 G 的子群 H 叫 G 的**次正规子群**(或称H 在 G 中**次正规**), 是指存在子群链满足

$$H_0 = H \lhd H_1 \lhd H_2 \cdots \lhd H_n = G \tag{2.5}$$

即 H_i 在 H_{i+1} 中正规.如果 H_i 为 H_{i+1} 的极大正规子群, 则说(2.5)为 H 到 G 的**合成群列**.

定理2.5.3

设 H 为 G 的指标（即 $[G:H]$ ）有穷的次正规子群, 则存在从 H 到 G 的合成群列.特别地, 有限群必有合成群列[5].

证明　对 $[G:H]$ 进行归纳.如果 $[G:H]=1$, 则 $G=H$.
设 $[G:H]<k$ 时, 有从 H 到 G 的合成群列.
当 $[G:H]=k$ 时, 有

$$H_0 = H \lhd H_1 \lhd H_2 \cdots \lhd H_{n-1} \lhd H_n = G$$[6]

因为 $[H_{n-1}:H]<[G:H]$, 由归纳假设知, 存在 H 到 H_{n-1} 的合成群列(1).又因为 $H_{n-1} \lhd H_n = G$, 且 $[G:H_{n-1}]<[G:H]$, 依归纳假设也有从 H_{n-1} 到 G 的合成群列(2).将(1), (2)合在一起即可得到 H 到 G 的合成群列. □

定理2.5.4

设 $H, K \leqslant G$, H 在 G 中次正规, 则

(1)　$H \cap K$ 在 K 中次正规.

(2)　$K \trianglelefteq G$ 时, HK 在 G 中次正规.

证明　(1) 设 $H = H_0 \lhd H_1 \lhd H_2 \cdots \lhd H_n = G$, 则

$$H \cap K \leqslant H_1 \cap K \cdots \leqslant H_n \cap K = K \tag{2.6}$$

[5] $[G:\{e\}]$ 为有穷

因为 $H_i \trianglelefteq H_{i+1}, H_{i+1} \cap K \leqslant H_{i+1}$, 由第二同构定理(50页)知

$$H_i \cap K = (H_{i+1} \cap K) \cap H_i \trianglelefteq H_{i+1} \cap K$$

即由次正规定义知, $H \cap K$ 在 K 中次正规.

(2)设 $K \trianglelefteq G$ 时, 因为 $H_i \trianglelefteq H_{i+1}$, 所以由引理2.4.2的(2)(51页)知 $H_iK \trianglelefteq H_{i+1}K$. 从而

$$HK = H_0K \lhd H_1K \lhd H_2K \cdots \lhd H_nK = GK = G \qquad \square$$

作业：

(1) 设 $G_1, \ldots, G_k$ 为 G 的次正规子群, 证明 $\bigcap_{i=1}^{k} G_i$ 在 G 中次正规.(利用数学归纳法和定理2.5.4的(1))

2.6　导群与可解群

定义2.6.1

设 G 为群, 对 $x, y \in G$, 我们称

$$[x, y] = x^{-1}y^{-1}xy = (yx)^{-1}xy$$

为 x, y **换位子**.
如果 $H, K \leqslant G$, 则让

$$[H, K] = \langle [h, k] : h \in H,\ k \in K \rangle$$

$G' = [G, G]$ 叫 G 的**导群（或换位子群）**

注意

1. $[x, y] = e \Leftrightarrow (yx)^{-1}xy = e \Leftrightarrow xy = yx$
2. $[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y, x]$
3. $H, K \leqslant G$ 时,

$$\begin{aligned}[H, K] &= \langle [h, k] : h \in H,\ k \in K \rangle \\ &= \langle [h, k]^{-1} : h \in H,\ k \in K \rangle \\ &= \langle [k, h] : h \in H,\ k \in K \rangle \\ &= [K, H]\end{aligned}$$

定理2.6.1

设 $H \trianglelefteq G$, $K \trianglelefteq G$, 则 $[H, K] \trianglelefteq G$, 特别地 $H \trianglelefteq G$ 时, $H' = [H, H] \trianglelefteq G$.

证明　设 $g \in G$, $h \in H$, $k \in K$, 则

$$g[h, k]g^{-1} = gh^{-1}g^{-1}gk^{-1}g^{-1}ghg^{-1}gkg^{-1} = [ghg^{-1}, gkg^{-1}] \in [H, K]$$
$$g[h, k]^{-1}g^{-1} = g[k, h]g^{-1} \in [K, H] = [H, K]$$

因为 $\forall x \in [H, K]$, 有

$$x = [h_1, k_1]^{\varepsilon_1} \cdots\ [h_n, k_n]^{\varepsilon_n}$$

其中 $\varepsilon_i \in \{\pm 1\}$.
则由前面所证可知

$$gxg^{-1} = g[h_1, k_1]^{\varepsilon_1}g^{-1}g[h_2, k_2]^{\varepsilon_2}g^{-1} \cdots g[h_n, k_n]^{\varepsilon_n}g^{-1} \in [H, K] \qquad \square$$

定理2.6.2

群 G 的导群 G' 是使 G/H 为 Abel 群的 G 的最小正规子群 H.

证明　因为 $G \trianglelefteq G$, 所以 $G' = [G,G] \trianglelefteq G$. 任给 $H \trianglelefteq G$,

$$\begin{aligned} G/H\text{为 Abel 群} &\Leftrightarrow \text{对 } \forall x,y \in G, xHyH = yHxH \\ &\Leftrightarrow \text{对 } \forall x,y \in G, xyH = yxH \\ &\Leftrightarrow \text{对 } \forall x,y \in G, (yx)^{-1}xyH = H \\ &\Leftrightarrow \text{对 } \forall x,y \in G, (yx)^{-1}xy = [x,y] \in H \\ &\Leftrightarrow G' \subseteq H \quad \square \end{aligned}$$

例2.6.1

群 G 是Abel群, 则 $G' = \{e\}$, $G/\{e\}$ 为Abel群.

定义2.6.2

对于群 G, 让 $G^{(0)} = G$, $G^{(1)} = G' \ldots G^{(n+1)} = (G^{(n)})'$, 其中 $G^{(n)}$ 叫 G 的 n **阶导群**.

定理2.6.3

设 G 为群, $n \in \mathbb{N}$, 则 $G^{(n)} \trianglelefteq G$, 且 $H \trianglelefteq G$ 时,

$$(G/H)^{(n)} = G^{(n)}H/H$$

证明　对 n 进行归纳.$n = 0$ 时, 有 $G^{(0)} = G \trianglelefteq G$, 且

$$(G/H)^{(0)} = G/H = G^{(0)}/H$$

设已有 $G^{(n)} \trianglelefteq G$, $(G/H)^{(n)} = G^{(n)}H/H$, 则由定理2.6.1(57页)知

$$G^{(n+1)} = (G^{(n)})' \trianglelefteq G$$

$$
\begin{aligned}
(G/H)^{(n+1)} &= \big((G/H)^{(n)}\big) \\
&= \big(G^{(n)}H/H\big)' \\
&= \langle (xH)^{-1}(yH)^{-1}xHyH : xH, yH \in G^{(n)}H/H \rangle \\
&= \langle x^{-1}y^{-1}xyH : x, y \in G^{(n)} \rangle \\
&= \langle [x,y]H : x, y \in G^{(n)} \rangle \\
&= \{gH : g \in \langle [x,y] : x, y \in G^{(n)} \rangle\} \\
&= \{ghH : g \in G^{(n+1)},\ h \in H\} \\
&= \{xH : x \in G^{(n+1)}H\} \\
&= G^{(n+1)}H/H \quad \square
\end{aligned}
$$

定义2.6.3

对于群 G

$$G = G^{(0)} \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \cdots \trianglerighteq G^{(n)} \cdots$$

叫做 G 的**导列**. 如果 $G^{(n)} = G^{(n+1)}$, 则说 G 的导列长为 n.

定义2.6.4

设 G 为群, 对于群 G 的正规群列（不一定为合成群列）

$$G_0 = \{e\} \triangleleft G_1 \triangleleft G_2 \cdots \triangleleft G_n = G \tag{2.7}$$

如果诸商群 G_i/G_{i-1} 都是 Abel 群, 则说(2.7)为 **Abel 列**.
G **可解**是指存在 G 的 Abel 列.

定理2.6.4

设 G 为群, 则 G 可解等价于 $\exists n \in \mathbb{N}$, $G^{(n)} = \{e\}$

证明　(1)必要性：设 $G^{(n)} = \{e\}$, 则

$$G^{(0)} = G \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \cdots \trianglerighteq G^{(n)} = \{e\}$$

且由定理2.6.2(58页)知道, $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ 是Abel群, 故 G 的导列为Abel列.

(2)充分性：设 G 有Abel列

$$G_0 = G \trianglerighteq G_1 \trianglerighteq G_2 \cdots \trianglerighteq G_n = \{e\}$$

下证 $G^{(i)} \leqslant G_i$. $i = 0$ 时, $G^{(0)} = G \leqslant G_0$. 设 $G^{(i-1)} \leqslant G_{i-1}$, 则因为 G_{i-1}/G_i 是Abel群, 由定理2.6.2(58页)知道

$$G^{(i)} = (G^{(i-1)})' \leqslant (G_{i-1})' \leqslant G_i \text{ [1]} \tag{2.7}$$

从而得到 $G^{(n)} \leqslant G_n = \{e\}$. □

定理2.6.5

仅有的可解单群为素数阶循环群.

证明　(1) 设 G 为 p 阶群, 其中 p 为素数, 则 G 循环, 从而 G 为Abel群, 于是 G 可解.

(2) 任给可解单群 G, 由于 G 可解, 所以有 $n \in \mathbb{N}$ 使 $G^{(n)} = \{e\}$, 于是 $G' \neq G$, 而 $G' \trianglelefteq G$, 故 $G' = \{e\}$, 从而 G 为Abel群.任取 $a \in G \backslash \{e\}$, 则 $\langle a \rangle \trianglelefteq G$, 又 G 为单群 [2], 所以 $G = \langle a \rangle$.

如果 $o(a) = \infty$, 则 $\{e\} \neq \langle a^2 \rangle \trianglelefteq G$, 这与 G 为单群矛盾.

下设 $o(a) = n > 1$, 如果 n 为合数, d 为 n 的真因子 [3].则 $o(a^{\frac{n}{d}}) = d$, $H = \langle a^{\frac{n}{d}} \rangle \trianglelefteq G$, 这与 G 为单群矛盾.故综上可得, G 为素数阶循环群. □

定理2.6.6

设 p 为素数, G 为 p^n 阶群, 则 G 有 p^i 阶正规子群 H_i $(i = 0, 1, 2, \dots, n)$, 使

$$H_0 = e \leqslant H_1 \leqslant H_2 \cdots \leqslant H_n = G$$

这是 G 的一个合成群列, 且 G 可解.

---

[1] 由此处可知, 可解群的导列是下降最快的Abel列, 即对于 G 的任意Abel列

$$\begin{aligned} G_0 &= G \trianglerighteq G_1 \trianglerighteq G_2 \cdots \trianglerighteq G_n = \{e\} \\ G^{(0)} &= G \trianglerighteq G^{(1)} \trianglerighteq G^{(2)} \cdots \trianglerighteq G^{(n)} = \{e\} \end{aligned}$$

有 $G^{(i)} \leqslant G_i$.

[2] 单群定义参见42页的定义2.2.2.

[3] $1 < d < n$, $d \mid n$.

证明　对 n 进行归纳. $n=0$ 时, $G=\{e\}$, 让 $H_0=\{e\}=G$, 则 $|H_0|=p^0$.
$n=1$ 时, 因为 G 为 p 阶群, 所以 $H_0=\{e\}\lhd H_1=G$.
下设 $n>1$, 且对更小的 n 结论正确, 由定理2.2.2(41页)知 p 群 G 的中心 $Z(G)$ 中有 $z\neq e$. 则

$$\{e\}\neq\langle z\rangle\leqslant G,\ o(z)=|\langle z\rangle|\ \big|\ |G|=p^n$$

设 $o(z)=p^m\,(1\leqslant m\leqslant n)$, 则 $o(z^{p^{m-1}})=p$, 即 $H=\langle z^{p^{m-1}}\rangle$ 为 G 的 p 阶子群. 当 $g\in G, h\in H$ 时, 因为 $H\leqslant Z(G)$, 所以

$$ghg^{-1}=hgg^{-1}=h\in H$$

故 $H\trianglelefteq G$, 且 $|G/H|=\frac{|G|}{|H|}=p^{n-1}$, 依归纳假设知, $\overline{G}=G/H$ 有 p^{i-1} 阶子群 $\overline{H_{i-1}}\,(i=1,2,\ldots,n)$ 使

$$\overline{H_0}\leqslant\overline{H_1}\leqslant\cdots\leqslant\overline{H_{n-1}}=\overline{G}$$

依第一同构定理的(1)(49页)知 $\overline{H_{i-1}}$ 形如 H_i/H, 其中

$$H_0=\{e\}\leqslant H=H_1\leqslant H_2\cdots\leqslant H_n=G$$

因为 $H_i/H=\overline{H_{i-1}}\trianglelefteq\overline{G}=G/H$, 所以由第一同构定理的(2)(49页)知道 $H_i\trianglelefteq G$, 且

$$|H_i|=|H_i/H||H|=|\overline{H_{i-1}}||H|=p^i$$

注意到 H_i/H_{i-1} 为素数阶群, 故 H_i/H_{i-1} 为单群, 且为循环群. 所以 G 是可解群. □

定理2.6.7

设 G 为有限群, 则 G 可解 $\Longleftrightarrow$ 存在正规群列

$$G_0=\{e\}\lhd\cdots\lhd G_n=G$$

使 G_i/G_{i-1} 均为素数阶循环群.

证明　(1) "$\Leftarrow$" : 素数阶群是循环群, 从而 G_i/G_{i-1}为 Abel 群, 即 G 有Abel列, 故 G 可解.
(2) "$\Rightarrow$" :设 G 有Abel列:

$$H_0=\{e\}\lhd H_1\lhd\cdots\lhd H_n=G$$

因为 $H_{i-1}\lhd H_i$, 根据定理2.5.3(55页), 存在从 H_{i-1} 到 H_i 的合成群列

$$H_{i-1,0}=H_{i-1}\lhd H_{i-1,1}\lhd\cdots\lhd H_{i-1,l_i}=H_i \tag{2.8}$$

由第一同构定理(49页)知

$$H_{i-1,j}/H_{i-1,j-1} \leqslant H_i/H_{i-1,j-1} \cong (H_i/H_{i-1}) \Big/ (H_{i-1,j-1}/H_{i-1})$$

其中前面假设知, H_i/H_{i-1} 为 Abel 群, 从而

$$H_i/H_{i-1,j-1} \cong (H_i/H_{i-1}) \Big/ (H_{i-1,j-1}/H_{i-1}) \text{ 为 Abel 群}$$

即得 $H_{i-1,j}/H_{i-1,j-1}$ 为 Abel 单群.从而(2.8)为 Abel 列 [4].
注意到Abel列(2.8)的商群列中 $H_{i-1,j}/H_{i-1,j-1}$ 为 Abel 单群.由2.2节的作业（42页）知 $H_{i-1,j}/H_{i-1,j-1}$ 为素数阶. 故 G 有合成群列, 商群为素数阶. □

推论2.6.1

设有限可解群 G 的合成群列长为 n, 则 $|G|$ 是 n 个素数乘积.

证明 设 $G_0 = \{e\} \lhd G_1 \lhd \cdots \lhd G_n = G$ 为合成群列, 则 $p_i = |G_i/G_{i-1}|$ 为素数, 故

$$|G| = [G : G_0] = [G_n : G_{n-1}] \cdots [G_1 : G_0] = p_n p_{n-1} \cdots p_1$$ □

推论2.6.2 (算术基本定理)

大于1的整数 n 可表示成有限个素数的乘积, 不计因子顺序时, 分解方式是唯一的.

证明 $G = \mathbb{Z}/n\mathbb{Z}$, 依剩余类加法构成 n 阶循环群, 设 G 的合成群列长为 k, 则 $n = |G|$ 是 k 个素数 $p_1, \ldots, p_k$ 的乘积, 且

$$G = \mathbb{Z}/n\mathbb{Z} \rhd p_1\mathbb{Z}/n\mathbb{Z} \rhd p_1p_2\mathbb{Z}/n\mathbb{Z} \rhd \cdots \rhd p_1p_2\cdots p_k\mathbb{Z}/n\mathbb{Z} = \{e\} \tag{2.9}$$

如果 n 还有素数分解式 $q_1, \ldots, q_l$, 则 G 有合成群列

$$G = \mathbb{Z}/n\mathbb{Z} \rhd q_1\mathbb{Z}/n\mathbb{Z} \rhd q_1q_2\mathbb{Z}/n\mathbb{Z} \rhd \cdots \rhd q_1q_2\cdots q_l\mathbb{Z}/n\mathbb{Z} = \{e\} \tag{2.10}$$

[4]另一种方法：因为 H_i/H_{i-1} 为 Abel 群, 所以

$$H'_{i-1,j} \leqslant H'_i \leqslant H_{i-1} \leqslant H_{i-1,j-1}$$

故由定理2.6.2的证明(58页)知 $H_{i-1,j}/H_{i-1,j-1}$ 为 Abel 群.

根据定理2.5.2的(2)(54页), (2.9)与(2.10)等价, 故 $l=k$, 且 $\exists\sigma\in S_k$ 使得

$$\begin{aligned}&(q_1\cdots q_{i-1}\mathbb{Z}/n\mathbb{Z})\Big/(q_1\cdots q_{i-1}q_i\mathbb{Z}/n\mathbb{Z})\\ \cong\ &(p_1\cdots p_{\sigma(i)-1}\mathbb{Z}/n\mathbb{Z})\Big/(p_1\cdots p_{\sigma(i)-1}p_{\sigma(i)}\mathbb{Z}/n\mathbb{Z})\end{aligned}$$

即 $q_i=p_{\sigma(i)}$ 。 □

定理2.6.8

(1) 可解群的子群与商群也可解.

(2) 设 $H\trianglelefteq G$, 如果 H 与 G/H 都可解, 则 G 可解.

(3) 设 $H\trianglelefteq G$, $K\trianglelefteq G$, 则 $G/(H\cap K)$ 可解 $\Longleftrightarrow G/H$ 与 G/K 可解.

证明 (1)设 $H\leqslant G$, G的一个Abel列为

$$G_0=\{e\}=\trianglelefteq G_1\trianglelefteq\cdots\trianglelefteq G_n=G$$

因为 $G_{i-1}\trianglelefteq G_i$, $H\cap G_i\leqslant G_i$, 所以由第二同构定理(50页)知

$$H\cap G_{i-1}=G_{i-1}\cap(H\cap G_i)\trianglelefteq H\cap G_i$$

且

$$\begin{aligned}(H\cap G_i)\Big/(H\cap G_{i-1})&=(H\cap G_i)\Big/(G_{i-1}\cap(H\cap G_i))\\&\cong G_{i-1}(H\cap G_i)\Big/G_{i-1}\leqslant G_i/G_{i-1}\end{aligned}$$

则因为 G_i/G_{i-1} 为Abel群, 故 $(H\cap G_i)\Big/(H\cap G_{i-1})$ 为Abel群.所以

$$G_0\cap H\trianglelefteq G_1\cap H\trianglelefteq\cdots\trianglelefteq G_n\cap H=H$$

为 H 的一个Abel列, 即 H 可解.

设 $\overline{G}=G/H$ 为 G 的一个商群, 因为 G 为可解群, 由定理2.6.4(59页)知 $\exists n\in\mathbb{N}$, $G^{(n)}=\{e\}$. 再由定理2.6.3(58页)知

$$\overline{G}^{(n)}=(G/H)^{(n)}=G^{(n)}H/H=\{e\}H/H=\{\overline{e}\}$$

所以由定理2.6.4(59页)知 $\overline{G}=G/H$ 为可解群.

(2)设 $H\leqslant G$ 有Abel列

$$H_0=\{e\}\trianglelefteq H_1\trianglelefteq\cdots\trianglelefteq H_n=H$$

G/H 有Abel列

$$G_0/H = H/H \trianglelefteq G_1/H \trianglelefteq \cdots \trianglelefteq G_m/H = G/H$$

因为 $H \trianglelefteq G$, $H \leqslant G_{i-1} \leqslant G_i$, 由第一同构定理(49页)知

$$G_i/H \trianglelefteq G_{i+1}/H \Leftrightarrow G_i \trianglelefteq G_{i+1}$$

且

$$G_{i+1}/G_i \cong (G_{i+1}/H)\Big/(G_i/H)$$

因为 $(G_{i+1}/H)\Big/(G_i/H)$ 为Abel群, 故 G_{i+1}/G_i 为Abel群, 故 G 有Abel列

$$H_0 = \{e\} \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_n = H = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_m = G$$

即 G 可解.

(3) "$\Rightarrow$" : 由于 $G/(H \cap K)$ 可解, 且 $H \trianglelefteq G$, $H \cap K \trianglelefteq G$, 所以

$$H/(H \cap K) \trianglelefteq G/(H \cap K)$$

所以由第一同构定理(49页)知

$$G/H \cong G/(H \cap K)\Big/H/(H \cap K)$$

由(1)可知 $G/(H \cap K)\Big/H/(H \cap K)$ 可解, 所以 G/H 可解.同理可得 G/K 可解.

"$\Leftarrow$" : 由第二同构定理(50页)知

$$K/(H \cap K) \cong HK/H \leqslant G/H$$

由于 G/H 可解, 由(1)知, 所以 HK/H 可解, 所以 $K/(H \cap K)$ 可解.由第一同构定理(49页)知

$$G/(H \cap K)\Big/K/(H \cap K) \cong G/K$$

因为 G/K 可解, 所以 $G/(H \cap K)\Big/K/(H \cap K)$ 可解.利用(2)知 $G/(H \cap K)$ 可解. □

推论2.6.3

p^2q 阶群 G 可解.

证明　因为 p^2q 阶群 G 必有正规的 Sylow p-子群或正规的 Sylow q-子群.不妨设 $\{e\} \neq H \leqslant G$, 则

(1) H 为 G 正规的 Sylow p-子群, 则 $|G/H| = q$, 故 G/H 可解, 又由定理2.6.6(60页)知, H 可解, 由定理2.6.8(2)知, G 可解.

(2) H 为 G 正规的 Sylow q-子群, 则 $|G/H| = p^2$, 由定理2.6.6(60页)知, G/H 可解, 又 H 为素数阶群, 故 H 也可解, 由定理2.6.8(2)知, G 可解. □

定理2.6.9 (Burnside定理)

设 p, q 为不同的素数, 则 $p^a q^b$ 阶群可解, 还可证 $p_1 \cdots p_k$ 阶群可解.

定理2.6.10 (Feit-Thmpson 定理)

奇数阶群可解, 奇合数阶群不是单群

作业:

(1)　仅有的可解单群为素数阶循环群.（定理2.6.5）

(2)　G 可解, 则 $H \leqslant G$ 可解, 如果 $H \trianglelefteq G$, 则 G/H 可解.（定理2.6.8的(1)）

2.7　对称群 S_n 、交错群 A_n

定义2.7.1

$S(X)=\{X\text{上置换}\}$ [1], 如果 $X=\{x_1,\ldots,x_n\}$, 则 X 上的置换形如

$$\begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{\sigma(1)} & x_{\sigma(2)} & \ldots & x_{\sigma(n)} \end{pmatrix}$$

其中 σ 为 $\{1,\ldots,n\}$ 上置换, 当 $|X|=n$ 时, $S(X)\cong S_n=S(\{1,2,\ldots,n\})$

定义2.7.2

设 X 为非空集, $a_1,\ldots,a_l$ 为 X 中的不同元素, 让 $(a_1\,a_2\cdots a_l)$ 表示下述置换

$$\sigma(a_1)=a_2,\cdots,\sigma(a_{l-1})=a_l,\,\sigma(a_l)=a_1$$

称 $(a_1\,a_2\cdots a_l)$ 是长为 l 的轮换或循环置换.
特别地, 长为 1 的轮换 $(a)=I$, 长为 2 的轮换 $(a\,b)$ 叫对换.

定理2.7.1

设 $\sigma=(a_1\,a_2\cdots a_k)$ 与 $\tau=(b_1\,b_2\cdots b_l)$ 为 X 上两个不相交的轮换 [2], 则 $\sigma\tau=\tau\sigma$

证明　当 $x\notin\{a_1,\,a_2\ldots,a_k\}\bigcup\{b_1,\,b_2\ldots,b_l\}$ 时, $\sigma\big(\tau(x)\big)=\tau\big(\sigma(x)\big)=x$.
注意到

$$\sigma\big(\tau(a_i)\big)=\sigma(a_i)=\begin{cases} a_{i+1} & i<k \\ a_1 & i=k \end{cases} \qquad \tau\big(\sigma(a_i)\big)=\sigma(a_i)=\begin{cases} a_{i+1} & i<k \\ a_1 & i=k \end{cases}$$

类似地, 有 $\sigma\big(\tau(b_j)\big)=\tau\big(\sigma(b_j)\big)$. □

[1] X 上置换即为 X 到 X 的双射, 可复习第14页的例1.2.16
[2] 两个轮换不相交即是 $\{a_1,\,a_2\ldots,a_k\}\bigcap\{b_1,\,b_2\ldots,b_l\}=\emptyset$.

定理2.7.2

设 X 为有穷非空集, 对每个 $\sigma \in S(X)$ 有唯一的 X 上分类

$$X = \{\{a_{11}, \dots a_{1l_1}\}, \{a_{21}, \dots a_{2l_2}\}, \dots, \{a_{k1}, \dots a_{kl_k}\}\}$$

使 $\sigma = (a_{11} \cdots a_{1l_1}) \cdots (a_{k1} \cdots a_{kl_k})$. 除了因子顺序外（长为 1 的轮换省略）分解唯一.即 $\sigma \in S(X)$ 可表成一些不相交轮换的乘积.

证明 对于 $x, y \in X$, 如果 $\exists m \in \mathbb{Z}\,(\sigma^m(x) = y)$, 则称 $x \sim y$. 下证"$\sim$"是一种等价关系.

(1)自反性: $\sigma^0(x) = I(x) = x$, 故 $x \sim x$.

(2)对称性: $x \sim y$, 则 $\exists m \in \mathbb{Z}\,(\sigma^m(x) = y)$, 则可得到 $\sigma^{-m}(y) = x$, 故 $y \sim x$.

(3)传递性: $x \sim y$, $y \sim z$, 则 $\exists m, n \in \mathbb{Z}$, 使得 $\sigma^m(x) = y, \sigma^n(y) = z$, 所以得到 $\sigma^{m+n}x = z$, 故 $x \sim z$.

所以 $\sim$ 是 X 上的一个等价关系.设 $A_1, A_2, \dots, A_k$ 是 X 上的根据 $\sim$ 一个分划, 其中 $A_i = \{a_{i1}, \dots, a_{il_i}\}$. 根据 $\sim$ 的定义可知 $\sigma(a_{ij}) \in A_i$, 故不妨设

$$\sigma(a_{ij}) = \begin{cases} a_{i,j+1} & j < l_i \\ a_{i1} & i = l_i \end{cases}$$

则可知 $\sigma = (a_{11} \cdots a_{1l_1}) \cdots (a_{k1} \cdots a_{kl_k})$. 设 $A'_1, \dots A'_m$ 为 X 中满足定理要求的另一种分类, 则 $a_i, a_j \in A'_i$ 当且仅当 $a_i \sim a_j$, 故可知 $A'_1, \dots A'_m$ 与 $A_1, A_2, \dots, A_k$ 相同.故唯一性得证. □

例2.7.1

S_4 有 $4! = 24$ 个元素,列举如下

e	(12)	(13)	(14)	(23)	(24)
(34)	(123)	(132)	(124)	(142)	(134)
(143)	(234)	(243)	(1234)	(1243)	(1342)
(1324)	(1423)	(1432)	(12)(34)	(13)(24)	(14)(23)

其中 $e = I = (1) = (2) = (3) = (4)$.

定理2.7.3

设 X 为有穷非空集, 则 X 上长为 l 的轮换可表示成 $l-1$ 个对换的乘积, 因而每个 $\sigma \in S(X)$ 可表示成一些对换的乘积.

证明　设 $(a_1\,a_2\cdots a_l)$ 是 X 上长为 l 的轮换, 则

$$(a_1\,a_2\cdots a_l)=(a_1\,a_l)(a_1\,a_{l-1})\cdots(a_1\,a_2)\text{（从右开始）}$$

□

定义2.7.3

对于 $\sigma\in S_n$, 如果 $1\leqslant i<j\leqslant n$, 但是 $\sigma(i)>\sigma(j)$, 则说关于 σ 有个**逆序**.σ 的逆序总个数记为

$$N_\sigma=|\{\langle i,j\rangle : i<j,\,\sigma(i)>\sigma(j)\}|$$

如果 N_σ 为奇（偶）数, 则称 σ 为**奇（偶）置换**.即

$$\operatorname{sgn}(\sigma)\triangleq(-1)^{N_\sigma}=\begin{cases}1 & \sigma\text{为偶置换}\\ -1 & \sigma\text{为奇置换}\end{cases}$$

$$\prod_{1\leqslant i<j\leqslant n}(\sigma(j)-\sigma(i))=(-1)^{N_\sigma}\prod_{1\leqslant i<j\leqslant n}(j-i)$$

定理2.7.4

(1) 对 $\sigma,\tau\in S_n$, $\operatorname{sgn}(\sigma\tau)=\operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

(2) 对 $\sigma\in S_n$, σ 为偶置换$\Leftrightarrow\sigma$ 为偶数个对换的乘积.（对奇置换类同）

证明　(1) 设 $1\leqslant k<l\leqslant n$, 则

$$\begin{aligned}\prod_{1\leqslant i<j\leqslant n}(\sigma(j)-\sigma(i))&=(\sigma(l)-\sigma(k))\times\prod_{\substack{1\leqslant i<j\leqslant n\\ \{i,j\}\cap\{k,l\}=\emptyset}}(\sigma(j)-\sigma(i))\\&\quad\times\prod_{k<i<l}(\sigma(i)-\sigma(k))\,(\sigma(l)-\sigma(i))\\&\quad\times\prod_{\substack{i<k\\ \text{或}i>l}}(\sigma(k)-\sigma(i))\,(\sigma(i)-\sigma(l))\\&=(\sigma(l)-\sigma(k))\times\prod_{\substack{1\leqslant i<j\leqslant n\\ \{i,j\}\cap\{k,l\}=\emptyset}}(\sigma(j)-\sigma(i))\\&\quad\times(-1)^{l-k-1}\prod_{i\neq k,l}(\sigma(i)-\sigma(k))(\sigma(i)-\sigma(l))\end{aligned}$$

如果将 $\sigma(k)$ 与 $\sigma(l)$ 对调后, $\prod_{1\leqslant i<j\leqslant n}(\sigma(j)-\sigma(i))$ 符号改变.
注意到 $\prod_{1\leqslant i<j\leqslant n}\big((\sigma(kl))(j)-(\sigma(kl))(i)\big)$ 等于把

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

中 $\sigma(k)$ 与 $\sigma(l)$ 对调, 于是 $\mathrm{sgn}(\sigma(kl))=-\mathrm{sgn}(\sigma)$. 对于 $\forall\tau\in S_n$, 有
$\tau=(i_1j_1)\cdots(i_rj_r)$. 于是

$$\mathrm{sgn}(\sigma\tau)=\mathrm{sgn}(\sigma(i_1j_1)\cdots(1_rj_r))=(-1)^r\mathrm{sgn}(\sigma)$$

令 $\sigma=I$, 可得 $\mathrm{sgn}(\tau)=(-1)^r$, 所以 $\mathrm{sgn}(\sigma\tau)=\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)$.
(2) 由(1)知 τ 是 r 个对换的乘积 $\Leftrightarrow\mathrm{sgn}(\tau)=(-1)^r$. 即证得结论. □

推论2.7.1

设 $n\geqslant1$, 则 $A_n=\{\sigma\in S_n:\sigma\text{为偶置换}\}\trianglelefteq S_n$, 且 $n\geqslant2$ 时, $|S_n/A_n|=2$, 从而

$$A_n=\frac{n!}{2}\quad S_n/A_n\cong\{\pm1\}=C_2$$

证明　$\mathrm{sgn}:\sigma\mapsto\mathrm{sgn}(\sigma)\in\{\pm1\}$ 是 S_n 到 C_2 的满同态.同态核为

$$A_n=\{\sigma\in S_n:\mathrm{sgn}(\sigma)=1\}$$

故由同态基本定理(33页)知

$$S_n/A_n\cong\{\pm1\}$$ □

例2.7.2

$$\det(a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}=\sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)a_{1\sigma(1)}\cdots a_{n\sigma(n)}$$

例2.7.3

$i\notin\{j_1,\ldots,j_l\}$ 时, $(j_1\cdots j_l)=(i\,j_1\cdots j_l)(i\,j_l)$, 即$(j_1\cdots j_l)$ 可拆换成含 i 的对换乘积.又注意到 $(j_m\,j_n)=(j_m\,i)(j_n\,i)(j_m\,i)$, 所以

$$S_n=\langle(1\,2),(1\,3),\ldots,(1\,n)\rangle$$

又

$$(1\,m)=(m{-}1\,m)(m{-}2\,m{-}1)\cdots(2\,3)(1\,2)(2\,3)\cdots(m{-}1\,m)$$
$$(i\,i{+}1)=(1\,2\,3\cdots n)(i{-}1\,i)(1\,2\,3\cdots n)^{-1}$$

所以 $S_n = \langle (1\,2), (1\,2\,3\cdots n)\rangle$
设 $2 \leqslant i, j \leqslant n$, 且 $i \neq j$ 时, A_n 的元素均可表示成偶数个形如 $(1\,i)$ 的对换的乘积, 因为

$$(1\,i)(1\,j) = (1\,j\,i) = (1\,2\,i)^{-1}(1\,2\,j)(1\,2\,i)$$

又

$$((1\,2)(1\,i))^{-1} = (1\,i)(1\,2) = (1\,2\,i)$$

故

$$A_n = \langle (1\,2\,3), (1\,2\,4), \ldots, (1\,2\,n)\rangle$$

定理2.7.5

(1) $S_n' = A_n$

(2) $n \leqslant 3$ 时, $S_n'' = A_n' = \{e\}$

(3) $S_4'' = A_4'$ 为 *Klein* 四元群, $K = \{e, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$, $S_4''' = A_4'' = K' = \{e\}$

证明 (1) S_n/A_n 为 2 阶循环群, 从而为 *Abel* 群, 故由定理2.6.2(58页)知 $A_n \supseteq S_n'$.
再证 $A_n = \langle (1\,2\,3), \ldots, (1\,2\,n)\rangle \subseteq S_n'$, 即证 $2 < i \leqslant n$ 时, $(1\,2\,i) \in S_n'$ 即可.注意到

$$\begin{aligned}
(1\,2\,i) &= (1\,i\,2)^2 \\
&= (1\,2)(1\,i)(1\,2)(1\,i) \\
&= (1\,2)^{-1}(1\,i)^{-1}(1\,2)(1\,i) \\
&= [(1\,2)(1,i)] \in S_n'
\end{aligned}$$

即证.

(2) $n \leqslant 3$ 时, $|A_n| \leqslant \frac{3!}{2} = 3$, 注意到 $2, 3$ 都为素数, 所以A_n 为循环群, 从而为 *Abel* 群, 则 $S_n'' = A_n' = \{e\}$.

(3)$|A_4| = \frac{4!}{2} = 2^2 * 3$, 由推论2.6.3(64页)知 A_4 可解, $A_4' \neq A_4$.
令

$$a = (1\,2)(3\,4) \quad b = (1\,3)(2\,4) \quad c = (1\,4)(2\,3)$$

易见 $a^2 = b^2 = c^2 = e$, 且

$$ab = ba = c \quad ac = ca = b \quad bc = cb = a$$

则 K 为 Klein 四元群。注意到

$$(1\,2)(3\,4) = (1\,2\,3)^{-1}(1\,2\,4)^{-1}(1\,2\,3)(1\,2\,4) = [(1\,2\,3)(1\,2\,4)] \in A_4'$$

类似地有 $b=[(1\,3\,2)(1\,3\,4)]\in A_4'$, $c=[(1\,4\,2)(1\,4\,3)]\in A_4'$。故 $K\subseteq A_4'<A_4$. 注意到

$$[A_4:K]=\frac{12}{4}=3=[A_4:A_4'][A_4':K]$$

因为 $[A_4:A_4']>1$, 所以 $[A_4':K]=1$, 即 $A_4'=K$, 注意到 K 为 Abel 群, 所以

$$S_4'''=A_4''=K'=\{e\}$$

□

定理2.7.6 (Galois)

对于 $n\geqslant 5$

(1)　A_n 是单群

(2)　S_n 与 A_n 都不是可解群

证明　(1) 先证明 (1) $\Rightarrow$ (2) , 因为 $(1\,2\,3)(1\,2\,4)\neq(1\,2\,4)(1\,2\,3)$, 故 A_n 不是 Abel 群, 所以 $A_n\trianglerighteq A_n'\neq\{e\}$, 因为 A_n 是单群[3], 且由定理2.7.5的(1)知 $S_n'=A_n$, 所以

$$A_n'=A_n\Rightarrow S_n^{(m+1)}=A_n^{(m)}\neq\{e\}$$

(2) 直接证明(2), 任给 $3\leqslant i\leqslant n$, 由于 $n\geqslant 5$, 可取不同于 $1,2,i$ 的另两个不同元 j 与 k. 注意到

$$(1\,2\,i)=(1\,2\,k)(1\,i\,j)(1\,k\,2)(1\,j\,i)=[(1\,k\,2)(1\,j\,i)]\in A_n'$$

故 $A_n=\langle(1\,2\,3),\dots,(1\,2\,n)\rangle\subseteq A_n'\subseteq A_n$, 所以 $A_n'=A_n$. 从而

$$S_n^{(m+1)}=A_n^{(m)}=A_n\neq\{e\}$$

由定理2.6.4(59页)知 S_n, A_n 不可解.

(3) 直接证明(1). 设 $H\trianglelefteq A_n$ 且 $H\neq\{e\}$. 要证

$$H=A_n=\langle(1\,2\,3),\dots,(1\,2\,n)\rangle$$

分为两步进行。第一步证明 H 中含有长度为 3 的轮换。设 $X=\{1,2,\dots,n\}$. H 作用在 X 上, 即 $\sigma\in H$, $x\in X$ 时

$$\sigma\circ x=\sigma(x)\in X$$

[3] 如果 $|G|>1$, 且 G 的正规子群只有 $\{e\}$ 与 G, 则说 G 为单群.

可以验证 $\circ$ 为群作用[4]. 对 $\sigma \in H$,

$$\operatorname{Fix}(\sigma)=\{x\in X:\sigma(x)=x\}=\{1\leqslant i\leqslant n:\sigma(i)=i\}$$

取 $\tau\in H\backslash\{e\}$, 使 $|\operatorname{Fix}(\tau)|$ 最大. 因为 $\tau\neq I$, 所以 $|\operatorname{Fix}(\tau)|\neq n-1,n$.
如果 $|\operatorname{Fix}(\tau)|=n-2$, 则 τ 为对换, 这与 $\tau\in H\subseteq A_n$ 矛盾[5].
如果 $|\operatorname{Fix}(\tau)|=n-3$, 则 τ 为长度为 3 的轮换.
下面用反证法证明 $|\operatorname{Fix}(\tau)|=n-3$. 假设 $|\operatorname{Fix}(\tau)|\leqslant n-4$, 考虑 τ 的轮换分解式, 有两种情形
(i) τ 的轮换分解式中有长度至少为 3 的轮换 $(i_1\,i_2\,i_3\cdots)$
(ii) τ 的轮换分解式只有对换 $\tau=(i_1\,i_2)(i_3\,i_4)\cdots$
考虑 (i) 的情形, 因为 τ 为偶置换, 所以至少有 5 个动点, 不妨设另外两个为 i_4,i_5. 在(ii)中可取 $i_5\in\{1,\dots,n\}$. 取 $\sigma=(i_3\,i_4\,i_5)$, 则 σ 为偶置换. 可验证

$$\sigma\tau\sigma^{-1}\overset{\text{(i)}}{=}\{i_1\,i_2\,i_4\cdots\}\neq\tau$$
$$\sigma\tau\sigma^{-1}\overset{\text{(ii)}}{=}\{i_1\,i_2\}\{i_4\,i_5\}\cdots\neq\tau$$

所以无论哪种情况下 $\tau'=\tau^{-1}\sigma\tau\sigma^{-1}=[\tau,\sigma^{-1}]\neq e$.
由于 $\tau\in H\trianglelefteq A_n$, $\sigma\in A_n$, 所以 $\sigma\tau\sigma^{-1}\in H$, 故 $\tau'=\tau^{-1}\sigma\tau\sigma^{-1}\in H$. 下证

$$|\operatorname{Fix}(\tau')|>|\operatorname{Fix}(\tau)|$$

对 $j\in\{1,\dots,n\}\backslash\{i_1,i_2,i_3,i_4,i_5\}$, 如果 j 为 τ 的不动点, 则

$$\begin{aligned}\tau'(j)&=\tau^{-1}\sigma\tau\sigma^{-1}(j)\\&=\tau^{-1}\sigma\tau(j)\\&=\tau^{-1}(j)\\&=j\end{aligned}$$

所以 j 也为 τ' 的不动点. 又因为 $\sigma\tau\sigma^{-1}(i_1)=i_2$, 从而

$$\tau'(i_1)=\tau^{-1}\sigma\tau\sigma^{-1}(i_1)=\tau^{-1}(i_2)=i_1$$

即 $i_1\in\operatorname{Fix}(\tau')\backslash\operatorname{Fix}(\tau)$.
在 (i) 中, $i_1,\dots,i_5\notin\operatorname{Fix}(\tau)$, 所以 $\operatorname{Fix}(\tau')$ 至少比 $\operatorname{Fix}(\tau)$ 多一个 i_1.
在 (ii) 中, $i_1,\dots,i_4\notin\operatorname{Fix}(\tau)$, 虽然$i_5$ 是否属于 $\operatorname{Fix}(\tau)$ 未知. 可是注意到

$$\sigma\tau\sigma^{-1}\overset{\text{(ii)}}{=}\{i_1\,i_2\}\{i_4\,i_5\}\cdots$$

可得

$$\tau'(i_2)=\tau^{-1}\left(\sigma\tau\sigma^{-1}(i_2)\right)=i_2$$

[4] $\circ$ 为群作用即满足(1) $e\circ x=x$ (2) $(g_1g_2)\circ x=g_1\circ(g_2\circ x)$.
[5]因为对换为奇置换, 注意到 A_n 定义即得矛盾.

所以 $i_1, i_2 \in \mathrm{Fix}(\tau')$, 从而 $|\mathrm{Fix}(\tau')| > |\mathrm{Fix}(\tau)|$.

第二步：证明 H 包含所有长度为 3 的轮换, 如此

$$A_n \subseteq \langle (1\,2\,3), \ldots, (1\,2\,n) \rangle \subseteq H$$

由第一步知 H 中有长度为 3 的轮换, 不妨设为 $\tau = (i_1\, i_2\, i_3)$, 由于 $n \geqslant 5$, 所以可再取两不同点 $i_4, i_5 \neq i_1, i_2, i_3$. 任给一个 3 - 轮换 $(j_1\, j_2\, j_3)$, 做 $\sigma \in S_n$, 使

$$\sigma(i_1) = j_1 \quad \sigma(i_2) = j_2 \quad \sigma(i_3) = j_3$$

让 $\sigma' = \sigma(i_4\, i_5)$, 故 σ', σ 中必有一个为偶置换, 又因为 $H \trianglelefteq A_n$, 则

$$\begin{aligned}\sigma'(i_1\, i_2\, i_3)(\sigma')^{-1} &= \sigma(i_4\, i_5)(i_1\, i_2\, i_3)(i_4\, i_5)^{-1}\sigma^{-1} \\ &= \sigma(i_1\, i_2\, i_3)\sigma^{-1} = (j_1\, j_2\, j_3)^{\,6} \in H\end{aligned}$$

从而 H 包含所有长度为 3 的轮换. 故综上可得 A_n 为单群. □

有限单群的分类：无穷簇, $\mathbb{Z}_p$ (p 为素数), A_n ($n \geqslant 5$), Ree群, 散在单群(26个).

作业：

(1) 设 $\sigma = (1\,2\,3\,4)(5\,6\,7)$, $\tau = (2\,5\,7)(1\,3\,4\,6)$, 求 $\sigma\tau\sigma^{-1}, \tau\sigma\tau^{-1}$, 并把它们写成不相交轮换的乘积.

(2) 证明：

  (i) $n \neq 2$ 时, $Z(S_n) = \{e\}$, $Z(S_2) = S_2$.

  (ii) $n \neq 3$ 时, $Z(A_n) = \{e\}$, $Z(A_3) = A_3$.

(3) 代数学引论第99页的39题

[6]这步可自己验证, 分别讨论 (1) $j \neq j_1, j_2, j_3$, (2) $j = j_1, j_2, j_3$.

2.8　群的直积与 Abel 群结构

定义2.8.1

设 $G_1,\cdots,G_n$ 为群, 让

$$G=G_1\times\cdots\times G_n=\{x=\langle x_1,x_2\ldots,x_n\rangle : x_i\in G_i\}$$

对 $x=\langle x_1,x_2\ldots,x_n\rangle$, $y=\langle y_1,y_2\ldots,y_n\rangle\in G$, 定义

$$x\circ y=\langle x_1y_1,x_2y_2,\ldots,x_ny_n\rangle\in G$$

易验证 $(x\circ y)\circ z=x\circ(y\circ z)$, 让 $e=\langle e_1,e_2,\ldots,e_n\rangle$, 其中 e_i 为 G_i 的单位元, 则 $xe=x=ex$. x 有逆元 x^{-1}

$$x^{-1}=\langle x_1^{-1},x_2^{-1},\ldots,x_n^{-1}\rangle$$

群 G 叫做 $G_1,\ldots,G_n$ 的**外直积**.

例2.8.1

$C_2=\{\pm1\}$, 则 $C_2\times C_2=\{\langle x,y\rangle : x,y\in C_2\}$, 即

$$C_2\times C_2=\{\langle 1,1\rangle,\langle 1,-1\rangle,\langle -1,1\rangle,\langle -1,-1\rangle\}$$

注意到 $C_2\times C_2$ 为 Kelin 四元群, 即 Kelin 四元群$\cong C_2\times C_2$.

定理2.8.1

设 $G_1,\cdots,G_n$ 为群, G 为它的外直积, 让

$$G_i^*=\{\langle e_1,\ldots,e_{i-1},x_i,e_{i+1},\ldots,e_n\rangle : x_i\in G_i\}$$

则

(1) $G_i\cong G_i^*\trianglelefteq G$, 且 $G_i^*\cap G_1^*\cdots G_{i-1}^*G_{i+1}^*\cdots G_n^*=\{e\}$.

(2) $G_1^*G_2^*\cdots G_n^*=G$.

证明 (1) 作 $\sigma: x \in G_i \mapsto \langle e_1, \dots, e_{i-1}, x, e_{i+1}, \dots e_n\rangle \in G$. 因为

$$\begin{aligned}\sigma(xy) &= \langle e_1, \dots, e_{i-1}, xy, e_{i+1}, \dots e_n\rangle \\ &= \langle e_1, \dots, e_{i-1}, x, e_{i+1}, \dots e_n\rangle \circ \langle e_1, \dots, e_{i-1}, y, e_{i+1}, \dots e_n\rangle \\ &= \sigma(x) \circ \sigma(y)\end{aligned}$$

所以 σ 为群同态且为单射, 所以 $\ker\sigma = \{e_i\}$, 故由同态基本定理(33页)知

$$G_i/\{e_i\} = \mathrm{Im}\sigma = G_i^*$$

因为 $G_i \cong G_i/\{e_i\}$, 所以 $G_i \cong G_i^*$.
任取 $y \in G$, 不妨设 $y = \langle y_1, y_2 \dots, y_n\rangle \in G$

$$\begin{aligned}&y\langle e_1, \dots, e_{i-1}, x, e_{i+1}, \dots e_n\rangle y^{-1} \\ =\ & y = \langle y_1, y_2 \dots, y_n\rangle \circ \langle e_1, \dots, e_{i-1}, x, e_{i+1}, \dots e_n\rangle \circ \langle y_1^{-1}, y_2^{-1} \dots, y_n^{-1}\rangle \\ =\ & \langle e_1, \dots, e_{i-1}, y_i x y_i^{-1}, e_{i+1}, \dots e_n\rangle \in G_i^*\end{aligned}$$

故 $G_i^* \trianglelefteq G$.
设 $x \in G_i^* \bigcap G_1^* \cdots G_{i-1}^* G_{i+1}^* \cdots G_n^*$, 由于 $x \in G_i^*$, 所以 $j \neq i$ 时, $x_j = e_j$, 又由于

$$x \in \prod_{j \neq i} G_j^*$$

所以 $x_i = e_i$, 故 $x = e$.

(2) 任取 $x = \langle x_1, x_2 \dots, x_n\rangle \in G$, 注意到

$$\begin{aligned}x &= \langle x_1, x_2 \dots, x_n\rangle \\ &= \langle x_1, e_2, \dots, e_n\rangle \circ \langle e_1, x_2, \dots, e_n\rangle \circ \cdots \circ \langle e_1, e_2, \dots, x_n\rangle \in G_1^* G_2^* \cdots G_n^*\end{aligned}$$

即得 $G \subseteq G_1^* G_2^* \cdots G_n^*$, 又由于 $G_i^* \subseteq G$, 故 $G_1^* G_2^* \cdots G_n^* \subseteq G$, 即证. □

引理2.8.1

设 $H \trianglelefteq G$, $K \trianglelefteq G$ 且 $H \cap K = \{e\}$, 证明 $\forall h \in H, k \in K$ 时, $hk = kh$.

证明 $\forall h \in H$, $k \in K$, 因为

$$hk = kh \Leftrightarrow k^{-1}hkh^{-1} = e$$

要证明引理, 我们只需证明 $k^{-1}hkh^{-1} = e$ 即可. 因为 $K \trianglelefteq G$, 所以 $hkh^{-1} \in K$, 即 $k^{-1}hkh^{-1} \in K$, 同理因为 $H \trianglelefteq G$, 所以 $k^{-1}hk \in H$, 即 $k^{-1}hkh^{-1} \in H$. 故综上可得 $k^{-1}hkh^{-1} \in H \cap K$, 即 $k^{-1}hkh^{-1} = e$, 即 $hk = kh$. □

定理2.8.2

设 $G_1,\dots,G_n$ 为 G 的正规子群, 则下列几条相互等价

(1) 对 $i=1,\dots,n$ 有 $G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n=\{e\}$.

(2) 每个 $x\in G$ 至多可用一种方式表成 $x_1x_2\cdots x_n$, 其中 $x_i\in G$.

(3) e 表示成 $x_1x_2\cdots x_n\,(x_i\in G_i)$ 时, $x_i=e$.

证明 (1) $\Rightarrow$ (2): 设 $x_1x_2\cdots x_n=y_1y_2\cdots y_n$, 其中 $x_i,y_i\in G_i$, 则

$$(x_1x_2\cdots x_{n-1})^{-1}(y_1y_2\cdots y_{n-1})=x_ny_n^{-1}\in G_1\cdots G_{n-1}\cap G_n=\{e\}$$

所以 $x_n=y_n$, 则 $x_1x_2\cdots x_{n-1}=y_1y_2\cdots y_{n-1}$, 类似地利用上法可得

$$x_i=y_i\,(i=1,2,\dots,n).$$

(2) $\Rightarrow$ (3): 注意到 $e=e\cdots e$, $e=x_1\cdots x_n$, 所以由(2)可知 $x_i=e$.

(3) $\Rightarrow$ (1): 设 $x_i=x_1\cdots x_{i-1}x_{i+1}\cdots x_n$, 其中 $x_i\in G_i$, 则

$$x_i\in G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n$$

由于 $G_j\trianglelefteq G$, 所以 $x_j'=x_i^{-1}x_jx_i\in G_j$, 即 $x_i^{-1}x_j=x_j'x_i^{-1}$. 于是

$$\begin{aligned}e=x_i^{-1}x_i&=x_i^{-1}x_1\cdots x_{i-1}x_{i+1}\cdots x_n\\&=x_1'x_i^{-1}x_2\cdots x_{i-1}x_{i+1}\cdots x_n\\&=x_1'x_2'\cdots x_{i-1}'x_i^{-1}x_{i+1}\cdots x_n\end{aligned}$$

由(3)知 $x_1'=x_2'=\cdots=x_{i-1}'=x_i^{-1}=x_{i+1}=\cdots=x_n=e$, 从而 $x_i=e$, 故

$$G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n=\{e\}$$ □

定义2.8.2

设 G 为群, $G_1,\dots,G_n$ 为 G 的正规子群. 如果 G 的每个元可唯一表成 $x_1x_2\cdots x_n\,(x_i\in G_i)$ 的形式 [1], 则说 G 是 $G_1,G_2,\dots,G_n$ 的**内直积**.

P.S. 如果让 $G=G_1\times\cdots\times G_n$, 由定理2.8.1(74页)知 $G_1\times\cdots\times G_n$ 是 $G_1^*,\dots,G_n^*$ 的内直积.

[1]注意到定理2.8.2可得 $G_1G_2\cdots G_n=G$ 且 $G_i\bigcap G_1\cdots G_{i-1}G_{i+1}\cdots G_n=\{e\}$.

定理2.8.3

设群 G 是其正规子群 $G_1,\ldots,G_n$ 的内直积, 则 $G\cong G_1\times G_2\times\cdots\times G_n$

证明 定义 $G_1\times G_2\times\cdots\times G_n$ 到 G 的映射 σ 如下

$$\sigma(\langle x_1,x_2,\ldots,x_n\rangle)=x_1x_2\cdots x_n$$

由于 G 为 $G_1,\ldots,G_n$ 的内直积, 故 σ 为双射.
对于 $x=\langle x_1,x_2\ldots,x_n\rangle$, $y=\langle y_1,y_2\ldots,y_n\rangle\in G_1\times G_2\times\cdots\times G_n$

$$\sigma(xy)=(x_1y_1)(x_2y_2)\cdots(x_ny_n)$$

当 $i\neq j$ 时,

$$G_i\cap G_j\subseteq G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n=\{e\}$$

由引理2.8.1(75页)知, $y_ix_j=x_jy_i$, $y_iy_j=y_jy_i$. 如此

$$\sigma(xy)=x_1x_2\cdots x_ny_1y_2\cdots y_n=\sigma(x)\sigma(y)$$

故 σ 为同态, 且因为 σ 为双射, 故 $G\cong G_1\times G_2\times\cdots\times G_n$. □

推论2.8.1

设 $H\trianglelefteq G$, $K\trianglelefteq G$, 如果 $|H||K|=|G|$, $H\cap K=\{e\}$, 则 $G\cong H\times K$.

证明 因为 $HK\leqslant G$, $H\trianglelefteq G$, 所以 $H\trianglelefteq HK$, 同理 $K\trianglelefteq HK$, 又因为

$$H\cdot K=HK\quad H\cap K=\{e\}$$

故 HK 为 H 与 K 的内直积.从而 $HK\cong H\times K$. 故

$$|HK|=|H\times K|=|H|\times|K|\,[2]=|G|$$

又因为 $HK\leqslant G$, 所以 $HK=G$, 从而 $G\cong H\times K$ □

[2] $|H\times K|=|H|\times|K|$ 是因为由定理2.8.2知任意的 $x\in HK$ 均可唯一地表示为 $hk\,(h\in H,k\in K)$ 的形式.

定义2.8.3

对于有限群 G, 使 $\forall x\in G\,(X^n=e)$ 成立的最小正整数 n 叫 G 的**幂指数**, 记为 $\exp(G)$.
实际上 $\exp(G)$ 是 $o(x)\,(x\in G)$ 的最小公倍数, 对于 n 阶循环群 C_n, $\exp(C_n)=n$.

$$\exp(C_{n_1}\times C_{n_2}\times\cdots\times C_{n_k})=[n_1,n_2,\ldots,n_k]\,(n_1,n_2,\ldots,n_k\text{的最小公倍数})$$

例2.8.2

设 p 为素数, 使决定出所有不同构的 p^2 阶群.
解: 设 G 为 p^2 阶群, 如果 G 不是循环群, 任取 $a\in G\backslash\{e\}$, 因为 $o(a)\mid p^2$ 且 $\langle a\rangle\neq G$, 所以 $o(a)=p$. 取 $b\in G\backslash\langle a\rangle$, 则同理可得 $o(b)=p$, 因为 $\langle a\rangle\cap\langle b\rangle$ 为 $\langle a\rangle$ 的子群, 且 $\langle a\rangle\cap\langle b\rangle\neq\langle a\rangle$, 所以 $\langle a\rangle\cap\langle b\rangle=\{e\}$ [3]. 则

$$|\langle a\rangle||\langle b\rangle|=p^2=|G|$$

由推论2.8.1(77页)知 $G\cong\langle a\rangle\times\langle b\rangle$.
下面证明 $G=\langle a\rangle\langle b\rangle$ 为 $\langle a\rangle$ 与 $\langle b\rangle$ 的内直积.
如果 $H\trianglelefteq G$, $K\leqslant G$, 由第二同构定理(50页)知 $HK/H\cong K/(H\cap K)$, 所以

$$(\langle a\rangle\langle b\rangle)/\langle a\rangle\cong\langle b\rangle/(\langle a\rangle\cap\langle b\rangle)$$

因为 $\langle a\rangle\cap\langle b\rangle=\{e\}$, 所以

$$|\langle a\rangle\langle b\rangle|=|\langle a\rangle||\langle b\rangle|=p^2=|G|$$

则 $G=\langle a\rangle\langle b\rangle$ 为 $\langle a\rangle$ 与 $\langle b\rangle$ 的内直积. 通过上述说明, 我们已证 G 如果不是循环群, 则 $G\cong C_p\times C_p$.
又因为 $C_p\times C_p$ 中无 p^2 阶元, 故 $C_p\times C_p\ncong C_{p^2}$.

定理2.8.4

设 G 为有限 Abel 群, 则

$$\exp(G)=\max_{g\in G}o(g)$$

证明　取 $a\in G$, 使 $o(a)=\max_{g\in G}o(g)$. 下面证明 $x\in G$ 时, $o(x)\mid o(a)$.
假如有 $x\in G$, 使 $o(x)\nmid o(a)$, 于是有素数 p, 使

$$\alpha=\mathrm{ord}_p(o(a))<\beta=\mathrm{ord}_p(o(x))$$ [4]

[3] 注意到素数阶循环群 G 的子群只有它自己和 $\{e\}$.
[4] ord_p 的定义在43页的定义2.3.1

记

$$o(a)=p^{\alpha}m\,(p\nmid m)\quad o(x)=p^{\beta}n\,(p\nmid n)$$

则 $o(a^{p^{\alpha}})=m$ 与 $o(x^n)=p^{\beta}$ 互素, 故由定理1.4.1的(2)(27页)知

$$o(a^{p^{\alpha}}\cdot x^n)=p^{\beta}m>p^{\alpha}m=o(a)$$

这与 a 的选取矛盾. □

推论2.8.2

设 $n_1,\ldots,n_k$ 为两两互素的正整数, 则 $C_{n_1}\times C_{n_2}\times\cdots\times C_{n_k}\cong C_{n_1n_2\cdots n_k}$.

证明　让 $G=C_{n_1}\times C_{n_2}\times\cdots\times C_{n_k}$, 则 $\exp(G)=[n_1,n_2,\ldots,n_k]=n_1n_2\cdots n_k$. 同时由 G 的定义可知

$$|G|=|C_{n_1}||C_{n_2}|\cdots|C_{n_k}|=n_1n_2\cdots n_k$$

此外由 G 的定义也可知 G 为 Abel 群, 依定理2.8.4知, 有 $a\in G$, 使得 $o(a)=\exp(G)=|G|$, 故 $G=\langle a\rangle$ 为循环群. □

定理2.8.5

设 G 为有限 Abel 群, $|G|=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}$, 其中 $p_1,\ldots,p_n$ 为不同的素数, 让 G_i 为 G 的 Sylow p_i-子群的子群（因为 Abel 群的子群均为正规子群, 所以由推论2.3.1（45页）知 G_i 唯一.）, 则

$$G\cong G_1\times G_2\times\cdots\times G_n$$

证明　由定理2.8.3(77页)知只要证群 G 是其 Sylow p_i-子群 $G_1,\ldots,G_n$ 的内直积即可, 即

$$\begin{cases}G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n=\{e\}\\ G_1G_2\cdots G_n=G\end{cases}$$

假设 $H\trianglelefteq G$, $K\trianglelefteq G$, 由第二同构定理(50页)知 $HK/H\cong K/(H\cap K)$, 从而

$$|HK|=|H|[K:H\cap K]\;\Big|\;|H||K|$$

于是

$$|G_1\cdots G_{i-1}G_{i+1}\cdots G_n|\;\Big|\;\prod_{j\neq i}|G_j|=\prod_{j\neq i}p_j^{\alpha_j}$$

注意到

$$G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n\leqslant G_i$$
$$G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n\leqslant G_1\cdots G_{i-1}G_{i+1}\cdots G_n$$

所以由 Lagrange 定理(22页)知

$$|G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n|\mid|G_i|$$
$$|G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n|\mid|G_1\cdots G_{i-1}G_{i+1}\cdots G_n|$$

所以

$$|G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n|\mid(|G_i|,|G_1\cdots G_{i-1}G_{i+1}\cdots G_n|)\mid(p_i^{\alpha_i},\prod_{j\neq i}p_j^{\alpha_j})=1$$

故 $G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n=\{e\}$, $G_1\cdot G_2\cdots G_n$ 是 $G_1,\ldots,G_n$ 的内直积, 于是由定理2.8.3(77页)知

$$G_1\cdot G_2\cdots G_n\cong G_1\times G_2\times\cdots\times G_n$$

从而

$$|G_1\cdot G_2\cdots G_n|=|G_1\times G_2\times\cdots\times G_n|=\prod_{i=1}^n|G_i|=\prod_{i=1}^n p_i^{\alpha_i}=|G|$$

故 $G=G_1\cdot G_2\cdots G_n\cong G_1\times G_2\times\cdots\times G_n$. □

注记：如果注意到 $x\in G_i\Leftrightarrow o(x)$ 为 p_i 的幂次 [5], 则若

$$x\in G_i\cap G_1\cdots G_{i-1}G_{i+1}\cdots G_n$$

则 $o(x)$ 为 p_i 幂次, 又

$$x=\prod_{j\neq i}x_j\text{ 且 }o(x_j)\mid p_j^{\alpha_j}$$

则 $x_j^{p_j^{\alpha_j}}=e$, 从而 $x^{\prod_{j\neq i}p_j^{\alpha_j}}=e$, 由裴蜀定理 [6]知

$$x^{(k,l)}=x^{ks+lt}$$

因为 $x^k=e$, $x^l=e$, 从而 $x^{(k,l)}=e$. 故

$$x=x^{(p_i^{\alpha_i},\prod_{j\neq i}p_j^{\alpha_j})}=e$$

[5](1) 如果 $x\in G_i$, 则 $\langle x\rangle\leqslant G_i$, 从而

$$o(x)=|\langle x\rangle|\mid|G_i|=p_i^{\alpha_i}$$

即 $o(x)$ 为 p_i 的幂次.
(2) 如果 $\langle x\rangle$ 是 p_i 子群, 由 Sylow 第二定理(44页)知 $\langle x\rangle$ 必包含在一个 Sylow p_i-子群中, 由于 G 为 Abel 群, 故 Sylow p_i-子群唯一, 且为 G_i

[6]裴蜀定理为：若 a,b 是整数, 且 $(a,b)=d$, 那么对于任意的整数 x,y, $ax+by$ 都一定是 d 的倍数, 特别地, 一定存在整数 x,y, 使 $ax+by=d$ 成立.

定理2.8.6 (有限 Abel 群结构定理)

设 G 是阶大于 1 的有限 Abel 群, 则

(1) 有唯一的一组正整数 $1 < n_1, \dots, n_k$, 满足 $n_i \mid n_{i+1}\,(i = 1, 2, \dots, k-1)$, 使

$$G \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_k}$$

(2) G 可唯一表成一些循环 p-群的直积. 如果 G 为 Abel p-群, 则

$$G = C_{p^{\alpha_1}} \times \cdots \times C_{p^{\alpha_k}}\ (\alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_k)$$

证明　可利用定理2.8.5来证, 但主要在于应用, 故证明略 □

例2.8.3

有多少个不同构的36阶 Abel 群?

解：因为 $36 = 2 \times 18 = 3 \times 12 = 6 \times 6$, 故由定理2.8.6的(1)知有四种不同的同构, 分别为

$$C_{36} \quad C_2 \times C_{18} \quad C_3 \times C_{12} \quad C_6 \times C_6$$

或者利用定理2.8.6的(2)知

$$\begin{aligned} C_2 \times C_2 \times C_3 \times C_3 &\cong C_6 \times C_6 \\ C_2 \times C_2 \times C_{3^2} &\cong C_2 \times C_{18} \\ C_{2^2} \times C_3 \times C_3 &\cong C_3 \times C_{12} \\ C_{2^2} \times C_{3^2} &\cong C_{36} \end{aligned}$$

定理2.8.7 (有限生成 Abel 群结构定理)

设 G 为有限生成的 Abel 群 [7], 则

$$\mathrm{Tor}(G) = \{a \in G : o(a) < \infty\}$$

为 G 的有限子群(挠子群), 且有唯一的 $r \in \mathbb{N}$, 使

$$G \cong \mathrm{Tor}(G) \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r\text{个}}$$

记 $r = \mathrm{r}(G)$, 为 G 的秩. [8]

证明　略　□

作业：

(1) 证明 4 阶群或者同构与 C_4 或同构与 $C_2 \times C_2$. (不要利用定理2.8.6, 证明方法同例2.8.2)

(2) 证明引理2.8.1, 即：设 $H \trianglelefteq G$, $K \trianglelefteq G$ 且 $H \cap K = \{e\}$, 证明 $\forall h \in H, k \in K$ 时, $hk = kh$.

[7] G 为有限生成的 Abel 群即有 $G_1, \ldots, G_r \in G$, 使 $G = \langle G_1, G_2, \ldots, G_r \rangle$.

[8] 这个定理在2011年的考试中没有考, 估计以后不会考.

第 3 章　环论

3.1　环的基本概念与性质

定义3.1.1

设 R 为非空集，其上有“加法”和“乘法”两种运算，如果 R 按加法构成 Abel 群,按乘法构成半群，且乘法对加法有分配律：

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

则说 R 按 $+$ 与 $\cdot$ 构成一个**环**，或说 $\langle R, +, \cdot\rangle$ 为**环结构**.
如果环 R 中乘法满足交换律，即对 $\forall a, b \in R$, $ab = ba$，则说 R 为**可换环**(或**交换环**).
如果环 R 中有元素 1 满足对 $\forall a \in R$, $1 \cdot a = a \cdot 1 = a$，则说 1 为环 R 的**（乘法）单位元**，R 是带**单位元的环（幺环）**.
对于环 R 中有非零元 a, b 满足 $ab = 0$，则说 R 有**零因子**，a 叫**左零因子**，b 叫**右零因子**.
无零因子的交换幺环称为**整环**.

例3.1.1

全体整数在整数加乘法下构成整环. $\mathbb{Z}$ 称为整数环.

例3.1.2

设 $m \in \mathbb{Z}^+$, $\mathbb{Z}/m\mathbb{Z} = \{\bar{a} = a + m\mathbb{Z} : a \in \mathbb{Z}\}$ 按剩余类加乘法构成环. 其中剩余类加乘法的定义

$$a + b \triangleq \overline{a+b} \quad \bar{a}\,\bar{b} \triangleq \overline{ab}$$

$\mathbb{Z}/m\mathbb{Z}$ 叫模 m 的剩余类.
易得 $\bar{a}(\bar{b}+\bar{c}) = \bar{a}\overline{b+c} = \overline{a(b+c)} = \overline{ab+ac} = \bar{a}\bar{b} + \bar{a}\bar{c}$ 　$\bar{1}\bar{a} = \bar{a}\bar{1} = \bar{a}$
当 $m > 1$ 时，如果 m 为合数，则存在 $1 < a, b < m$ 满足 $m = ab$，则 $\bar{a}, \bar{b} \neq 0$，但 $\bar{a}\bar{b} = \overline{m} = \bar{0}$，即 $\mathbb{Z}/m\mathbb{Z}$ 有零因子.
如果 $m = p$ 为素数,则 $\bar{a}\bar{b} = 0 \Rightarrow p \mid ab \Rightarrow p \mid a$ 或 $p \mid b \Rightarrow \bar{a} = 0$ 或 $\bar{b} = 0$，即 $\mathbb{Z}/m\mathbb{Z}$ 为整环.

例3.1.3

设 R 为环，$R[x] = \{\sum_{i=0}^{n} a_i x^i : a_0, \ldots, a_n \in R\}$ [1]，定义 $R[x]$ 中的加法和乘法如

[1] $R[x]$ 中的元素是多项式，而不是幂级数，即 n 有限.

下

$$\sum a_i x^i + \sum b_i x^i = \sum (a_i + b_i) x^i$$
$$(\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} b_j x^j) = \sum_k (\sum_{i+j=k} a_i b_j) x^k$$

$R[x]$ 叫 R 上的**一元多项式环**.
如果 R 有单位元 1, 则 $R[x]$ 有单位元 $1 = x^0$.
如果 R 交换, 则 $R[x]$ 也可换. 如果 R 无零因子, 则 $R[x]$ 也无零因子 [2], 即 R 为整环 $\Rightarrow R[x]$ 也是整环.

例3.1.4
设 R 为环, 让 $M_n(R) = \{n$ 阶方阵 $A = (a_{ij})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}} : a_{ij} \in R\}$ 按矩阵加乘法构成环, 如果 R 有单位元 1, 则 $M_n(R)$ 有单位元 I, R 无零因子时, $M_n(R)$ 可能有零因子. 例如

$$\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}\begin{pmatrix} 6 & 10 \\ -3 & -5 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

定理3.1.1

设 R 为环, 则

(1) 对 $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$

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

且对任何 $a \in R$, 有 $0a = a0 = 0$.

(2) 对 $m \in \mathbb{Z}$ 及 $a, b \in R$, 有 $a(mb) = (ma)b = m(ab)$.

(3) R 无零因子 $\Leftrightarrow R$ 中有如下消去律:

$$ab = ac \overset{a\neq 0}{\Longrightarrow} b = c \quad ba = ca \overset{a\neq 0}{\Longrightarrow} b = c$$

(4) R 为交换环时, 对 $a, b \in R$ 及 $n \in \mathbb{Z}^+$, 有

$$(a+b)^n = a^n + \sum_{k=1}^{n-1} \binom{n}{k} a^k b^{n-k} + b^n$$

[2] 这是因为如果假设 $R[x]$ 有零因子, 不妨设左零因子为 $\sum_{i=0}^{n} a_i x^i$, 右零因子为 $\sum_{j=0}^{m} b_j x^j$, 其中 $a_n, b_m \neq 0$, 则因为 $(\sum_{i=0}^{n} a_i x^i)(\sum_{j=0}^{m} b_j x^j) = 0$, 所以 x^i 的系数都为 0, 注意到 x^{n+m} 的系数为 $a_n b_m$, 则得到 $a_n b_m = 0$, 这与 R 无零因子矛盾.

证明 (1) 记 $a=\sum_{i=1}^m a_i$, 则

$$
\begin{aligned}
a\sum_{j=1}^n b_j &= a((b_1+b_2+\cdots++b_{n-1})b_n)\\
&= a(b_1+b_2+\cdots+b_{n-1})+ab_n\\
&= \cdots\\
&= ab_1+ab_2\cdots+ab_n\\
&= \sum_{j=1}^n ab_j
\end{aligned}
$$

同理可得

$$ab_j=a_1b_j+\cdots+a_mb_j$$

则因为 R 为 Abel 加法群, 可证得结论.
因为 $a(b-c)+ac=a(b-c+c)=ab$, 故 $a(b-c)=ab-ac$, 类似地
$(b-c)a=ba-ca$. 令 $b=c$ 得 $a\cdot 0=0$ $0\cdot a=0$.

(2)由(1)知 $a(0b)=a0=0=0(ab)$, $(0a)b=0b=0$, 故命题对 $m=0$ 成立.
$m=n\in\mathbb{Z}^+$ 时,

$$
\begin{aligned}
a(nb)&=a\underbrace{(b+\cdots+b)}_{n}=\underbrace{ab+\cdots+ab}_{n}=n(ab)\\
(na)b&=\underbrace{(a+\cdots+a)}_{n}b=\underbrace{ab+\cdots+ab}_{n}=n(ab)
\end{aligned}
$$

因为 $a(-b)+ab=a(-b+b)=a0=0$, 所以 $a(-b)=-ab$. 类似地, 因为
$(-a)b+ab=(-a+a)b=0b=0$, 所以 $(-a)b=-ab$, 故 $a(-b)=(-a)b=-ab$.
故可得 $a(-nb)=-a(nb)=-n(ab)$　$(-na)b=-(na)b=-n(ab)$, 所以
$a(-nb)=(-na)b=-n(ab)$.

(3) "$\Rightarrow$" : R 无零因子时

$$\begin{cases} ab=ac\\ a\neq 0\end{cases}\Rightarrow\begin{cases} a(b-c)=ab-ac=0\\ a\neq 0\end{cases}\xRightarrow{R\text{ 无零因子}} b-c=0 \text{ 即 } b=c$$

同理可证

$$\begin{cases} ba=ca\\ a\neq 0\end{cases}\Rightarrow b=c$$

"$\Leftarrow$" : 假如 R 中有所说的消去律, 如果 $a\neq 0$, 且 $ab=0$, 则由(2)知
$ab=0=a0$, 从而 $b=0$, 证得 R 无零因子.

(4) 对 n 进行归纳. $n=1$ 时, $(a+b)^1=a+b$ 显然成立.

设 $(a+b)^n = a^n + \sum_{k=1}^{n-1}\binom{n}{k}a^k b^{n-k} + b^n$ 成立, 则

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)(a^n + \sum_{k=1}^{n-1}\binom{n}{k}a^k b^{n-k} + b^n) \\
&= a^{n+1} + \sum_{k=1}^{n-1}\binom{n}{k}a^{k+1}b^{n-k} + ab^n + a^n b + \sum_{k=1}^{n-1}\binom{n}{k}a^k b^{n-k+1} + b^{n+1} \text{ [3]} \\
&= a^{n+1} + \sum_{k=1}^{n}\binom{n}{k}a^k b^{n+1-k} + \sum_{j=1}^{n}\binom{n}{j-1}a^j b^{n+1-j} + b^{n+1} \\
&= a^{n+1} + \sum_{k=1}^{n}\left[\binom{n}{k} + \binom{n}{k-1}\right]a^k b^{n+1-k} + b^{n+1}
\end{aligned}$$

注意到 $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$ [4], 即证得结论. □

定义3.1.2

设 R 为环, $\emptyset \neq S \subseteq R$, 如果 S 关于 $+$ 构成一个 Abel 群, 且对 $\cdot$ 封闭（在 S 上限制）, 则说 S 为 R 的**子环**, 记为 $S \leqslant R$. 即 $S \leqslant R$ 当且仅当 S 按加法也构成 R 的加法子群（即对 $\forall a, b \in S$, 都有$a \pm b \in S$）, 且对 $\forall a, b \in S$, $ab \in S$, 即等价于 S 对加减乘封闭.

R 中的最小子环 $0 = \{0\}$, R 中的最大子环 R.
如果 R 中有非零元 a 时, 且 R 如果有(乘法)单位元 1 , 则因为 $1a = a$, $0a = 0$, 则 $1 \neq 0$, 即加法单位元与乘法单位元不同.

[3]此步用到了 R 的交换性.

[4]

$$\begin{aligned}
\binom{n}{k} + \binom{n}{k-1} &= \frac{n\cdot(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k} + \frac{n\cdot(n-1)\cdots(n-k+2)}{1\cdot 2\cdots(k-1)} \\
&= \frac{n\cdot(n-1)\cdots(n-k+2)\cdot(n-k+1) + n\cdot(n-1)\cdots(n-k+2)\cdot k}{1\cdot 2\cdots k} \\
&= \frac{n\cdot(n-1)\cdots(n-k+2)(n-k+1+k)}{1\cdot 2\cdots k} \\
&= \frac{(n+1)\cdot n\cdots(n-k+2)}{1\cdot 2\cdots k} \\
&= \binom{n+1}{k}
\end{aligned}$$

定义3.1.3

设 R 为环, $\emptyset \neq I \subseteq R$, 如果 I 满足如下两点

(1) I 对加减法封闭.

(2) $r \in R,\ a \in I \Rightarrow ar, ra \in I$

则说 I 为环 R 的**理想**, 记为 $I \trianglelefteq R$.

注：环中“理想”作用类似于群中“正规子群”.

设 $I \trianglelefteq R$, 对 $a, b \in R$, 记 $a \equiv b \pmod I$, 表示 $a - b \in I$ (a与b模理想 I 同余), 下证这个关系是等价关系.

证明 (1) 自反性：因为取 $i \in I$, 且 I 对加减法封闭, 所以 $i - i = 0 \in I$, 故对于任意 R 中理想 I, 都有 $0 \in I$, 所以 $a - a = 0 \in I$, 故 $a \equiv b \pmod I$.

(2) 对称性：如果 $a \equiv b \pmod I$, 则 $a - b \in I$, 由于 I 对加减法封闭, 且 $0 \in I$, 所以 $b - a = 0 - (a - b) \in I$, 即 $b \equiv a \pmod I$.

(3) 传递性：如果 $a \equiv b \pmod I$, $b \equiv c \pmod I$, 则 $a - b \in I, b - c \in I$, 注意 $a - c = (a - b) + (b - c)$, 所以 $a - c \in I$, 故 $a \equiv c \pmod I$. □

此外我们还可得到：

性质3.1.1

$$\begin{cases} a \equiv b \pmod I \\ c \equiv d \pmod I \end{cases} \Rightarrow \begin{cases} a \pm c \equiv b \pm d \pmod I \\ ac \equiv bd \pmod I \end{cases}$$

这是因为 $(a \pm c) - (b \pm d) = (a - b) \pm (c - d) \in I$, $ac - bd = (a - b)c + b(c - d) \in I$.

定义3.1.4

记 a 所在的**模剩余类** $\bar{a} = \{r \in R : r \equiv a \pmod I\}$, 定义

$$\underline{\bar{a} + \bar{b} \triangleq \overline{a + b} \quad \bar{a}\bar{b} \triangleq \overline{ab}}$$

定义的合理性是因为性质3.1.1.
令 $R/I = \{\bar{a} = a + I : a \in R\}$, 称为 R 按理想 I 做成的**商环**.

3.2　环的同态与同构

定义3.2.1

设 σ 是从环 R 到环 $\overline{R}$ 的映射, 如果对 $\forall a,b\in R$ 都有

$$\sigma(a+b)=\sigma(a)+\sigma(b)$$
$$\sigma(ab)=\sigma(a)\sigma(b)$$

则称 σ 是环 R 到 $\overline{R}$ 的一个**同态**.
如果 σ 既是单射(满射)又是同态时成为**单(满)同态**.
如果 σ 是双射且为同态时, 称之为**同构**. 环 R 同构于环 $\overline{R}$ 是指存在 R 到 $\overline{R}$ 的同构 σ, 记为 $R\cong\overline{R}$.

定理3.2.1 (环的同态基本定理)

设 σ 是环 R 到环 $\overline{R}$ 的同态, 则

(1)　$\ker\sigma=\{a\in R:\sigma(a)=\bar{0}\ (\overline{R}\text{ 中加法单位元})\}\trianglelefteq R$, 即 $\ker\sigma$ 为 R 的理想.

(2)　$\mathrm{Im}\sigma=\{\sigma(a):a\in R\}=\sigma(R)\leqslant\overline{R}$, 即 $\mathrm{Im}\sigma$ 为 $\overline{R}$ 的子环.

(3)　$R/\ker\sigma\cong\mathrm{Im}\sigma$.

证明　(1) 因为 $\sigma(0)+\sigma(0)=\sigma(0+0)=\sigma(0)$, 所以 $0\in\ker\sigma=I$. 如果 $a,b\in I$, 则

$$\sigma(a\pm b)=\sigma(a)\pm\sigma(b)=\bar{0}\pm\bar{0}$$

从而 $a\pm b\in I$. 如果 $a\in I$, $r\in R$, 则

$$\sigma(ra)=\sigma(r)\sigma(a)=\sigma(r)\bar{0}=\bar{0}$$

类似可得 $\sigma(ar)=\bar{0}$, 所以 $ar,ra\in I$, 从而 $I\trianglelefteq R$.
(2) $\sigma(0)=\bar{0}$, 故 $\bar{0}\in\mathrm{Im}\sigma$, 对于任意 $\bar{a},\bar{b}\in\mathrm{Im}\sigma$, 必有 $a,b\in R$, 使得
$\bar{a}=\sigma(a)$, $\bar{b}=\sigma(b)$, 则

$$\bar{a}+\bar{b}=\sigma(a)+\sigma(b)=\sigma(a+b)\in\mathrm{Im}\sigma$$
$$\bar{a}\bar{b}=\sigma(a)\sigma(b)=\sigma(ab)\in\mathrm{Im}\sigma$$

故 $\mathrm{Im}\sigma\leqslant R$.

(3) 定义 $\bar{\sigma}: R/I \to \mathrm{Im}\sigma$ 如下：

$$\bar{\sigma}(a+I)=\sigma(a)$$

注意

$a+I=b+I \Leftrightarrow a-b\in I$ [1] $\Leftrightarrow \sigma(a-b)=\bar{0} \Leftrightarrow \sigma(a)=\sigma(b) \Leftrightarrow \bar{\sigma}(a+I)=\bar{\sigma}(b+I)$

故 $\bar{\sigma}$ 定义合理且为单射, 又因为 $\forall \bar{a}\in \mathrm{Im}\sigma$, 都有 $a\in R$, 满足 $\bar{a}=\sigma(a)$, 又 $\bar{\sigma}(a+I)=\sigma(a)=\bar{a}$, 所以 $\bar{\sigma}$为满射, 故 $\bar{\sigma}$ 为双射.
又因为

$$\begin{aligned}
\bar{\sigma}\left((a+I)+(b+I)\right) &= \bar{\sigma}(\bar{a}+\bar{b}) \\
&= \bar{\sigma}(\overline{a+b})\ {}^{2} \\
&= \bar{\sigma}(a+b+I) \\
&= \sigma(a+b) \\
&= \sigma(a)+\sigma(b) \\
&= \bar{\sigma}(a+I)+\bar{\sigma}(b+I) \\
\bar{\sigma}\left((a+I)(b+I)\right) &= \bar{\sigma}(ab+I)\ {}^{3} \\
&= \sigma(ab) \\
&= \sigma(a)\sigma(b) \\
&= \bar{\sigma}(a+I)\bar{\sigma}(b+I)
\end{aligned}$$

从而 $\bar{\sigma}$ 为同态, 又前面已证 $\bar{\sigma}$ 为双射, 所以 $\bar{\sigma}$ 为同构, 故 $R/I\cong \mathrm{Im}\sigma$. □

定理3.2.2

设 σ 是环 R 到环 $\overline{R}$ 的同态, $I=\ker\sigma$, 则

(1) R 的包含 I 的子环与 $\sigma(R)=\mathrm{Im}\sigma$ 的子环一一对应（即 $I\subseteq S\leqslant R$ 对应 $\sigma(S)\leqslant\sigma(R)$）.

(2) R 包含 I 的理想与 $\sigma(R)$ 的理想一一对应（即 $I\trianglelefteq R$, $J\trianglelefteq R$, $I\subseteq J$ 对应 $\sigma(J)\trianglelefteq\sigma(R)$）.

(3) $I\subseteq J\trianglelefteq R$ 时, $R/J\cong\sigma(R)/\sigma(J)$.

[1] $a+I=b+I\Leftrightarrow a-b\in I$ 是因为:(1) $a+I=b+I\Rightarrow a\in b+I\Rightarrow a-b\in I$
(2) $a-b\in I\Rightarrow a\equiv b\pmod I$, 所以对于 $\forall x\in a+I$, 因为 $x\equiv a\pmod I$, 故 $x\equiv b\pmod I$, 即 $a+I\subseteq b+I$, 用类似方法可得 $b+I\subseteq a+I$, 所以 $a+I=b+I$.

[2] 这一步是因为定义3.1.4(87页) $\bar{a}+\bar{b}\triangleq\overline{a+b}$.

[3] 这是因为定义3.1.4(87页) $\bar{a}\bar{b}\triangleq\overline{ab}$.

证明 (1) $I \subseteq S \leqslant R$ 时, 因为 $\sigma \restriction_S$ [4]是 S 到 $\sigma(R)$ 的同态, 所以

$$\sigma(S) = \{\sigma(s) : s \in S\} = \mathrm{Im}(\sigma \restriction_S) \leqslant \mathrm{Im}\sigma = \sigma(R)$$

对于 $a \in R$, 注意到

$$\begin{aligned} &\sigma(a) \in \sigma(S) \\ \Leftrightarrow\ &\exists s \in S,\ \text{使得}\ \sigma(a) = \sigma(s) \\ \Leftrightarrow\ &\exists s \in S,\ \text{使得}\ \sigma(a-s) = \bar{0} \\ \Leftrightarrow\ &\exists s \in S,\ \text{使得}\ a - s \in \ker\sigma = I \\ \Leftrightarrow\ &a \in S + I = S \end{aligned}$$

所以 $I \subseteq S, T \leqslant R$ 时, 如果 $S \neq T$, 则 $\exists t \in T$, 使得 $t \notin S$, 则由上可知
$\sigma(t) \notin \sigma(S)$, 从而 $\sigma(S) \neq \sigma(T)$ [5].
任给 $\sigma(R)$ 的一个子环 ξ, 让 $S = \{a \in R : \sigma(a) \in \xi\}$. 若 $a \in I$, 则 $\sigma(a) = \bar{0} \in \xi$, 故 $I \subseteq S$.
如果 $a, b \in S$, 则 $\sigma(a \pm b) = \sigma(a) \pm \sigma(b) \in \xi$, $\sigma(ab) = \sigma(a)\sigma(b) \in \xi$, 故
$a \pm b, ab \in S$, 即 $I \subseteq S \leqslant R$.
注意到 $\xi \subseteq \sigma(R)$, 所以 ξ 的任一元素 x 都必定可写为 $\sigma(a)$ 的形式, 其中 a 为 R 中的某个元素, 又 $\sigma(a) \in \xi \Leftrightarrow a \in S \Leftrightarrow \sigma(a) \in \sigma(S)$, 故 $\xi = \sigma(S)$ [6].
(2) 设 $I \subseteq J \trianglelefteq R$, σ 如(1)中的定义. 注意到

$$\begin{aligned} &\sigma(J) \trianglelefteq \sigma(R) \\ \Leftrightarrow\ &\text{对}\ \forall a \in J, r \in R, \begin{cases} \sigma(r)\sigma(a) \in \sigma(J) \\ \sigma(a)\sigma(r) \in \sigma(J) \end{cases} \\ \Leftrightarrow\ &\text{对}\ \forall a \in J, r \in R,\ \sigma(ar), \sigma(ra) \in \sigma(J) \\ \Leftrightarrow\ &\text{对}\ a \in J, r \in R,\ ar, ra \in J \\ \Leftrightarrow\ &J \trianglelefteq R \end{aligned}$$

注意到如果 $J \trianglelefteq R$, 则 $J \leqslant R$, 所以 σ 为双射已由(1)中证得. (3) 设 $I \subseteq J \trianglelefteq R$, 则 $\sigma(J) \trianglelefteq \sigma(R)$, 下证 $R/J \cong \sigma(R)/\sigma(J)$.
做 $\bar{\sigma} : R/J \to \sigma(R)/\sigma(J)$ 如下:

$$\bar{\sigma}(a + J) = \sigma(a) + \sigma(J) \in \sigma(R)/\sigma(J)$$

注意 $a + J = b + J \Leftrightarrow a - b \in J \Leftrightarrow \sigma(a-b) \in \sigma(J) \Leftrightarrow \sigma(a) - \sigma(b) \in \sigma(J) \Leftrightarrow \sigma(a) + \sigma(J) = \sigma(b) + \sigma(J)$, 故 $\bar{\sigma}$ 定义合理且为单射, 显然 $\bar{\sigma}$ 为满射.

[4] $\sigma \restriction_S$ 表示 σ 限制在 S 上.
[5] 上述这些证明了映射 $\sigma : S \mapsto \sigma(S)$ 是从 R 的包含 I 的子环到 $\sigma(R) = \mathrm{Im}\sigma$ 的映射, 且为单射.
[6] 这是为了证明映射 $\sigma : S \mapsto \sigma(S)$ 是满射

又

$$
\begin{aligned}
\bar{\sigma}\left((a+J)+(b+J)\right) &= \bar{\sigma}\left((a+b)+J\right) \\
&= \sigma(a+b)+\sigma(J) \\
&= \sigma(a)+\sigma(b)+\sigma(J) \\
&= \sigma(a)+\sigma(J)+\sigma(b)+\sigma(J) \\
&= \bar{\sigma}(a+J)+\bar{\sigma}(b+J) \\
\bar{\sigma}\left((a+J)(b+J)\right) &= \bar{\sigma}\left(ab+J\right) \\
&= \sigma(ab)+\sigma(J) \\
&= \sigma(a)\sigma(b)+\sigma(J) \\
&= \left(\sigma(a)+\sigma(J)\right)\left(\sigma(b)+\sigma(J)\right) \;^{7} \\
&= \bar{\sigma}(a+J)\bar{\sigma}(b+J)
\end{aligned}
$$

所以 $\bar{\sigma}$ 为同态, 又由上所证, $\bar{\sigma}$ 为双射, 所以 $\bar{\sigma}$ 为同构, 故
$R/J \cong \sigma(R)/\sigma(J)$. □

推论3.2.1

设 $I \trianglelefteq R$, 则

(1) R/I 的理想形如 J/I, 其中 $I \subseteq J \leqslant R$.

(2) 如果 $I \leqslant J \trianglelefteq R$, 则 $(R/I)\big/(J/I) \cong R/J$.

证明 (1) $\sigma: a \mapsto a+I$ 是环 R 到 R/I 的满同态, $\ker\sigma = \{a \in R : a+I = 0+I\} = I$, 则由定理3.2.2的(2)知 $\sigma(R) = R/I$ 的理想形如 $\sigma(J) = J/I$, 其中 $I \leqslant J \trianglelefteq R$.
(2) $I \subseteq J \trianglelefteq R$ 时, 由定理3.2.2的(3)知 $\sigma(R)\big/\sigma(J) = (R/I)\big/(J/I) \cong R/J$. □

定理3.2.3

设 $S \leqslant R$, $I \trianglelefteq R$, 则 $I+S \leqslant R$, $I \cap S \trianglelefteq S$, 且

$$S\big/(I \cap S) \cong (I+S)\big/I$$

[7] 这是因为定义3.1.4(87页) $(ab+I) = \bar{ab} = \bar{a}\bar{b} = (a+I)(b+I)$.

证明 当 $a, a' \in I$, $s, s' \in S$ 时,

$$(a+s)+(a+s')=(a+a')+(s+s')\in I+S$$

注意到理想的性质有 $as', sa' \in I$, 故

$$(a+s)(a'+s')=aa'+as'+sa'+ss'\in I+S$$

因此 $I+S \leqslant R$.
作 $\sigma : S \to R/I$ 如下:

$$\sigma(s)=s+I\in R/I$$

可知 σ 为同态, 又

$$\ker\sigma=\{s\in S:\sigma(s)=I\}=\{s\in S:s+I=I\}=I\cap S\trianglelefteq S$$
$$\mathrm{Im}\sigma=\{s+I:s\in S\}=\{s+a+I:s\in S,\,a\in I\}=(I+S)\Big/I$$

则由定理3.2.1的(3)(88页)知 $S\Big/(I\cap S)\cong(I+S)\Big/I$. □

推论3.2.2

设 $m, n \in \mathbb{Z}^+$, 则 $(m,n)[m,n]=mn$.

证明 因为 $(m)=m\mathbb{Z}\trianglelefteq\mathbb{Z}$, $(n)=n\mathbb{Z}\trianglelefteq\mathbb{Z}$, 则由定理3.2.3知

$$(m)/\left((m)\cap(n)\right)\cong\left((m)+(n)\right)/(n)$$

因为 $(m)\cap(n)=([m,n])$, 又由裴蜀定理[8]知

$$(m)+(n)=\{mx+ny:x,y\in\mathbb{Z}\}=(m,n)\mathbb{Z}$$

所以 $m\mathbb{Z}\Big/[m,n]\mathbb{Z}\cong(m,n)\mathbb{Z}\Big/n\mathbb{Z}$, 从而 $\frac{[m,n]}{m}=\frac{n}{(m,n)}$, 故
$(m,n)[m,n]=mn$. □

[8]裴蜀定理为: 若 a,b 是整数, 且 $(a,b)=d$, 那么对于任意的整数 x,y, $ax+by$ 都一定是 d 的倍数, 特别地, 一定存在整数 x,y, 使 $ax+by=d$ 成立.

3.3　环的直和与中国剩余定理

定义3.3.1

设 $R_1,\dots,R_n$ 为环, $R=R_1\times\cdots\times R_n=\{x=(x_1,x_2,\dots,x_n:x_i\in R_i)\}$ 定义

$$x+y=(x_1+y_1,\dots,x_n+y_n)\quad xy=(x_1y_1,\dots,x_ny_n)$$

则可知 R 按上述加乘法构成环, 称 R 为 $R_1,\dots,R_n$ 的外直和, 记为

$$R_1\oplus\cdots\oplus R_n$$

令 $R_i^*=\{(0,0,\dots,0,r_i,0,\dots,0):r_i\in R_i\}$, 则可知

$$R_i\cong R_i^*\leqslant R_1\oplus\cdots\oplus R_n=R$$

还可得

$$R_1^*+\cdots+R_n^*=R\quad R_i^*\cap(R_1^*+\cdots+R_{i-1}^*+R_{i+1}^*+\cdots+R_n^*)=(0)(\text{零理想})$$

定义3.3.2

设 $R_1,\dots,R_n$ 为环 R 的理想, 如果

$$R_1+\cdots+R_n=R,\ R_i\cap(R_1+\cdots+R_{i-1}+R_{i+1}+\cdots+R_n)=(0)$$

即 R 中每个元 r 可唯一地表成 $r_1+\cdots+r_n\,(r_i\in R_i)$ [1], 则说 R 是其理想 $R_1,\dots,R_n$ 的**内直和**.

定理3.3.1

设环 R 是其理想 $R_1,\dots,R_n$ 的内直和, 则 $R\cong R_1\oplus\cdots\oplus R_n$.

[1]唯一性是因为如果 r 可分别表示为 $r_1+\cdots+r_n$ 和 $r_1'+\cdots+r_n'$, 则因为 $r_1+\cdots+r_n=r_1'+\cdots+r_n'$, 可得

$$r_i-r_i'=(r_1-r_1')+\cdots+(r_{i-1}-r_{i-1}')+(r_{i+1}-r_{i+1}')+\cdots+(r_n-r_n')\in R_i\cap(R_1+\cdots+R_{i-1}+R_{i+1}+\cdots+R_n=(0)$$

即知 $r_i=r_i'$.

证明　作 $\sigma: R_1 \oplus \cdots \oplus R_n \to R$ 如下

$$\sigma((r_1, \ldots, r_n)) = r_1 + r_2 + \cdots + r_n$$

因为由定义3.3.2知 R 中每个元素均可以唯一地表为 $r_1 + \cdots + r_n\,(r_i \in R_i)$, 所以 σ 是双射.

此外

$$\begin{aligned}\sigma((r_1, \ldots, r_n) + (s_1, \ldots, s_n)) &= \sigma((r_1 + s_1) + \cdots + (r_n + s_n)) \\ &= (r_1 + s_1) + \cdots + (r_n + s_n) \\ &= (r_1 + \cdots + r_n) + (s_1 + \cdots + s_n) \\ &= \sigma((r_1 + \cdots + r_n)) + \sigma((s_1 + \cdots + s_n)) \\ \sigma((r_1, \ldots, r_n)(s_1, \ldots, s_n)) &= \sigma((r_1 s_1, \ldots, r_n s_n)) \\ &= r_1 s_1 + \cdots + r_n s_n\end{aligned}$$

当 $i \neq j$ 时, 因为 $r_i \in R_i, s_j \in R_j$, 且 R_i, R_j 为 R 中的理想, 故由理想的性质可知 $r_i s_j \in R_i$, $r_i s_j \in R_j$, 所以

$$r_i s_j \in R_i \cap R_j \subseteq R_i \cap (R_1 + \cdots + R_{i-1} + R_{i+1} + \cdots + R_n) = (0)$$

即 $r_i s_j = 0$. 因此可得

$$\begin{aligned}\sigma((r_1, \ldots, r_n) + (s_1, \ldots, s_n)) &= r_1 s_1 + \cdots + r_n s_n \\ &= (r_1 + \cdots + r_n)(s_1 + \cdots + s_n) \\ &= \sigma((r_1, \ldots, r_n))\,\sigma((s_1, \ldots, s_n))\end{aligned}$$

故 σ 为从 $R_1 \oplus \cdots \oplus R_n$ 到 R 的同态, 又由上已证 σ 为双射, 所以 σ 为同构, 即 $R \cong R_1 \oplus \cdots \oplus R_n$. □

定义3.3.3

设 R 为环, $\emptyset \neq X \subseteq R$, $\langle X \rangle = \bigcap_{X \subseteq I \trianglelefteq R} I$ 是包含 X 的最小理想, 它叫**由 X 生成的理想**.
事实上, R 为幺环的时候, $\langle X \rangle = \{\sum_{i=1}^n r_i x_i s_i : r_i, s_i \in R, x_i \in X\}$.
R 为交换幺环时, $\langle X \rangle = \{\sum_{i=1}^n r_i x_i : r_i \in R, x_i \in X\}$.

定义3.3.4

记 $(a) = \{ra : r \in R\} = Ra$, 则 $a_1, a_2, \ldots, a_n$ 的系数在 R 中的线性组合的全体可表示为

$$(a_1, a_2 \ldots, a_n) = Ra_1 + \cdots + Ra_n = (a_1) + (a_2) + \cdots + (a_N)$$

定义3.3.5

设 I,J 为环 R 的理想, 定义 IJ 如下

$$IJ=\{\text{有限和}\sum_{i=1}^{n}a_ib_i : a_i\in I, b_i\in J\}$$

则 IJ 仍为 R 中的理想 [2], 称之为 I 与 J 的乘积

例3.3.1

$\mathbb{Z}$ 为整环, 它的理想形如 $(n)=n\mathbb{Z}$, 其中 $n\in\mathbb{N}=\{0,1,2,\ldots\}$, 是循环群 $\mathbb{Z}$ 的加法子群, 也为加法循环群.

则可得

$$\begin{aligned}(m)+(n)&=\{mx+ny : x,y\in\mathbb{Z}\}=((m,n))=(m,n)\mathbb{Z}\\(m)\cap(n)&=\{x\in\mathbb{Z} : m \mid x, n \mid x\}=([m,n])=[m,n]\mathbb{Z}\\(m)(n)&=\{\sum_i mx_iny_i : x_i,y_i\in\mathbb{Z}\}=(mn)=mn\mathbb{Z}\end{aligned}$$

定义3.3.6

设 I,J 为 R 中的理想, 如果 $I+J=R$, 则称 I 与 J **互素(互质)**

例3.3.2

在 $\mathbb{Z}$ 中, (m) 与(n) 互素 $\Leftrightarrow (m)+(n)=\mathbb{Z}=(1)\Leftrightarrow((m,n))=(1)\Leftrightarrow (m,n)=1$, 即 m,n 互素.

[2](1) 因为

$$\sum_{i=1}^{n}a_ib_i+\sum_{j=1}^{m}c_jd_j=\sum_{i=1}^{n+m}a_ib_i\ (a_i,c_j\in I,\ b_i,d_j\in J)$$

其中 $a_{n+j}=c_j,b_{n+j}=d_j$, 故 I,J 对加法封闭, 类似可证 I,J 对减法封闭.

(2) $\forall r\in R$,

$$\begin{aligned}r\sum_{i=1}^{n}a_ib_i&=\sum_{i=1}^{n}(ra_i)b_i\\\sum_{i=1}^{n}a_ib_i\cdot r&=\sum_{i=1}^{n}a_i(b_ir)\end{aligned}$$

注意到 I,J 为 R 中的理想, 所以 $ra_i\in I$, $b_ir\in J$, 故对 $r\in R,x\in IJ$, 有 $rx\in IJ, xr\in IJ$.

引理3.3.1

设 I, J, K 为幺环 R 的理想,

(1) I 与 J, K 都互素时, I 与 JK 互素.

(2) I 与 J 互素时, $IJ+JI=I\cap J$, 特别地, R 可换时, I, J 互素 $\Rightarrow IJ=I\cap J$.

证明 (1) $I+J=R=(1)$ [3], 故有 $i\in I, j\in J$ 使 $i+j=1$. 同样因为 $I+K=(1)$, 故又有 $i'\in I, k\in K$ 使 $i'+k=1$, 于是

$$1=(i+j)(i'+k)=ii'+ik+ji'+jk$$

因为 I 为 R 中的理想, 所以 $ii'+ik+ji'\in I$, 故
$1=ii'+ik+ji'+jk\in I+JK$. 即得 $I+JK=R$, 故 I 与 JK 互素.

(2) 因为 I, J 为 R 中理想, 故 $IJ\in I, IJ\in J$, 所以 $IJ\in I\cap J$, 类似可得 $JI\in J\cap I$, 故 $IJ+JI\subseteq I\cap J$.
由于 $I+J=R$, 有 $i\in I, j\in J$ 使 $i+j=1$, 任给 $k\in I\cap J$, 有
$k=1\cdot k=(i+j)k=ik+jk$, 因为 $k\in I\cap J$, 所以 $ik\in I, jk\in JI$, 故
$k=ik+jk\in IJ+JI$, 即得 $I\cap J\subseteq IJ+JI$, 故 $IJ+JI=I\cap J$.
R 交换时, $I\cap J=IJ+JI=IJ+IJ=IJ$. □

推论3.3.1

对于整数 a, b, c,

(1) a 与 b, c 都互素 $\Rightarrow a$ 与 bc 互素

(2) a 与 b 互素 $\Rightarrow [a,b]=|ab|$

证明 (1) 因为 a 与 b, c 都互素, 由例3.3.2可知 (a) 与 $(b), (c)$ 都互素, 注意到 $\mathbb{Z}$ 为幺环, 由引理3.3.1的(1)知 (a) 与 (bc) 互素, 即得 a 与 bc 互素.

(2) 因为 a 与 b 互素, 所以 (a) 与 (b) 互素, 注意到 $\mathbb{Z}$ 为交换幺环, 由引理3.3.1的(2)和例3.3.1(95页) 知 $(ab)=(a)\cap(b)=([a,b])$, 故 $[a,b]=|ab|$ □

[3] 由定义3.3.4知 $(1)=\{r\cdot 1 : r\in R\}=R$.

定理3.3.2 (环形式的中国剩余定理)

设 $A_1,\ldots,A_k$ 是幺环 R 的两两互素的理想, 则

$$R\Big/\bigcap_{i=1}^{k}A_i\cong R/A_1\oplus\cdots\oplus R/A_k$$

R 可换时,

$$R\Big/\prod_{i=1}^{k}A_i\cong R/A_1\oplus\cdots\oplus R/A_k$$

证明　作 $\sigma:R\to R/A_1\oplus\cdots\oplus R/A_k$ 如下

$$\sigma(a)=\langle a+A_1,a+A_2,\ldots,a+A_k\rangle$$

因为

$$\begin{aligned}\sigma(a)\sigma(b)&=\langle(a+A_1)(b+A_1),\ldots,(a+A_k)(b+A_k)\rangle\\&=\langle ab+A_1,\ldots,ab+A_k\rangle\\&=\sigma(ab)\\\sigma(a)+\sigma(b)&=\langle a+A_1+b+A_1,\ldots,a+A_k+b+A_k\rangle\\&=\langle a+b+A_1,\ldots,a+b+A_k\rangle\\&=\sigma(a+b)\end{aligned}$$

故 σ 为同态, 其中

$$\begin{aligned}\ker\sigma&=\{a\in R:\langle a+A_1,a+A_2,\ldots,a+A_k\rangle=\langle 0+A_1,0+A_2,\ldots,0+A_k\rangle\}\\&=\{a\in R:a\in A_1,a\in A_2,\ldots,a\in A_k\}\\&=\bigcap_{i=1}^{k}A_i\end{aligned}$$

由环的同态基本定理(88页)知 $R\Big/\bigcap\limits_{i=1}^{k}A_i\cong\mathrm{Im}\sigma$, 下证明 σ 为满射.
因为 σ 为满射, 等价于对 $\forall a_1,\ldots,a_k\in R$, 存在 $a\in R$ 满足 $a+A_i=a_i+A\,(i=1,2,\ldots,k)$. 由引理3.3.1的(1)(96页)并利用数学归纳法知 $B_i=A_1\cdots A_{i-1}A_{i+1}\cdots A_k$ 与 A_i 互素, 故 $A_i+B_i=R=(1)$, 即 $1\in A_i+B_i$. 故存在 $x_i\in B_i,a_i\in A_i$ 使 $1=x_i+a_i$, 从而 $x_i=1-a_i$, 即 $x_i\in 1+A_i$, 注意到 $j\neq i$ 时, $x_i\in B_i\subseteq A_j$, 故令

$$\delta_{ij}=\begin{cases}1 & j=i\\0 & j\neq i\end{cases}$$

则 $x_i \in \delta_{ij} + A_j$. 让 $x = \sum\limits_{i=1}^{k} a_i x_i$, 则 $x - a_j = \sum\limits_{i=1}^{k} a_i(x_i - \delta_{ij}) \in A_j$. 所以 σ 为满射.
因为 $\mathrm{Im}\sigma = R/A_1 \oplus \cdots \oplus R/A_k$ 故

$$R\Big/\bigcap_{i=1}^{k} A_i \cong R/A_1 \oplus \cdots \oplus R/A_k$$

如果 R 为交换幺环, 则由引理3.3.1(96页)知 $A_1 \cap A_2 = A_1A_2$, A_1A_2 与 A_3 互素, 故

$$A_1 \cap A_2 \cap A_3 = A_1A_2 \cap A_3 = A_1A_2A_3$$

类似地利用数学归纳法知 $A_1 \cdots A_k = \bigcap\limits_{i=1}^{k} A_i$. □

定理3.3.3 (数论形式的中国剩余定理)

设 $n_1, \ldots, n_k$ 为两两互素的正整数, $a_1, \ldots, a_k \in \mathbb{Z}$, 则同余式组

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad\vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \tag{3.1}$$

的整数通解为 $x \equiv \sum\limits_{i=1}^{k} a_i M_i M_i^* \pmod{M}$, 其中 $M = n_1 \cdots n_k$, $M_i = M/n_i = \prod\limits_{j \neq i} n_j$, M_i^* 满足 $M_i M_i^* \equiv 1 \pmod{n_i}$.

证明　由于 n_i 与 $\prod\limits_{j\neq i} n_j = M_i$ 互素, 由裴蜀定理知, 有 $x, y \in \mathbb{Z}$, 使 $1 = M_i x + n_i y$, 从而 $M_i x \equiv 1 \pmod{n_i}$ 有解, 即 M_i^* 存在. 令 $x_0 = \sum\limits_{i=1}^{k} a_i M_i M_i^*$, 注意到

$$M_i M_i^* = \begin{cases} 1 & \pmod{n_i} \\ 0 & \pmod{n_j}\ (j \neq i) \end{cases}$$

令 $M_i M_i^* \equiv \delta_{ij} \pmod{n_j}$, 则知

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

故可知 $x_0 \equiv \sum_{i=1}^{k} a_i \delta_{ij} = a_j \pmod{n_j}$, 其中 $j = 1, 2, \ldots, k$.
注意到 (3.1) 成立当且仅当 $j = 1, 2, \ldots, k$ 时, $x \equiv a_j \equiv x_0 \pmod{n_j}$, 即 $j = 1, 2, \ldots, k$ 时, $n_j \mid x - x_0$, 也就是 $[n_1, n_2, \ldots, n_k] \mid x - x_0$.
所以 (3.1) 成立当且仅当 $M = n_1 n_2 \cdots n_k \mid x - x_0$. □

例3.3.3

求解

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

解：$M = 3 \times 5 \times 7 = 105$, $M_1 = \frac{105}{3} = 35$, 因为$M_1 M_1^* \equiv 1 \pmod 3$, 可取 $M_1^* = -1$.
$M_2 = \frac{105}{5} = 21$, 因为 $M_2 M_2^* = 1 \pmod 5$, 所以取 $M_2^* = 1$.
$M_3 = 15$, $M_3 M_3^* \equiv 1 \pmod 7$, M_3^* 取 1 .
所以通解为 $x \equiv 1 \times 35 \times (-1) + 2 \times 1 \times 21 + 3 \times 15 \times 1 = 52 \pmod{105}$.

推论3.3.2

设 $n > 1$ 有素数分解式 $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, 其中 $p_1, \ldots, p_k$ 为不同的素数, $a_1, \ldots, a_k \in \mathbb{Z}^+$, 则 $A_i = (p_i^{\alpha_i}) = p_i^{\alpha_i}\mathbb{Z}$ 为 $\mathbb{Z}$ 的理想, 因为 $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ 两两互素, 所以由例3.3.2(95页)知 $A_1, \ldots, A_k$ 两两互素, 注意到 $\mathbb{Z}$ 为交换幺环, 且 $\prod_{i=1}^{k} A_i = (n)$, 所以依定理3.3.2(97页)知

$$\mathbb{Z}/n\mathbb{Z} \cong Z/p_1^{\alpha_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$$

定义3.3.7

对于幺环 R, $a \mid b$ 是指存在 $q \in R$ 使 $aq = b = qa$, 由 $a \mid b$, 可得 $(b) \subseteq (a)$[4]. 如果 $u \in R$ 且 $u \mid 1$, 即有 $v \in R$, 使 $uv = 1 = vu$ （u 有乘法逆元）, 则称 u 为 R 的一个**单位**. 且 $R = (1) \supseteq (u) \supseteq (1)$, 故 $(u) = (1) = R$.
如果 u, v 为单位, 则有 $(uv)^{-1} = v^{-1}u^{-1}$, 即得 uv 为单位. 如果 u 为单位, 则 u^{-1} 也为单位.
$\mathrm{U}(R) = \{u \in R : u\text{为单位}\}$ 构成乘法群, 叫 R 的**单位群**. 如果 R 为交换幺环, 且 $\mathrm{U}(R) = R^* = R \backslash \{0\}$, 则称 R 为**域**.

例3.3.4

$\mathbb{Q}$ 为有理数域, $\mathbb{R}$为实数域, $\mathbb{C}$ 为复数域, $\mathbb{Z}$为整数环, 且
$\mathrm{U}(\mathbb{Z}) = \{\pm 1\} = \langle -1 \rangle$ (二阶循环群).

注意：

$$\begin{aligned} \mathrm{U}(R_1 \oplus \cdots \oplus R_n) &= \{\langle x_i, x_2, \ldots, x_n \rangle : x_i\text{为}R_i\text{中乘法可逆元}\} \\ &= \mathrm{U}(R_1) \times \mathrm{U}(R_2) \times \cdots \times \mathrm{U}(R_n) \end{aligned}$$

作业：

[4]因为 $\forall x \in (b)$, 则 $x = rb$, 其中 $r \in R$, 如果$a \mid b$, 故 $x = rb = rqa \in (a)$. 所以由 $a \mid b$, 可得 $(b) \subseteq (a)$

(1) 设诸 $I_\lambda\,(\lambda\in\Lambda)$ 为环 R 的理想, 证明 $I=\bigcap\limits_{\lambda\in\Lambda} I_\lambda$ 为 R 的理想.(直接利用理想的定义证明)

(2) I,J 为 R 的理想时, $I+J=\{i+j: i\in I, j\in J\}$ 为 R 的理想. (直接利用理想的定义证明)

(3) 求解

$$\begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 5 \\ x\equiv 3 \pmod 7 \\ x\equiv 4 \pmod 9 \end{cases}$$

(仿照例3.3.3的方法即可, 答案为 $137+630n$)

(4) 代数学引论 P_{130} 的13题和14题.

3.4　素理想和极大理想

定义3.4.1

设 R 为交换幺环, $I \neq R$ 为 R 的理想. 如果 $ab \in I \Rightarrow a \in I$或 $b \in I$, 则称 I 为 R 的**素理想**.
设 I 为 R 的理想, $I \neq R$, 如果 $I \subseteq J \trianglelefteq R \Rightarrow J = I$ 或 R, 则说 I 为 R 的**极大理想**.

例3.4.1

决定出 $\mathbb{Z}$ 的素理想与极大理想.
解：$\mathbb{Z}$ 的理想形如 $n\mathbb{Z} = (n)$, 其中 $n \in \mathbb{N} = \{0, 1, 2, \ldots\}$.
首先 $0 = (0) = \{0\}$ (零理想)不是极大理想, 因为 $(0) \subsetneq (2) \subsetneq \mathbb{Z}$.
因为

$$ab \in (0) \;\Leftarrow ab = 0 \;\Leftarrow\; a = 0 \text{ 或 } b = 0 \;\Leftarrow\; a \in (0) \text{ 或 } b \in (0)$$

故 (0) 为 $\mathbb{Z}$ 的素理想.
设 $n > 1$, (n) 为 $\mathbb{Z}$ 的极大理想当且仅当没有 $d \in \mathbb{N}$ 使 $(n) \subset (d) \subset \mathbb{Z} = (1)$, 即 n 没有真因子(n 的异于 $1, n$ 的正整数因子).
故 (n) 为 $\mathbb{Z}$ 的极大理想当且仅当 n 为素数.
(n) 为 $\mathbb{Z}$ 的素理想当且仅当对 $\forall a, b \in \mathbb{Z}$, 如果 $ab \in (n)$, 则$a \in (n)$ 或 $b \in (n)$, 即对 $\forall a, b \in \mathbb{Z}$, 如果 $n \mid ab$, 则 $n \mid a$ 或 $n \mid b$ [1].
所以(n) 为 $\mathbb{Z}$ 的素理想当且仅当 n 为素数.

定理3.4.1

设 R 为交换幺环, 则 R 的极大理想 M 必为素理想.

证明　利用反证法. 不妨设 R 的某个极大理想 M 不是素理想, 则有 $a, b \notin M$ 使 $ab \in M$. 因为 R 为交换幺环时, $(a) = \{ra : r \in R\}$ 为 R 中的理想 [2]. 注意到 $0 \in M, a \in (a)$, [3]所以 $a = 0 + a \in M + (a)$, 又 $a \notin M$, 所以 $M \neq M + (a)$, 又因为 $0 \in (a)$, 故对 $\forall m \in M$, 有 $m + 0 \in M + (a)$, 即 $M \subset M + (a)$. 因为如果 I, J 为 R 的理想, 则 $I + J$ 也为 R 的理想. [4] 所以 $M + (a) \trianglelefteq R$. 由 M 为 R 的极大理想, 且 $M \neq M + (a)$ 所以 $M + (a) = R$. 类似可得 $M + (b) = R$. 因此

$$R = [M + (a)][M + (b)] = MM + (a)M + M(b) + (ab) \subset M \neq R$$

[1]这一步是因为：$a \in (n)$ 等价于 $a = xn$, 其中 $x \in \mathbb{Z}$, 故 $a \in (n)$ 等价于 $n \mid a$.
[2]这是因为：(1)对于 $ra, r'a \in (a)$, 有 $ra \pm r'a = (r \pm r')a \in (a)$.
(2)对于 $r' \in R, ra \in (a)$, 有 $r'ra = (r'r)a \in (a)$, $rar' = rr'a = (rr')a \in (a)$.
[3]如果 I 为 R 的理想, 则因为对 $\forall r \in R, a \in I$, 有 $ra \in I$, 取 $r = 0$ 由定理3.1.1的(1)(84页)知 $0a = 0 \in I$. 即对 R 中的理想 I, 均有 $0 \in I$.
[4]参见100页的作业.

故得出矛盾, 则命题得证. □

定理3.4.2

设 R 为交换幺环, 则

(1) R 为整环 $\Leftrightarrow 0=(0)$ 为素理想.

(2) R 为域 $\Leftrightarrow 0=(0)$ 为极大理想.

证明 (1) R 为整环当且仅当 R 无零因子, 即对 $\forall a, b \in R$, 如果 $ab=0$, 则 $a=0$ 或 $b=0$, 这意味着 $0=(0)$ 为素理想.

(2) "$\Rightarrow$": R 为域时, 如果 R 中的理想 I 有非零元 a, 则由域的定义知 $1=a^{-1}a \in I$, 从而 $I=(1)=R$. 故 R 为域时, 0 为极大理想.

"$\Leftarrow$" 如果 $0=(0)$ 为 R 的极大理想, 对于 R 中的非零元 a, 因为 R 为交换幺环, 所以 $(a) \trianglelefteq R$, 又因为 $0 \subset (a)$, 且 $0 \neq (a)$, 故 $(a)=R$, 即 $1 \in (a)$, 故 a 可逆, 从而知 R 为域. □

P.S.注意到定理3.4.1, 我们知道 R 的极大理想必为素理想, 故由定理3.4.2可得 R 为域 $\Rightarrow 0=(0)$ 为极大理想 $\Rightarrow 0=(0)$ 为素理想 $\Rightarrow R$ 为整环, 即<u>域必为整环</u>.

定理3.4.3

设 R 为交换幺环

(1) 对于 R 的理想$P \neq R$, <u>有 R/P 为整环 $\Leftrightarrow P$ 为 R 的素理想</u>.

(2) 对于 R 的理想$M \neq R$, <u>有 R/M 为域 $\Leftrightarrow M$ 为 R 的极大理想</u>.

证明 (1) $R/P=\{\bar{a}=a+P : a \in R\}$, 故

$$\begin{aligned}R/P \text{ 为整环} &\Leftrightarrow \forall a, b \in R,\ \text{如果 } \bar{a}\bar{b}=\bar{0},\ \text{则 } \bar{a}=\bar{0} \text{ 或 } \bar{b}=\bar{0} \\ &\Leftrightarrow \text{对 } \forall a, b \in R,\ \text{如果 } ab \in P,\ \text{则 } a \in P \text{ 或 } b \in P \\ &\Leftrightarrow P \text{ 为 } R \text{ 的素理想}\end{aligned}$$

(2) $R/M=\{\bar{a}=a+M : a \in R\}$, 故

$$\begin{aligned}M \text{ 为 } R \text{ 的极大理想} &\Leftrightarrow \text{如果 } M \subseteq I \trianglelefteq R,\ \text{则 } I=M \text{ 或 } I=R \\ &\Leftrightarrow \text{如果 } M/M \subseteq I/M \trianglelefteq R/M,\ \text{则 } I/M=R/M \text{ 或 } M/M^{5} \\ &\Leftrightarrow R/M \text{ 的零理想为极大理想.} \\ &\Leftrightarrow R/M \text{ 为域.}\end{aligned}$$

□

定理3.4.4

设 σ 是交换幺环 R 到 $\overline{R}$ 的同态, 则 R 的包含 $\ker\sigma$ 的极大理想（素理想）与 $\mathrm{Im}\sigma$ 的极大理想（素理想）一一对应.

证明 (1) 设 M 为 R 的理想, $\ker\sigma\subseteq M\subseteq I\trianglelefteq R$, 由定理3.2.2(90页)知, R 的包含 $\ker\sigma$ 的理想与 $\sigma(R)$ 的理想一一对应, 故 $\sigma(M)\subseteq\sigma(I)\trianglelefteq\sigma(R)=\mathrm{Im}\sigma$, 且

$$I\neq M,R\Leftrightarrow\sigma(I)\neq\sigma(M),\sigma(R)$$

故 M 为 R 的极大理想 $\Leftrightarrow$ 如果 $M\subseteq I\trianglelefteq R$, 则 $I=M$ 或 $I=R\Leftrightarrow$ 如果 $\sigma(M)\subseteq\sigma(I)\trianglelefteq\sigma(R)$, 则$\sigma(I)=\sigma(M)$ 或 $\sigma(I)=\sigma(R)\Leftrightarrow\sigma(M)$ 为 $\mathrm{Im}\sigma=\sigma(R)$ 的极大理想.

(2) $\ker\sigma\leqslant P\trianglelefteq R$, 则同样可得 $\sigma(P)\trianglelefteq\sigma(R)$, 且由定理3.2.2的(3)(90页)知 $\sigma(R)/\sigma(P)\cong R/P$, 由定理3.4.3知 $\sigma(P)$ 为 $\sigma(R)$ 的理想 $\Leftrightarrow\sigma(R)/\sigma(P)$ 为整环 $\Leftrightarrow R/P$ 为整环 P 为 R 的素理想. [6] □

定理3.4.5

设 R 为交换幺环, I 为 R 的理想, $a\in R$ 且 $I\cap\{a^n:n=0,1,2,\dots\}=\emptyset$, 则 R 必有包含 I 的素理想 P 使 $P\cap\{a^n:n=0,1,2,\dots\}=\emptyset$.

因为证明中需要用到集合论中的 Zorn 引理, 故先把 Zorn 引理[7]列出

Zorn 引理. *设 X 为非空半序集, 如果 X 的每个全序子集[8]在 X 中有上界, 则 X 中必有极大元.*

下面我们证明定理3.4.5

---

[5]注意到推论3.2.1(91页), 可知 R/M 的理想的形式均为 I/M, 其中 I 满足 $M\subseteq I\trianglelefteq R$, 其次注意 $M/M=\bar{0}$ 为 R/M 的零理想.

[6]定理3.4.4中的理想之间的一一对应性由定理3.2.2证, 本证明只是证明了在 $\overline{R}$ 中与 R 中的极大理想(素理想)一一对应的理想为 $\overline{R}$ 中的极大理想(素理想), 反之亦然.

[7]Zorn 引理与集合论中的选择公理等价

[8]粗略地说, 全序集就是在一个集合上对其中的元素上定义了一种大小关系, 且这个集合中的任意两个元素都可以比较大小. 例如 $\mathbb{R}$ 在一般意义下的大小关系下就是全序集.

证明　让 $A=\{J\trianglelefteq R: I\subseteq J,\ J\cap\{a^n:n\in\mathbb{N}\}=\emptyset\}$, 因为 $I\in A$, 所以 $A\neq\emptyset$, 且 A 依 $\subseteq$ 构成半序集.

设 $\{I_\lambda:\lambda\in\Lambda\}$ 为 A 的一个全序子集. 让 $J=\bigcup\limits_{\lambda\in\Lambda}I_\lambda$, 如果 $b,c\in J$, 则 $\exists u,\lambda\in\Lambda\,(b\in I_u, c\in I_\lambda)$, 则 $b,c\in I_u\cup I_\lambda$, 因为 $\{I_\lambda:\lambda\in\Lambda\}$ 为全序子集, 所以 I_u 与 I_λ 有包含关系. 不妨设 $I_u\subseteq I_\lambda$, 则 $b,c\in I_\lambda$, 故 $b\pm c\in I_\lambda=I_u\cup I_\lambda\subseteq J$.

另外 $r\in R$ 时, $a\in I_\lambda$, 由于 I_λ 为 R 的理想, 所以 $ra\in I_\lambda\subseteq J$, 故 $J\trianglelefteq R$.

又 $\lambda\in\Lambda$ 时, $I_\lambda\in A$, 故 $I\subseteq I_\lambda$, 所以 $I\subseteq J$, 且

$$J\cap\{a^n:n\in\mathbb{N}\}=\bigcap_{\lambda\in\Lambda}(I_\lambda\cap\{a^n:n\in\mathbb{N}\})=\emptyset$$

故由上述所证, 知道 A 的每个全序子集 $\{I_\lambda:\lambda\in\Lambda\}$ 在 A 中有上确界 $J=\bigcup\limits_{\lambda\in\Lambda}I_\lambda$, 依 Zorn 引理知 A 有极大元 P, 下面利用反证法证明 P 为素理想.

假设 P 不为素理想, 则有 $b,c\notin P$ 使 $bc\in P$, 则

$$((b)+P)((c)+P)=(bc)+(b)P+P(c)+PP\subseteq P$$

故 $((b)+P)((c)+P)$ 不含 a 的幂次, 但是因为 P 为 A 中的极大元, 故 $(b)+P\notin A$, 所以有 $m\in\mathbb{N}$ 使 $(b)+P$ 包含 a^m, 同理也存在 $n\in\mathbb{N}$, 使 $a^n\in(c)+P$, 如此 $((b)+P)((c)+P)$ 包含 a^{m+n}, 得出矛盾, 故 P 为素理想. □

推论3.4.1

设 R 为交换幺环, $I\neq R$ 为 R 的理想, 则有 R 有包含 I 的极大理想, 特别地, 因为 $I=0$ 为 R 的一个理想, 故<u>交换幺环 R 至少有一个极大理想</u>.

证明　如果 $1\in I$, 则 $I=(1)=R$, 与 $I\neq R$ 矛盾, 所以 $1\notin I$, 故 $I\cap\{1^n:n\in\mathbb{N}\}=\emptyset$, 在定理3.4.5的证明中取 $a=1$, 可知 $A=\{J\trianglelefteq R: I\subseteq J,\ J\cap\{1^n:n\in\mathbb{N}\}=\emptyset\}$ 有极大元 M, 下证 M 为极大理想.

如果 M 不为极大理想, 则存在 $M\subseteq M'\trianglelefteq R$, 且 $M'\neq M,R$, 因为 $M'\neq R$, 所以 $M'\cap\{1^n:n\in\mathbb{N}\}=\emptyset$. 又因为 $I\subseteq M\subseteq M'$, 所以 $M'\in A$, 这与 M 为 A 中的极大元矛盾, 故 M 为极大理想. □

定理3.4.6

设 R 为交换幺环, 则 $\mathrm{r}(R)=R$ 中所有素理想的交 $=\{a\in R:\exists n>0\,(a^n=0)\}$, 其中 $\mathrm{r}(R)$ 叫 R 的**诣零根**, $\{a\in R:\exists n>0\,(a^n=0)\}$ 称为 R 中的幂零元.

证明　如果 a 为幂零元, 则 $\exists n>0$ 使 $a^n=0$, 任给素理想 P, 因为 $\underbrace{a\cdot a\cdots a}_{n}=0\in P$, 则 $a\in P$ [9]. 于是 $a\in \mathrm{r}(R)$.

设 a 不为幂零元, 则因为 $0\cap a^n: n\in\mathbb{N}=\emptyset$, 且 0 为 R 的理想, 故由定理3.4.5知有素理想 P 不含 $a^n\,(n\in\mathbb{N})$, 故 $a\notin \mathrm{r}(R)$. □

作业:

(1) 设 R 为幺环, 则 $1-ab$ 可逆 $\Rightarrow 1-ba$ 可逆. [10]

(2) 设 R 为交换幺环, $I\trianglelefteq R$, 证明 $\sqrt{I}=\{a\in R:\exists n>0\,(a^n\in I)\}$ 也是 R 的理想.

(3) 代数学引论133页第52题.

[9] 如果 $a^n\in P$, 因为 P 为素理想, 则 $a^{n-1}\in P$ 或 $a\in P$, 如果 $a\in P$, 则得证. 如果 $a^{n-1}\in P$, 则类似地递推下去最终可得 $a\in P$.

[10] 不妨设 m 为 $1-ab$ 的逆, 则令

$$A=\begin{pmatrix}1-ab & a\\ 0 & 1\end{pmatrix}\quad B=\begin{pmatrix}m & -ma\\ 0 & 1\end{pmatrix}\quad C=\begin{pmatrix}1 & 0\\ -b & 1\end{pmatrix}$$
$$D=\begin{pmatrix}1 & 0\\ b & 1\end{pmatrix}\quad T=\begin{pmatrix}1 & a\\ b & 1\end{pmatrix}\quad I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\quad F=\begin{pmatrix}1 & a\\ 0 & 1-ba\end{pmatrix}$$

可知 $AB=BA=I$, $CD=DC=I$, 故 A,B,C,D 均可逆, 又注意到 $AD=T$, 所以 T 可逆, 且逆元为 CB, 注意到 $F=CT$, 又 C,T 均可逆, 所以 F 可逆, 且逆元为 CBD, 又因为

$$F^{-1}=CBD=\begin{pmatrix}m-mab & -ma\\ -bm+bmab+b & bma+1\end{pmatrix}=\begin{pmatrix}1 & -ma\\ 0 & bma+1\end{pmatrix}$$

故 $F^{-1}F=I$, 即 $(bma+1)(1-ba)=bma-bmaba-ba+1=bm(1-ab)a-ba+1=ba-ba+1=1$, 同样也可得 $(1-ba)(bma+1)=1$

3.5　多项式环与形式幂级数环

定义3.5.1

R 为幺环时, $R[x]=\{\sum\limits_{i=0}^{n}a_ix^i:a_0,\ldots,a_n\in R\}$ 称为 R 上的**一元多项式环**.
$\sum\limits_{n=0}^{\infty}a_nx^n\,(a_0,\ldots,a_n,\ldots\in R)$ 称为 R 上的**形式幂级数**. 定义

$$\sum_{n=0}^{\infty}a_nx^n=\sum_{n=0}^{\infty}b_nx^n \text{ 当且仅当 } a_n=b_n\,(n\in\mathbb{N})$$
$$\sum_{n=0}^{\infty}a_nx^n+\sum_{n=0}^{\infty}b_nx^n=\sum_{n=0}^{\infty}(a_n+b_n)x^n$$
$$\left(\sum_{n=0}^{\infty}a_nx^n\right)\left(\sum_{n=0}^{\infty}b_nx^n\right)=\sum_{n=0}^{\infty}(\sum_{k+l=n}a_kb_l)x^n$$

则可知 R 上的形式幂级数依上述加乘法构成环, 记为 $R[[x]]$, 称为 R 上的**形式幂级数环**.
考察 R 中元序列 $\{a_n\}_{n=0}^{\infty}\,(a_n\in R)$ 定义

$$\{a_n\}+\{b_n\}\triangleq\{a_n+b_n\}\quad \{a_n\}*\{b_n\}\triangleq\{c_n\}\,(c_n=\sum_{k+l=n}a_kb_l)$$

则全体这种序列按上述加乘法构成环.
记 $x=(0,1,0,\ldots)$, 则 $x^n=(0,0,\ldots,0,1,0,\ldots)$, 其中 1 在第 $n+1$ 个位置.
$a\in R$ 时, 把 a 等同于 $(a,0,\ldots)$, $a_n\in R$时, $a_nx^n=\{0,\ldots,0,a_n,0,\ldots\}$, 其中 a_n 在第 $n+1$ 个位置. 我们利用 $\sum\limits_{n=0}^{\infty}a_nx^n$ 表示序列 $\{a_n\}_{n=0}^{\infty}$, 这就是给出的形式幂级数的严格定义.
$R[x]=\{\sum\limits_{n=0}^{\infty}a_nx^n:a_0,\ldots,a_n,\ldots\in R$ 且只有有限个 a_i 非零$\}$, 这是 $R[[x]]$ 中包含 R 与 x 的最小子环.
定义 R 上的**二元多项式环**

$$\begin{aligned}R[x,y]&=R[x][y]\\&=\{\sum_{i\geqslant 0,j\geqslant 0}a_{i,j}x^iy^j:\text{只有有限个 } i,j \text{ 使 } a_{i,j} \text{ 非零}\}\end{aligned}$$

一般地, R 上 n **元多项式**如下定义:

$$\begin{aligned}&R[x_1,x_2,\ldots,x_n]=R[x_1,x_2,\ldots,x_{n-1}][x_n]\\&=\left\{\sum_{i_1,\ldots,i_n\geqslant 0}a_{i_1,\ldots,i_n}x_1^{i_1}\cdots x_n^{i_n}:\text{只有有限个 }\{i_1,\ldots,i_n\}\text{ 使 }a_{i_1,\ldots,i_n}\text{ 非零}\right\}\end{aligned}$$

定理3.5.1

设 R 为整环[1], 则 R 上 n 元多项式 $R[x_1,\dots,x_n]$ 也是整环, 且

$$\mathrm{U}(R[x_1,\dots,x_n])=\mathrm{U}(R)$$

其中 $\mathrm{U}(R)=\{u\in R:u\text{ 为单位}\}$ 是 R 的单位群(99页的定义3.3.7).

证明 对 n 进行归纳, $n=1$ 时, R 为整环, 如果假设 $R[x]$ 有零因子, 不妨设左零因子为 $\sum_{i=0}^{n}a_ix^i$, 右零因子为 $\sum_{j=0}^{m}b_jx^j$, 其中 $a_n,b_m\neq 0$, 则因为 $(\sum_{i=0}^{n}a_ix^i)(\sum_{j=0}^{m}b_jx^j)=0$, 所以 x^i 的系数都为 0 , 注意到 x^{n+m} 的系数为 a_nb_m, 则得到 $a_nb_m=0$, 这与 R 无零因子矛盾. 故 $R[x]$ 为整环.
设 $f(x),g(x)\in R[x]$, 如果 $f(x)\cdot g(x)=1$, 则 $f(x)=g(x)$ 为非零常数, 即为 R 中的单位. 又可知 R 中的单位必为 $R[x]$ 中的单位. 故 $\mathrm{U}(R[x_1,\dots,x_n])=\mathrm{U}(R)$.
设 $n-1$ 时, $R[x_1,\dots,x_{n-1}]$ 为整环, 由定义3.5.1知
$R[x_1,\dots,x_{n-1},x_n]=R[x_1,\dots,x_{n-1}][x_n]$, 故 $R[x_1,\dots,x_{n-1},x_n]$ 可看成是在整环 $R[x_1,\dots,x_{n-1}]$ 上定义的一元多项式环, 故由上述证明知 $R[x_1,\dots,x_{n-1},x_n]$ 为整环, 且 $\mathrm{U}(R[x_1,\dots,x_{n-1},x_n])=\mathrm{U}(R[x_1,\dots,x_{n-1}])=\mathrm{U}(R)$. □

定理3.5.2 (带余除法)

设 R 为交换幺环, $f(x),g(x)\in R[x]$ 且 $g(x)\neq 0$（即 $g(x)$ 不是零多项式）, 如果 $g(x)$ 首项系数为 R 的单位, 则存在唯一的 $q(x),r(x)\in R[x]$, 使

$$f(x)=g(x)q(x)+r(x)$$

其中 $r(x)=0(\deg 0=-\infty)$ 或 $\deg r(x)<\deg g(x)$.

证明 让 $S=\{f(x)-g(x)h(x):h(x)\in R[x]\}$. 设 S 中次数最低的一个多项式为 $r(x)=f(x)-g(x)q(x)$, 其中 $q(x)\in R[x]$.
假如 $m=\deg r(x)\geqslant n=\deg g(x)$, 不妨设
$r(x)=a_mx^m+\cdots+a_0$, $g(x)=b_nx^n+\cdots+b_0$, 令
$\overline{r(x)}=r(x)-a_mb_n^{-1}g(x)x^{m-n}$, 可知 $\deg\overline{r(x)}<m=\deg r(x)$. 又因为 $q(x)+a_mb_n^{-1}x^{m-n}\in R[x]$, 所以

$$\overline{r(x)}=r(x)-a_mb_n^{-1}g(x)x^{m-n}=f(x)-g(x)(q(x)+a_mb_n^{-1}x^{m-n})\in S$$

[1]整环：无零因子的交换幺环. (83页的定义3.1.1)

这与 $r(x)$ 的选取矛盾, 故 $r(x)$ 次数小于 $g(x)$.

假如 $f(x)=g(x)q(x)+r(x)=g(x)\widetilde{q}(x)+\widetilde{r}(x)$, 则

$$r(x)-\widetilde{r}(x)=g(x)(\widetilde{q}(x)-q(x))$$

因为 $r(x)-\widetilde{r}(x)$ 的次数小于 $g(x)$ 的次数, 且 $\widetilde{q}(x)-q(x)\in R[x]$, 所以 $q(x)=\widetilde{q}(x)$, $r(x)=\widetilde{r}(x)$, 故唯一性得证. □

推论3.5.1

设 R 为交换幺环, $f(x)\in R[x]$, 对于 $c\in R$, $x-c\mid f(x)\Leftrightarrow f(c)=0$.

证明 设 $g(x)=x-c$, 依带余除法定理知

$$f(x)=(x-c)q(x)+r(x) \tag{3.2}$$

其中 $\deg r(x)<\deg(x-c)=1$, 故 $r(x)$ 是个常数 r, 将 $x=c$ 带入 (3.2) 中得 $f(c)=r$, 故

$$f(x)=(x-c)q(x)+f(c)$$

故 $x-c\mid f(x)\Leftrightarrow f(c)=0$. □

定理3.5.3

设 R 为整环, 则 R 上一元 n 次非零多项式在 R 中至多有 n 个不同的零点 [2].

证明 对 n 进行归纳. $n=0$ 时, 可知命题成立.

设 $n>0$ 且命题对更小的 n 结论正确, 设 $f(x)\in R[x]$ 且 $\deg f(x)=n$, 如果 $f(x)=0$ 在 R 中无解, 则结论得证. 否则设 $f(c)=0$, 其中 $c\in R$, 则由推论3.5.1知, $x-c\mid f(x)$, 故 $f(x)=(x-c)g(x)$, 其中 $g(x)\in R[x]$, 故 $\deg(g[x])=n-1$‘, 所以依归纳假设 $g(x)=0$ 在 R 中至多有 $n-1$ 个不同根, 又因为 R 为整环, 所以 $f(x_0)=0\Leftrightarrow x_0-c=0$ 或 $g(x_0)=0$, 故 $f(x)=0$ 在 R 中至多有 n 个不同根. □

[2] 如果 R 不为整环, 则此定理不一定成立, 具体的反例参照证明后面的例3.5.1.

例3.5.1

$R=\mathbb{Z}/8\mathbb{Z}$ 是交换幺环，但不是整环，因为 $\bar{2}\cdot\bar{4}=\bar{8}=\bar{0}\,(\bar{a}=a+8\mathbb{Z})$，因为 $(2n+1)^2=4n(n+1)+1\equiv 1 \pmod 8$，故 $x^2=\bar{1}$ 在 $R=\mathbb{Z}/8\mathbb{Z}$ 中有四个解 $x=\bar{1},\bar{3},\bar{5},\bar{7}$.

P.S.因为域为整环 [3]，所以 F 为域时，F 上的一元 n 次方程在 F 中至多有 n 个根. 利用复变函数的知识我们可以得到代数基本定理.

代数基本定理. *复数域 $\mathbb{C}$ 上 n 次多项式 $f(x)\in\mathbb{C}[x]$ 可分解成 n 个一次式的乘积.*

例3.5.2

(Y.Bilu 猜想) 设 $f(x),g(x)\in\mathbb{Z}[x]$，$g(x)$ 为首一多项式，如果有无穷多个 $m\in\mathbb{Z}$ 使 $g(m)\mid f(m)$，则在 $\mathbb{Z}[x]$ 中 $g(x)\mid f(x)$.

证明 作带余除法 $f(x)=g(x)q(x)+r(x)$，其中 $\deg r(x)<\deg g(x)$，因为有无穷多个 $m\in\mathbb{Z}$，使 $g(m)\mid f(m)=g(m)q(m)+r(m)$，故有无穷多个 $m\in\mathbb{Z}$，使 $g(m)\mid r(m)$，因为 $|m|$ 很大时，$|r(m)|<|g(m)|$，所以有无穷多个 $m\in\mathbb{Z}$ 使 $r(m)=0$，由定理3.5.3知 $r(m)$ 为零多项式. □

定理3.5.4

设 R 为整环，则 $\mathrm{U}(R)$ 的有限子群必为循环群，特别地，F 为域时，乘法群 $F^*=F\backslash\{0\}$ 的有限子群必为循环群.

证明 设 G 为 $\mathrm{U}(R)$ 的有限子群，因为 R 为整环(无零因子的交换幺环)，则 G 为有限 Abel 群，任给 $n\in\mathbb{Z}^+$，由定理3.5.3知 $x^n-1=0$ 的根至多有 n 个，故

$$|\{x\in G: x^n=1\}|\leqslant|\{x\in R: x^n=1\}|\leqslant n$$

由定理2.8.4(78页)知，存在 $a\in G$ 使 a 的阶 $o(a)=n=\exp(G)$. 因为 $x\in G\Rightarrow x^n=1$，所以

$$|\{x\in G: x^n=1\}|=|G|\leqslant n=|\langle a\rangle|$$

从而 $G=\langle a\rangle$ 为循环群. □

作业：

(1) 代数学引论132页的21和22题(看成一题).

(2) 代数学引论132页的46题.

(3) 代数学引论132页的50题.

[3]具体证明可见102页的定理3.4.2

3.6　Euclid 整环与主理想整环

定义3.6.1

设 R 为整环, 如果有 Euclid 函数 $N: R\backslash\{0\} \to \mathbb{N} = \{0,1,2,\ldots\}$ 使对 $a \in R, b \in R\backslash\{0\}$, 有 $q, r \in R$ 使 $a = bq + r$, 且 $r = 0$ 或 $N(r) < N(b)$, 则称 R 为 Euclid 整环.

验证环为 Euclid 整环分为两步：(1) 验证为整环. (2)取 Euclid 函数 N, 并加以验证.

例3.6.1

整数环 $\mathbb{Z}$ 是 Euclid 整环(取 $N(x) = |x|$ 即可).
F 为域时, $F[x]$ 为 Euclid 整环.(取 $N(f(x)) = \deg f(x) \in \mathbb{N}$ 即可.)
$\mathbb{Z}[x]$ 不是 Euclid 整环, 证明需用到定理3.6.2.

定理3.6.1

Gauss 整数环 $\mathbb{Z}[i] = \{a+bi : a, b \in \mathbb{Z}\}$ 与 Eisenstein 环 $\mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$ 为 Euclid 整环.（其中 $\omega = \frac{-1+\sqrt{3}i}{2}, \omega^3 = 1$ ）

证明　$R[\alpha] = \{p(\alpha) : p(x) \in R[x]\}$ 是 R 添加 α 生成的环. $\mathbb{Z}[i]$ 与 $\mathbb{Z}[\omega]$ 显然为整环. 因为 $\bar{\omega} = -1 - \omega$, 故 $\mathbb{Z}[i]$ 与 $\mathbb{Z}[\omega]$ 对取共轭封闭.
令 $R = \mathbb{Z}[i]$ 或 $\mathbb{Z}[\omega]$, 定义 $N : z \to z\bar{z} = |z|^2, z \in R$ 时, 因为

$$N(a+bi) = a^2 + b^2 \in \mathbb{N} \quad N(a+b\omega) = (a+b\omega)(a+b\bar{\omega}) = a^2 - ab + b^2$$

所以 $N(z) = z\bar{z} \in \mathbb{N}$. 任给 $\alpha \in R, \beta \in R\backslash\{0\}$, 因为
$\alpha\bar{\beta} \in R, N(\beta) = |\beta|^2 = \beta\bar{\beta} \in Z^+$, 所以

$$\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}} = \begin{cases} r + si & R = \mathbb{Z}[i] \\ r + s\omega & R = \mathbb{Z}[\omega] \end{cases} \quad (r, s \in \mathbb{Q})$$

让 m 是最靠近 r 的整数, n 是最靠近 s 的整数, 则 $|r-m| \leqslant \frac{1}{2}, |s-n| \leqslant \frac{1}{2}$, 作

$$\eta = \begin{cases} m + ni & R = \mathbb{Z}[i] \\ m + n\omega & R = \mathbb{Z}[\omega] \end{cases}$$

则 $\eta \in R$, 且

$$|\frac{\alpha}{\beta} - \eta|^2 = \begin{cases} |r-m|^2 + |s-n|^2 & R = \mathbb{Z}[i] \\ |r-m|^2 + |s-n|^2 - (r-m)(s-n) & R = \mathbb{Z}[\omega] \end{cases}$$

注意到 $|r-m|^2+|s-n|^2<1, |r-m|^2+|s-n|^2-(r-m)(s-n)<1$, 故存在 $\eta\in R$ 使 $|\frac{\alpha}{\beta}-\eta|^2<1$.
让 $\gamma=\alpha-\beta\eta\in R$, 则 $\alpha=\beta\eta+\gamma$, 且

$$N(\gamma)=|\gamma|^2=|\frac{\alpha}{\beta}-\eta|^2|\beta|^2<|\beta|^2=N(\beta)$$ □

定义3.6.2

交换幺环 R 的一个元素生成的理想 $(a)=Ra$ 叫**主理想**, 如果整环 R 的每个理想都是主理想, 则称 R 为**主理想整环(P.I.D)** [1].

例3.6.2

$\mathbb{Z}$ 是 P.I.D , 因为 $\mathbb{Z}$ 的所有理想形如 $n(\mathbb{Z})=(n)$.

定理3.6.2

设 R 为 Euclid 整环, 则 R 为 P.I.D .

证明　设相关的 Euclid 函数为 $N: R\backslash\{0\}\to\mathbb{N}$, 任给 R 的一个理想 I, 如果 $I=0=\{0\}$, 则 $I=(0)$, 下设 I 中有非零元.
取 I 中非零元 a 使 $N(a)$ 达最小, 因为 $a\in I$, 所以 $(a)\subseteq I$, 再证 $I\subseteq(a)$.
假设 $b\in I\backslash(a)$, 做带余除法 $b=aq+r$, 则 $r\neq 0$ 且 $N(r)<N(a)$, 注意到 $r=b-aq\in I$, 所以这与 a 的选取矛盾, 由上 $I=(a)$ 为主理想. 故 Euclid 整环为 P.I.D . □

例3.6.3

证明：$\mathbb{Z}[x]$ 不为 Euclid 整环.

证明　因为 $(2,x)=\{2p(x)+xq(x): p(x),q(x)\in\mathbb{Z}[x]\}$ 是 $\mathbb{Z}[x]$ 上的理想, 我们来证明 $(2,x)$ 不为主理想.
假设 $(2,x)$ 为主理想, 则存在 $a(x)\in\mathbb{Z}[x]$ 设 $(2,x)=(a(x))$, 因为 $1\notin(2,x)$, 所以 $a(x)\neq\pm1$, 又因为 $2\in(a(x))$, 所以存在 $p(x)\in\mathbb{Z}[x]$ 使 $p(x)a(x)=2$, 因为 $\deg(p(x)a(x))=\deg p(x)+\deg a(x)$, 所以 $p(x),a(x)$ 必须都为常数, 故 $a(x)\in\{\pm2\}$. 又因为 $x\in(2,x)$, 所以存在 $q(x)\in\mathbb{Z}[x]$ 使 $x=2q(x)$, 这是不可能的, 矛盾. 所以 $\mathbb{Z}[x]$ 不为 P.I.D , 由定理3.6.2知$\mathbb{Z}[x]$ 不为 Euclid 整环. □

[1] Euclid 整环：Euclidean Domains, 主理想整环：Principal Ideal Domains(P.I.D).

定义3.6.3

设 d 为无平方因子的整数,

$$R_d=\begin{cases}\{a+b\sqrt{d}:a,b\in\mathbb{Z}\}=\mathbb{Z}[\sqrt{d}] & d\not\equiv 1 \pmod 4\\ \{a+b\frac{-1+\sqrt{d}}{2}:a,b\in\mathbb{Z}\}=\mathbb{Z}[\frac{-1+\sqrt{d}}{2}] & d\equiv 1 \pmod 4\end{cases}$$

可知 $Z[\frac{-1+\sqrt{d}}{2}]=\{\frac{x+y\sqrt{d}}{2}:x,y\in\mathbb{Z},x\equiv y \pmod 2\}$, 其中 $d\equiv 1 \pmod 4$.

例3.6.4

$R_{-1}=\mathbb{Z}[i]$, $R_{-3}=\mathbb{Z}[\omega]$.

定理.

$$R_d \text{为 } Euclid \text{ 整环}$$
$$\Leftrightarrow d=-1,-2,-3,-7,-11,2,3,5,6,7,11,13,19,21,29,33,37,41,57,73$$

这个定理比较难证, 但是考试时一般只考给一个 d 来证明 R_d 为 Euclid 整环.

Gauss 猜测 $d<0$ 时, R_d 为 P.I.D $\Leftrightarrow$ $d=$-1,-2,-3,-7,-11,-19,-43,-67,-163.
$d>0$ 时, 有无穷多个 d使 R_d 为 P.I.D .
$\mathbb{Z}[e^{2\pi i/n}]=\{\sum\limits_{k=0}^{n-1}a_ke^{2\pi i\frac{k}{n}}:a_k\in\mathbb{Z}\}$ 为 P.I.D $\Leftrightarrow$ n =3,4,5,7,8,9,. . . ,60,84

定义3.6.4

R 为<u>整环</u>, 如果存在单位 $u\in \mathrm{U}(R)$ 使 $a=bu$ (等价于 $a\mid b$, $b\mid a$ [2]), 则称 a 与 b **相伴**, 记为 $a\sim b$, 则 $\sim$ 为等价关系.
对 R 中非零且非单位元 p, 如果由 $p=ab$, 可得 $p\sim a$ 或 $p\sim b$, 则称 p **不可约**.
如果由 $p\mid ab$, 可得 $p\mid a$ 或 $p\mid b$, 则称 p 为**素元**.

定理3.6.3

设 R 为整环, 则

(1) R 中素元必为不可约元.

(2) R 为 P.I.D 时, R 中不可约元也是素元.

[2]如果 $a\mid b$, $b\mid a$, 则存在 $p,q\in R$ 使 $a=bq,b=aq$, 则 $b=bpq$, 因为 R 为整环, 故 $pq=1$, 所以 q 为单位.

证明 (1) 设 R 中非零非单位元 p 为素元, 如果 $p=ab$, 于是 $p \mid a$ 或 $p \mid b$, 不妨设 $p \mid a$, 由于 $a \mid ab=p$, 所以 $a \sim p$, 其中 b 为单位, 故 p 不可约.

(2) 设 R 中非零非单位元 p 不可约, 因为如果 $p=da$, 那么 $p \sim d$ 或 d为单位, 故如果 $(p) \subseteq (d) \subseteq R$, 那么 $(d)=(R)$ 或 $(d)=R$, 而 R 为 P.I.D , 所以 (p) 为极大理想[3]. 因为整环必为交换幺环, 故由定理3.4.1(101页)知, (p) 为素理想, 则 $ab \in (p) \Rightarrow a \in (p)$ 或 $b \in (p)$, 即 $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$, 即 p 为素元. □

推论3.6.1

设 R 为 P.I.D , 则 R 的一个非零理想是素理想 $\Leftrightarrow$ 它是极大理想.

证明 (1) "$\Leftarrow$" : 定理3.4.1(101页)已证.

(2) "$\Rightarrow$" : 因为 R 为 P.I.D , 因为 (p) 为素理想, 故如果 $ab \in (p)$, 则 $a \in (p)$ 或 $b \in (p)$, 即 $p \mid ab \Rightarrow p \mid a$ 或 $p \mid b$, 所以 p 为素元, 又因为 R 为 P.I.D , 所以由定理3.6.3知, p 为不可约元, 设 $(p) \subseteq (d) \subseteq R$, 故 $p=da$, 因为 p 为不可约元, 所以 $p \sim d$ 或 d 为单位, 即 $(d)=(p)$ 或 $(d)=R$. 故 (p) 为极大理想. □

定理3.6.4 (P.I.D 中唯一分解定理)

设 R 为 P.I.D , S 是由 R 中的一些素元(不可约元)构成的集合, 它满足

(1) 每个素元与 S 中某个元相伴.

(2) S 中任两个不相伴

则每个 $a \in R\backslash\{0\}$ 可唯一地表成 $u \prod_{p\in S} p^{e(p)}$, 其中 u 为单位, $e(p) \in \mathbb{N}$ 且只有有限多个 $p \in S$ 使 $e(p) \neq 0$

证明 课上并没有讲这个定理证明, 证明可参考 David S.Dummit 和 Richard M.Foote 所写的 Abstract Algebra 第8.3节(Unique Factorization Domains). □

[3]极大理想: 设 I 为 R 的理想, 如果 $I \subseteq J \trianglelefteq R \Rightarrow J=I$ 或 R, 则说 I 为 R 的极大理想.(可见101页的定义3.4.1)

从这个定理可以得到：域 $\subset$ Euclid 整环 $\subset$ 主理想整环(P.I.D.s) $\subset$ U.F.D.s $\subset$ 整环.

例3.6.5

$R=\mathbb{Z}$, 取 $S=\{p\in\mathbb{Z}:p$ 为正素数$\}$.

F 为域, $R=F[x]$, 取 $S=\{$首一不可约多项式$\}$

作业：

(1) 证明 $R_{-11}=\mathbb{Z}[\theta]\,(\theta=\frac{-1+\sqrt{-11}}{2})=\{\frac{x+y\sqrt{-11}}{2}:x\equiv y\pmod 2\}$ 按 $N(z)=z\bar{z}$ 构成 Euclid 整环.（仿代数学引论140页的例2的证明）

3.7 Noether 环

定义3.7.1

如果交换幺环 R 的每个理想都是有限生成的, 那么称 R 为 **Noether 环**, 即 R 的每个理想 I 形如

$$I=(a_1,\dots,a_n)=\{\sum_{i=1}^{n}r_ia_i:r_i\in R\}=Ra_1+\cdots+Ra_n$$

由定义可知, P.I.D 是 Noether 环.

定理3.7.1

设 R 是 Noether 环, 则下列几条等价:

(a) R 是 Noether 环.

(b) (理想升链条件)如果有理想升链

$$I_0\subseteq I_1\subseteq I_2\subseteq\cdots \tag{3.3}$$

则必有 $N\in\mathbb{N}$ 使 $I_N=I_{N+1}=\cdots$.

(c) R 的每个非空理想簇 $\{I_\lambda\}_{\lambda\in\Lambda}$ 必有(关于 $\subseteq$)极大元.

证明 (1) (a)$\Rightarrow$(b): 设 3.3为理想升链, 令 $I=\bigcup\limits_{k=0}^{\infty}I_k$, 如果 $a,b\in I$, 则有 $k,l\in\mathbb{N}$ 使 $a\in I_k, b\in I_l$, 令 $n=\max\{k,l\}$, 则 $a,b\in I_n$, 故 $a\pm b\in I_n\subseteq I$. 如果 $a\in I_k$, $r\in R$, 则 $ra\in I_k\subseteq I$, 故 I 为 R 的理想.
由条件(a)知, I 有限生成, 即 $I=(a_1,\dots,a_N)$. 对 $\forall 1\leqslant j\leqslant n$ 时, $a_j\in I=\bigcap\limits_{k=0}^{\infty}I_k$, 故有 k_j 使 $a\in I_{k_j}$, 让 $N=\max\{k_1,\dots,k_n\}$, 则 $a_1,\dots,a_n\in I_N$, 且 $I=(a_1,\dots,a_n)\subseteq I_N\subseteq I_{N+i}\subseteq I$, 故

$$I=I_{N+i}\,(i=0,1,2,\dots)$$

(2) (b)$\Rightarrow$(c): 利用反证法. 假如非空理想链 $\{I_\lambda\}_{\lambda\in\Lambda}$ 无极大元. 任取 $\lambda_1\in\Lambda$, 因为 I_{λ_1} 不是极大, 故有 $\lambda_2\in\Lambda$, 使 $I_{\lambda_1}\subset I_{\lambda_2}$, 如此下去可得一个严格理想升链

$$I_{\lambda_1}\subset I_{\lambda_2}\subset\cdots$$

这个与(b)矛盾, 故非空理想链 $\{I_\lambda\}_{\lambda\in\Lambda}$ 有极大元.

(3) (c)⇒(a): 利用反证法. 任给 R 的一个理想 I, 如果 I 不是有限生成的, 取 $a_1\in I$, 则 $I\neq(a_1)=I_1$, 故有 $a_2\in I-(a_1)$. 因为 $I\neq(a_1,a_2)=I_2$, 所以有 $a_3\in I-(a_1,a_2)=I-(a_1)-(a_2)$, 令 $I_3=(a_1,a_2,a_3)$, 依次下去, 可得 $I_1\subset I_2\subset I_3\subset\cdots$, 则可知 $\{I_i\}_{i+1}^{\infty}$ 无极大元, 与 (c) 矛盾. □

定理3.7.2 (Hilbert 基定理)

设 R 为 Noether 环, 则 $R[x]$ 也是 Noether 环.

证明 任给 $R[x]$ 的一个理想 I. 令

$$\begin{aligned}I_n&=\{a_n\in R:\exists a_0,\ldots,a_n\in R,\ \text{使}\ a_0+a_1x+\cdots+a_nx^n\in I\}\\&=\{p(x)\ \text{中}x^n\ \text{的系数}[x^n]p(x):p(x)\in I\ \text{且}\ \deg p(x)\leqslant n\}\end{aligned}$$

显然 I_n 对加减法封闭, 因为 $0\in I$, 故 $0\in I_n$. 注意到如果 $p(x)=\sum\limits_{i=0}^{n}a_ix^i\in I$, 因为 I 为 $R[x]$ 中的理想, 且 $r\in R[x]$, 故 $rp(x)=\sum\limits_{i=0}^{n}(ra_i)x^i\in I$, 从而 $ra_n\in I_n$, 因此 I_n 为 R 的理想. 此外因为 $p(x)\in I, x\in R[x]$, 所以 $xp(x)=\sum\limits_{i=0}^{n}a_ix^{i+1}\in I$, 所以可以得到 $a_n\in I_n\Rightarrow a_n\in I_{n+1}$, 于是 $I_n\subseteq I_{n+1}\,(n=0,1,\ldots)$. 故 $I_0\subseteq I_1\subseteq I_2\subseteq\cdots$ 为 R 的一个理想升链, 因为 R 为 Noether 环, 故有 $m\in\mathbb{N}$ 使 $I_m=I_{m+1}=\cdots$.

当 $0\leqslant n\leqslant m$ 时, 因为 R 是 Noether 环, 故 I_n 是有限生成的, 假设 $I_n=(a_{n1},\ldots,a_{nl_n})$. 当 $0\leqslant n\leqslant m, 1\leqslant j\leqslant l_n$ 时, $a_{nj}\in R$, 于是有多项式 $p_{nj}(x)\in I$, 使 $\deg p_{nj}(x)\leqslant n$ 且 $[x^n]p_{nj}(x)=a_{nj}$.

让 $J=\langle p_{nj}(x):0\leqslant n\leqslant m,\ 1\leqslant j\leqslant l_n\rangle$, 显然 $J\subseteq I$, 下证 $I\subseteq J$

对 $p(x)$ 次数进行归纳来证明 $p(x)\in I\Rightarrow p(x)\in J$, 首先 $p(x)=0$ 时, $0\in J$. 假如 $p(x)$ 的次数为 0 , 设 $p(x)=cx^0\,(c\in R, c\neq 0)$, 因为 $p(x)\in I$, 所以 $c\in I_0=(a_{01},\ldots,a_{0l_0})$, 故 $1\leqslant j\leqslant l_0$ 时, $a_{0j}\in I_0$, 则 $[x^0]p_{0j}(x)=a_{0j}$ 且 $\deg p_{0j}(x)\leqslant 0$, 故 $p_{0j}(x)=a_{0j}$, 则

$$p(x)=c\in(a_{01},\ldots,a_{0l_0})=(p_{01}(x),\ldots,p_{0l_0}(x))\subseteq J$$

下设 $p(x)\in I$ 且 $\deg p(x)=n>0$, 假定 I 中次数小于 n 的多项式都属于 J. 令 $a_n=[x^n]p(x)\in I_n=I_{\bar n}$, 其中 $\bar n=\min\{n,m\}\leqslant m$. 因为 $I_{\bar n}=(a_{\bar n1},\ldots,a_{\bar nl_{\bar n}})$, 于是有 $c_1,\ldots,c_{l_{\bar n}}$ 使 $a_n=\sum_{j=1}^{l_{\bar n}}c_ja_{\bar nj}$.

令

$$Q(x)=p(x)-\left(\sum_{j=1}^{l_{\bar n}}c_jp_{\bar nj}(x)\right)\cdot x^{n-\bar n}$$

则 $\deg Q(x) \leqslant n$, 又因为 $[x^n]Q(x) = a_n - \sum_{j=1}^{l_{\bar{n}}} c_j a_{\bar{n}j} = 0$, 故 $\deg Q(x) < n$. 注意 $p(x), p_{\bar{n}j}(x) \in I$, 所以 $Q(x) \in I$, 由归纳假设知 $Q(x) \in J$, 所以

$$p(x) = Q(x) + x^{n-\bar{n}} \left(\sum_{j=1}^{l_{\bar{n}}} c_j p_{\bar{n}j}(x) \right) \in J$$

故由归纳假设知 $I \subseteq J$, 故 $I = J$. □

例3.7.1

因为 $\mathbb{Z}$ 为 P.I.D, 从而为 Noether 环, 故 $\mathbb{Z}[x], \mathbb{Z}[x,y], \ldots, \mathbb{Z}[x_1, \ldots, x_n]$ 为 Noether 环.

因为 F 为 P.I.D, 从而为 Noether 环, 故 $F[x], F[x,y], \ldots, F[x_1, \ldots, x_n]$ 为 Noether 环.

定理3.7.3

设 R 为 Noether 环, 对 R 的每个理想 I 都有有限个素理想 $P_1, P_2, \ldots, P_n$ 使 $P_1 P_2 \cdots P_n \subseteq I$.

证明　设 $A = \{I \trianglelefteq R : \text{不存在素理想 } P_1, \ldots, P_n \text{ 使 } P_1 P_2 \cdots P_n \subseteq I\} \neq \emptyset$, 由于 R 为 Noether 环, 所以由定理3.7.1知 A 有极大元 $M \neq R$. 由 A 的性质知, P 为素理想时, $P \not\subseteq M$, 故 M 不是素理想, 于是有 $a, b \in R$ 使 $ab \in M$ 但 $a, b \notin M$. 因为 M 为 A 中的极大元, 故 $M + (a), M + (b) \notin A$, 于是有素理想 $P_1 \cdots P_n \subseteq M + (a)$, $Q_1 \cdots Q_m \subseteq M + (b)$, 于是

$$P_1 \cdots P_n Q_1 \cdots Q_n \subseteq (M + (a))(M + (b)) = MM + (a)M + M(b) + (ab) \subseteq M$$

这与 $M \in A$ 矛盾. □

作业:

(1) 设 R 为 Noether 环, $I \trianglelefteq R$, 证明 R/I 也为 Noether 环. [4]

(2) 代数学引论158页的第36题.

[4] 由推论3.2.1(91页)知 R/I 的理想形如 J/I, 其中 $I \leqslant J \trianglelefteq R$, 因为 J 有限生成, 不妨设 $J = (a_1, \ldots, a_n)$, 则任意 $x \in J$, 有 $x = \sum\limits_{i=1}^{n} r_i a_i$, 则相应的 $\bar{x} \in J/I$, 有

$$\bar{x} = \sum_{i=1}^{n} r_i a_i + I = \sum_{i=1}^{n} (r_i a_i + I) = \sum_{i=1}^{n} (r_i + I)(a_i + I) = \sum_{i=1}^{n} \overline{r_i a_i}$$

故 J/I 有限生成.

第 4 章　域论简介

由于我们这级的大二下学期的时间较短, 所以讲到域论简介时, 时间非常少, 其中第二节代数扩张最后的有些定理并没有详讲, 对这些定理我也没有整理它的证明, 应该知道就可以了. 第三节 Galois 理论简介老师只是略微的介绍下, 并没有讲证明, 而且第三节这些我们那年并没有考. 如果老师后来详细讲述了这些定理, 最好自己整理下.

4.1　域的特征及扩张次数

定义4.1.1

如果 F 为环且 $F^* = F\backslash\{0\}$ 按乘法构成 Abel 群, 则称 F 为**域**.

可知域F 的理想只有 $0 = (0)$ 和 $F = (1)$ [1], 且域必为整环, 为P.I.D.

验证 F 为域需要：(1)验证 F 为整环. (2)验证 F 中非零元均有乘法逆元.

[1]设 I 为域 F 的理想, 如果 I 中有非零元 a, 因为 F^* 构成群, 故 a 可逆, 故 $1 = aa^{-1} \in I$, 所以 $I = F$, 故域 F 的理想只有 $0 = (0)$ 和 $F = (1)$.

定义4.1.2

设 R 为整环, 在 $R\times R^*\,(R^*=R\backslash\{0\})$ 上定义商等价 $\sim$ 如下

$$\langle a,b\rangle\sim\langle c,d\rangle\Leftrightarrow ad=bc$$

可知 $\sim$ 具有自反性, 对称性, 和传递性[2], 从而 $\sim$ 为等价关系.
定义 $\langle a,b\rangle$ 所在等价类为

$$\frac{a}{b}=\{\langle c,d\rangle\in R\times R^*:\langle c,d\rangle\sim\langle a,b\rangle\}$$

让 $F=\{\frac{a}{b}:a\in R,b\in R^*\}$, 在 F 上定义 $+$ 与 $\cdot$ 如下:

$$\frac{a}{b}+\frac{c}{d}\triangleq\frac{ad+bc}{bd}\qquad\frac{a}{b}\cdot\frac{c}{d}\triangleq\frac{ac}{bd}$$

可以说明此定义合理[3].
F 构成域, 因为 $a,b\in R^*$ 时, $\frac{a}{b}\cdot\frac{b}{a}=\frac{1}{1}$, 故 $\left(\frac{a}{b}\right)^{-1}=\frac{b}{a}$, 可知 $\sigma:a\to\frac{a}{1}$ 是环 R 到域 F 的单同态, 注意到 σ 为单同态时, $\ker\sigma=1$, 故由环的同态基本定理(88页)知 F 的子环 $\{\frac{a}{1}:a\in R\}\cong R/\{1\}\cong R$.

设 F 为域, 对于 $a\in F$, $na=\underbrace{a+\cdots+a}_{n\text{个}}$, $(-n)a=\underbrace{-a-\cdots-a}_{n\text{个}}$, $0a$ 指 F 的零元"0".

$\langle a\rangle=\{ma:m\in\mathbb{Z}\}$ 是由 a 生成的加法子群, 使 $na=0$ 的最小正整数 n 叫 a 的**加法阶**. 当 $a\in F^*=F\backslash\{0\}$ 时, 因为 $na=ea+\cdots+ea=(e+\cdots+e)=(ne)a$, 又 F 为域且 $a\neq0$, 所以 $ne=0$, 故 $na=0\Leftrightarrow ne=0$, 即 a 的加法阶等于 e 的加法阶.所以我们可给出如下定义.

[2]自反性和对称性易证, 只给出 $\sim$ 的传递性证明: 设 $\langle a,b\rangle\sim\langle c,d\rangle$, $\langle c,d\rangle\sim\langle e,f\rangle$, 则可知 $ad=bc$, $cf=ed$, 故 $adcf=bced$, 由于 R 为整环, 且 $d\in R^*$, 故 $afc=bec$. 如果 $c\neq0$, 则可得 $af=be$; 若 $c=0$, 则可知 $a=e=0$, 故 $af=be$, 综上可得 $\langle a,b\rangle\sim\langle e,f\rangle$.

[3]要说明定义合理, 即要说明如果 $\frac{a}{b}=\frac{a'}{b'}$, $\frac{c}{d}=\frac{c'}{d'}$, 则所定义的和与积相同. 注意到 $ab'=a'b$, $cd'=c'd$, 所以

$$(ad+bc)b'd'=adb'd'+bcb'd'=ab'dd'+cd'bb'=a'bdd'+c'dbb'=(a'd'+b'c')bd$$
$$(ac)(b'd')=ab'cd'=a'bc'd=(a'c')(bd)$$

故 $\langle ad+bc,bd\rangle\sim\langle a'd'+b'c',b'd'\rangle$, $\langle ac,bd\rangle=\langle a'c',b'd'\rangle$, 即可得 $\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$, $\frac{ac}{bd}=\frac{a'c'}{b'd'}$, 所以定义合理.

定义4.1.3

使 $ne=0$ 的<u>最小正整数</u>叫域 F 的**特征**. 如果 $e,2e,3e,\ldots$ 都不等于 0, 则说 F 的特征为 0, F 的特征记为 $\mathrm{ch}(F)$.

性质4.1.1

如果 $\mathrm{ch}(F)$ 为正整数 p 时, 则 <u>p 必为素数</u>, 假设 $p=kl\,(1<k,l<p)$, 则 $(ke)(le)=(kl)e=pe=0$, 于是 $ke=0$ 或 $le=0$, 这与 p 的最小性矛盾, 故 p 为素数.

例4.1.1

$\mathbb{Q},\mathbb{R},\mathbb{C}$ 的特征为 0.

例4.1.2

设 p 为素数,则 $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}=\{\bar{a}=a+p\mathbb{Z}:a\in\mathbb{Z}\}$ 是 p 元域.

这是因为设 $\bar{a}\neq\bar{0}$, 则

$$\bar{a}\bar{s}=\bar{a}\bar{t}\Rightarrow p\mid as-at\overset{p\nmid a}{\Rightarrow}p\mid s-t\Rightarrow\bar{s}=\bar{t}$$

所以 $\bar{a}\bar{0},\ldots,\bar{a}\overline{p-1}$ 两两不等. 于是 $\mathbb{Z}/p\mathbb{Z}=\{\bar{a}\bar{x}:x=0,1,\ldots,p-1\}$, 所以存在 $x\in\mathbb{Z}$ 使 $\bar{a}\bar{x}=1$, 故 $\bar{a}$ 在 $\mathbb{Z}_p$ 中有乘法逆元, 故 $\mathbb{Z}_p$ 为域.

$\mathbb{Z}_p$ 中乘法单位元为 $\bar{1}=1+p\mathbb{Z}$, 则 $n\bar{1}=\underbrace{\bar{1}+\cdots+\bar{1}}_{n\text{个}}=\bar{n}$, 所以

$$n\bar{1}=0\Leftrightarrow\bar{n}=0\Leftrightarrow n\equiv 0\pmod p\Leftrightarrow p\mid n$$

故 $\mathrm{ch}(\mathbb{Z}_p)=p$.

设 F 为特征为素数 p 的域, 做 $\sigma:\mathbb{Z}\to F$ 如下

$$\sigma(m)=me$$

可知 σ 为环同态, 注意到

$$\ker\sigma=\{m\in\mathbb{Z}:me=0\}=\{m\in\mathbb{Z}:p\mid m\}=p\mathbb{Z}=(p)$$
$$\mathrm{Im}\sigma=\{me:m\in Z\}=(e)=\{0,e,\ldots,(p-1)e\}=E$$

依环的同态基本定理(88页), $\mathbb{Z}/p\mathbb{Z}\cong E$, 因为 $\mathbb{Z}/p\mathbb{Z}$ 为 p 元域, 所以 E 为 F 的 p 元子域.(E 是 F 的最小子域 [4])

[4]因为设 F' 为 F 的子域, 且 $F'\neq 0$, 则有非零元 $a\in F'$, 因为 F' 为域, 故 $a^{-1}\in F'$, 所以 $e=a^{-1}a\in E$, 即可得 $E\subseteq F'$.

性质4.1.2

如果 F 为特征为素数 p 的域, 则 $(a+b)^p=a^p+b^p$, $(b-a)^p=b^p-a^p$, 一般地 $(a_1+\cdots+a_m)^{p^k}=a_1^{p^k}+\cdots+a_m^{p^k}$

证明 设 F 为特征为素数 p 的域, $1\leqslant k\leqslant p-1$ 时,

$$\binom{p}{k}=\frac{p\cdot(p-1)\cdots(p-k+1)}{k!}$$

因为 $p\mid k!\binom{p}{k}$, 而 $p\nmid k!$, 故 $p\mid\binom{p}{k}$.
对 $a,b\in F$, $(a+b)^p=a^p+\sum\limits_{k=1}^{p-1}\binom{p}{k}a^kb^{p-k}+b^p$, 注意 $p\mid\binom{p}{k}$, 所以 $\binom{p}{k}a^kb^{p-k}=0$, 故 $(a+b)^p=a^p+b^p$. 还可得到

$$(a+b)^{p^2}=((a+b)^p)^p=(a^p+b^p)^p=a^{p^2}+b^{p^2}$$
$$(a+b+c)^p=(a+b)^p+c^p=a^p+b^p+c^p$$
$$(a+b+c)^{p^k}=a^{p^k}+b^{p^k}+c^{p^k}$$

一般地, 在特征为素数 p 的域里我们有

$$(a_1+\cdots+a_m)^{p^k}=a_1^{p^k}+\cdots+a_m^{p^k}$$

如果我们将 $b=b-a$ 代入, 可得 $(b-a)^p=b^p-a^p$. $\square$

定义4.1.4

我们称域 F 为**有限域**, 如果域 F 中只有有限个元素. 一般地 $|F|$ 是正整数 q 时, 称 F 为 q 元域.

定理4.1.1

设 F 为 q 元域, 则 $x^q-x=\prod\limits_{a\in F}(x-a)$

证明 因为 $x^q - x = x(x^{q-1} - 1)$, $\prod\limits_{a\in F}(x-a) = x\prod\limits_{a\in F^*}(x-a)$, 故只需要证明 $x^{q-1} - 1 = \prod\limits_{a\in F^*}(x-a)$ 即可.

因为 F^* 是 $q-1$ 阶乘法群, 由定理3.5.4(110页)知 F^* 为循环群, 故 $a^{q-1} = e$. 让

$$p(x) = x^{q-1} - 1 - \prod_{a\in F^*}(x-a)$$

可知 F^* 中的 $p-1$ 个元均为 $p(x) = 0$ 的根, 又 $\deg p(x) < n-1$, 故 $p(x)$ 必为零多项式. □

定义4.1.5

V 是域 F 上**线性空间**指

(1) V 按加法构成 Abel 群.

(2) $a \in F, x \in V \Rightarrow a \circ x \in V$, 称 $\circ$ 为数乘运算, 且满足

(i) $1 \circ x = x$

(ii) $(ab) \circ x = a \circ (b \circ x)$

(iii) $a \circ (x+y) = a \circ x + a \circ y$

(iv) $(a+b) \circ x = a \circ x + b \circ x$

定义4.1.6

设 K 为域 L 的子域, 对 $a \in K$ 及 $\alpha \in L$ 定义 $a \circ \alpha = a\alpha \in L$, 可知 $\circ$ 满足定义4.1.5中的(i),(ii),(iii),(iv)四条, 故 L 为域 K 上的线性空间, 它的维数记为 $[L:K]$, 称为 L/K （L 是 K 的扩域）的**扩张次数**.

4.2　代数扩张

定义4.2.1

K 是域 L 子域时也称 L 为 K 的**扩域**, 并用 L/K 表示这个域扩张.
设 L/K 为域扩张, $X \subseteq L$, $K[X] = \bigcap_{L \supseteq R \supseteq K \cup X} R$ 是包含 K 与 X 的 L 的最小子环.
$K(X) = \bigcap_{\substack{K \subseteq F \subseteq L \\ X \subseteq F}} F$ 是包含 K 与 X 的 L 中最小子域, 称为 X 生成的 K 的扩域.
其中 R 为环, F 为域.
$X = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ 时, $K[X]$ 可写成 $K[\alpha_1, \alpha_2, \ldots, \alpha_n]$, $K(x)$ 可写成 $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
事实上

$$K[\alpha_1, \alpha_2, \ldots, \alpha_n] = \{P(\alpha_1, \alpha_2, \ldots, \alpha_n) : P(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]\}$$

$$K(\alpha_1, \ldots, \alpha_n) = \{\frac{P(\alpha_1, \ldots, \alpha_n)}{Q(\alpha_1, \ldots, \alpha_n)} : P(x_1, \ldots, x_n), Q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n] \\ \text{且} Q(\alpha_1, \ldots, \alpha_n) \neq 0\}$$

其中 $K[x_1, x_2, \ldots, x_n]$ 为 K 上 n 元多项式环 [1]. 特别地 $K(\alpha)/K$ 叫域 K 的**单扩张**.

定义4.2.2

设 L/K 为域扩张, $\alpha \in L$, 如果有非零多项式 $f(x) \in K[x]$ 使 $f(\alpha) = 0$, 则说 α 为 K 上**代数元**. $\alpha \in L$ 不为 K 上代数元时, 称之为 K 上**超越元**.
特别地, $\mathbb{Q}$ 上的代数元叫做代数数, $\alpha \in \mathbb{C}$ 不是代数数时, 称为超越数, 如 e, π 等.

其实我们可以知道代数数是可数的, 实的超越数不可数, 且有理数都是代数数.
$(r \in \mathbb{Q}, x - r = 0)$

[1] 可见108页的定义3.5.1

性质4.2.1

设 L/K 为域扩张, $\alpha \in L$ 为 K 上代数元, 可知 $I = \{g(x) \in K[x] : g(\alpha) = 0\}$ 是 $K[x]$ 是非零理想[2].由例3.6.1(111页) 知 $K[x]$ 是 Euclid 整环, 故为 P.I.D[3], 故有唯一的首一多项式 $f(x) \in K[x]$ 使 $I = (f(x))$, 称此 $f(x)$ 是 α 在 K 上**极小多项式**[4]. 且

$$g(\alpha) = 0 \Leftrightarrow g(x) \in I \Leftrightarrow f(x) \mid g(x)$$

此外 $f(x) \in K[x]$ 不可约, 因为如果 $f(x) = f_1(x)f_2(x)$, 其中 $0 < \deg f_1(x), \deg f_2(x) < \deg f(x)$, 则 $f_1(\alpha)f_2(\alpha) = 0$, 因为 $K[x]$ 为整环, 故 $f_1(\alpha) = 0$ 或 $f_2(\alpha) = 0$, 但是 $f(x) \nmid f_1(x)$, $f(x) \nmid f_2(x)$, 得到矛盾.

例4.2.1
$i = \sqrt{-1}$ 是 $\mathbb{R}$ 上的代数元, 且 i 在 R 上的极小多项式为 $x^2 + 1$.

定义4.2.3

K 上代数元 α 的极小多项式为 n 次时, 称 α 为 K 上的 **n 次代数元**.

定理4.2.1

设 L/K 为域扩张, $\alpha \in L$ 为 K 上 n 次代数元, 极小多项式为 $f(x)$, 则

(1) $K(\alpha) = K[\alpha]$, $[K(\alpha) : K] = n$, 且 $1, \alpha, \ldots, \alpha^{n-1}$ 为 K 上线性空间 $K(\alpha)$ 的一组基.

(2) $K(\alpha) \cong K[x]/(f(x))$

证明 (1) $k(\alpha) = \{\frac{P(\alpha)}{Q(\alpha)} : P(x), Q(x) \in K[x], Q(\alpha) \neq 0\}$, 设 $g(x) \in K[x]$, 且 $g(\alpha) \neq 0$, 故 $f(x) \nmid g(x)$, $(f(x), g(x)) = 1$[5], 则存在 $u(x), v(x) \in K[x]$ 使 $f(x)u(x) + g(x)v(x) = 1$. 取 $x = \alpha$, 则 $g(\alpha)v(\alpha) = 1$, 即 $\frac{1}{g(\alpha)} = v(\alpha)$, 故 $\frac{1}{g(\alpha)} = v(\alpha)$, 故 $\frac{P(\alpha)}{Q(\alpha)} = P(\alpha)Q'(\alpha) \in K[x]$, 其中 $Q'(\alpha)Q(\alpha) = 1$, 所以

$$K(\alpha) = K[\alpha] = \{\sum_{i=0}^{m} c_i a^i : c_0, c_1, \ldots, c_m \in K\}$$

[2] 因为 α 为代数元, 故有 I 中有非零多项式.
[3] 这由112页的定理3.6.2得到.
[4] 即所有满足 $p(\alpha) = 0$ 中次数最低的多项式.
[5] 如果 $(f(x), g(x)) = q(x)$, 且 $\deg q(x) \geqslant 1$, 则因为 $g(\alpha) \neq 0$, 故 $q(\alpha) \neq 0$, 令 $f(x) = p(x)q(x)$, 则 $p(\alpha) = 0$, 注意到 $\deg p(x) < \deg f(x)$, 这与 $f(x)$ 为 α 的极小多项式矛盾.

设 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n$, 则
$\alpha^n=-a_1\alpha^{n-1}-\cdots-a_n\in K\alpha^{n-1}+K\alpha^{n-2}+\cdots+K$, 两边同乘 α 可得,
$\alpha^{n+1}\in K\alpha^n+K\alpha^{n-1}+\cdots+K\subseteq K\alpha^{n-1}+K\alpha^{n-2}+\cdots+K$, 利用归纳法可得 $\alpha^m\in K+K\alpha+\cdots+K\alpha^{n-1}\,(m=0,1,2,\ldots)$ 故
$K[\alpha]=\{\sum_{i=0}^{n-1}c_i\alpha^i:c_0,\ldots,c_{n-1}\in K\}$, 所以 $\{\alpha^0,\ldots,\alpha^{n-1}\}$ 为 K 上线性空间 $K(\alpha)$ 的生成系.
如果有 $c_0,\ldots,c_{n-1}\in K$ 使 $g(\alpha)=\sum_{i=0}^{n-1}c_i\alpha^i=0$, 因为 $f(x)\mid g(x)$, 且 $\deg g(x)<\deg f(x)$, 故 $g(x)$ 为零多项式, 即
$\sum_{i=0}^{n-1}c_i\alpha^i=0\Leftrightarrow c_0=c_1=\cdots=c_{n-1}=0$, 故 $\alpha^0,\ldots,\alpha^{n-1}$ 在 K 上线性无关,
综上可得 $1,\alpha,\ldots,\alpha^{n-1}$ 为 K 上线性空间 $K(\alpha)$ 的一组基.

(2) 做 $\sigma:K[x]\to K(\alpha)$ 如下

$$\sigma(p(x))=p(\alpha)$$

则因为 $K(\alpha)=K[\alpha]=\{p(\alpha):p(x)\in K[x]\}$, 所以 σ 为满同态, 且

$$\ker\sigma=\{p(x)\in K[x]:p(\alpha)=0\}=(f(x))$$

依同态基本定理(88页)知 $K[x]/\ker\sigma=K[x]/(f(x))\cong K(\alpha)$. □

例4.2.2

i 是 $\mathbb{R}$ 上二次单位元, 故极小多项式为 x^2+1,
$\mathbb{R}(i)=\mathbb{R}[i]=\{a+bi:a,b\in\mathbb{R}\}=\mathbb{C}$, 且

$$\mathbb{R}(i)\cong\mathbb{R}[x]/(x^2+1)=\{f(x)\bmod x^2+1:f(x)\in\mathbb{R}[x]\}$$

定义4.2.4

$[L:K]<\infty$ 时, 称 L/K 为**有限扩张**, $\alpha\in L$ 为 K 上超越元时, $1,\alpha,\ldots,\alpha^n,\ldots$ 中任何有限个线性无关, 故 $[L:K]=\infty$.
设 L/K 为域扩张, 如果 L 中元都是 K 上代数元, 则称 L/K 为**代数扩张**, 否则为**超越扩张**.

引理4.2.1

设 L/K 为域扩张, $\alpha\in L$, 则称 α 是 K 上代数元, 如果存在不全为 0 的 $\alpha_1,\ldots,\alpha_n\in L$ 使对 $V=K\alpha_1+\cdots+K\alpha_n$, 有 $\alpha V\subseteq V$

证明 “$\Rightarrow$”：设 α 是 K 上 n 次代数元, $\alpha^n+a_1\alpha^{n-1}+\cdots+a_n=0\,(a_i\in K)$, 故 $\alpha^n\in V$. 让 $V=K+K\alpha+\cdots+K\alpha^{n-1}=\{\sum_{i=0}^{n-1}c_i\alpha^i:c_i\in K\}$, 注意到 $\alpha^n\in V$, 则$\alpha V\subseteq V$.

“$\Leftarrow$”：因为 $\alpha\alpha_i\in\alpha V\subseteq V$, 所以 $\alpha\alpha_i$ 可表成 $\sum_{j=1}^n a_{ij}\alpha_j\,(a_{ij}\in K)$, 故可得

$$\alpha\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=A\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}\quad(A=(a_{ij}))$$

所以

$$(\alpha I_n-A)\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$$

即方程组

$$(\alpha I_n-A)\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}\text{ 有非零解.}$$

由高等代数的知识知道 $|\alpha I_n-A|=0$, 故 α 是

$$p(x)=\begin{vmatrix}x-a_{11}&-a_{12}&\cdots&-a_{1n}\\ -a_{12}&x-a_{22}&\cdots&-a_{2n}\\ \vdots&\vdots&\ddots&\vdots\\ -a_{n1}&-a_{n2}&\cdots&x-a_{nn}\end{vmatrix}=0\text{ 的根}$$

注意到 $k(x)\in K[x]$, 所以 α 为代数元. □

定理4.2.2

设 L/K 为域扩张, 则 $M=\{\alpha\in L:\alpha\text{ 为 }K\text{ 上代数元}\}$ 为 L 的子域

证明 设 α 是 K 上 n 次代数元, β 是 K 上 m 次代数元.让

$$V=\sum_{\substack{0\leqslant i<n\\ 0\leqslant j<m}}K\alpha^i\beta^j$$

由于

$$\alpha^n\in K+K\alpha+\cdots+K\alpha^{n-1}$$
$$\beta^m\in K+K\beta+\cdots+K\beta^{m-1}$$

所以 $\alpha V\subseteq V$, $\beta V\subseteq V$, 故 $(\alpha\pm\beta)V\subseteq\pm\beta V\subseteq V$, 另外
$(\alpha\beta)V=\alpha(\beta V)\subseteq\alpha V\subseteq V$. 故依引理4.2.1知 $\alpha\pm\beta,\alpha\beta$ 为 K 上代数元.
设 $\alpha\neq 0$, 如果 $\alpha^n+c_1\alpha^{n-1}+\cdots+c_n=0$, 则 $1+c_1\frac{1}{\alpha}+\cdots+c_n(\frac{1}{\alpha})^n=0$, 故 $\alpha^{-1}=\frac{1}{\alpha}$ 为 K 上代数元, 故由上 $M=\{\alpha\in L:\alpha$ 为 K 上代数元$\}$ 为 L 的子域. □

定义4.2.5

首一整系数多项式的根叫**代数整数**, 记 $\mathrm{O}_k=\{K$ 中代数整数$\}$. $\mathbb{Q}$ 的有限次扩域 K 叫**代数数域**.

性质4.2.2

全体代数整数构成环.

例4.2.3

$d\in\mathbb{Z}$ 不是完全平方数时, $\mathbb{Q}(\sqrt{d})=\mathbb{Q}[\sqrt{d}]=\{a+b\sqrt{d}:a,b\in\mathbb{Q}\}$ 为二次数域.
可证

$$\mathrm{O}_{\mathbb{Q}(\sqrt{d})}=\begin{cases}\mathbb{Z}[d]=\mathbb{Z}+\mathbb{Z}[d] & d\not\equiv 1 \pmod 4\\ Z[\frac{-1+\sqrt{d}}{2}] & d\equiv 1 \pmod 4\end{cases}=R_d$$

是 Noether 环.

定义4.2.6

设 K 为域, 如果 $K[x]$ 中每个非零多项式可在 $K[x]$ 中分解成一次式的乘积, 则称 K 为**代数闭域**.

例4.2.4

由代数基本定理知 $\mathbb{C}$ 为代数闭域.
可证 {全体代数数} 是代数闭域.

定理4.2.3

q 元域存在等价于 q 为素数幂次, q 元域如果存在在同构意义下唯一.

证明　课上只证明了 q 元域存在等价于 q 为素数的幂次.设 $\mathrm{ch}(F)=p$, 令 $E=\{0,e,\dots,(p-1)e\}$, 设 F/E 是 n 次扩张, 则 $\alpha_1,\dots,\alpha_n$ 为 F 的一组基底, 则 $F=\{\sum_{i=1}^n a_i\alpha_i : a_i\in E\,(i=1,2,\dots,n)\}$. 因为 $\alpha_1,\dots,\alpha_n$ 为 F 的一组基底, 故如果 $a_1,\dots,a_n$ 与 $b_1,\dots,b_n$ 不完全相同, 则 $\sum_{i=1}^n a_i\alpha_i$ 与 $\sum_{i=1}^n b_i\alpha_i$ 不同, 又每个 $a_i\in E$, 所以 F 为有限域, 且 $|F|=|E|^n=p^n$. □

作业：

(1) 设 M/K 与 L/M 为域扩张, 证明 $[L:K]=[L:M][M:K]$.

(2) 设 P_1,P_2 为交换幺环 R 的素理想, I 为 R 的理想, 如果 $I\subseteq P_1\cup P_2$, 证明：$I\subseteq P_1$ 或 $I\subseteq P_2$ [6].

(3) $\mathbb{Z}[x]$ 是否为主理想整环 [7].

[6]利用反证法, 如果 $a_1\in P_1, a_2\in P_2$, $a_1,a_2\in I$, 但是 $a_1\notin P_2, a_2\notin P_1$, 则 $a_1+a_2\notin P_1\cup P_2$, 但是 $a_1+a_2\in I$, 得到矛盾.

[7]证明可参照112页的例3.6.3

4.3　Galois 理论简介

定义4.3.1

对域 F 和 $f(x) \in F[x]$, 如果域 F 的扩域 K 满足 $f(x)$ 可以分解成一次式的乘积, 且 $f(x)$ 在 K 的任何包含 F 的真子域上都不能分解成一次式的乘积, 则称 K 为 $f(x)$ 的一个**分裂域**.
设 L/K 为代数扩张, $\alpha \in L$ 在 K 上极小多项式在其分裂域中无重根, 则称 α 为**可分**(或**可离**).
L 中每个元为 K 上可分时, 称 L/K 为**可分扩张**.
如果 $K[x]$ 上任意不可约多项式 $f(x)$ 在 L 中有零点, 则所有零点均属于 L[1], 则称 L/K 为**正规扩张**.
有限可分的正规扩张叫 **Galois 扩张**.
域扩张的 Galois 群: $\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) : \forall a \in K(\sigma(a) = a)\}$ 为 $\mathrm{Aut}(L)$ 的子群, $K \leqslant M \leqslant L$ 时, $\mathrm{Gal}(L/M) \leqslant \mathrm{Gal}(L/K)$.
$H \leqslant \mathrm{Gal}(L/K)$ 时, $\mathrm{Inv}(H) = \{\alpha \in L : \forall \sigma \in H(\sigma(\alpha) = \alpha)\}$.

Galois 理论基本定理. *设 L/K 为 Galois 扩张*

(1) *设 $K \leqslant M \leqslant L$, 则 L/M 也是 Galois 扩张, 且 $\mathrm{Gal}(L/M) \leqslant \mathrm{Gal}(L/K)$, $|\mathrm{Gal}(L/M)| = [L : M]$, $\mathrm{Inv}(\mathrm{Gal}(L/M)) = M$*

(2) *任给 $H \leqslant \mathrm{Gal}(L/K)$, 则 $K \leqslant M = \mathrm{Inv}(H) = L$, $|\mathrm{Gal}(L/M)| = [L : M]|$.*

(3) *设 $K \leqslant M \leqslant L$, 则 M/K 是正规扩张 $\Leftrightarrow \mathrm{Gal}(L/M) \trianglelefteq \mathrm{Gal}(L/K)$, 且*

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K) \big/ \mathrm{Gal}(L/M)$$

Galois 理论中还有根式扩张等定义, 不一一列举.

定理(Galois). *K上 $f(x) = 0$ 根式可解 $\Leftrightarrow \mathrm{Gal}(L/K)$ 为可解群, 其中 L 为 $f(x)$ 在 K 上分裂域.*

[1]这句话等价于如果 $f(x)$ 在 L 上有一个根时, 则 $f(x)$ 在 L 上可以完全分解成一次式乘积.