§1. 群的定义

定义1.1 设 G 是一个非空集合，我们说 G 对于代数运算·作成一个群，如果满足：

G0. G 对于乘法·封闭；

G1. 结合律成立；

G2. 存在一个$e \in G$，使得 $\forall a \in G$都有

$$e \cdot a = a \cdot e = a.$$

G3. $\forall a \in G$都存在$a^{-1} \in G$，使得

$$a^{-1} \cdot a = a \cdot a^{-1} = e\ .$$

注：此时我也称群（G，$\cdot$）或群G;

群里的代数运算通常称为乘法运算，简称乘法，

$a \cdot b$ 也记为 ab .

例. (平凡群) G只包含一个元g. 乘法是 $gg = g$.

则 G对于这个乘法来说作成一个群.

例. 在数集中,关于普通的加法乘法运算。

例 在矩阵集合关于矩阵加法乘法运算.

例 向量空间是一个加法群

例 (重新定义的运算) 在 $\mathbb{Z}$上定义运算

$$a \oplus b = a + b - 1$$

判断 $\mathbb{Z}$ 关于给定的运算是否构成群.

定理1.2 （1）在一个群里存在一个并且只存在一个元，能使
对于 G 的任意元 a，都有 $ea = ae = a$.

（2）对于群 G 的每一个元 a 来说，在 G 里存在一个而且只存在一个元 a^{-1} ，能使

$$a^{-1}a = aa^{-1} = e.$$

定义1.3 一个群 G 的唯一的能使
$ea = ae = a$ 对于 G 的任意元 a 都成立
的元 e 叫做群 G 的单位元.

唯一的能使 $a^{-1}a = aa^{-1} = e$
的元 a^{-1} 叫做元 a 的**逆元**（有时简称**逆**）.

例 我们已经知道全体不等于零的有理数对于普通乘法来说作成一个群. 这个群的单位元 1，a 的逆元是 $\frac{1}{a}$.

例 全体整数对于普通加法来说作成一个群. 这个群的单位元是零，a 的逆元是 $-a$.

定理1.4 设G是一个非空集合，且G上的运算$\cdot$适合结合律，则下列命题相互等价：

（1）（G，$\cdot$）是一个群

（2）G4. 对于G的任意两个元a，b来说，方程

$$ax = b \quad \text{和} \quad ya = b$$

都在G中有解.

（3）G2'. 存在$e \in G$,使得$\forall a \in G$，都有$ea = a$；

G3'. $\forall a \in G$都存在$a' \in G$，使得

$$a' \cdot a = e\ .$$

(1)⟹ (2)：

因为G是群，任取a, b ∈ G则存在$a^{-1} \in G$，

易知$x = a^{-1}b$是$ax = b$在G中的解，

$y = ba^{-1}$是$ya = b$在G中的解.

(2)⟹ (3)：

对于一个固定的元 b，

$$yb = b$$

在 G 里有解．我们任意取一个解 e，即：$eb = b$.

我们要证明这个 e就是左单位元，即：对于G 的任意元a，都有 $ea = a$ 成立.

又 $bx = a$有解,记为 c，即$bc = a$，从而有

$$ea = e(bc) = (eb)c = bc = a.$$

而a'可以取$ya = e$的解.

(3)$\Longrightarrow$ (1)：

任取$a \in G$，则有元a'，使得$a'a = e$.

且有 a'' ，使得$a''a' = e$.

从而有

$$aa' = e(aa') = (a''a')(aa') = a''ea' = a''a' = \mathrm{e}.$$

即有$aa' = a'a = \mathrm{e}$.

故$ae = a(a'a) = (aa')a = ea = a$.

一个群G的元素的个数可以有限也可以无限．我们规定

定义1.5　一个群叫做**有限群**，如果这个群的元的个数是一个有限数．否则这个群叫做**无限群**．一个有限群的元的个数叫做这个**群的阶**，记为$|G|$.

在一个群里结合律是对的，所以

$$a_1 a_2 \cdots a_n$$

有意义，是 G的某一个元．这样，我们当然可以把 n个相同的元来相乘，我们也用普通乘方的符号 a^n 来表示，即

$$a^n = \overbrace{aa\ldots a}^{n次}, \qquad n \in Z^+,$$

并且也把它叫做 a 的 n 次**乘方**（简称 n 次方）．

当m,n是正整数时，我们已经规定过符号的意义，并且

$$a^n a^m = a^{n+m} \quad \text{与} \quad (a^n)^m = a^{nm} \qquad (*)$$

现在我们利用唯一的单位元 e 和 a 的逆元 a^{-1} 规定：

$$a^0 = e$$

$$a^{-n} = (a^{-1})^n \quad (\text{n正整数})$$

这样规定以后， (*)式对于任何整数都对.

$(ab)^n = a^n b^n$ 成立吗??

在一般的群里交换律未必成立.

定义1.6 一个群叫做**交换群**(Abelian group)，假如

$$ab = ba$$

对于 G 的任何两个元 a ，b都成立.

定义1.6' 如果一个交换群 G 的运算称为加法,这个群就称为加群. 加法用符号 "+"来表示.

群论里的许多符号都是因为把群的代数运算叫做了乘法才那样选择的。因此在加群里我们也选择新符号，从而计算规则的形式也跟着改变 .

一个加群的唯一的单位元我们用0表示，并且把它叫做**零元:**

$$0+a=a+0=a(a\text{是任意元}).$$

元 a 的唯一的逆元我们用 $-a$ 来表示，并且把它叫做 a 的**负元**（简称负 a ）:

$$a+(-a)=0$$

群的加法适合结合律，n个元 $a_1, a_2, \cdots, a_n$ 的和有意义，这个和我们有时用符号 $\sum_{i=1}^{n} a_i$ 来表示：

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \cdots + a_n$$

n个 a 的和（n是正整数）我们用符号 na 来表示

$$na = \overbrace{a + a + \cdots + a}^{\text{n个}}$$

如乘法群的情形一样，我们进一步规定

$0a=0.$

(这里第一个0是整数零，第二个0是加群的零元)

$$(-n)a = -(na).$$

加群运算规律:

$na + ma = ?$

$m(na) = ?$

$n(a + b) = ?$

这几个公式与乘法群的相当完全平行。
我们要注意，这里的整数m，n一般不是加群的元。

定义1.7 群 G 的一个元 a ，使得

$$a^m = e$$

的最小的正整数 m 叫做 a 的**阶**. 若是这样的一个 m 不存在，我们说， a 是无限阶的. a 的阶记为$\circ(a)$.

例 G 刚好包含 $x^3=1$ 的三个根：

$$1,\quad \varepsilon_1=\frac{-1+\sqrt{-3}}{2},\qquad \varepsilon_2=\frac{-1-\sqrt{-3}}{2}$$

对于普通乘法来说，G 作成一个群：

- G0和G1:显然；
- G2: 1 是的单位元；
- G3: 1 的逆元是 1，ε_1的逆元是 ε_2，ε_2的逆元是 ε_1.

1 的阶是1，ε_1的阶是3，ε_2的阶是3.

定理1.8 群 G 的一个元 a 的阶为m，则

$$a^n = e \Leftrightarrow m|n.$$

证明：⇐：若$m|n$ ，则有$mt = n,$

于是 $a^n = a^{mt} = (a^m)^t = e^t = e.$

⇒：设 $a^n = e$，则令$n = mq + r, 0 \leq r < m,$
于是 $e = a^n = a^{mq+r} = (a^m)^q \cdot a^r = e \cdot a^r = a^r.$
又$m = \circ(a)$, 故有$r=0$,从而有$m|n.$

定理1.9 一个群的乘法适合消去律，即

G5. 若 $ax = ax'$ ，那么 $x = x'$；

若 $ya = y'a$ ，那么 $y = y'$.

推论1.10 在一个群里，方程

$ax = b$ 和 $ya = b$

各有唯一的解.

一个群一定满足:
G0. 闭合性
G1. 结合律
G5. 消去律
但反过来不对，即一个集合适合G0，G1，G5，
它不一定构成群。

例 G ={所有不等于零的整数}.

对于普通乘法来说这个G适合G0，G1，G5，但不构成群.
但如果 G 是一个有限集合时，情形就不同了.

定理1.11 一个有乘法的有限集合 G，若适合G0，G1，G5，那么G构成群.

证明： 我们先证明$\forall a, b \in G$, 则$ax = b$在G中一定有解.

假定G有n个元，并记$G = \{a_1, \cdots a_n\}$.

我们用a从左边来乘所有的a_i作成一个集合

$$G' = \{aa_1, \cdots aa_n\} \subseteq G.$$

由消去律知G'的阶与G的阶相同，从而$G' = G$.

从而存在$a_k \in G$，使得$aa_k = b$，
于是a_k即为$ax = b$在G中的解.

同理可证$ya = b$在G中一定有解.

由这个定理我们可以得到

有限群的另一定义 我们说，一个有乘法的有限不空集合 G 作成一个群，假如G0，G1，G5能被满足.

有限群的运算可以用乘法表给出，由于单位元和消去律，表里一定有且仅有一行元同横线上的元一样，也一定有一列元同垂线左边的元一样. 同样，有且仅有一列与竖线左边的元一样.任意元比在每一行（也在每一列）出现一次.

遗憾的是，结合律从表里不容易看出来.

例 $G = \{a, b, c, d\}$

$\circ$	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	b	d
d	d	c	a	b

§2. 群同态

定理2.1 假定 G 是群，$\overline{G}$ 是非空集合，如果对 G 的乘法，以及 $\overline{G}$ 的乘法，有一个 G 到 $\overline{G}$ 的满同态，则 $\overline{G}$ 也是一个群.

证明: $\overline{G}$ 显然适合群定义的条件G0，

又 G 的乘法适合结合律，而 G 到 $\overline{G}$ 有满同态，

从而 $\overline{G}$ 的乘法也适合结合律.

设 $e \in G$ 是单位元，记满同态为

$$\varphi : G \to \overline{G}.$$

则对 $\forall \bar{a} \in \bar{G}$，都有 $a \in G$，使得 $\bar{a} = \varphi(a)$.

令 $\bar{e} = \varphi(e)$，于是有

$$\bar{e}\bar{a} = \varphi(e)\varphi(a) = \varphi(ea) = \varphi(a) = \bar{a},$$

从而 $\bar{e}$ 是 $\bar{G}$ 单位元.

假定 $\overline{a}$ 是 $\overline{G}$ 的任意元，a 是 $\overline{a}$ 的一个逆象，则

$$\varphi(a^{-1})\overline{a} = \varphi(a^{-1}a) = \varphi(e) = \overline{e},$$

从而 $\varphi(a^{-1})$ 是 $\overline{a}$ 的左逆元.

注：讨论$(G,\cdot)$和$(\overline{G},\cdot)$两个代数系统之间的态射时，它们的乘法可以用相同的符号表示而不会出现歧义和混淆.

注： 我们要注意，假如 G 同 $\overline{G}$ 的次序掉换一下，那么定理2.1不一定对，换一句话说，假如 $\overline{G}$ 到 G 有满同态，那么 $\overline{G}$ 不一定是一个群.

例: $\overline{G}$ ＝｛所有奇数｝． 对于普通乘法来说 $\overline{G}$ 不作成一个群． 而 $G=\{e\}$ 对于乘法 $ee=e$ 来说显然作成一个群.

但 $\varphi:\overline{a}\to e$ 显然是 G 到 $\overline{G}$ 的一个同态满射.

例： 设G $=\{a,b,c\}$，G上的运算有下表给出，证明G是一个群.

$\circ$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

证明： 设G'是由 $x^3=1$ 的三个根构成的集合：

$$1,\quad \varepsilon_1=\frac{-1+\sqrt{-3}}{2},\qquad \varepsilon_2=\frac{-1-\sqrt{-3}}{2}$$

对于普通乘法来说, G' 作成一个群.

构造一个G'到G的同构映射.

由定理2.1的证明我们直接可以看出

推论2.2 假定G和$\overline{G}$是两个群．在G到$\overline{G}$的一个同态满射之下，G的单位元e的象是$\overline{G}$的单位元，G的元a的逆元a^{-1}的象是a的象的逆元.

注： 同构的两个群，单位元相互对应，相对应的元的逆相对应.

§3. 变换群

集合 A到 A自己的映射称为A上的变换.

设 τ 是 A 上变换,记其在元素a上的作用为:

$$\tau:\ \mathrm{A} \to \mathrm{A}$$
$$a \to \tau(a) := a^{\tau}$$

对集合 A，记 A上的所有变换构成的集合为

$$\mathrm{S} = \{\tau,\ \lambda,\ \mu,\ \cdots\}.$$

规定S上的乘法·如下

$$\tau:\ a \to a^{\tau},\ \lambda:\ a \to a^{\lambda}$$
$$\tau \cdot \lambda:\ a \to (a^{\tau})^{\lambda}$$

$\tau \cdot \lambda$是A上的变换，从而S对乘法·封闭.

例 $A=\{1,\ 2\}$.

τ_1 : $1\to 1,\quad 2\to 1$

τ_2 : $1\to 2,\quad 2\to 2$

τ_3 : $1\to 1,\quad 2\to 2$

τ_4 : $1\to 2,\quad 2\to 1$

是 A的所有的变换. 其中 τ_3, τ_4是一一变换.

(1)$\{\tau_3,\ \tau_4\}$构成群?

(2)$\{\tau_1\}$构成群吗?

注： 区别于映射的复合.

讨论(S,·)是否构成群：

G1: $(\tau\lambda)\mu$: $a \to （a^{\tau\lambda}）^{\mu} = ((a^{\tau})^{\lambda})^{\mu}$

$\tau(\lambda\mu)$: $a \to （a^{\tau}）^{\lambda\mu} = ((a^{\tau})^{\lambda})^{\mu}$.

G2: A的恒等变换记为ε为单位元.

G3: 不一定成立

比如 $A = \{1, 2\}$

τ_1 ： $1 \to 1,$ $2 \to 1$

A的任意变换乘以τ_1 都还是τ_1，不可能是ε.

定理3.1 假定 G 是集合 A 的若干个变换所作成的集合，并且 G 包含恒等变换 ε ．若是对于上述乘法来说 G 作成一个群，那么 G 只包含 A 的一一变换.

证明: 恒等变换 ε 就是单位元 e.

令 τ 是 G 的任意元，因为 G 是群，有逆元 τ^{-1}，使得 $\tau^{-1}\tau = \tau\tau^{-1} = \varepsilon$.

τ 是满射：$\forall a \in A$, 取 $b = a^{\tau^{-1}}$，则 $b^{\tau} = a$.

τ 是单射：任取 $a, b \in A$,

若 $a^{\tau} = b^{\tau}$，则 $(a^{\tau})^{\tau^{-1}} = (b^{\tau})^{\tau^{-1}}$

即有 $a=b$.

定义3.2 一个集合 A的若干个一一变换对于乘法作成的一个群叫做 A 的一个变换群.

定理3.3 A上全体一一变换关于映射的乘法构成群.

例 设 A 是一个平面的所有的点作成的集合，那么平面的一个绕一个定点的旋转可以看成 A 的一个一一变换．令 G 表示所有绕一个定点的旋转构成的集合，则 G 作成一个变换群．因为假如我们用

τ_θ来表示转 θ 角的旋转，则有

G0. $\tau_{\theta_1}\tau_{\theta_2} = \tau_{\theta_1+\theta_2}$;

G1. 结合律当然成立;

G2. $\varepsilon = \tau_0 \in G$;

G3. ${\tau_\theta}^{-1} = \tau_{-\theta}$.

定理3.4 (Cayley 定理) 任何一个群G都与G一个变换群同构.

证明： 任意取出一个元 $x \in G$ ，利用x构造集合G的一个变换τ_x如下:

$$\tau_x : G \to G,$$

$$g \to \tau_x(g) = gx, \quad \forall g \in \mathrm{G}.$$

我们把所有这样得来的G的变换放在一起，作成一个集合$\overline{G} = \{\tau_x | \ x \in G\}$.

我们将证明$G \cong \overline{G}$.

为此,构造 $\varphi: G \to \overline{G}$ 如下:

$$\varphi(x) = \tau_x.$$

(1)$\varphi: G \to \overline{G}$显然是满射.

(2)$\varphi: G \to \overline{G}$是单射:

$\forall x, y, g \in G$，且$x \neq y$，则

$$g^{\tau_x} = gx \neq gy = g^{\tau_y},$$

即$\tau_x \neq \tau_y$.

(3) $\forall x, y, g \in G$，我们有

$$g^{\tau_{xy}} = g(xy) = (gx)y = (g^{\tau_x})^{\tau_y} = g^{\tau_x \cdot \tau_y}.$$

从而$\overline{G}$对乘法封闭，且φ保持运算.

于是φ是同构映射，故$\overline{G}$是一个群.

又恒等变换$\varepsilon = \tau_e \in \overline{G}$，由定理3.1知$\overline{G}$是由一一变换构成的变换群，且$G \cong \overline{G}$.

这个定理告诉我们，任意一个抽象群都能够在变换群里找到一个具体的实例．换一句话说，我们不必害怕，以后会找得到一个抽象群，这个群完全是我们的脑子造出来的空中楼阁．

§4. 置换群

置换群是变换群的一种特例,提供了有限群的一种模型. 这类群在代数里占一个很重要的地位 . 这类群还有一个特点，就是它们的元可以用一种很具体的符号来表示，使得这种群里的计算比较简单.

定义4.1 一个有限集合的一个一一变换叫做这个集合的一个**置换**.

一个有限集合的若干个置换作成的一个群叫做这个集合的一个**置换群**.

定义4.2 一个包含 n 个元的集合的全体置换作成的群叫做 n 次**对称群**.

这个群用 S_n 来表示.

注： n 次对称群 S_n 的阶是 $n!$.

定理4.3 每一个有限群都与一个置换群同构.

现在我们要看一看表示一个置换的符号．这种符号有两种，我们先看第一种．

给一个有限集合 A ，有 n 个元 $a_1, a_2, \ldots a_n$．任取一个置换

$$\pi: a_i \to a_{k_i}, \quad i = 1,2,\ldots n.$$

这样一个置换所发生的作用完全可以由 $(1,k_1)$，$(2,k_2)$ ，…，(n,k_n) 这 n 对整数来决定．

表示置换的第一个方法就是把以上这个置换写成

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}.$$

这种形式不唯一. 在这种表示方法里，第一行的 n 个数字的次序显然无关紧要，例如上述π我们也可表示为

$$\pi = \begin{pmatrix} 2 & 1 & 3 & \cdots & n \\ k_2 & k_1 & \cdots & & k_n \end{pmatrix}.$$

例 取 $n = 3$， $\pi: a_1 \to a_2, a_2 \to a_3, a_3 \to a_1.$

则 $\pi = \begin{pmatrix} 123 \\ 231 \end{pmatrix} = \begin{pmatrix} 132 \\ 213 \end{pmatrix} = \begin{pmatrix} 213 \\ 321 \end{pmatrix} = \begin{pmatrix} 231 \\ 312 \end{pmatrix} = \begin{pmatrix} 312 \\ 123 \end{pmatrix} = \begin{pmatrix} 321 \\ 132 \end{pmatrix}.$

π

例 S_3 有 6 个元．这 6 个元可以写成

$$\begin{pmatrix}123\\123\end{pmatrix}, \begin{pmatrix}123\\132\end{pmatrix}, \begin{pmatrix}123\\213\end{pmatrix}, \begin{pmatrix}123\\213\end{pmatrix}, \begin{pmatrix}123\\312\end{pmatrix}, \begin{pmatrix}123\\321\end{pmatrix}$$

$$\begin{pmatrix}123\\132\end{pmatrix}\begin{pmatrix}123\\213\end{pmatrix}=\begin{pmatrix}123\\231\end{pmatrix},$$

$$\begin{pmatrix}123\\213\end{pmatrix}\begin{pmatrix}123\\132\end{pmatrix}=\begin{pmatrix}123\\312\end{pmatrix},$$

所以 s_3不是交换群.

无限非交换群我们已经看到过，这是我们的第一个有限非交换群的例子．s_3 可以说是一个最小的有限非交换群，因为一个有限非交换群至少要有六个元.

为了说明置换的第二种表示方法，我们先证明：

引理4.4 设有两个置换

$$\pi_1=\begin{pmatrix} j_1 \cdots & j_k & j_{k+1} \cdots j_n \\ {j_1}^{(1)} \cdots {j_k}^{(1)} & & j_{k+1} \cdots j_n \end{pmatrix},\quad \pi_2=\begin{pmatrix} j_1 & \cdots\ j_k & j_{k+1} \cdots & j_n \\ j_1 \cdots j_k & & {j_{k+1}}^{(2)} \cdots & {j_n}^{(2)} \end{pmatrix}.$$

那么以下公式成立：

$$\pi_2\pi_1=\pi_1\pi_2=\begin{pmatrix} j_1 \cdots & j_k & j_{k+1} \cdots & j_n \\ {j_1}^{(1)} \cdots {j_k}^{(1)} & & {j_{k+1}}^{(2)} \cdots & {j_n}^{(2)} \end{pmatrix}.$$

证明: π_1是 a_{j_1} ，a_{j_2} ， …， a_{j_n} 这 n 个元的一一变换，而在 π_1 之下，$a_{j_{k+1}}$，…， a_{j_n} 已经各是 $a_{j_{k+1}}$ ，…， a_{j_n} 的象,所以它们不能再是 $a_{j_i}(i \le k)$ 的象，从而 ${j_1}^{(1)} \cdots {j_k}^{(1)}$ 只能取自 $j_1 \cdots\ j_k$，而这部分元在 π_2之下保持不变.

定义4.5 S_n的一个把变成a_{i_1}变到a_{i_2}，a_{i_2}变到a_{i_3}，…，a_{i_k}变到a_{i_1}，而使得其余的元（假如还有的话）不变的置换，叫做一个k-**循环置换**，也叫做k-轮换. 这样的一个置换我们用符号

$(i_1 i_2 \cdots i_k)$，或$(i_2 i_3 \cdots i_k i_1)$，…，或$(i_k i_1 \cdots i_{k-1})$

来表示.

2-轮换称为对换.

恒等置换记为（1），或（2），…，或（n）.

两个轮换互相没有共同数字，则称这两个轮换是不相交的（不相连的）.

例 我们看 S_5，这里

$$\begin{pmatrix}12345\\23145\end{pmatrix} = (123) = (231) = (312)$$

$$\begin{pmatrix}12345\\23451\end{pmatrix} = (12345) = (23451) = \cdots = (51234)$$

$$\begin{pmatrix}12345\\12345\end{pmatrix} = (1) = (2) = (3) = (4) = (5).$$

一个任意的置换当然不一定是一个循环置换．如

例 S_4 的 $\pi = \begin{pmatrix}1234\\2143\end{pmatrix}$ 就不是一个循环置换．

但是， $\pi = \begin{pmatrix}1234\\2134\end{pmatrix}\begin{pmatrix}1234\\1243\end{pmatrix} = (12)(34).$

一般来说，我们有

定理4.6 每一个 n个元的置换 π都可以写成若干个不相交轮换的乘积.

证明：我们再用归纳法.

1. 当 π 不使任何元变动的时候，即当 π是恒等置换的时候，定理是对的.

2. 假定对于最多变动 $r-1(r \leq n)$ 个元的 π 定理是对的. 现在我们看一个变动 r 个元的 π .

我们任意取一个被 π 变动的元 a_{i_1}，从 a_{i_1} 出发我们找 a_{i_1}的象 a_{i_2}，a_{i_2}的象 a_{i_3}，这样找下去，直到我们第一次找到一个元，而该元的象不再是一个新的元，而是我们已经得到过的一个元，即有 a_{i_k}，使得 $a_{i_{k-1}}^{\pi} = a_{i_k}$，而 $a_{i_k}^{\pi} = a_{i_j}, j \leq k.$

因为我们一共只有有限个元，所有这样的a_{i_k}是一定存在的．而且我们有$a_{i_k}^{\pi} = a_{i_1}$.这是因为 $a_{i_j}(2 \leq j \leq k)$ 已经是 $a_{i_{j-1}}$的象，不能再是 a_{i_k}的象.

从而我们有$a_{i_1} \to a_{i_2} \to \cdots \to a_{i_k} \to a_{i_1}$. 我们记

$$\pi_1 = \begin{pmatrix} i_1 & i_2 \cdots i_k & i_{k+1} \cdots i_r & i_{r+1} \cdots i_n \\ i_2 & i_3 \cdots i_1 & i_{k+1} \cdots i_r & i_{r+1} \cdots i_n \end{pmatrix} = (i_1 i_2 \cdots i_k).$$

因为 π只使 r 个元变动,$k \le r$.

假如$k = r$,则$\pi = \pi_1$，本身已经是一个轮换，结论成立.

假如$k < r$，则有

$$\pi = \begin{pmatrix} i_1 i_2 \cdots i_k i_{k+1} \cdots i_r i_{r+1} \cdots i_n \\ i_2 i_3 \cdots i_1 i'_{k+1} \cdots i'_r i_{r+1} \cdots i_n \end{pmatrix}$$

$$= \begin{pmatrix} i_1 i_2 \cdots i_k i_{k+1} \cdots i_r i_{r+1} \cdots i_n \\ i_2 i_3 \cdots i_1 i_{k+1} \cdots i_r i_{r+1} \cdots i_n \end{pmatrix} \begin{pmatrix} i_1 \cdots i_k i_{k+1} \cdots i_r i_{r+1} \cdots i_n \\ i_1 \cdots i_k i'_{k+1} \cdots i'_r i_{r+1} \cdots i_n \end{pmatrix}$$

$$= (i_1 i_2 \cdots i_k)\pi_2$$

$$= \pi_1 \, \pi_2,$$

其中 $\pi_2 = \begin{pmatrix} i_1 \cdots i_k i_{k+1} \cdots i_r i_{r+1} \cdots i_n \\ i_1 \cdots i_k i'_{k+1} \cdots i'_r i_{r+1} \cdots i_n \end{pmatrix}$.

但π_2只使得$r-k<r$个元变动，有归纳假设知，可以写成不相交轮换的乘积：

$$\pi_2 = \eta_1\eta_2\cdots\eta_m.$$

在这些η_i里$i_1, i_2, \ldots, i_k$不会出现. 这是因为，如果有

$$\eta_l = (\cdots i_p i_q \cdots), \qquad p \le k$$

那么i_p同i_q不会再在其余的η_i中出现, π_2也必使

$$a_{i_p} \to a_{i_q}.$$

而我们知道, π_2使得a_{i_p}不动,这是一个矛盾.

从而,π是不相交轮换的乘积:

$$\pi = \pi_1\eta_1\eta_2\cdots\eta_m.$$

注： 1. 上述定理的表示法唯一，即

若$\pi = \sigma_1\sigma_2\cdots\sigma_n = \eta_1\eta_2\cdots\eta_m$，则

$$m = n,$$

且经过次序调换必有

$$\sigma_1 = \eta_1\ ,\ \sigma_2 = \eta_2,\ \cdots.$$

证明： 若 $a_{i_1}^{\sigma_1} = a_{i_2}$ 必有 $a_{i_1}^{\pi} = a_{i_2}$.

2.每一个置换可以写出对换的乘积，且对换个数的奇偶性是固定的，分别称为奇置换和偶置换.

提示: $(i_1 i_2\cdots i_k) = (i_1 i_k)(i_1 i_{k-1})\cdots(i_1 i_3)(i_1 i_2).$

例 S_4 的全体元用轮换的方法写出来是：

(1);

(12)，(34)，(13)，(24)，(14)，(23);

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

(1234)，(1243)，(1324)，(1342)，(1423)，(1432);

(12)(34)，(13)(24)，(14)(23).

§5. 循环群

定义5.1 若一个群G的每一个元都是G的某一个固定元a的乘方，我们就称G是循环群；我们也说，G是由a元所生成的，并且用符号

$$G = (a)$$

来表示．而a叫做G的一个**生成元**。

例 整数加群Z.

这个群的全体的元就都是 1 的乘方．这一点假如把G的代数运算不用＋而用 “ ∘ ” 来表示，就很容易看出．我们知 1 的逆元是－ 1 ．假定m是任意正整数，那么

$$m = \overbrace{1+1+\cdots+1}^{m} = \overbrace{1\circ 1\circ\cdots\circ 1}^{m} = 1^m$$

$$-m = \overbrace{(-1)+(-1)+\cdots+(-1)}^{m} = \overbrace{(-1)\circ(-1)\circ\cdots\circ(-1)}^{m} = 1^{-m}$$

$$0 = 1^0.$$

例　G包含模n的n个剩余类．我们要规定一个G的代数运算,我们把这个代数运算叫做加法，并用普通表示加法的符号＋来表示,规定：

$$[a]+[b]=[a+b].$$

首先,必须证明这样规定的“＋”是定义好的:

如果　$a'\in[a]$，　$b'\in[b]$　，　即　$[a']=[a]$，$[b']=[b]$.

又　　$[a']+[b']=[a'+b']$,

从而有　$[a+b]=[a'+b']$.

（1）G0.

（2）G1. $[a]+([b]+[c])=[a]+[b+c]=[a+(b+c)]=[a+b+c]$

$([a]+[b])+[c]=[a+b]=[c]=[(a+b)+c]=[a+b+c]$

$[a]+([b]+[c])=([a]+[b])+[c]$

（3）G2. $[0]+[a]=[0+a]=[a]$

（4）G3. $[-a]+[a]=[-a+a]=[0]$

所以对于这个加法来说G作成一个群．这个群叫做模n的**剩余类加群**, 记为 $Z/_{nZ}$ 或 Z_n.

定 理5.2 ： 假定G是一个由元a所生成的循环群

$$G = (a) = \{a^n | n \in Z\},$$

那么G的结构由生成元a的阶来决定：

(1) 如果a的阶是无穷大，那么G同构于整数加群；

(2) 如果 $\text{ord}(a) = n > 0$，那么G同构于模n的剩余类加群.

证明：（1） $a^h = a^k \Leftrightarrow a^{h-k} = e \Leftrightarrow h - k = 0 \Leftrightarrow h = k.$

从而 $a^h \to h$ 确定从G到Z的一个一一映.

又$a^h \cdot a^k = a^{h+k} \to h + k$，从而该映射是同构.

（2） $a^h = a^k \Leftrightarrow a^{h-k} = e \Leftrightarrow n | h - k \Leftrightarrow [h] = [k].$

从而 $a^h \to [h]$ 确定从G到$Z/_{nZ}$的一个映射，且是单射.

又显然是满射，从而是一一映射.

又$a^h \cdot a^k = a^{h+k} \to [h + k] = [h] + [k]$，

从而该映射是同构.

从而我们有：

（1）生成元的阶无限大时，我们有

$G = (a) = \{a^n | n \in Z\} = \{\cdots a^{-2}, a^{-1}, e, a^1, a^2 \cdots\}.$

乘法为$a^h \cdot a^k = a^{h+k}$.

（2）生成元的阶为n时，我们有

$G = (a) = \{a^n | n \in Z\} = \{a^0 = e, a^1, a^2, \cdots, a^{n-1}\}.$

乘法为$a^h \cdot a^k = a^r$，其中r为$h+k$ 被n整除的余数.

注:

(1)设$G = (a)$是由a生成的循环群，则$|G| = \mathrm{ord}(a)$.

(2)G是有限群，且$a \in G$，则G是由a生成的循环群当且仅当$|G| = \mathrm{ord}(a)$.

代数系统研究内容：

I.分类: 同构的分成同一类,存在及数量

II. 每一类的内部结构

III.表示

对于循环群的存在问题，数量问题，构造问题都已完全解答.

这一节的研讨是近世代数的研讨的一个缩影．在近世代数里，不管是在群论里还是在其它系统里，我们研究一种代数系统就是要解决这一种系统的存在问题，数量问题和构造问题．假如我们对于这三个问题能得到如同我们对于循环群所得到的这样完美的解答，我们的目的就算达到了.

§6. 子群

讨论子对象是一个常用的代数方法.我们看一个群 G . 假如由 G 里取出一个非空子集 H 来，那么利用 G 的乘法可以把 H 的两个元相乘. 对于这个乘法来说，H 也可能也作成一个群. 我们往往用这样的群去讨论群 G 本身.

定义6.1一个群 G 的一个非空子集 H 叫做 G 的一个**子群**，如果 H 对于 G 的乘法来说作成一个群, 记为 $H \leq G$.

例 给了一个任意群 G，则 G 至少有两个子群：

$$G, \quad \{e\}$$

它们叫做 G 的平凡子群.

例 $G = S_3$，$H = \{(1)，(12)\}$．那么 H 是 S_3 的一个子群.

因为：

G0. H 对于 G 的乘法来说是闭的，

$(1)(1) = (1)$ ，$(1)(12) = (12)$，

$(12)(1) = (12)$ ，$(12)(12) = (1)$;

G1. 结合律对于所有 G 的元都对，对于 H 的元也对；

G2. $(1) \in H$ 是单位元；

G3. $(1)(1) = (1)$ ，$(12)(12) = (1)$ ．

注1:H的乘法必须是G的乘法；

注2: 验证H是子群时有些条件可以省略.

定理6.2 一个群G的一个不空子集H作成G的一个子群的充分而且必要条件是：

（ⅰ） $a,b \in H \Rightarrow ab \in H$，

（ⅱ） $a \in H \Rightarrow a^{-1} \in H$.

证明：若是（ⅰ），（ⅱ）成立，H作成一个群：

G0．由于（ⅰ），H是对乘法封闭；

G1．结合律在G中成立，H在中自然成立；

G2’．因为H至少有一个元a，由（ⅱ），H也包含a^{-1}，所以由（ⅰ）知$a^{-1}a = e \in H$.

G3’．由（ⅱ），对于H的任意元a来说，H中有a^{-1}，使得$a^{-1}a = e$.

反过来，若H是一个子群，则（ⅰ）显然成立.

又存在H的单位元e_H，任取$a \in H$，则$e_H a = a$，从而$e_H = e$.

又$a_H^{-1} \in H$，从而$a_H^{-1}a = e_H = e$，故$a_H^{-1} = a^{-1} \in H$.

由上述证明知

推论6.3: 设 $H \leq G$ **，那么**

(1) $e_H = e_G$;

(2) $a_H^{-1} = a_G^{-1}$, 对于 $a \in H$成立.

定理6.4 一个群 G 的一个非空子集 H 作成 G 的一个子群的充分而且必要条件是：

（iii） $a,b \in G \Rightarrow ab^{-1} \in H.$

证明: 先证若（ i ）和（ ii ）成立，则（iii）就也成立.

任取$a,b \in H$，由（ii）知 $b^{-1} \in H$，再由（ i ），$ab^{-1} \in H.$

再证明，由（iii）可以得到（ i ）和（ ii ）.

任取$a,b \in H$，则

$$b,b \in H \Longrightarrow bb^{-1} = e \in H;$$

$$e,b \in H \Longrightarrow eb^{-1} \in H \Longrightarrow b^{-1} \in H \Longrightarrow \text{（ii）};$$

$$a,b^{-1} \in H \Longrightarrow a(b^{-1})^{-1} = ab \in H \Longrightarrow \text{(i)}.$$

假如所给子集 H 是一个有限集合，那么 H 作成子群的条件更要简单.

定理6.5 一个群 G 的一个不空有限子集 H 作成 G 的一个子群的充分而且必要条件是：

$$a, b \in H \Rightarrow ab \in H$$

证明： 必要性显然.

下证充分性.

由 $a, b \in H \Rightarrow ab \in H$ 知，H对乘法封闭，

而结合律和消去律显然成立，从而H是子群.

现在我们介绍一种找一个子群的一般方法.

我们在一个群 G 里任意取出一个非空子集 S 来，S 包含元 a，b，c，d，....那么 S 当然不见得是一个子群，但是我们可以把 S 扩大一点，而得到一个包 S 含的子群.

利用 S 的元以及这些元的逆元我们可以作各种乘积，比方说，

$$ab，a^{-2}c，a^3cb^{-1}，d，c^{-1}$$

等等. 设集合 H 刚好包含所有这样的乘积，可以证明:

(1) H 作成一个子群.

因为两个这样的乘积乘起来还是一个这样的乘积，

一个这样的乘积的逆元也是一个这样的乘积，

(2) 对任何一个包含 S 的子群 H'，H' 一定包含 H，即

$$H' \supseteq H.$$

由 (1)和(2)，H是包含S的最小的子群.

定义6.6 如上得到的H 叫做由S 生成的子群，我们用符号 (S) 或$< S >$ 来表示它.

假如我们取一个只包含一个元 a的子集 S ，那么

$$(S) = (a)$$

是一个循环子群.

设A，B是群G的两个非空子集,规定

$AB = \{ab | a \in A, b \in B\}$， $A^{-1} = \{a^{-1} | a \in A\}$.

特别地， $Ha = \{ha | h \in H\}$, $aH = \{ah | h \in H\}$.

容易证明:

$(AB)C = A(BC)$ ， $A(B \cup C) = (AB) \cup (AC)$,

$(AB)^{-1} = B^{-1}A^{-1}$, $(A^{-1})^{-1} = A$.

从而有

$$< S >= \{a_1 a_2 \cdots a_n | a_i \in S \cup S^{-1}\}.$$

§7. 子群的陪集

我们看一个群 G 和 G 的一个子群 H . 我们规定一个的元 G 中间的关系 $\sim$:

$a \sim b$ 当且仅当 $ab^{-1} \in H.$

给了 a 和 b ，我们可以唯一决定 ab^{-1} 是不是属于 H ，所以 $\sim$ 是一个关系,并且:

(1)$aa^{-1} = e \in H$，从而$a \sim a$.

（2）$ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H$，
从而$a \sim b \Rightarrow b \sim a$.

（3）ab^{-1}，$bc^{-1} \in H \Rightarrow ac^{-1} \in H$，
从而$a \sim b$，$b \sim c \Rightarrow a \sim$ c.

从而~是G上的一个等价关系.

定理7.1 在上述等价关系~下，$a\in G$所在等价类[a]是Ha.

证明: $Ha=\{ha|h\in H\}$,

$x\in[a]\Leftrightarrow xa^{-1}\in H\Leftrightarrow xa^{-1}=h\in H\Leftrightarrow x=ha\in Ha.$

定义7.2 由上面的等价关系~所决定的等价类叫做子群H的一个右陪集. Ha的任何元叫做右陪集代表元.

G的一个全体代表团，叫做G对H的一个右陪集代表系.

从而

$G=\bigcup_{a\in S}Ha$，这里S是G对H的一个右陪集代表系.

— G对H的右陪集分解

我们看一个群 G 和 G 的一个子群 H . 我们规定一个的元 G 中间的关系 $\sim'$:

$a \sim' b$, 当且仅当 $b^{-1}a \in H.$

同样可以证明 $\sim'$是G上的一个等价关系,并且有

定理7.3 在上述等价关系~′下，$a\in G$所在等价类[a]是aH.

定义7.4 由上面的等价关系~′所决定的等价类叫做子群H的一个左陪集. aH的任何元叫做左陪集代表元. G的一个全体代表团，叫做G对H的一个左陪集代表系.

从而

$G = \bigcup_{a\in S} aH$，这里S是G对H的一个左陪集代表系.

— G对H的左陪集分解

注：陪集的一些性质：

$a \sim b$

$\Leftrightarrow Ha = Hb$

$\Leftrightarrow a \in Hb$

$\Leftrightarrow b \in Ha$

$\Leftrightarrow ab^{-1} \in H$

$\Leftrightarrow ba^{-1} \in H$

$\Leftrightarrow b^{-1} \in a^{-1}H$

$\Leftrightarrow a^{-1} \in b^{-1}H$

$\Leftrightarrow a^{-1}H = b^{-1}H$

$\Leftrightarrow a^{-1} \sim {}' b^{-1}$

定理7.5 一个子群的右陪集个数和左陪集个数相等（或都是无限大，或都是有限且相等）.

证明: 令S_r表示子群H的右陪集构成的集合，

S_l表示子群H的右陪集构成的集合，

构造：$\varphi: S_r \to S_l$

$Ha \to a^{-1}H.$

(1)定义好的：

$Ha = Hb \Rightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H$

$\Rightarrow a^{-1}H = b^{-1}H$.

（2）单射：

$a^{-1}H = b^{-1}H \Rightarrow (a^{-1})^{-1}b^{-1} = ab^{-1} \in H \Rightarrow Ha = Hb.$

（3） S_l的任意元aH是 S_r的元Ha^{-1}的象，所以φ是一个满射.

定义7.6 一个群 G 的一个子群 H 的右陪集（或左陪集）的个数叫做 H 在 G 里的**指数**，记为[G:H].

引理7.7 H, aH, Hb 之间存在一一映射.

证明：作 $H \to aH$

$h \to ah$.

满射显然，而由消去律可知这是单射，从而是一一映射.

同理可证H与Hb之间也有一一映射.

定理 7.8 设 H 是一个有限群 G 的一个子群. 那么 H 的阶和它在 G 里的指数都能整除 G 的阶，并且

$$|G| = |H|[G:H].$$

证明：设$G = \bigcup_{a \in S} Ha$ 是G对H的一个右陪集分解.

由上述引理知Ha有$|H|$个元，从而G是$[G:H]$个含有个$|H|$元的集合的无交并，从而有$|G| = |H|[G:H]$.

定理 7.9 一个有限群G的任一个元a的阶都整除G的阶.

证明： 令$H =< a >$，则H是G的子群，且$|H| = o(a)$.

由拉格朗日定理知的a阶都整除G的阶.

例 素数阶的群必为循环群.

证明：设G的阶是素数p，则G中有非单位的元a.

于是$o(a)|p$，从而$o(a) = |G|$，故是G循环群.

例 非交换群的阶最小是6.

证明： S_3是非交换群（(12)(23)=(132)≠(23)(12)=(123)），而S_3的阶是6.

又阶数为素数的群必为循环群从而是交换群，

所以阶为2，3，5的群是交换群.

现设$|H| = 4$. 若H有四阶元，则H是循环群，从而是交换群. 若H中只有1阶或2阶元，则$\forall a \in H$, 都有$a^2 = e$, 从而是交换群（见习题）.

习题：循环群的子群还是循环群.

定理7.10（1）无限循环群的子群除{e}外都是无限循环群；
（2）有限n阶循环群的子群的阶是n的正因子，且对n的每一个正因子q，有且仅有一个q阶子群.

证明：设$G =< g >$是一个循环群，H是一个子群，则H由g^s生成，这里s是使$g^k \in H$的最小正整数.

(1)当<g>是无限循环群时，如果$n \neq m$，则$g^n \neq g^m$，

于是g^{ms} (m=0，±1，±2，…)两两不同，H是无限循环群.

(2)设G是n阶循环群，其子群的阶均整除n.

任取n的正因子q，并记$s = \frac{n}{q}$，以及

$$H =< g^s >=< g^{\frac{n}{q}} >= \{g^s, g^{2s}, \cdots, g^{(q-1)s}, g^{qs} = g^n = e\}.$$

任取整数i, j，且$1 \leq i, j \leq q$，如果$g^{is} = g^{js}$，则有$g^{\frac{i-j}{q} \cdot n} = e$.

又$o(g) = n$，从而$i=j$，故$|H|=q$.

下证q阶子群的唯一性.

设H′是G的一个q阶子群,则$H' =< g^{s'} >$,这里s'是使$g^k \in H$的最小正整数，且$s'|k$.

由$g^{s'q} = e$知， $sq = n \mid s'q$，从而$s \mid s'$，故$g^{s'} \in H$.

于是我们有$\mathrm{H}' \subseteq H$，且都是q阶子群，故$\mathrm{H}' = H$.

且由$g^s \in H'$知，$s'|s$，从而$s = s'$，即有$H' =< g^{\frac{n}{q}} >$.

推论7.11 设$o(g) = n$，且q是n的正因子，则$o(g^{\frac{n}{q}}) = q$.

§8. 正规子群和商群

例 $G = S_3 = \{(1)，\ (12)，\ (13)，\ (23)，\ (123)，\ (132)\}$

$H = \{(1)，(12)\}.$

H的左陪集：

$(1)H = \{(1),(12)\},$

$(13)H = \{(13),(132)\},$

$(23)H = \{(23),(123)\}.$

H的右陪集：

$H(1) = \{(1),(12)\},$

$H(13) = \{(13),(123)\},$

$H(23) = \{(23),(132)\}.$

$N = \{(1)，(123)，(132)\}.$

N的左陪集：

$(1)N = \{(1)，(123)，(132)\},$

$(12)N = \{(12),(13),(23)\}.$

N的右陪集：

$N(1) = \{(1)，(123)，(132)\},$

$N(12) = \{(12),(13),(23)\}.$

定义8.1 一个群G的一个子群N叫做一个**正规子群**,假如对于G的每一个元a来说,都有

$$aN = Na.$$

一个正规子群N的一个左(或右)陪集叫做N的**一个陪集**.

注1. 正规子群记作$N \lhd G$.

注2. 正规子群也叫不变子群.

注3. 弱交换性

$x \in N, g \in G$,则xg和gx不一定相等,

但$xg \in Ng = gN$，从而存在$x' \in N$，使得$xg = gx'$.

例 一个任意群 G 的子群 G 和 $\{e\}$ 总是正规子群.

例 一个交换群 G 的每一个子群 H 都是正规子群. 因为 G的每一个元 a可以和任意一元x交换：$xa = ax$，所以对于一个子群H来说一定有 $Ha = aH$.

例 $G = S_3$, 则$N = \{(1)，(123)，(132)\}$是一个正规子群.

例 N刚好包含群G的所有有以下性质的元 n：

$$N = \{n \in G \mid na = an, \forall a \in G\}.$$

(1) N是子群. 因为 $e \in N$ ，所以 N是非空的.

$\forall a \in G$, 都有$n_1 a = a n_1$，从而$n_2 a = a n_2 \Rightarrow n_1 n_2 a = a n_1 n_2$.

于是$na = an \Rightarrow n^{-1}a = n^{-1}a(nn^{-1}) = n^{-1}(na)n^{-1} = an^{-1}$.

(2) $aN = Na$. G的每一个元a 可以同N 的每一个元 n 交换，所以$Na = aN$，即 N是正规子群群.

这个正规子群N叫做 G的**中心**.

现在复习一下群G的子集的乘积: 设A，B是群G的两个非空子集,则

$$AB = \{ab | a \in A, b \in B\}, \qquad A^{-1} = \{a^{-1} | a \in A\}.$$

由于群运算结合律成立, S_1，S_2，…，S_m的乘积有意义：

$$S_1 S_2 \cdots S_m = \{s_1 s_2 \cdots s_m \mid s_i \in S_i, \forall i\}.$$

易知 $(S_1 S_2) S_3 = S_1 (S_2 S_3)$.

定理8.2 一个群G的一个子群N是一个正规子群的充分而且必要条件是：

$$aNa^{-1} = N$$

对于G的任意一个元a都成立.

证明：因为N是正规子群，故对于G的任意一个元a都有

$$aN = Na.$$

从而$Na \cdot a^{-1} = aN \cdot a^{-1}$，即 $N = aNa^{-1}$.

反过来，若对于G的任意一个元a都有 $aNa^{-1} = N$，

从而 $Na = (aNa^{-1}) \cdot a = aN$.

注. $aNa^{-1} = N$ 可以换成 $a^{-1}Na = N$.

定理8.3 一个群 G的一个子群 N是一个正规子群的充分而且必要条件是：

$$\forall a \in G\ ,\ n \in N,\ \text{都有}\ ana^{-1} \in N.$$

证明： 这个条件的必要性是定理8.2的直接结果.
现在证明充分性.

$\forall a \in G\ ,\ n \in N,$ 都有$ana^{-1} \in N$，则

$$aNa^{-1} \subseteq N.$$

因为 a^{-1}也是G的元，在上式中以 a^{-1}代替a,

则 $N \subseteq aNa^{-1}$，从而有$aNa^{-1} = N.$

推论8.4 一个群 G的一个子群 N是一个正规子群的充分而且必要条件是：

$$\forall a \in G\text{都有}\ aNa^{-1} \subseteq N.$$

正规子群的陪集，对于某种与原来的群有密切关系的代数运算来说，也作成一个群.

我们看一个群G的一个正规子群N 的所有陪集作成一个集合

$$\overline{\mathrm{G}} = \{aN, bN, cN \cdots\} = \{gN | g \in G\}.$$

注：（1）aN 相对 $\overline{\mathrm{G}}$ 是一个元素, aN相对 G是一个子集.

(2) aN 有不同的表示方式.

(3) 我们可以定义代数运算.

我们定义：

$$\overline{G} \times \overline{G} \longrightarrow \overline{G}$$
$$(xN, yN) \rightarrow (xN) \cdot (yN) = (xy)N.$$

现设$x'N = xN, y'N = yN$，则存在n_1， $n_2 \in N$，使得

$$x' = x \cdot n_1, \quad y' = y \cdot n_2.$$

于是$x'y' = (x \cdot n_1)(y \cdot n_2)$.

又N是正规子群，从而$Ny = yN$，故存在$n_3 \in N$，使得

$$n_1 \cdot y = y \cdot n_3.$$

于是$x'y' = (x \cdot n_1) \cdot (y \cdot n_2) = x(y\, n_3)\, n_2 = xyn_3n_2 \in (xy)N$.

综上，上述定义了$\overline{G}$上的一个代数运算，称为为$\overline{G}$上的乘法.

现证明按上述乘法， $\overline{G}$ 构成一个群：

G0. 已证.

G1. $(xN \cdot yN) \cdot zN = [(xy)N] \cdot zN = (xyz)N$

$xN \cdot (yN \cdot zN) = xN \cdot [(yz)N] = (xyz)N.$

G2. $eN \cdot xN = (ex)N = xN = xN \cdot eN,$

故eN是单位元.

G3. $x^{-1}N \cdot xN = (x^{-1}x)N = eN = xN \cdot x^{-1}N.$

定义8.5 一个群 G 的一个正规子群 N 的陪集按照上述乘法所作成的群叫做 G **模** N **的商群**. 通常我们用符号 G/N 来表示.

注：（1）G/N 的乘法继承了 G 的乘法;

（2）G/N 是 G 模掉 N 的性质得到的，即相差 N 的元的两个元相同;

（3）因为 N 的指数就是 N 的陪集的个数，故商群 G/N 的元的个数等于 N 的指数. 若 G 是有限群，我们有

$$[G:N]=\frac{G\text{的阶}}{N\text{的阶}}=G/N \text{ 的阶}.$$

从商群的角度重新认识剩余类加群 Z_n.

$Z_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$.
运算为$\bar{a}+ \bar{b}= \overline{a+b}$.

$G =$ （Z， $+$），　$N = (n) = \{kn | k \in Z\}$，则

Z_n即为 G/N，成为模n的剩余类加群.

§9. 同态基本定理

正规子群，商群与同态映射之间存在几个极为重要的关系．知道了这几个关系，我们才能看出正规子群和商群的重要意义．

定理9.1 一个群G同它的每一个商群G/N有一个自然满同态.

证明： 我们规定G到G/N的一个法则ϕ：

$$\phi(a) = aN \quad (\forall a \in G).$$

这显然是G到G/N的一个满射.

并且对于G的任意两个元a和b，都有

$$\phi(ab) = abN = (aN)(bN) = \phi(a)\phi(b).$$

所以它是一个同态满射.

注：上述满同态ϕ称为自然同态.

由群 G的一个子群可以推测整个群 G 的性质．假如我们有一个正规子群 N，就同时有两个群可以供我们利用，一个是N本身，另一个是商群 G/N ．现在上述定理又告诉我们， G与 G/N 之间有满同态，这样我们更容易讨论G的性质.

在一定意义之下，定理9.1的逆定理也是对的，这就是同态基本定理.

定义9.2 假定φ是一个群G到另一个群$\overline{G}$的一个同态映射. $\overline{G}$的单位元$\overline{e}$在φ之下的所有逆象所作成的G的子集叫做同态满射φ的**核, 记为**$\ker\varphi$,即:

$$\ker\varphi = \varphi^{-1}(\overline{e}) = \{x | x \in G, \varphi(e) = \overline{e}\}.$$

集合$\varphi(G) = \{\varphi(x) | x \in G\}$叫做$\varphi$的像，记为$\mathrm{Im}\,\varphi$.

定理9.3 假定φ是一个群G到另一个群G'的一个同态映射，则$\ker\varphi$是G的一个正规子群.

证明：任取$a, b \in \ker\varphi$，则$\varphi(a) = \varphi(b) = e'$，这里$e'$是G'的单位元.

又$\varphi(b^{-1}) = (\varphi(b))^{-1} = e'$, 从而$\varphi(ab^{-1}) = e'$, 即$ab^{-1} \in \ker\varphi$.

故$\ker\varphi$是G的一个子群.

任取$a \in \ker\varphi$, $g \in G$, 有$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(gg^{-1}) = e'$.

故$gag^{-1} \in \ker\varphi$，从而$\ker\varphi$是G的正规子群.

定理9.4 假定G和$\overline{G}$是两个群，并且有满同态 $G \xrightarrow{\varphi} \overline{G}$，

则 $G/N \cong \overline{G}$, 这里 $\mathrm{N} = \ker \varphi$.

证明: 定义 ϕ： $G/N \to \overline{G}$,

$$\phi(aN) = \varphi(a), \forall a \in G \ .$$

设$\overline{e}$是$\overline{G}$的单位元，则有

$$aN = bN \Leftrightarrow b^{-1}a \in N \Leftrightarrow \varphi(b^{-1}a) = \overline{e} \Leftrightarrow \varphi(a) = \varphi(b).$$

从而ϕ是定义好的，且是单射.

对任意$\overline{a} \in \overline{G}$，则有$a \in \mathrm{G}$，使得$\varphi(a) = \overline{a}$,

从而$\phi(aN) = \varphi(a) = \overline{a}$，即$\phi$是满的.

又$\phi(aN \cdot bN) = \phi(abN) = \varphi(ab) = \varphi(a)\varphi(b)$

$= \phi(aN)\phi\,(bN)$,

故ϕ保持运算，从而是同构.

注1：上述定理成为群的同态基本定理.

注2：抽象地来看，一个群只到它的商群有满同态.

注3：两个群之间有满同态，则这两个群的差别在于核,即如果把核的性质模掉(两个元相差的是核中的元素，则把它们等同起来），得到的两个群一样（同构）.

注4：$\varphi:\ G \to \overline{G}$是群同态，则同态基本定理变为

$$G/\ker\varphi \cong \mathrm{Im}\,\varphi.$$

定义9.5 假定f是集合A到集合$\overline{A}$的一个映射.

1. S是A的一个子集, 则S在f之下的象为

$$f(S) = \{f(s)|s \in S\}$$

它刚好包含所有S的元在f之下的象.

2. $\overline{S}$是$\overline{A}$的一个子集, $\overline{S}$在f之下的逆象为

$$f^{-1}(\overline{S}) = \{x|x \in A, f(x) \in \overline{S}\}.$$

它刚好包含所有A中在f之下的像属于$\overline{S}$的元.

定理9.6 假定 G 和 G' 是两个群，并且 G 与 G' 有满同态 φ,则

（ⅰ）G 的一个子群 H 的象是 G' 的一个子群；

（ⅱ）G 的一个正规子群 H 的象是 G' 的一个正规子群.

证明：考察H在 G' 中的像 $\varphi(H)$.

（ⅰ）对 $\forall a', b' \in G'$, 都有 $a, b \in H$，使得 $a' = \varphi(a), b' = \varphi(b)$.

从而 $a'b'^{-1} = \varphi(a)\left(\varphi(b)\right)^{-1} = \varphi(ab^{-1}) \in \varphi(H)$.

故 $\varphi(H)$ 是 G' 的子群.

（ⅱ）任取 $g' \in G', h' \in \varphi(H)$，则总有 $g \in G, h \in H$，使得

$g' = \varphi(g), h' = \varphi(h)$.

又 H 是正规子群，从而 $ghg^{-1} \in H$.

于是 $g'h'g'^{-1} = \varphi(g)\varphi(h)\ \varphi(g^{-1}) = \varphi(ghg^{-1}) \in \varphi(H)$,

故 $\varphi(H)$ 是 G' 的正规子群.

定理9.7 假定 G 和 G' 是两个群，并且 G 与 G' 有同态 φ,则

（ⅰ）G' 的一个子群 H' 的逆象是 G 的一个子群；

（ⅱ）G' 的一个正规子群 H' 的逆象是 G 的一个正规子群.

证明留给大家.

注： 1. 上述定理中不要求 φ 是满的;

2. 满同态保持子群，正规子群;

3. $\ker\varphi \lhd G$ 是（ⅱ）的推论.