子群和拉格朗日定理

2023 年 6 月 8 日

目录

1 子群和拉格朗日定理

群G中的子群是一个子集，子群在G中的相同运算下构成一个群，下列的定义会让后面的这句话更准确

1.1 定义：封闭

设$*$是集合G上的一个运算，并设$S \subseteq G$是一个子集，我们说S在$*$下是封闭的，则对任意$x, y \in S$有$x * y \in S$

G上的一个操作是函数$* : G \times G \to G$，若$S \subseteq G$，则$S \times S \subseteq G \times G$，并且我们说$S$对运算$*$封闭的意思是$*(S \times S) \subseteq S$，例如：加法群$Q$的子群$Z$的有理数在$+$下封闭。若$Q^\times$是一个非零有理数的乘法群，则$Q^\times$在$\times$下封闭。但不关于$+$封闭，因为$-2+2=0 \notin Q^\times$

1.2 定义：子群

群G的一个子集H是子群，如果

1. $1 \in H$
2. 若$x, y \in H$，则$xy \in H$对运算$*$封闭
3. 若$x \in H$则$x^{-1} \in H$

我们记$H \leq G$来表示H是群G的一个子群。注意到$\{1\}$和G总是G的子群。其中$\{1\}$表示为由单一的元素1构成的子集。我们称G的子群为真子群，若有$H \neq G$并记为$H < G$。我们把H称为非平凡的，当且仅当$H \neq \{1\}$。等一下我们给出一些有趣的例子：

1.2.1 命题

每个G中的子群$H \leq G$都是一个群。

证明： 定义1.2的第二个定义已经讲了H对G中的运算是封闭的，所以H有一个运算，并且该运算是满足结合律的，因此方程对每个$x, y, z \in G$有$(xy)z = x(yz)$成立，特别的，对所有$x, y, z \in H$都成立。（因为一个运算$* : G \times G \to H \times H \subseteq G \times G$），最后，根据定义1他有单位元，根据定义三他有逆元，并且满足结合律和封闭。所以，子群H是一个群。

检验群G的子集H是一个子群（因为命题1.3告诉我们子群也是一个群）

比验证H的群公理要快得多，对结合律则是从G上的运算继承下来的，所以我们不需要重新证明结合律。

例1

1. 回忆一下，平面上所有等距同构组成的群是$\mathbf{Isom}(R^2)$，它的一个子集$O_2(R)$由所有固定原点的等距同构组成,这是$\mathbf{Isom}(R^2)$中的一个子群，若$\Omega \subseteq R^2$，则其对称群$\Sigma(\Omega)$也是一个$\mathbf{Isom}(R^2)$中的一个子群。若Ω的重心在原点，则该对称群$\Sigma(\Omega)$是正交群$O_2(R)$的子群，即$\Sigma(\Omega) \leq O_2(R)$

2. 下列四个置换

$$V = \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

   是一个群，因为V是一个S_4中子群。其中$(1) \in V$，并且$\alpha^{-1} = \alpha \in V$，$V - \{(1)\}$中的任意两个元素的乘积是集合中的第三个元素，所以满足封闭性，这确实是一个子群。我们也叫做4$-$置换群，或者克莱因（Klein Group,V是德语$Vierergruppe$的缩写）群。

   若要验证交换律$a(bc) = a(bc)$，则每个a, b, c都有4种选择，那么我们要验证$4^3 = 64$个等式，若去除(1)，也要验证$3^3 = 27$个等式。但不管怎么说，验证V是S_4中的子群显然是最好的方法，对于S_4每个选择有24种置换，要验证3^{24}是个非常大的工作量。

3. 若R^2是一个平面被考虑为是加法阿贝尔群，则有任意过原点的线L是一个子群。一个比较简单的方法就是选择直线上的点(a, b)，并注意L由所有的的标量倍数(ra, rb)组成。我们现在来验证一下这是一个子群：由于这是个加法群，则直线上的任意两个点$\alpha = (a, b), b = (s, v)$，那么有$b = (ra, rb)$有$a + b = (ra + a, rb + b) \in L$满足封闭，并且单位元是原点$O$，逆元是$-a \in L$，所以是一个子群。而对于加法，结合律总是成立的。

   实际上，我们可以简化子集是子群的三个条件。

1.2.2 命题

群G中的子集H是一个子群，当且仅当H是非空的且对$x, y \in H$都有$xy^{-1} \in H$

证明： 若H是一个子群，有$1 \in H$所以是非空的，由定义3有:元素$x, y \in H$存在$y^{-1} \in H$。在利用定义2就有$xy^{-1} \in H$

反过来，假设H是满足一些新的条件的子集，所以这个子集它非空，包含着某些元素，我们记为h，取$x = h = y$，那么由定义1就有$1 = hh^{-1} \in H$。而由定义3，如果$y \in H$，则设$x = 1$（因为1已经在集合内），给定$y^{-1} \in H$则有$1y^{-1} = y^{-1} \in H$。最后，我们知道$(y^{-1})^{-1} = y$(因为$a * a^{-1} = e$则$x^{-1} * a^{-1} = e$，所以$x^{-1} = (a^{-1})^{-1} = a$)，所以，若$x, y \in H$，则$xy \in H = x(y^{-1})^{-1} \in H$，所以$H$是一个群。

因为每个子群都包含单位元1，则把非空子集替换存在单位元$1 \in H$。

注意的是：若G中的运算是加法，则命题1.4就变成：H是非空的且$x, y \in H$有$x - y \in H$。

伽罗瓦提出：S_n中的子集H在合成的运算下封闭，若$\alpha, \beta \in H$，则$\alpha\beta \in H$，A·凯莱在1854年第一次定义了抽象群、结合律、逆元和单位元的概念。

1.2.3 命题：

一个有限群G上的非空子集H是子群，当且仅当H对G中运算封闭。即：设$a, b \in H$，则$ab \in H$。特别的，S_n的非空子集是子群当且仅当对合成封闭。

证明： 利用定义1，可知每个子群是非空的。利用定义2，该子群对运算封闭。

反过来，假设H是G中的非空子集，对G中的运算封闭，那么就满足定义2，于是H包含其元素的所有幂次。特别的，因为H非空，则有一些元素$a \in H$且对任意$n \geq 1$有$a^n \in H$。

就像我们在置换中学到的，每个G中的元素都是有限阶的，则有一些整数m使得$a^m = 1$，因此$1 \in H$满足定义1。最后，若$h \in H$和$h^m = 1$，则$h^{-1} = h^{m-1}$(因为$hh^{m-1} = h^m = 1 = h^{m-1}h$)，则$h^{-1} \in H$满足定义3，综上所述，$H$是一个群。

关于命题1.5有的时候会在无限群G中失效，例如加法群Z中的子集N对$+$封闭。但它不是一个Z的子群。

例2

S_n中的子集A_n由所有偶置换组成，则它是一个子群，因为对所有合成，偶置换$\circ$偶置换都是偶置换这个S_n中的子群我们叫n次交错群。记为A_n

1.3 定义：循环子群

设G是一个群和$a \in G$，记：

$$\langle a \rangle = \{a^n : n \in Z\} = \{\text{含有a的所有幂}\}$$

$\langle a \rangle$叫做通过a生成G的循环子群

若G是一个循环群，则对于某个$a \in G$有$G = \langle a \rangle$，我们把a叫做G的生成元。

我们可以很轻易的看到$\langle a \rangle$是一个子群。因为$1 = a^0 \in \langle a \rangle$，$a^n a^m = a^{n+m} \in \langle a \rangle$，$a^{-1} \in a \langle a \rangle$。前两个比较明显，第三个是因为循环子群包含$a$的所有幂次，所以也包括$-1$次幂。其中的一个运算是指数运算。所以是一个子群。

对每个$n \geq 1$，则乘法群$\Gamma_n = \{\zeta^k : 0 \leq k < n\}$是由$n$次单位根组成的循环群。其生成元是本原单位根$\zeta = e^{2\pi i/n}$

一个循环群可能会有几个不同的生成元，例如$\langle a \rangle = \langle a^{-1} \rangle$，且刚才的例子里面若有$(k,n) = 1$，那么$\zeta = e^{2\pi k i/n}$也可以是一个生成元

1.3.1 命题

若$G = \langle a \rangle$是阶为n的循环群。则a^k是一个G的生成元当且仅当$\gcd(k,n) = 1$

证明： 若a^k是生成元，则$a \in \langle a^k \rangle$，那么存在$s$使得$a = a^{ks}$，那么我们可以得到$a^{ks-1} = 1$，这意味$a^{ks-1}$被元的阶数整除，有$n | ks-1$，那么对于整数$t$有$ks - 1 = tn = 1$得到$ks - tn = 1$，所以$(k,n) = 1$

反过来，若$1 = sk + tn$，则有$a = a^{sk+tn} = a^{sk}$（因为$a^{nt} = 1$），所以$a \in \langle a^k \rangle$，这意味着$\langle a \rangle \leq \langle a^k \rangle$，所以$G = \langle a^k \rangle$

上述命题很好理解，如果生成元的幂等于阶或者阶的倍数，那么我们将看到全部的群都是单位元的奇怪情况。

1.3.2 推论：

阶数为n的生成元有$\phi(n)$个

证明： 利用命题1.7，我们知道阶数为n的群和生成元的幂次k的关系是gcd $(n,k)=1$。而在整数$n\geq 1$中，$\phi(n)$是满足$1\leq k<n$的整数k的个数。那么我们来证明后半句话。

$\phi(n)$是割圆多项式的次数，而这个次数是由所有的本原多项式组成的。所以根据多项式分解定理，我们可以把x^n-1分解为具有n个根的多项式乘积。其中乘积的次数总和就是根的个数。并且由于是本原多项式，所以除了0和n，中间的次数不能使得$a^k=1$。所以这意味着$\phi(n)$中的次数刚刚好就是$(k,n)=1$的个数。因为n和其倍数会使得$a^{tn}=1$。

这其实和我们的群非常相似：把阶和本原单位根放到一起看就知道了。

1.3.3 命题

循环群$G=\langle a\rangle$的子群S本身是一个循环。实际上，若a^m是S中的生成元，则m是满足$a^m\in S$中的最小正整数。

证明： 我们假设S是不平凡的，即$S\neq\{1\}$，而当$S=\{1\}$，则这个命题显然是真的。现在设$I=\{m\in Z:a^m\in S\}$，我们来证明I满足如下三个条件：

设I是Z的子集，满足

1. $0\in I$
2. $n,m\in I$，则$m-n\in I$
3. $m\in I,i\in Z$，则$im\in I$

则I的所有元素都是m的倍数。

所以，如果n是m的一个倍数，不妨假设m是I中最小正整数，由除法算式有$n=im+r$, $0\leq r<m$,利用三个条件，有$im\in I$，$r=n-im\in I$，但m是最小元，所以$r<m$不成立，有$r=0$，所以n是m的倍数。

对于$a^0=1\in S$，则有$0\in I$，若$m,n\in I$，则$a^m,a^n\in S$并且$a^m a^{-n}=a^{m-n}\in S$，所以$m-n\in S$，若$m\in I$和$i\in I$，则$(a^m)^i\in S$，所以$im\in I$。

因为$S\neq\{1\}$，则存在$a^q\in S$，因此$q\in I$且$q\neq 0$。若k是I中的最小正整数，则$k|m$对每个I中的数成立。我们声称$\langle a^k\rangle=S$，显然$\langle a^k\rangle\leq S$，反过来，取$s\in S$，则对某个m有$s=a^m$，因为$m\in I$和对某个l有$m=kl$所以$s=a^m=a^{kl}\in\langle a^k\rangle$有$S\leq\langle a^k\rangle$，所以$S=\langle a^k\rangle$

1.3.4 命题

设G是有限群和$a\in G$，则a的阶就是$\langle a\rangle$中元素的个数

G是有限的，为此对于整数$k\geq 1$，有$1,a,a^2,\cdots,a^{k-1}$是由k生成的不同元素。而$1,a,\cdots,a^k$有重复的元素，而$a^k\in\{1,a,\cdots,a^{k-1}\}$，则对某个$i,0\leq i<k$有$a^i=a^k$。如果$i\geq 1$，则$a^{k-i}=1,k-i\neq 0$（因为$a^k=a^i$，所以$a^{-i}$是一个逆元。）这与我们没有重复的列矛盾。所以$a^k=a^0=1$，且$k$是$a$的阶数。若$H=\{1,a,a^2,\cdots,a^{k-1}\}$，则$|H|=k$，足以表明$H=\langle a\rangle$，明显的，因为$\langle a\rangle$包含$a$的所有阶，所以$H\subseteq\langle a\rangle$。对于反包含，取$a^i\in\langle a\rangle$，由于$a^i\in\langle a\rangle$，则存在一个$k$使得$a^i=a^{qk+r}=a^{qk}a^r=a^r\in H$，其中$0\leq r<k$由此$\langle a\rangle\subseteq H$，则$\langle a\rangle=H$

1.4 定义：群的阶

若G是一个有限群，则G中含有的元素个数记为$|G|$，并称为G的阶

阶有两种意思，一种是群中元素$a\in G$的，另一种是关于$|G|$的。而命题1.10告诉了我们群元素a的阶等于$|\langle a\rangle|$

而对于接下来关于有限群的描述将会证明有限域的乘法群是循环的。

1.4.1 命题

一个n阶群是循环的，当且仅当对每个n中的因子d有唯一的循环子群的阶是d，反之，若至多存在一个阶为d的循环子群，其中$d\mid n$，则G是循环群。

设$G=\langle a\rangle$是一个阶为n的循环群。若我们声称$\langle a^{n/d}\rangle$的阶为d，则有$(a^{n/d})^d=a^n=1$，则我们要证明d是最小的正整数。若$(a^{n/d})^r=1$，则$n\mid(n/d)r$[1]，那么存在整数s使得$(n/d)r=ns$，$r=ds$和$r\geq d$，所以d是最小的整数。

[1] 设k是a的阶，而$a^n=1$，则有$n=sk+r$满足$a^{sk+r}=1$，其中$0\leq r<k$因为k是最小的整数有$r=0$，所以$k|n$

现在我们来证明唯一性。设C是G的d阶子群，通过命题1.9，可知C是一个循环群，则$C = \langle x\rangle$，取G中的另一个阶为d的子群$\langle a^{n/d}\rangle$。现在有$x = a^m$是一个n阶的元素，则$1 = (x^m)^d$，因此$n|md$，则对某个整数k有$md = nk$，因此$x = a^m = (a^{n/d})^k$，所以$C = \langle x\rangle \subseteq \langle a^{n/d}\rangle$，又由于两个子群的阶相同，则有$C = \langle a^{n/d}\rangle$

反之，定义一个群上的等价关系$a \equiv b$为$\langle a\rangle = \langle b\rangle$。则$a \in G$的等价类$[a]$由所有$C = \langle a\rangle$的所有生成元组成，我们用gen(C)来表示[a]，则G为

$$G = \bigcup_{\text{C是循环群}} \text{gen}(C)$$ [2]

因此$n = |G| = \sum_C |gen(C)|$，其中$G$是所有循环子群上的和。利用推论1.8可知$|\text{gen}(C)| = \phi(|C|)$[3]。我们通过$G$的假设知任意阶只有一个循环子群，那么

$$n = \sum_C |\ \text{gen}(C)\ | \leq \sum_{d|n} \phi(d) = n$$ [4]

所以对n的每个因子d，一定存在阶为d的循环子群C，只需要分配$\phi(d)$给$\sum_C |\ \text{gen}(C)\ |$)，特别的，其中肯定存在n阶循环子群$C$，所以$G$是一个循环群。

那么我们就有一种构造新子群的方法。

1.4.2 推论：

群G的任何一族子群的交 $\bigcap_{i\in I} H_i$也是G的子群。特别的，若H, K都是G的子群，那么$H \cap K$也是G的子群

设$D = \bigcap_{i\in I} H_i$是子群的交，现在通过验证定义来证明D是一个子群。首先，$D \neq \emptyset$，因为对所有$i \in I$有$1 \in H_i$有$1 \in D$。若$x \in D$，则x存在每个$x \in H_i$中。由于每个H_i是子群，所以存在$x \in H_i$就有$x^{-1} \in H_i$，所以有$x^{-1} \in D$。最后，$x, y \in D$则$x, y \in H_i$，又由于xy在每个H_i中满足封闭，即$xy \in D$成立。而为此D是一个子群。

[2]等价类满足三个性质：自反、对称、传递，所以a的等价类的一个可以是自己全部并起来就是C

[3]因为群的阶是群的元素个数，且C的阶就是最高次幂，根据定义，ϕ就是集合的最高幂次，所以因为阶=幂次有$\phi(|C|) = \phi(\text{群的幂次})$

[4]d|n是因为d取遍所有n的本原单位根，并且d都是n的因子。

1.4.3 推论：

若X是G的子集，则存在G中包含X的一个最小子群$\langle X\rangle$，即：对G中包含X的每个子群H都有$\langle X\rangle \leq H$

首先，注意到G包含X的子群存在。例如G自身就包含X，定义$\langle X\rangle = \cap_{X\subseteq H} H$为$G$的所有包含$X$的子群$H$的交。依据推论1.3 $\langle X\rangle$是G的子群。当然，因为每个H都包含X，所以$\langle X\rangle$包含X，最后，若H是任意一个包含X的子群，则H是构成子集族$\langle X\rangle$中的一个子群，因此 $\langle X\rangle \leq H$

注意：推论1.14并没有对子集有限制，这就是说$X=\emptyset$也是可以的，因此空集是所有集合的子集，我们有$\emptyset \subseteq H$对每个G的子群H成立。因此$\langle\emptyset\rangle$是所有G的子群的交集，其中之一是$\{1\}$，因此$\langle\emptyset\rangle = \{1\}$

1.5 定义

若X是群G的子集，则$\langle X\rangle$称为由X生成的子群。

例3

- 若$G=\langle a\rangle$是由a生成的循环群，则G是由子集$X=\{a\}$生成的。
- 正多边形π_n的对称群$\Sigma(\pi_n)$是通过a,b生成的，其中a是绕原点O旋转$(360//n)^\circ$，b是反射。这些生成元满足条件$a^n = 1$和$b^2=1$和$bab=a^{-1}$[a]，且$\Sigma(\pi_n)$是一个二面体群D_{2n}

[a] 因为$bab(v1) = ba(v_{n-1}) = b(v_0) = v_0 = a^{-1}(v_1)$

1.6 定义：群的字

设X是群G的非空子集。则X的字是指单位元或者是G中的形如

$$\omega = x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$$

其中$n\geq 1$且对所有i有$x_i\in X$和$e_i=\pm 1$

所以能看出来，字是一些元与逆元的乘积：$1=xx^{-1}$或者$xyy^{-1}1x=x^2$

1.6.1 命题

若X是群G的子集，则$\langle X\rangle$是X上的所有字组成的集合

证明： 我们首先证明X上的所有字构成的集合W是G的一个子群。由定义可知，$1\in W$，若$w,w'\in W$，那么$w=x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$，$w'=y_1^{f_1}y_2^{f_2}\cdots y_m^{f_m}$，其中$y_j\in X$并且$f_j=\pm1$，则$ww'=x_1^{e_1}\cdots x_n^{e_n}y_1^{f_1}\cdots y_m^{f_m}\in W$，最后有$(w)^{-1}=x_n^{-e_n}\cdots x_1^{-e_1}\in W$，所以$W$是G的子群，并且$W$含有每个$X$的元素[5]，那么利用推论1.4.3有$\langle X\rangle\leq W$

对于这个不等式的另一个情况的证明：我们要证明若S是任意G中包含X的子群，则S包含每个X上的字。因为S是一个子群，它包含x^e且其中$x\in X$和$e=\pm1$，S也包括其中每个元素的乘积。因此$W\leq S$对每个S成立。则$W\leq\cap S=\langle X\rangle$

综上所述 $W=\langle X\rangle$

1.6.2 命题

设a,b是整数和$A=\langle a\rangle$和$B=\langle b\rangle$是Z生成的循环子群。

1. 若$A+B$定义为$\{a+b:a\in A,b\in B\}$，则$A+B=\langle d\rangle$，$d=$gcd(a,b)
2. $A\cap B=\langle m\rangle$，其中$m=\mathrm{lcm}(a,b)$

证明： 我们能够很简单的检查$A+B$是Z中的子群（事实上，$A+B$恰好是a和b的所有线性组合的集合。）利用命题1.3.3可知$A+B$依然是循环群 (利用命题1.6.1并把运算换成加法可知，$A+B$是所有A和B的线性组合，一个线性组合对应着一个字，则$A+B$是由这些字生成的群。) 由于$A+B$是子群，那么它由一个生成元生成的我们记为$A+B=\langle d\rangle$，所以利用命题1.3.3可知d是我们能选到的最小非负整数。而这个最小的线性组合恰好就是满足$sa+tb=d$的数，我们知道这个d就是两者的最大公因子[6]因此$d=\gcd(a,b)$

对于第二个命题，若$c\in A\cap B$，则$c\in A$有$a|c$。同样的，对于$c\in B$也有$b|c$，因此每个$A\cap B$中的元素是一些关于a和b的倍数。

[5]这里原文写的是：X是G的子集且包含自身，推出$\langle X\rangle\leq W$，但这里的X应该是W，因为我们证明的实际上是W是子群而不是X是子群。

[6]在数论那边我们已经证明了满足线性组合的最小数是最大公因子gcd(a,b)

相反的，每个公倍数都包含在交集内，则利用命题1.3.3有$A\cap B$是循环子群，那么有$A\cap B=\langle m\rangle$。并且m也是$A\cap B$中的最小非负整数。并且m满足$a|m,b|m$，则若$(a,b)=1$，$m=ab$，若$(a,b)=d$，那么分解质因数后提取出相同的公因子d把剩下的互素数一并乘起来就是一个最小公倍数，因此$m=\mathrm{lcm}(a,b)$

关于有限群G的子群H的一些基本事实是：它们的阶都受约束，有$|H|\leq|G|$，还有$|H|$是$|G|$的一个因子。为了证明这个，我们先引入陪集的概念。

1.7 定义：陪集

若H是群G的子群，且$a\in G$，则陪集aH指的是G的子集aH，其中

$$aH=\{ah:h\in H\}$$

当然，我们可以有$a=a1\in H$，但陪集常常不是一个子群。例如：若$a\notin H$，则$1\notin aH$（否则$1=ah$对一些$h\in H$有$a=h^{-1}\in H$）

若我们使用G的运算符号$*$，则陪集aH又可以记为$a*H$有

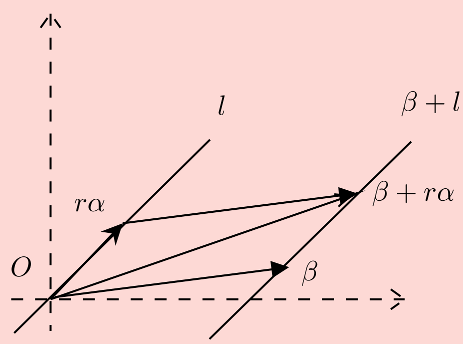
$$a*H=\{a*h:h\in H\}$$

特别的，若运算是加，则陪集记为

$$a+H=\{a+h:h\in H\}$$

例4

1. 考虑平面R^2上的加法群且令l是过原点O的直线，则直线l是R^2的一个子群。若$\beta \in R^2$，则陪集$\beta + l$是包含β且与l平行的直线l'。取l上一点$r\alpha$，由平行四边形法则可以得到$\beta + r\alpha \in l'$



2. 设$G = S_3$和$H = \langle(1\ 2)\rangle$，则H 恰好有三个陪集，即：

$$
\begin{aligned}
H =& \{(1), (1\ 2)\} = (1\ 2)H \\
(1\ 3)H =& \{(1\ 3), (1\ 3)(1\ 2) = (1\ 2\ 3)\} = (1\ 2\ 3)H \\
(2\ 3)H =& \{(2\ 3), (1\ 3\ 2)\} = (1\ 3\ 2)H
\end{aligned}
$$

   且每个大小都是2

在这些例子中，我们注意到给定的子集的不同陪集是不相交的。

若H是群G的子群，则定义一个G上的关系：

$$a \equiv b \ \text{若}\ a^{-1}b \in H$$

是G上的一个等价关系。若$a \in G$，则$a^{-1}a = 1 \in H$，所以$a \equiv a$满足自反性；若$a \equiv b$，则取$a^{-1}b \in H$对逆满足封闭。而$(a^{-1}b)^{-1} = b^{-1}a \in H$，所以$b \equiv a$满足对称性。若$a \equiv b$和$b \equiv c$，则$a^{-1}b, b^{-1}c \in H$，由于群对乘法封闭，那么$a^{-1}bb^{-1}c = a^{-1}c \in H$，所以$a \equiv c$。因此$\equiv$是满足传递性的，因此它是一个等价关系

我们断言$a \in H$的等价类是陪集aH，若$x \equiv a$，就存在$h \in H$使得$a^{-1}x = h$，则有$x = ah \in aH$，得到$[a] \subseteq aH$，对于反包含，则有$x = ah \in aH$，有$x^{-1}a = (ah)^{-1}a = h \in H$得到$x \equiv a$ 这说明$aH \subseteq [a]$，则$[a] = aH$，并且

等价类意味着等价类的两个元素作用到的两个命题是一样的（详情看关于同余）

1.7.1 引理

设H是群G的子群，且设$a, b \in G$

1. $aH = bH$当且仅当$b^{-1}a \in H$，特别的$aH = H$当且仅当$a \in H$
2. 若$aH \cap bH \neq \emptyset$，则$aH = bH$
3. 对所有$a \in G$有$|aH| = |H|$

证明： 对于第一个命题，其实是等价类引理的特殊情况[7]（注意小注）。在刚才已经讲了aH可以作为一个等价类，利用引理，$aH = bH$当且仅当其中的元素$a \equiv b$，而等价由定义就有$b^{-1}a \in H$。

对于命题2，需要引用引理[8]由于等价类俩俩不相交，所以$aH \cap bH = \emptyset$，并且因为等价类俩俩不相交，则有$aH = bH$。

最后，函数$f : H \to aH$通过$f(h) = ah$给出，这很容易看出来是一个双射，因为它的逆$aH \to H$由$ah \to a^{-1}(ah) = h$给出。这意味着aH和H具有相同的元素数量。

2 定理：拉格朗日定理

若H是有限群G的子群，则$|H|$整除$|G|$，或者说$|H|$是$|G|$的一个因子

证明： 设$\{a_1H, a_2H, \cdots, a_tH\}$为$G$中关于$H$的不同陪集。则

$$G = a_1H \cup a_2H \cup \cdots \cup a_tH$$

因为每个$g \in G$位于陪集gH，且$gH = a_iH$对某个i成立，利用引理1.8有不同的陪集是不相交的，则我们有

$$|G| = |a_1H| + |a_2H| + \cdots + |a_tH|$$

但根据引理1.8的命题3，我们知道$|aH| = |H|$，则$|G| = t|H|$

[7]引理：若$\equiv$是集合上的等价关系，$x \equiv y$当且仅当$[x] = [y]$

[8]若$\equiv$是集合X上等价关系，则等价类构成X的一个分类

2.1 定义：群的指数

G中子群H的指数记为$[G:H]$，它是G中的陪集H的个数。

当G是有限的，指数$[G:H]$就是上面关于拉格朗日定理的证明中公式$|G|=t|H|$中的数字t，那么有

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

所以这个公式也说明了$[G:H]$是$|G|$的一个因子

2.1.1 推论

若H是有限群G的子群，则

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

证明： 利用刚才拉格朗日的定理证明可得

一个正n边型的对称群$\sum(\pi_n)$是阶为$2n$的二面体群，它包含所有阶为n的循环子群，由旋转a生成。并且其子群$\langle a\rangle$的指数为$[\sum(\pi_n):\langle a\rangle]=2$，所以有两个陪集：$\langle a\rangle$和$b\langle a\rangle$，$b$是在$\langle a\rangle$之外的任何一个对称。

现在我们看到了为什么S_5中的元素的个数都是120的因子，剧透一下，S_5中任意给定循环结构的置换个数都是120的一个因子。

2.1.2 推论

若G是有限群并且$a\in G$，则a的阶是$|G|$的因子

证明： 元素a的阶数是子群$\langle a\rangle$的个数，所以由拉格朗日定理可得a的阶是$|G|$的因子

2.1.3 推论

若有限群G的阶数为m，则对所有$a\in G$有$a^m=1$

由推论2.1.2可知a的阶d满足$d\mid m$，则存在某个整数k使得$m=dk$有$(a^d)^k=1=a^m$

2.1.4 推论

若p是素数，则阶为p的群G都是循环群

证明： 取$a \in G$和$a \neq 1$，令$H = \langle a \rangle$是生成元为a的循环子群。由拉格朗日定理有$\mid H \mid$是$\mid G \mid = p$的因子，由于p是素数且$\mid H \mid > 1$，则$\mid H \mid = p = \mid G \mid$，因此$H = G$。

拉格朗日定理说的是：有限群G的子群的阶是$\mid G \mid$的因子，但我们还不知道逆命题是否成立，即d是$\mid G \mid$的一个因子，则存在G中阶为d的子群吗？答案是不一定的，一个例子就是交错群A_4是阶为12的群，但没有阶为6的子群。

3 习题

> 令G是有限群且设子群为H, K，若$H \leq K$，证明
> $$[G:H] = [G:K][K:H]$$

证明： 由拉格朗日定理有：$[G:H] = \mid G \mid / \mid H \mid$，$[G:K] = \mid G \mid / \mid K \mid$，$[K:H] = \mid K \mid / \mid H \mid$，则

$$[G:K][K:H] = \frac{\mid G \mid}{\mid K \mid}\frac{\mid K \mid}{\mid H \mid} = \frac{\mid G \mid}{\mid H \mid} = [G:H]$$

> 若H, K是G的子群，$\mid H \mid, \mid K \mid$是互素的，证明$H \cap K = \{1\}$

证明： 即证$\mid H \cap K \mid = 0$，由于H, K互素，设H, K的阶为h, k，那么由拉格朗日定理可知，H, K的子群阶都是互素的。设元素$n \in H, K$，则由推论2.1.3可知，则n有$n^h = n^k = 1$是成立的，但H, K中的子群的阶都是互素的，这意味着$(h, k) = 1$有$n^h \neq n^k$，所以对H, K所有元素的阶都不同，只有$\mid H \cap K \mid = 1$，即$H \cap K = \{1\}$

> 证明一个无限群包含无限个子群。

证明： 我们来证明逆否命题：一个无限子群包含有限个子群。

利用命题1.6.1，我们设$\langle X \rangle$是G上所有字组成的集合，那么由于G是无限群，则其中一个字w包含无穷多个元素，那么该集合$\langle X \rangle$是无限群。又因

为$\langle X\rangle$是无穷集生成的无限群，则其中的每个元生成的群的个数是无穷多个的，因此逆否命题不成立，所以无限群包含无限多个子群。

设G是有限群，并设S,T(不一定不同)是非空子集，证明$G=ST$或者$\mid G\mid\geq\mid S\mid+\mid T\mid$

证明： 题设要么证$G=ST$，要么$\mid G\mid\geq\mid S\mid+\mid T\mid$，对于$G=ST$，即

$$ST=\{st:s\in S,t\in T\}$$

首先，$ST\subseteq G$是绝对的，我们设$G\neq ST$（即$G\not\subseteq ST$），那么存在不被ST包含的元素$a\in G,a\notin ST$，设$S^{-1}=\{s^{-1}:s\in S\}$，那么集合$aS^{-1}\cap T=\emptyset$。

否则存在$x\in aS^{-1}\cap T$，有$x=as^{-1}=t$，$t\in T$得到$a=st$，说明$a\in ST$，但我们已经有$a\notin ST$，所以$aS^{-1}\cap T=\emptyset$。

所以$aS^{-1}\cap T=\emptyset$，那么$T\subseteq G-aS^{-1}$。由于S^{-1}中每个元素都不同，因此 $as_i^{-1}\neq as_j^{-1}$对所有的$s_i^{-1},s_j^{-1}\in S^{-1}$成立。则$\mid T\mid\leq\mid G\mid-\mid aS^{-1}\mid=\mid G\mid-\mid S^{-1}\mid=\mid G\mid-\mid S\mid$，综上所述$\mid S\mid+\mid T\mid\leq\mid G\mid$

反之，若$\mid S\mid+\mid T\mid>\mid G\mid$，则$G$被$ST$包含。但$S,T$是群的子集，则对所有的$S,T$中的元素都有$st\in G,s\in S,t\in T$。所以反过来$ST\subseteq G$，因此$G=ST$

综上所述，要么$G=ST$，要么$\mid G\mid\geq\mid S\mid+\mid T\mid$

1. 若$\{S_i:i\in I\}$是G的子群族，证明陪集的交集$\cap_{i\in I}x_iS_i$是空的，或者是$\cap_{i\in I}S_i$的陪集
2. 若群H是有限多个陪集的并

$$H=x_1S_1\cup\cdots\cup x_nS_n$$

证明至少有一个子群S_i在G中的指数是有限的

证明： 设$\bigcap_{i\in I} x_iS_i \neq \emptyset$，并设$A=\bigcap_{i\in I} S_i$是其中的子群，那么由于$A$是每个$S_i$中的子群，则每个$S_i, i\in I$都可以写为一些$A$的不同陪集之并，则$x_iS_i, i\in I$可以由$A$的一些陪集生成，由于$\bigcap_{i\in I} x_iS_i$非空，这部分子集又是$A$中的陪集生成，不妨设该元素为$z$，有$zA\in\bigcap_{i\in I} x_iS_i$，则$zA$这个陪集存在于每个子群$S_i$的陪集中，所以定义

$$zA=\bigcap_{i\in I} x_iS_i=\bigcap_{i\in I} zS_i=z\bigcap_{i\in I} S_i$$

证毕。[9]

对于命题2，当$S_1=S_2=\cdots=S_n$的时候，这意味着H由一个子群和其陪集组成。那么由于组成H的陪集是有限个的，那么显然命题成立。假设对$n-1$个本质不同的群成立，那么存在元素$a\notin x_nS_n$，但aS_n可以被前$n-1$个陪集包含，因为由一个子群组成的陪集互不相交。因此。我们取H中任意的一个元素h，则hS_n要么被陪集x_nS_n包含，要么被前$n-1$个陪集包含，所以H可以被表示为有限个陪集的并，所以它的指数是有限的。

设G为有限群，令$H\leq G$为子群，证明H在G中的左陪集个数等于H在G中的右陪集个数。

证明： 由于$H\subseteq G$是子群，则G可以写为一些H的陪集之并。考虑映射$aH\to Ha^{-1}$，这是由函数$f(aH)=Ha^{-1}$得到的。若其中存在右陪集有相等的情况，则有$f(aH)=Ha^{-1}=Hb^{-1}$，得到$Ha^{-1}b=H$但$aH\neq bH$，所以$H\neq a^{-1}bH$，这说明元素$a^{-1}b\notin H$，矛盾，所以$Ha^{-1}\neq Hb^{-1}$，现在，a^{-1}, b^{-1}是可逆的，且每个右陪集两两不等，这意味着函数是双射，综上所述，两个陪集的个数是相同的。

[9]我们证明的是逆否命题，若命题成立，逆否命题依然成立，反过来也是一样的。