# 1　商群

## 1.1　陪集与Lagrange定理

### 1.1.1　同余概念的推广

设H是G的子群，**在G上**定义模H同余关系：$\forall a, b \in G$，若$a * b' \in H$，则$a, b$模$H$同余，记作$a \equiv b(\mod H)$。

其实商就是把有等价关系的两个元素在新的群中看成同一个。

> 在数论中，我们有$a = b(\mod m) \Leftrightarrow m|(a-b)$，这是定义在整数加群上的同余关系，在整数加群上逆元为负元，因此$a * b' \sim a + (-b)$，这建立起了模H同余与模数同余的相似性。

### 1.1.2　模H同余的性质

（1）模H同余是G上的等价关系。

> （自反性）$a * a' = e \in H$
>
> （对称性）H是群，且$a * b' \in H$，则$(a * b')' = (b')' * a' = b * a' \in H$
>
> （传递性）$a * b' \in H, b * c' \in H$，由于H是群，所以$(a * b') * (b * c') = a * c' \in H$

（2）对于G上的模H同余关系，某个元素$a$的等价类是$Ha = \{h * a | h \in H\}$，称为G中H的一个**右陪集**，元素$a$是$Ha$的代表元。

> 等价类的定义：R是A上的等价关系，$a \in A$，则有$[a] = \{x | x \in A, aRx\}$。
>
> 元素$a$的等价类是$\{x | x \in G, a * x' \in H\}$，由于模H同余关系的对称性，书上写成了$\{x | x \in G, x * a' \in H\}$。真无语
>
> 再设$x * a' = h$，则$x = h * a$，也即$[a] = \{h * a | h \in H\}$，证毕。

（3）$He = H$;

（4）$a = b(\mod H) \Leftrightarrow Ha = Hb$;

> $h * a = \tilde{h} * a = (h * g) * a = (g * b * a') * a = g * b \in H$，其中$g \in H$，所以$Ha = Hb$

（5）$a \in H \Rightarrow Ha = H$

### 1.1.3 仿照右陪集，也可以定义左陪集

右陪集：对于G上的模H同余关系，元素$a$的等价类是$Ha=\{h*a|h\in H\}$

左陪集：对于G上的模H同余关系，元素$a$的等价类是$aH=\{a*h|h\in H\}$

> 定义左陪集不需要模H同余关系做任何修改，因为这一关系本身就是等价的，满足对称性

性质：H的所有左陪集的集合$S_L=\{aH|a\in H\}$与H的所有右陪集的集合$S_R=\{Ha|a\in H\}$等势

> 只要证明两个集合之间存在双射就可以了
>
> 令 $f:S_L\to S_R, f(aH)=Ha'$，先要证明映射与代表元选取无关，即$aH=bH\Rightarrow Ha'=Hb'$，通过群的性质可以证明，注意前者等价于$a'*b\in H$。
>
> 显然$f$是满射；
>
> 如果某个$Ha'$有两个原像$a_1H,a_2H$，则$Ha'=Ha_1'=Ha_2'$，则$a_1'*(a_2')'=a_1'*a_2\in H$，所以$a_1=a_2(\mod H)$，则$a_1H=a_2H$，则$f$是单射，综上是双射。
>
> **注意：$aH=bH$只能推出$Ha'=Hb'$，不能推出$Ha=Hb$。**

### 1.1.4 H在G中的指数

定义：群G关于子群H的左（右）陪集个数；记为$[G:H]$

### 1.1.5 Lagrange定理

若G是有限群，H是G的子群，那么$|G|=[G:H]|H|$

> 证明依据：G是有限群，故G中的右陪集全体构成G的一个分划。

### 1.1.6 Lagrange定理的推论

（1）有限群G中元素的阶是|G|的因子

> 有限群中所有元素的阶一定是有限的，设G中某个元素$a$的阶是m，令$H=\{a^0,a^1,\ldots,a^{m-1}\}$，显然H是m阶子群。则由拉格朗日定理$|G|=[G:H]\cdot m$。

（2）素数阶群都是循环群

> 设G是p阶群，则G中元素的阶为1或p，1是单位元的，则其它所有元素都是p阶的。

## 1.2 正规子群和商群

正规子群是一类特殊的子群。

### 1.2.1 正规子群

定义：H是G的子群。若对所有$g \in G, h \in H$都有$g' * h * g \in H$，则称H是G的正规子群，记为$H \lhd G$

定理：H是G的子群。H是G的正规子群当且仅当对于G中任意元素g，Hg=gH。

> ($\Rightarrow$) 任取 $x \in Hg$，则 $x = h_1 * g = g * g' * [h_1 * (g')']$，由正规子群的定义，$g' * h_1 * (g')' = h_2$，则$x \in gH$，所以$Hg \subseteq gH$。反过来类似。
>
> ($\Leftarrow$)显然。

举例：

（1）指数为2的子群是正规子群。

（2）交换群的任何子群都是正规子群。

### 1.2.2 G中H所有的右陪集$S_L$上的运算及代数结构

#### 1.2.2.1 乘法：$A \cdot B = \{a * b | a \in A, b \in B\}$

> 该运算满足结合律。

定理：若N是G上的一个正规子群，则$\langle \{Ng | g \in G\}, \cdot \rangle$是群，定义为G模N的商群，记作G/N。

> $Ng_1 \cdot Ng_2 = \{n_1 * g_1 * n_2 * g_2\}$，由正规子群满足$Ng = gN$，$Ng$中某元素$n * g$可以表示为$g * \bar{n}$，
>
> 于是$\{n_1 * g_1 * n_2 * g_2\} = \{n_1 * n_3 * g_1 * g_2\} = \{n * g_1 * g_2\} = \{n * g\} = Ng \in S_L$，封闭性满足。
>
> 结合律显然满足，因为这种乘法运算本身就满足结合律。
>
> 有单位元$N = Ne$，有逆元$(Ng)' = Ng'$。

推论：当G是有限群，G模N的商群*G/N*的元素个数就是N在G中的指数，$|G/N| = |G|/|N|$

定理：G是有限交换群，素数p是|G|的因子，那么群G中一定有一个p阶元

> 对G的阶数进行归纳证明。
>
> （1）当|G|=2时，显然成立；

> （2）设|G|<k时，命题成立；
>
> （3）当|G|=k时，设有个素数$p|k$。取G中某个t阶元g(t≠1)，显然t|k。
>
> 如果p|t，设t=rp，则$g^r$是G中的p阶元；
>
> 如果$p \nmid t$，则考虑G模正规子群$\langle g\rangle$的商群G/$\langle g\rangle$，$|G/\langle g\rangle| = |G|/t < |G| = k$，因此这商群仍然是有限交换群，p|k而$p \nmid t$，所以$p||G/\langle g\rangle|$，则在$G/\langle g\rangle$中有p阶元（归纳假设），因此在G中有p阶元，命题对k也成立。

注意：n阶群G，$d|n$，G中不一定有d阶子群。

## 1.3 群的同态

### 1.3.1 定义

$< G_1, *>, < G_2, \cdot >$是两个群，如果存在从$G_1$到$G_2$的映射$f$，使得对于任何$a, b \in G_1$，都有$f(a * b) = f(a) \cdot f(b)$，称$f$是从$G_1$到$G_2$的同态映射。

> 如果$f$是满射，称为满同态映射；
>
> 如果$f$是单射，称为单一同态映射；
>
> 如果$f$是双射，称为同构映射。

### 1.3.2 同态基本性质

$f(e_1) = e_2, [f(a)]' = f(a')$都成立

### 1.3.3 同态核

#### 1.3.3.1 定义

$f$的核是指$G_1$中通过$f$被映射到$G_2$的单位元$e_2$的那些元素构成的集合。记为Ker $f$。

$\ker f = \{a | a \in G_1, f(a) = e_2\}$

#### 1.3.3.2 性质

（1）$\ker f$是$G_1$的正规子群。

> 先要验证是子群、再验证是正规子群。证明略，按定义写出即可。

（2）$f$为单射当且仅当$\ker f = \{e_1\}$。

> 单射就是原像不同则像不同，若$f$是单射，则因为我们已经知道$f(e_1) = e_2$，故核里只能有$e_1$。

> 若反过来，已知$\ker f=\{e_1\}$，要证明f是单射，我们采用反证法。
>
> 假设f不是单射，就会存在两个不同的$h,g\in G$，但$f(h)=f(g)$。
>
> 那么$f(h*g')=f(h)\cdot[f(g)]'=f(h)\cdot[f(h)]'=e_2$，所以$h*g'=e_1$，推出$h=g$，矛盾。

（3）当$\ker f=G_1$时，任意$g\in G$，都有$f(g)=e_2$，称之为零同态映射。

### 1.3.4 同态的性质

（1）若$H_1\leq G_1$，则$f(H_1)\leq G_2$，特别$f(G_1)\leq G_2$；

（2）若$H_1\lhd G_1$，则$f(H_1)=f(G_1)$；

（3）若$H_2\leq f(G_1)$，则$f^{-1}(H_2)\leq G_1$；

（4）若$H_2\lhd f(G_1)$，则$f^{-1}(H_2)\lhd G_1$且$G_1/f^{-1}(H_2)\cong f(G_1)/H_2$；

> 先要注意$G_2$和$f(G_1)$不是相等的，$f(G_1)$可能缺少$G_2$中某些元素。
>
> 但是$f(G_1)$也是一个群，利用$f(H_1)\subseteq f(G_1)\subseteq G_2$，结合$1^\circ$的条件也可以知道$f(H_1)\leq f(G_1)$
>
> 证明都是拿定义操作，这里只想说明$f$和$f^{-1}$是保$\leq$、$\lhd$运算的。

（5）$\forall a\in G_1,f^{-1}[f(a)]=a\ker f$。

> 这里只需要补充$f^{-1}$的定义就可以看出，$f^{-1}[f(a)]=\{a|x\in G_1,f(x)=f(a)\}$。

### 1.3.5 群同态基本定理

（1）群$G_1$的任何商群都是$G_1$的同态像。

（2）若$G_2$是$G_1$的同态像，则$G_1/\ker f\cong G_2$。

> 定义$f:G_1\to G_1/H$，$f(a)=aH$，显然$f$是满同态，$f(G_1)=G_1/H$。
>
> 这里理解的话，不是说都是在$f$下，是指取不同的$f$，可以做到让每个商群都成为$G_1$的同态像。

### 1.3.6 举例

（1）$H\lhd G$，定义$f:G\to G/H$，$f(a)=aH$，称$f$为自然同态。

> $\ker f=\{x|x\in G,f(x)=H\}=\{x|x\in G,xH=H\}=H$
>
> $f(x)=[G/H\text{的单位元}]=H$。

（2）$H,K$均是G的正规子群，且$K\subseteq H$，则$G/H\cong\dfrac{G/K}{H/K}$