近世代数

计算机科学与技术学院
唐琳琳

内容

第二章 群

- 群的定义和初步性质
- 元素的阶
- 子群
- 循环群
- 变换群
- 置换群
- 陪集、指数和Lagrange定理
- 群在集合上的作用

群的定义和初步性质

- 群：

定义 1：非空集合G，$\circ$是它的一个代数运算，如果满足以下条件：

Ⅰ：结合律成立，即对G中任意元素 a，b，c 都有

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

Ⅱ：G中有元素 e，叫做G的左单位元，它对G中每个元素 a 都有

$$e \circ a = a$$

Ⅲ：对G中每个元素 a，在G中都有元素 a^{-1}，叫做 a 的左逆元，使

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

则称G对代数运算 $\circ$ 作成一个群。

群的定义和初步性质

- 交换群（Abel群）

定义：如果对群G中任二元素 a, b均有

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

即G的代数运算满足交换律，则称G为交换群（可换群）或**Abel**群；否则称G为非交换群（非可换群）或非**Abel**群。

例如：整数集Z对于数的普通加法显然作成了一个交换群，0是它的左单位元，整数 $-a$ 是整数a 的左逆元。这个群常称为整数加群。

需要注意的是，整数集Z对于数的普通乘法不能做成群。因为，尽管普通乘法是Z的代数运算，并满足结合律，也有左单位元1，但是，除去 ± 1，其他元素在Z中均没有左逆元。

非零有理数、正有理数关于普通乘法——非零有理数乘群、正有理数乘群

群的定义和初步性质

- 例 1：设G为整数集。问：G对运算

$$a \circ b = a + b + 4$$

是否乘群？

$$(a \circ b) \circ c = (a + b + 4) \circ c$$
$$= (a + b + 4) + c + 4 = a + b + c + 8$$

$$a \circ (b \circ c) = a \circ (b + c + 4)$$
$$= a + (b + c + 4) + 4 = a + b + c + 8$$

故有

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

即代数运算$\circ$满足结合律。

又对 $\forall a \in G$ ，总有 $(-4) \circ a = -4 + a + 4 = a$ ，于是知-4是G中左单位元；而 $(-8 - a) \circ a = -8 - a + a + 4 = -4$，知 $-8 - a$ 是 a 的左逆元

群的定义和初步性质

- 例 2：全体正整数作成的集合G对运算

$$a \circ b = a^b$$

是否作成群？

解：首先，运算是正整数集合上的代数运算

但是，

$$(a \circ b) \circ c = a^b \circ c = a^{bc}$$

$$a \circ (b \circ c) = a \circ b^c = a^{b^c}$$

一般不会相等。例如

$$a=2, b=1, c=2$$

因此，正整数集合对于这个代数运算不构成群。

群的定义和初步性质

- 一般来讲：对于一个集合，要考察它是否作成群，不仅要注意它的元素是什么，更应该注意它的代数运算是什么。同一个集合，对这个代数运算可能作成群，对另一个代数运算却不一定作成群；即使对两个不同的代数运算同时都作成群，那么一般来说，也被认为是两个不同的群。

- 符号非本质，常把群的代数运算叫做“乘法”，还把 $a \circ b$ 简记为 $a \cdot b$ 或 ab

群的定义和初步性质

- 群的阶

定义：一个群G中包含元素的个数为n，则称n为群G的阶，记为$|G|=n$ 。无限群的阶称为无限，被认为是大于任意的正数。例如,$|G|>1$ 意味着G可能是阶大于1的有限群，也可能是无限群。

例 3：全体n次单位根对于数的普通乘法作成一个群。这个群记为 U_n ，并称作n次单位根群。

首先，满足结合律的代数运算；

再有，1在其中为左单位元；

最后，每个n次单位根的左逆元也在其中；

并且，可交换；

故，U_n 作成了一个**n**阶有限交换群。

群的定义和初步性质

- 例 4：令

$$G=\{1,i,j,k,-1,-i,-j,-k\}$$

并规定G的乘法如下：

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

$$(-x)y=x(-y)=-xy$$

$$-(-x)=x$$

其中$x,y\in\{1,i,j,k\}$

封闭-----此定义乘法为G上代数运算；

1----左单位元

1和-1的左逆元均为自身，其余i与-i，j与-j，k与-k互为左逆元

重点验证“结合律”？

群的定义和初步性质

- i，j，k三元素对等，验证所有可能情况即可

$$(ii)i = i(ii),\quad (ii)j = i(ij),$$
$$(ji)i = j(ii),\quad (ij)i = i(ji),$$
$$(ij)k = i(jk).$$

都成立，故G对所规定的乘法作成一个群。它是一个8阶有限非交换群，通常称这个群为四元数群。

群的定义和初步性质

- **性质**
- **定理 1**：群G的左单位元也是右单位元，并且是唯一的。

证明：设e是G的左单位元，对$\forall a\in G$，有 $a^{-1}a=e$， 也有$a'a^{-1}=e$

$$ae=e(ae)=a'a^{-1}(ae)=a'(a^{-1}a)e$$
$$=a'ee=a'(a^{-1}a)=(a'a^{-1})a$$
$$=ea=a$$

即，左单位元也是右单位元。

若存在另一左单位元 e'，则

$$e'=e'e=e$$

即，单位元唯一。

群的定义和初步性质

- **定理 2**：群G中任意元素a的左逆元a^{-1}也是右逆元，并且唯一。

证明： $\forall a \in G$，$a'a^{-1} = e$

$$\begin{aligned} aa^{-1} &= e\left(aa^{-1}\right) = a'a^{-1}\left(aa^{-1}\right) \\ &= a'\left(a^{-1}a\right)a^{-1} \\ &= a'a^{-1} \\ &= e \end{aligned}$$

若有两个左逆元，设为 a^{-1} 和 b，则

$$\begin{aligned} a^{-1} &= a^{-1}e = a^{-1}(ba) \\ &= a^{-1}(ab) \\ &= \left(a^{-1}a\right)b \\ &= eb \\ &= b \end{aligned}$$

群的定义和初步性质

- 推论 1：在群中消去律成立，即

$$ab = ac \Rightarrow b = c$$

$$ba = ca \Rightarrow b = c$$

证明：两遍分别左乘、右乘 a^{-1} 即可。

群的定义和初步性质

- 半群：
- **定义 2**：设S是一个非空集合，如果它有一个代数运算满足结合律，则称S是一个半群。
- 如果半群S中有元素 e，它对S中任意的元素 a 都有

$$ea = a$$

则称 e 为半群S的一个左单位元；如果在 S中有元素 e'，它对S中的任意元素 a 都有

$$ae' = a$$

则称 e' 为半群S的一个右单位元。

如果一个半群S有单位元（既是左单位元又是右单位元），则称S为有单位元的半群，或简称幺半群（**monoid**）。

群的定义和初步性质

- 性质
- 在一个半群中，可能既没有左单位元，也没有右单位元；可能只有左单位元，而没有右单位元；也可能只有右单位元，而没有左单位元。但是，如果既有左单位元又有右单位元，则二者必相等，它就是半群的唯一的单位元。
- 例 5：正整数集对普通乘法作成一个半群，而且是一个幺半群，1是单位元。
- 例 6：正整数集对普通加法作成一个半群，它既没有左单位元也没有右单位元。
- 例 7：设S是任一非空集合，对S中任意元素a，b规定

$$a \circ b = b$$

则S作成一个半群，而且S中每一个元素都是左单位元。但当 $|S|>1$ 时，S没有右单位元。

多选题 1分

设置

以下关于半群的单位元说法正确的是（）

A 所有半群都有单位元。

B 半群中可能没有左单位元或没有右单位元。

C 半群的左单位元与右单位元一旦都存在，必然相等，且唯一。

D 半群若无单位元则必然是无左单位元且无右单位元。

提交

群的定义和初步性质

- **定理 3**：设G是一个半群。则G作成群的充要条件是，对G中任意元素a，b，方程

$$ax = b, \qquad ya = b$$

在G中都有解。

证明：**必要性**：若G作成群则任意元素均有逆元存在，故

$$x = a^{-1}b, \qquad y = b\,a^{-1}$$

自然的是上两个方程的解。

充分性：首先对任意的固定元素 $b \in G$ ，由于上两方程总有解，则存在e使得

$$eb = b$$

而对于$\forall a \in G$，有 $bx = a$ 总有解 c，于是 $bc = a$

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

即，e是G的左单位元。

而 $ya = e$ 对于$\forall a \in G$ 均有解，则解即为a的左逆元。即任意G中元素有左逆元。

群的定义和初步性质

- **推论 2**：有限半群G作成群的充分必要条件是， 在G中两个消去律成立。

证明：**必要性**：消去律为

$$ab = ac \Rightarrow b = c$$

$$ba = ca \Rightarrow b = c$$

若G作成群则上下式左、右两遍分别左乘和右乘一个a^{-1}即可自然得到结论成立。

充分性：设$|G| = n$，且 $G = \{a_1, a_2, \cdots, a_n\}$ ，在G中任取两个元素a，b，若半群满足消去律则必有

$$b \in G = \{aa_1, aa_2, \cdots, aa_n\}$$

即方程 $ax = b$ 在G中总是有解的，同理可证方程 $ya = b$ 在G中也是有解的。由定理3可知有限半群G作成群。

注：充分利用“有限”和“消去律”

要求群G是有限的是必要的，如正整数集对乘法作成半群，满足消去律，但是它是无限集，不能作成群。

群的定义和初步性质

- 注：
- 如果一个交换群的代数运算用加号“+”表示，常称其为一个加群。单位元用**0**表示，并称为G的零元；元素a的逆元用**-a**表示，并称为a的负元。
- 例如：整数加群、有理数加群…

- 以后的讨论中不管群是否可交换，都常用乘号或者省略这个乘号，并仍称为乘法。

群的定义和初步性质---作业

- P37. 5
- 5. 设 $G=\{(a,b)\mid a,b\text{为实数且}a\neq 0\}$，并规定

$$(a,b)\circ(c,d)=(ac,ad+b)$$

证明：G 对此运算做成一个群。又问：此群是否为交换群？

群中元素的阶

- 规定：

任取$a \in G$，n是一个正整数

$$a^0 = e, \quad a^n = \overbrace{aa\cdots a}^{n}$$

$$a^{-n} = \left(a^{-1}\right)^n = \overbrace{a^{-1}a^{-1}\cdots a^{-1}}^{n}$$

由此，不难推出常见的运算规则在群中也成立，其中m，n为任意整数：

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

阶

定义 1：设a为群G中的一个元素，使$a^n = e$

的最小正整数n，叫做元素a的阶。

如果这样的阶不存在，称a的阶为无限。元素a的阶常用$|a|$来表示。

群中元素的阶

- 例 1：$G=\{1,-1,i,-i\}$（i是虚数单位）关于数的普通乘法作成一个群，即4次单位根群，其中1的阶是1，-1的阶是2，i与-i的阶都是4。

- 例 2：正有理数乘群 Q^+ 中，除了单位元的阶是1外，其余元素的阶均为无限。

- 例 3：在非零有理数乘群Q^* 中，1的阶是1，-1的阶是2，其余元素的阶均为无限。
- **定理 1**：有限群中每个元素的阶均有限。

证明：设G为n阶有限群，任取 $a\in G$， 则$a,a^2,\cdots,a^n,a^{n+1}$中必有相等的。设 $a^s=a^t$ $(1\le t<s\le n+1)$，则 $a^{s-t}=e$，从而 a 的阶有限。

注：无限群中元素的阶可能无限，也可能有限，甚至每个元素的阶都有限。

群中元素的阶

- 例 4：设 U_i（i是正整数）是全体i次单位根对普通乘法作成的群，即i次单位根群。现在令

$$U = \bigcup_{i=1}^{\infty} U_i$$

则由于一个m次单位根与一个n次单位根的乘积必是mn次单位根，故 U 对普通乘法作成群，而且是一个无限可交换群。

这个群中的每个元素的阶都有限。

- **定义 2**：若群G中每个元素的阶都有限，则称G为周期群；若G中除单位元e外，其余元素的阶均无限，则称G为无扭群；既不是周期群又不是无扭群的群称为混合群。

- **定理 2**：设群G中元素a的阶是n，则

$$a^m = e \Leftrightarrow n \mid m$$

证明：设$a^m = e$，并令 $m = nq + r,\quad 0 \le r < n$。由上式可得

$$e = a^m = a^{nq+r} = \left(a^n\right)^q a^r = a^r$$

群中元素的阶

- 续

但由于$|a|=n$，故不会存在更小的正整数使得$a^r=e$，于是r=0，也即得$n|m$

反之，若$n|m$，令$m=nq$，因a的阶为n，则有

$$a^m=a^{nq}=\left(a^n\right)^q=e$$

总结：群G中元素a，有

$$|a|=n\Leftrightarrow a^n=e\text{且若}a^m=e\Leftrightarrow \mathrm{n}|m$$

•**定理 3**：若群中元素a的阶是n，则

$$\left|a^k\right|=\frac{n}{(k,n)}$$

其中k为任意整数,(k,n)为k与n的正的最大公因数。

证明：设$(k,n)=d$，且$n=dn_1$，　$k=dk_1$，　$(n_1,k_1)=1$。则由于$|a|=n$，故有

$$\left(a^k\right)^{n_1}=a^{kn_1}=a^{k_1n}=\left(a^n\right)^{k_1}=e$$

群中元素的阶

其次，设$\left(a^k\right)^m=e$，则$a^{km}=e$，于是由定理2可知

$$n\left|km,\quad n_1\right|k_1 m$$

但是$\left(n_1,k_1\right)=1$，故$n_1|m$，因此，a^k的阶是n_1，故由上可知

$$\left|a^k\right|=n_1=\frac{n}{(k,n)}$$

•**推论 1**：在群中若$|a|=st$，则$\left|a^s\right|=t$。其中 s,t 是正整数。

证明：由于$|a|=st$，由定理3可知

$$\left|a^s\right|=\frac{st}{(s,st)}=\frac{st}{s}=t$$

即得$\left|a^s\right|=t$

•**推论 2**：在群中若$|a|=n$，则$\left|a^k\right|=n\Leftrightarrow(k,n)=1$。

证明：根据定理3，显然成立。

群中元素的阶

- **定理 4**：群中a的阶为m，b的阶为n，当ab=ba，且（m，n）=1时，有 $|ab| = mn$，即

$$|ab| = |a| \cdot |b|$$

证明：由已知条件，

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

其次，若有正整数s使得 $(ab)^s = e$，则便有

$$e = (ab)^{sm} = (a^m)^s b^{sm} = b^{sm}$$

但是$|b| = n$，故 $n|sm$，又因为$(m,n)=1$，故$n|s$。同理可得 $m|s$。再根据 $(m,n)=1$，可得 $mn|s$。

从而$|ab| = mn$，即 $|ab| = |a| \cdot |b|$。

群中元素的阶

- 注：ab=ba很重要
- 反例：有理数域上的二阶线性群 $GL_2(Q)$,易知

$$a=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\qquad b=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$$

的阶都有限，分别是4，3，但其乘积

$$ab=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$$

的阶无限，即 $|ab|\neq|a|\cdot|b|$ 。这个例子也说明，一般来说一个群G的全体有限阶元素对G的乘法并不封闭。

又反例：$GL_2(Q)$ 中，

$$c=\begin{pmatrix}1 & 2\\ 0 & -2\end{pmatrix},\qquad d=\begin{pmatrix}1 & 0\\ 0 & \frac{1}{2}\end{pmatrix}$$

的阶无限，但乘积$cd=\begin{pmatrix}1 & 1\\ 0 & -1\end{pmatrix}$的阶有限为2。

群中元素的阶

- **定理 5**：设G为交换群，且G中所有元素有最大阶m，则G中每个元素的阶都是m的因数，从而群G中每个元素均满足方程 $x^m = e$ 。

证明：设群G中元素a的阶为m，b为G中任意一个元素，阶为n。如果 $n \nmid m$ ，则必存在素数p满足下等式：

$$m = p^k m_1, \quad p \nmid m_1$$

$$n = p^t n_1, \quad t > k$$

由于 $|a| = m$， $|b| = n$，故由上面推论1知

$$\left|a^{p^k}\right| = m_1, \quad \left|b^{n_1}\right| = p^t$$

但由于 $(m_1, p^t) = 1$ 且G是交换群，故由定理4知

$$\left|a^{p^k} b^{n_1}\right| = p^t m_1 > p^k m_1 = m$$

这与m是G中所有元素的最大阶矛盾，因此，$n \mid m$ 。从而由定理2知，群G中每个元素都满足方程 $x^m = e$ 。

多选题 1分

设置

以下关于群中元素的阶数叙述错误的是（）

A 群中元素乘积的阶数等于阶数的乘积。

B 群中任一元素的阶数都是其中最大阶数的因子。

C 有限群中元素的阶数都有限。

D 无限群中元素的阶数都无限。

提交

群中元素的阶---作业

P42. 1. 1）

证明：群中以下每组中的元素有相同的阶：

1） a ，a^{-1} ，cac^{-1}

P43. 4. 设群 G 中元素 a 的阶为 n 。证明：

$$a^s = a^t \Leftrightarrow n \mid (s-t)$$

子群

- 子群

- **定义 1**: 设G是一个群，H是G的一个非空子集。如果H本身对G的乘法也作成一个群，则称H为群G的一个子群。

- 如果 $|G|>1$ ，则群G至少有两个子群，一个是只由单位元e作成的子群 $\{e\}$（以后常简记为e），另一个是G本身。这两个子群称为群G的平凡子群。别的子群，如果存在的话，叫做G的非平凡子群或真子群。

$$H \leq G, \qquad H < G$$

•例 1：正有理数乘群是非零有理数乘群的一个子群，正实数乘群是非零实数乘群的子群。

•例 2：全体偶数或全体3的整倍数，更一般的，全体n的整倍数（n是一个固定的整数）作成的集合

$$\{\cdots,-3n,-2n,-n,0,n,2n,3n,\cdots\}$$

都是整数加群的子群。

子群

- 例 3：数域F上全体n阶满秩对角阵的集合G_1是F上一般线性群$GL_n(F)$的一个子群；又F上一切纯量矩阵aE（$0\neq a\in F$，E为n阶单位方阵）的集合G_2是G_1的一个子群，当然也是$GL_n(F)$的子群。
- **定理 1**：设G是群，$H\leq G$。则子群H的单位元就是群G的单位元，H中元素a在H中的逆元就是a在群G中的逆元。

证明：设e'是H中单位元，e是G中单位元，则

$$e'e'=e'=e'e$$

于是由消去律知，$e'=e$。

同样，若a'是a在H中的逆元，a^{-1}是a在G中的逆元，则

$$a'a=e=a^{-1}a$$

再有群中满足消去律可得 $a'=a^{-1}$。

子群

- **定理 2**：群G的一个非空子集H作成子群的充要条件是：

1）$a,b \in H \Rightarrow ab \in H$

2）$a \in H \Rightarrow a^{-1} \in H$

证明：必要性，显然。依据H作成群和定理1。

充分性，验证定义，由1）知G中代数运算也是H中的代数运算，由于H中元素都是G中元素，故结合律自然满足；其次，由2）知任意H中元素a的逆元也在H中，则再由1）可得

$$aa^{-1}=e \in H$$

即，单位元e在H中，故H作成群。有 $H \leq G$ 。

- **定理 3**：群G的一个非空子集H作成子群的充要条件是：

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

证明：必要性：显然，由定理2.

子群

- 充分性：设当$a,b \in H$时，$ab^{-1} \in H$，则若$a \in H$，便有

$$aa^{-1} = e \in H, \qquad a^{-1} = ea^{-1} \in H$$

于是当$a,b \in H$时有$a,b^{-1} \in H$，从而

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

故由定理2知，$H \le G$。

•注：这个定理中的条件

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

显然也可以改写成

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

•注：群G的有限子集H作成子群的充要条件是，H对G的乘法封闭，即：

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

利用了有限半群成群的充要条件（第一节推论2）

子群

- 例 4：令H为数域F上行列式等于1的全体n阶方阵作成的集合。由于

$$|A|=|B|=1\Rightarrow\left|AB^{-1}\right|=1$$

即有$A,B\in H$可得 $AB^{-1}\in H$，由定理2可知H作成数域F上一般线性群$GL_n\left(F\right)$的一个子群。这个子群常记为$SL_n\left(F\right)$，并称为F上的特殊线性群。

- **定义2**：令G是一个群，G中元素a如果同G中每个元素都可换，则称a是群G的一个中心元素。
- 群G的单位元e总是群G的中心元素，除e外可能还有别的中心元素。若群G的中心元素只有e，则称G为无中心群。
- 交换群的每个元素都是中心元素。
- $GL_n\left(F\right)$除去单位元外还有别的中心元素（例如纯量矩阵），但当n>1时，显然群中还有非中心元素。

子群

- **定理 4**：群G的中心元素作成的集合$C(G)$是G的一个子群，称为群G的中心。

证明：因为$e \in C(G)$，故 $C(G)$ 非空，对于$\forall a,b \in C(G)$，对于群G中任意的元素x 都有

$$ax = xa, \qquad bx = xb$$

由此可得

$$(ab)x = x(ab), \qquad a^{-1}x = xa^{-1}$$

故$ab, a^{-1} \in C(G)$，从而$C(G) \leq G$ 。

•注：群G的中心显然是G的一个交换子群，又显然G是交换群当且仅当

$$C(G) = G$$

- 群G的中心在不发生混淆时也常简记为C

子群

- **定义3**：设A，B是群G的任二非空子集，规定

$$AB=\{ab\,|\,a\in A,b\in B\},$$

$$A^{-1}=\{a^{-1}\,|\,a\in A\},$$

并分别称 AB 为A与B的乘积，A^{-1} 为A的逆。

由此易知，对群的任意三个非空子集A,B,C均有

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

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

- 由定理2和定理3可直接得到以下两个推论。
- **推论1**：设H是群G的一个非空子集，则

$$H\le G\Leftrightarrow HH=H\qquad \&\qquad H^{-1}=H$$

证明：**必要性**：设$H\le G$，则 $HH=H$ 显然。又若 $a\in H$，则必有$a^{-1}\in H$，从而$a=(a^{-1})^{-1}\in H^{-1}$故$H\subseteq H^{-1}$。类似有 $H^{-1}\subseteq H$，故 $H^{-1}=H$。

子群

充分性： 由 $HH = H$ 可知H对G的乘法封闭。另外，若 $a \in H$ ，则 $a \in H^{-1}$ 。于是有 $b \in H$ 使

$$a = b^{-1}, \quad a^{-1} = b \in H$$

于是由定理2知， $H \leq G$ 。

类似的

- **推论 2**：设H是群G的一个非空子集，则

$$H \leq G \Leftrightarrow HH^{-1} = H$$

特别地，若H是群G的一个非空有限子集，则

$$H \leq G \Leftrightarrow HH = H$$

- 注：一个群的两个子群的乘积一般不再是子群。但在一定条件下可以是子群。

子群

- **定理 5**：设H，K是群G的两个子群，则

$$HK \le G \Leftrightarrow HK = KH$$

证明：**必要性**：由于 $HK \le G$，则由推论1可知

$$(HK)^{-1} = HK$$

因为H和K都是子群，则有 $H^{-1} = H$， $K^{-1} = K$ 。于是又有

$$(HK)^{-1} = K^{-1}H^{-1} = KH$$

因此，$HK = KH$ 。

充分性：设$HK = KH$，则有

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

由推论2知，$HK \le G$ 。

子群---作业

- P47. 1、4
- 1. 证明：群G的任意个子群的交仍是G 的一个子群。

- 4. 证明：一般线性群 $GL_n(F)$的中心是一切纯量矩阵$aE(0 \neq a \in F)$作成的子群。