同态

2023 年 6 月 19 日

目录

1 同态 **2**

1.1 定义：同态 2

1.2 定义：乘法表 3

1.2.1 引理 5

1.3 定义：核和象 7

1.3.1 命题 9

1.4 定义：正规子群 9

1.5 定义：共轭元 10

1.6 定义：共轭映射 10

1.6.1 引理 11

1.6.2 引理： 13

1.7 定义：四元数群 13

1.7.1 引理： 14

2 习题 **15**

1 同态

一个非常重要的问题就是：确定两个给定的群G, H 是否相同。例如，我们研究S_3，它是所有关于集合$X = \{1,2,3\}$的置换组成的。但所有$Y = \{a,b,c\}$的置换构成的群S_Y和S_3是不同的，因为关于$\{1,2,3\}$的置换不同于$\{a, b,c\}$。但尽管这两个群内容上不同，但它们看起来非常相似，所以，我们引入同态和同构来比较不同的群。

1.1 定义：同态

若$(G,*)$和$(H,\circ)$是群（我们已经展示了每个操作），则函数$f : G \to H$是**同态** [a] ，如果对$x, y \in G$

$$f(x*y) = f(x) \circ f(y)$$

若f是双射，则我们把f称为**同构**。若G, H是同构的，则记为$G \cong H$，存在一个同构$f : G \to H$（同构也是任何群族上的一个等价关系），特别的，若$G \cong H$，则$H \cong G$

[a] 同态这个词来源于希腊语的"homo"意思是“相同”，而morph的意思是“形状”或者“形式”，所以同态将一个群带到另一个具有相似形式的群（它的像），而同构一次涉及希腊语 iso意思是相等，所以同构群具有相同的形式。

同态的两个明显例子是恒等变换：$1_G : G \to G$，恒等变换也是一个同构。还有一个是平凡的同态，$f : G \to H$为对所有$a \in G$定义$f(a) = 1$。

一些其他的例子有：令R是带有加法运算的所有实数构成的群，并且令$R^>$为带有乘法运算的正实数组成的群。则函数$f : R \to R^>$定义为$f(x) = e^x$，这是一个同态，对$x, y \in R$，则

$$f(x+y) = e^{x+y} = e^x e^y = f(x)f(y)$$

现在，f也是一个同构，它的反函数$g : R^> \to R$是$\ln(x)$，因此，加法群R是$R^>$的同构。并且注意到它的反函数g也是一个同构：

$$g(xy) = \ln(xy) = \ln(x) + \ln(y) = g(x) + g(y)$$

对于第二个例子，我们声称复数的加法群C是同构于加法群R^2，定义$f : C \to R^2$为

$$f : a + ib \to (a, b)$$

这很容易验证f是一个双射，f也是同态，因为

$$\begin{aligned}f([a+ib]+[a'+ib']) =& f([a+a']+i[b+b'])\\ =&(a+a',b+b')\\ =&(a,b)+(a',b')\\ =&f(a+ib)+f(a'+ib')\end{aligned}$$

1.2 定义：乘法表

令$a_1, a_2, \cdots, a_n$是阶为n的有限群G中的所有不重复元素，一个G的**乘法表**指的是一个$n\times n$矩阵，第i行j列的元素是a_ia_j

G	a_1	$\cdots$	a_j	$\cdots$	a_n
a_1	a_1a_1	$\cdots$	a_1a_j	$\cdots$	a_1a_n
a_i	a_ia_1	$\cdots$	a_ia_j	$\cdots$	a_ia_n
a_n	a_na_1	$\cdots$	a_na_j	$\cdots$	a_na_n

当我们写一个乘法表的时候，它的单位元是位列第一的，即$a_1=1$。在这个例子中，表的第一行和第一列只是重复了a_1到a_n。所以我们经常忽略这个。

现在，考虑两个不是很重要的群的例子，令Γ_2为乘法群 $\{1,-1\}$的记号，和P为奇偶群。首先Γ_2的单位元是1，并且-1的逆元是自身。并且$1,-1$做乘法也是这个集合的元素，毫无疑问，这是一个群。对于另一个群同样，同则偶，不同则奇。那么它们的乘法表如下：

Γ_2：

1	-1
-1	1

，P:

偶	奇
奇	偶

明显的是，Γ_2和P是不同的群，但同样明显的，它们之间没有比较显著的不同。而同构的概念使得上述讨论变得正式化。毫不掩饰的说，Γ_2和P是同构的，对于函数$f:\Gamma_2\to P$，定义$f(1)=$ 偶和$f(-1)=$ 奇。我们来简单的验证一下。由于同偶异奇，则$f(1*-1)=f(-1)=$ 奇 $=f(1)\circ f(-1)=$ 偶 $\circ$ 奇 $=$ 奇。而$f(1*1)=f(1)=f(-1*-1)=$ 偶 $=$ 奇 $\circ$ 奇。所以是个同构。

对于n阶群有很多的乘法表，它的元素一共有$n!$种排法。若$a_1, a_2, \cdots, a_n$是G中所有无重复元素组成的表，设$f : G \to H$是双射，则$f(a_1), f(a_2), \cdots, f(a_n)$是所有$H$中无重复元素组成的表。则这个表决定了$H$中的一个乘法表。而$f$是同构的意思是：我们把$G$的一个乘法表（由元素$a_1, \cdots, a_n$确定）添加到$H$上，并且表格能匹配上$H$中的一个表（由$f(a_1), \cdots, f(a_n)$确定）。若$a_ia_j$是G的乘法表中的$i$行$j$列元素，则$f(a_i)f(a_j) = f(a_ia_j)$为$H$的乘法表中的$i$行$j$列元素。从这个描述上说，同构群具备相同的乘法表，所以同构群本质上是相同的，只是元素和操作的符号不同。

例1

这里有一个算法来检查给出的双射$f : G \to H$是否是一个同构：列举G的元素$a_1, \cdots, a_n$。并从这个表写出G的乘法表，再从表$f(a_1), \cdots, f(a_n)$中得到H的乘法表。然后逐行比较表中n^2个元素。

对于$G = S_3$，为了说明这一点，考虑一个对称群的置换$\{1, 2, 3\}$和$H = S_Y$，这是所有$Y = \{a, b, c\}$的置换构成的对称群。首先，G的元素有

$$(1),\ (1\ 2),\ (1,3),\ (2,3),\ (1,2,3)\ (1,3,2)$$

我们定义一个函数$\psi : S_3 \to S_Y$来用字母替换数字：

$$(1),(a,b),(a,c),(b,c),(a,b,c),(a,c,b)$$

然后将 S_3的乘法表与其元素通过相应法则得到的S_Y中的乘法表做比较。我们来看看各自的乘法表，首先是S_3的

1	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)(1 2)	(1 2)(1 3)	(1 2)(2 3)	(1 2)(1 2 3)	(1 2)(1 3 2)
(1 3)	(1 3)(1 2)	(1 3)(1 3)	(1 3)(2 3)	(1 3)(1 2 3)	(1 3)(1 3 2)
(2 3)	(2 3)(1 2)	(2 3)(1 3)	(2 3)(2 3)	(2 3)(1 2 3)	(2 3)(1 3 2)
(1 2 3)	(1 2 3)(1 2)	(1 2 3)(1 3)	(1 2 3)(2 3)	(1 2 3)(1 2 3)	(1 2 3)(1 3 2)
(1 3 2)	(1 3 2)(1 2)	(1 3 2)(1 3)	(1 3 2)(2 3)	(1 3 2)(1 2 3)	(1 3 2)(1 3 2)

然后我们列出S_Y的

1	(a b)	(a c)	(b c)	(a b c)	(a c b)
(a b)	(a b)(a b)	(a b)(a c)	(a b)(a c)	(a b)(a b c)	(a b)(a c b)
(a c)	(a c)(a b)	(a c)(a c)	(a c)(b c)	(a c)(a b c)	(a c)(a c b)
(b c)	(b c)(a b)	(b c)(a c)	(b c)(b c)	(b c)(a b c)	(b c)(a c b)
(a b c)	(a b c)(a b)	(a b c)(a c)	(a b c)(b c)	(a b c)(a b c)	(a b c)(a c b)
(a c b)	(a c b)(a b)	(a c b)(a c)	(a c b)(b c)	(a c b)(a b c)	(a c b)(a c b)

所以，通过这个表我们能很容易的检查4行5列的元素(2 3)(1 2 3) = (1 3)，而在S_Y中为$(b\ c)(a\ b\ c) = (a\ c)$。

现在我们来看更一般的同态

1.2.1 引理

设$f : G \to H$是一个同态，则

1. f(1) = 1;
2. $f(x^{-1}) = f(x)^{-1}$
3. $f(x^n) = f(x)^n$对所有$n \in Z$成立

证明： 将1应用于函数f上，则$1 \cdot 1 = 1 \in G$得到$f(1)f(1) = f(1) \in H$，然后在等式两边乘上$f(1)^{-1}$得到$f(1) = 1$

对于第二个命题，将f用在等式$x^{-1}x = 1$上，则$f(x^{-1})f(x) = 1 \in H$，由逆的唯一性得到$f(x^{-1}) = f(x)^{-1}$

对于第三个，则用归纳法证明$f(x^n) = f(x)^n$对所有$n \geq 0$成立。利用第二个命题，我们考虑负指数，$(y^{-1})^n = y^{-n}$对所有$y \in G$成立。并且由归纳假设对$n-1$成立，则$f((x^{-1})^{n-1}x^{-1}) = f(x)^{-n-1}f(x)^{-1} = f(x)^{-n}$成立，所以

$$f(x^{-n}) = f((x^{-1})^n) = f((x^{-1}))^n = (f(x)^{-1})^n = f(x)^{-n}$$

例2

我们来证明两个循环子群G, H具备相同阶的时候是同构的。然后我们可以推出来两个群的阶为素数p的群也是同构。

设$G = \langle x \rangle$和$H = \langle y \rangle$，定义$f : G \to H$对$0 \le i < m$有$f(x^i) = y^i$，现在有$G = \{1, x, x^2, \cdots, x^{m-1}\}$，$H = \{1, y, y^2, \cdots, y^{m-1}\}$。因此$f$是双射，我们可以看到$f$是一个同态，但现在我们必须证明对所有$i, j$和$0 \le i, j < m$有$f(x^i x^j) = f(x^i)f(x^j)$，而方程$i + j < m$明显成立，对$f(x^{i+j}) = y^{i+j}$有

$$f(x^i x^j) = f(x^{i+j}) = y^{i+j} = y^i y^j = f(x^i)f(x^j)$$

若$i + j > m$，则$i + j = m + r$，对$0 \le r < m$有

$$x^{i+j} = x^{m+r} = x^m x^r = x^r$$

因为$x^m = 1$，类似我们可以得到$y^{i+j} = y^r$，则

$$f(x^i x^j) = f(x^{i+j}) = f(x^r) = y^r = y^{i+j} = f(x^i)f(x^j)$$

因此，f是同构且$G \cong H$

群G的一个性质若被其他跟G同构的群共享，则称其为G的**不变量**。例如：G的阶$\mid G \mid$是自身的不变量，因为同构群具有相同的阶。而交换律是阿贝尔群的一个不变量，因为所有阿贝尔群都满足交换律。(若a, b存在，则$ab = ba$并且$f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$，因此$f(a)$和$f(b)$存在)

因此R和$GL(2, R)$不是同构，因为R加法群是一个阿贝尔群，而$GL[2, R]$不是阿贝尔群，因为矩阵不满足交换。一般来说，对两个给定的群判断是否同构是一个挑战。

例3

我们给出两个同阶的非同构群：

令V为一个4−群，其元素为下列4个置换组成

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

并令$\Gamma_4 = \langle i \rangle = \{1, i, -1, -i\}$为乘法群的四次单位根，其中$i^2 = -1$。若存在同构$f : V \to \Gamma_4$，则因为$f$的满射限制则有一些$x \in V$和$i = f(x)$，但$x^2 = (1)$对所有$x \in V$成立，所以$i^2 = f(x)^2 = f(x^2) = f((1)) = 1$，但是矛盾，$i^2 = -1$，因此$V$和$\Gamma_4$不是同构。

我们给出其他对结果的证明。例如Γ_4是循环群但V不是；或者Γ_4的元素是四阶的但V不是；或者Γ_4只有一个二阶的元素，但V有三个。所以在这些证明面前，你真的应该相信V和Γ_4不是同构。

1.3 定义：核和象

若$f : G \to H$是同态，定义

$$核：f = \{x \in G : f(x) = 1\}$$

和

$$象：f = \{h \in H : h = f(x)\}对某些x \in G$$

所以我们经常吧核和象缩写为$\ker f$和$\mathrm{im} f$，象的集合也叫值域。并且$\ker f$的组成是G中的元素满足$f(x) = 1, x \in G$组成的一个集合。

例4

1. 若$\Gamma_n = \langle\zeta\rangle$，其中$\zeta = e^{2\pi i/n}$是原初$n$次单位根。则$f : Z \to \Gamma_4$由函数$f(m) = \zeta^m$给出，这个函数是满射同态的。因为$\ker f$为$m$的所有倍数（注意$\zeta^m = 1$），但不是同构，因为不满足双射。

2. 若Γ_2是乘法群且$\Gamma_2 = \{\pm 1\}$。则$\mathrm{sgn} : S_n \to \Gamma_2$是一个同构。因为对称群中的元素要么是偶（sgn(x)=1）的要么是奇的（sgn(x)=-1）。再利用定理：$\mathrm{sgn}(ab) = \mathrm{sgn}(a)\mathrm{sgn}(b)$可知，确实是一个同构。它的象$\mathrm{sgn} = \{\pm 1\}$，因此函数是满射的，而它的核是交错群$A_n$，$A_n$为所有偶置换组成的集合。

3. 行列式也是一个同态，定义$\det : \mathrm{GL}(2, R) \to R^\times$，其中$R^\times$为非零实数构成的乘法群，$\mathrm{GL}[2, R]$是可逆二阶矩阵。则$\operatorname{im}\det = R^\times$，因此det是满射，因为，若$r \in R^\times$，则$r = \det\left(\begin{bmatrix} r & 0 \\ 0 & 1 \end{bmatrix}\right)$，它的核是特殊线性群$\mathrm{SL}[2, R]$，其中元素为满足行列式为$ad - bc = 1$的矩阵$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$

4. 我们现在推广$\ker f$的构造。回忆一下逆的定义：若$f : X \to Y$是函数和$B \subseteq Y$为子集，则我们证明

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

若$f : G \to H$是同态和$B \leq H$是H中子群。则逆$f^{-1}(B)$是G的子群。我们有$1 \in f^{-1}(B)$对$f(1) = 1 \in B \leq H$成立。若$x, y \in f^{-1}(B)$，则$f(x), f(y) \in B$并且$f(x)f(y) \in B$，因此$f(xy) = f(x)f(y)$，有$xy \in B$。最后，若$x \in f^{-1}(B)$，则$f(x^{-1}) = f(x)^{-1} \in B$，所以$f(x) \in B$和$x^{-1} \in f^{-1}(B)$。特别的，若$B = \{1\}$，则$f^{-1}(B) = f^{-1}(1) = \ker f$。由此得到$f : G \to H$是一个同态，并且$B$是$H$的子群。则$f^{-1}(B)$是$G$的包含$\ker f$的子群。

1.3.1 命题

令$f: G \to H$为一个同态。

1. $\ker f$是G的子群且 $\mathrm{im} f$是H的子群
2. 若$x \in \ker f$和$a \in G$，那么$axa^{-1} \in \ker f$
3. f是单射当且仅当$\ker f = \{1\}$

证明 由引理1.3的对于$f(1) = 1$可知$1 \in \ker f$。接着，若$x, y \in \ker f$，则$f(x) = 1 = f(y)$，由于$f(xy) = f(x)f(y) = 1 \cdot 1 = 1$，所以$xy \in \ker f$。最后若$x \in \ker f$，则$f(x) = 1$并且$f(x^{-1}) = f(x)^{-1} = 1^{-1} = 1$意味着$x^{-1} \in \ker f$，所以$\ker f$是$G$的子群。

现在我们来证明后半部分。首先，$1 = f(1) \in \mathrm{im} f$。接着，若$h = f(x) \in \mathrm{im} f$，则$h^{-1} = f(x)^{-1} = f(x^{-1}) \in \mathrm{im} f$。最后，若$k = f(y) \in \mathrm{im} f$，则$hk = f(x)f(y) = f(xy) \in \mathrm{im} f$。所以$\mathrm{im} f$是$H$的子群。

对于第二个命题：若$x \in \ker f$，则$f(x) = 1$并且

$$f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)f(a)^{-1} = 1$$

所以$axa^{-1} \in \ker f$

最后，若f是单射，则$x \neq 1$意味着$f(x) \neq f(1) = 1$，所以$x \notin \ker f$。反之，假设$\ker f = \{1\}$，$f(x) = f(y)$，则$1 = f(x)f(y)^{-1} = f(xy^{-1})$，那么$xy^{-1} \in \ker f = 1$，因此$xy^{-1} = 1$ 由$x = y$，所以f是单射。

1.4 定义：正规子群

一个G中的子群H如果称为**正规子群**，如若它满足$k \in K$和$g \in G$有$gkg^{-1} \in K$。若K 是G的正规子群，则记为$K \lhd G$

这个定义告诉了我们，同态的核总是正规子群。若G是阿贝尔群，则每个子群都是正规的。对$k \in K, g \in G$，则$gkg^{-1} = kgg^{-1} = k \in K$。

一个循环子群$H = \langle (1\ 2) \rangle \in S_3$，它由两个元素$(1), (1\ 2)$组成。但它却不是$S_3$中的正规子群。若$\alpha = (1\ 2\ 3)$，则$\alpha^{-1} = (3\ 2\ 1)$，并且

$$\alpha (1\ 2) \alpha^{-1} = (1\ 2\ 3)(1\ 2)(3\ 2\ 1) = (2\ 3) \notin H$$

另一方面，$\langle (1\ 2\ 3) \rangle$却是正规子群。我们来看，选择任意$S_3$中的元素$(1\ 2)$，

则$(1\ 2)^{-1}=(1\ 2)$，那么有

$$(1\ 2)(1\ 2\ 3)(1\ 2)=(1\ 3\ 2)$$

而$(1\ 2\ 3)$生成的循环群为

$$\langle(1\ 2\ 3)\rangle=\{(1),(1\ 2\ 3),(3\ 1\ 2),(2\ 3\ 1),(1\ 2\ 3)^{-1},(2\ 3\ 1)^{-1},(3\ 1\ 2)^{-1}\}$$

而$(1\ 3\ 2)=(1\ 2\ 3)^{-1}$ 所以$\langle(1\ 2\ 3)\rangle$是正规子群

1.5 定义：共轭元

若G是群和$a\in G$，那么一个a的共轭元是G中形如

$$gag^{-1}$$

的元素，其中$g\in G$

若子群$K\leq G$是正规子群，当且仅当K包含其元素所有共轭元。若$k\in K$，则$gkg^{-1}\in K$对所有$g\in G$成立。再之前的置换中，我们已经证明了$\alpha,\beta\in S_n$是共轭的，当且仅当S_n有相同的循环结构。

若$H\leq S_n$，则$\alpha,\beta\in H$如在G中是共轭的并不意味着再H中也是共轭的。例如：$(1\ 2)(3\ 4)$和$(1\ 3)(2\ 4)$是S_4中的共轭元，但在例子3的群V中却不是共轭的。因为V是阿贝尔群。会得到两个共轭元等于自身的情况。

注意： 在线性代数中，一个线性变换$T:V\to V$，其中V是一个R上的n维向量空间。若使用一个V上的基，则可以确定一个$n\times n$的矩阵A。若使用其他的基，则可以从T确定另一个矩阵B。并且我们可以证明A,B是相似矩阵。若两个矩阵相似，则有相同的特征值，并且可以通过一个可逆矩阵P得到$PAP^{-1}=B$，因此$\mathrm{GL}[n,R]$上的共轭元是相似的。

1.6 定义：共轭映射

若G是群和$g\in G$，对所有$a\in G$定义一个G的**共轭映射**$\gamma_g:G\to G$为

$$\gamma_g(a)=gag^{-1}$$

1.6.1 引理

1. 若G是群并且$g \in G$，则共轭映射$\gamma_g : G \to G$是同构
2. 共轭元都具备相同的阶。

证明： 若$g, h \in G$，则

$$(\gamma_g \circ \gamma_h)(a) = \gamma_g(hah^{-1}) = g(hah^{-1})g^{-1} = (gh)a(gh)^{-1} = \gamma_{gh}(a)$$

因此，我们有

$$\gamma_g \circ \gamma_h = \gamma_{gh}$$

所以，γ_g是一个双射。对$\gamma_g \circ \gamma_{g^{-1}} = 1 = \gamma_{g^{-1}} \circ \gamma_g$。

现在我们来证明γ_g是同构。若$a, b \in G$，则

$$\gamma_g(ab) = g(ab)g^{-1} = (gag^{-1})(gbg^{-1}) = \gamma_g(a)\gamma_g(b)$$

所以共轭映射是双射，也是同态这说明共轭映射是一同构。

对于第二个命题，当我们再说a, b是共轭的时候，就是再说存在$g \in G$和$b = gag^{-1}$，所以$b = \gamma_g(a)$。但γ_g是一个同构，所以除了1之外没有任何满足$f(1) = 1$的情况出现，现在，我们不妨假设通过共轭映射$\gamma_g(a) = b$的阶是不同的，这意味着$b^m = 1$但$(gag^{-1})^m \neq 1$，但利用引理1.2.1的命题3，由于γ_g是同构，所以满足$f(a^m) = f(a)^m$，但$b^m \neq \gamma_g(a^m)$，这是一个矛盾。因此共轭元都具备相同的阶。

例5

群G的一个中心，记作$Z(G)$，它定义为：

$$Z(G)=\{z\in G:zg=gz\}\text{对所有}g\in G\text{ 成立}$$

所以，$Z(G)$由G中所有能和任意元素交换的元素组成(注意方程$zg=gz$可以重写为$z=gzg^{-1}$，所以G中没有其他的元素与其共轭)。
现在我们来证明$Z(G)$是G的子群。一般的，$1\in Z(G)$，因为1交换一切元素。若$z,y\in Z(G)$，则$yg=gy$和$zg=gz$对所有g成立。因此$(yz)g=y(gz)=g(yz)$。所以yz也和一切元素交换。因此$yz\in Z(G)$。最后，若$z\in Z(G)$，则$zg=gz$对所有g成立，特别的，$zg^{-1}=g^{-1}z$，因此

$$gz^{-1}=(zg^{-1})^{-1}=z^{-1}g$$

所以z的逆也在$Z(G)$中，得到$Z(G)$是一个子群。
而$Z(G)$是一个正规子群，若$z\in Z(G)$和$g\in G$，则

$$gzg^{-1}=zgg^{-1}=z\in Z(G)$$

藉由我们可以知道，若一个群G是阿贝尔群，当且仅当$Z(G)=G$。另一个极端是$Z(G)=\{1\}$。这种群我们称为**无中心的**，例如$Z(S_3)=\{1\}$，当然，所有对称群都是无中心的。

例6

一个4−群V是S_4中的正规子群。它的元素为：

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

利用在置换中学到的知识，我们知道两个转置的乘积的每个共轭元的循环结构是不变的，所以这意味着每个共轭元都是另一个元素。[a]，而S_4中只有3个V中的元素，所以V是一个S_4的正规子群。

[a] 令$\alpha,\gamma\in S_n$，对所有i，若$\gamma:i\to j$，则$\alpha\gamma\alpha^{-1}:\alpha(i)\to\alpha(j)$

1.6.2 引理：

1. 若H是G中指数为2的子群，则$g^2 \in H$对每个$g \in G$都成立。
2. 若H是G中指数为2的子群，则H为G的正规子群。

证明： 因为H指数为2，那么存在两个陪集。即H, aH，其中$a \notin H$。因此G可以变成两个不相交集合:$G = H \cup aH, H \cap aH = \emptyset$。取$g \in G$且$g \notin H$，则$g = ah$对某个$h \in H$成立。若$g^2 \notin H$，则$g^2 = ah'$，其中$h' \in H$。因此

$$g = g^{-1}g^2 = (ah)^{-1}ah' = h^{-1}a^{-1}ah' = h^{-1}h \in H$$

是一个矛盾。

对于第二个命题，我们要证明若$h \in H$，则共轭元$ghg^{-1} \in H$对每个$g \in G$成立。因为H的指数为2，则同样存在两个陪集aH, H。其中$a \notin H$。现在，有$g \in H$或者$g \in aH$。若$g \in H$，因为H是个群，则$ghg^{-1} \in H$。反之，对于另一个集合。记$g = ax$，其中$x \in H$。则$ghg^{-1} = a(xhx^{-1})a^{-1} = ah'a^{-1}$，其中$h' = xhx^{-1} \in H$。如果$ghg^{-1} \notin H$，则$ghg^{-1} = ah'a^{-1} \in aH$。因此$ah'a^{-1} = ay$对某个$y \in H$成立。那么去掉a，则$h'a^{-1} = y$，得到$y^{-1}h' = a$。因为$y \in H$，所以$y^{-1} \in H$这意味着$a \in H$。矛盾，因此$H$是$G$的正规子群

1.7 定义：四元数群

一个群的四元数[a] 指的是由GL$[2, C]$中的矩阵组成的阶为8的群Q。

$$Q = \{I, A, A^2, A^3, B, BA, BA^2, BA^3\}$$

我们要注意其中的元素$A \in Q$是阶为4的元素。所以$\langle A \rangle$是阶为4且指数为2的子群。它的陪集$B\langle A \rangle = \{B, BA, BA^2, BA^3\}$

[a]加减乘除这四个运算可以从R拓展到平面上，使得算术的所有普通法则都成立，当然，在这个背景下，我们一般把这个平面C叫做复数集C。而哈密尔顿(W.R.Hamilton)发明了一种方法，将这些运算从C拓展到四维空间，使得算术的所有普通法则都成立(除了乘法交换律)，他把这些新“数”叫做“四元数(quaternions)”。即通过给出四个特殊的四元组$1, i, j, k$的积来确定乘法

$$i^2 = -1 = j^2 = k^2$$

$$ij = k, ji = -k, jk = i, kj = -i, ki = j, jk = -j$$

而所有非零四元数构成一个乘法群，且四元数群是包含这四个元素的最小子群（阶为8

例7

在练习我们将证明Q是阶为8的非阿贝尔群。现在我们声称Q的每个子群是正规的，则由拉格朗日定理可知Q的每个子群都是8的除数。这意味着可能的阶数是$1, 2, 4, 8$。显然，$\{1\}$以及阶为8的子群（Q自身）都是正规子群。这是因为对于$\{1\}$，取任意的元素$x \in Q$都有$x1x^{-1} = xx^{-1} = 1 \in \{1\}$。利用引理1.6.2，阶为4的子群必是正规子群。因为其指数为2。最后，Q中阶为2的元素只有$= -I$，并且$\langle -I \rangle$是唯一一个阶为2的子群。对任意的矩阵M，则$M(-I) = (-I)M$，那么$M(-I)M^{-1} = -IMM^{-1} = -I \in \langle -I \rangle$，所以每个$Q$的子群都是正规子群。

上述例子表明了Q不是阿贝尔群。但因为其每个子群都是正规的，这长得很像阿贝尔群。实际上这种例子只有一个，其子群都为正规子群的有限群具有$Q \times A$的形式，其中A是$A = B \times C$的阿贝尔群。且B的每个非单位元素的阶为2，而C的每个元素的的阶是奇数。

拉格朗日指出有限群G的子群的阶是$\mid G \mid$的因子，这也有一个问题，即$\mid G \mid$的某个因子d是否也有一个阶数为d的子群对应。但下述结果表明这种结论是错的。

1.7.1 引理：

交错群A_4是阶为12的群，但没有阶为6的子群。

证明： 首先，$\mid A_4 \mid = 12$，若A_4包含6阶子群H，则H指数为2。利用引理1.6.2，那么存在$a^2 \in H$和对所有$a \in A_4$。若a是一个3−循环，那么a的阶为3。$a = a^4 = (a^2)^2$，所以H包含每个3−循环。这是一个矛盾，因为A_4有8个3−循环。

简单的讨论：但若G是n阶阿贝尔群，则对于每个n的因子d，存在一个d阶子群。

2 习题

若这有一个双射$f : X \to Y$(这是在说X, Y具有相同数量的元素。)，证明存在同构$\varphi : S_X \to S_Y$

证明： 只需要构造映射$\varphi(a) = faf^{-1}$由双射$f : X \to Y$给出。其中$a \in S_X$。首先$faf^{-1} \in S_Y$毋庸置疑，并且和S_X具有相同的循环结构。对于任意$a, b \in S_X$，则有

$$\varphi(ab) = f(ab)f^{-1} = (faf^{-1})(fbf^{-1}) = \varphi(a)\varphi(b)$$

这意味着S_X和S_Y是同态。其次，由于f是一个双射，设φ不是一个双射，这意味着可能有$\varphi(a) = \varphi(b)$，其中$a \neq b$，那么$faf^{-1} = fbf^{-1}$由消去律得到$b = (f^{-1}f)a(f^{-1}f) \Rightarrow b = a$是一个矛盾，因此$\varphi$是一个双射，综上所述，$S_X \cong S_Y$

1. 证明同态的复合是一个同态
2. 证明同构的逆是同构
3. 证明同构是任何群族上的等价关系
4. 证明若两个群同构于一个群，则两个群彼此同构

证明

1. 设两个同态f, w，则对群H, G的元素$h \in H, g \in G$有

   $$f(h * g) = f(h) * f(g) \quad w(h * g) = w(h) * w(g)$$

   则$fw(h * g) = f(w(h) * w(g)) = fw(h) * fw(g)$。因此同态的复合也是一个同态

2. 设两个群H, K，它们之间存在一个同构映射$f : H \to K$，则取任意$j \in K$存在一个运算$f^{-1}(j) = h \in H$是唯一确定的，取$h, k \in H$，由$f(h *$

$k) = f(h)f(k)$，则$f((h*k)^{-1}) = f(k^{-1}h^{-1}) = f(k^{-1}) * f(h^{-1}) = f(k)^{-1} * f(h)^{-1} = (f(h)f(k))^{-1} = f(h*k)^{-1}$也是唯一确定的，是一个双射。因此同构的逆是一个同态，并且因为满足双射。综上所述是一个同构。

3. 首先，对同构映射$f : H_i \to H_i$有任意$h, h' \in H_i$得到$f(h*h') = f(h) * f(h') = h * h'$成立，所以满足自反。其次对于一个同构$f : H_i \to H_j$，则有$f(h*h') = f(h) * f(h')$成立。反过来根据命题2，同构的逆也是同构，因此$f^{-1} : H_j \to H_i$也是一个同构映射。所以同构映射满足对称。最后，根据命题1，同态的复合依然是同态。那么构造两个同构，$f : H_i \to H_j$和$g : H_j \to H_k$，则对于其中的元素有

   $$g(f(h*h')) = g(f(h) * f(h')) = gf(h) * gf(h')$$

   是一个同构。利用命题2，在等式右方乘上f^{-1}得到

   $$gff^{-1}(h) * gff^{-1}(h') = g(h) * g(h') = g(h*h')$$

   因此H_i和H_k也是同构满足传递性。所以同构是一种等价关系。

4. 我们设两个群H_i, H_j同构于群G，则我们任意取$h_1, h_2 \in H_i$和$h'_1, h'_2 \in H_j$，且定义映射$\varphi : H_i \to H_j$有$\varphi(h_1) = h'_1$, $\varphi(h_2) = h'_2$ 则由题设有$f(h_1 * h_2) = f(h_1) * f(h_2) = f(h'_1 * h'_2)$，然后我们右乘$f^{-1}$得到$(f(h_1) * f(h_2))f^{-1} = (f(h'_1) * f(h'_1))f^{-1} \Rightarrow h_1 * h_2 = h'_1h'_2 = \varphi(h_1 * h_2) = \varphi(h_1) * \varphi(h_2)$，由$h_1, h_2$的任意性可知$\varphi$是一个同构映射。因此$H_i \cong H_j$

证明G是阿贝尔群当且仅当有函数$f : G \to G$是同态，其中f由$f(a) = a^{-1}$给出。

证明： 若G是阿贝尔群，则存在任意元素$a, b \in G$满足$ab = ba$。定义映射$f : G \to G$由$f(a) = a^{-1}$给出，则

$$f(a * b) = (a * b)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1} = f(a) * f(b)$$

所以映射是一个同态。

反之，设群G上的一个同态$f : G \to G$对其中不相同的元素$a, b \in G$有

$$f(a^{-1} * b^{-1}) = f(a)^{-1} * f(b)^{-1} = a * b = b * a$$

所以，G是一个阿贝尔群。

这个练习给出一些群G的不变量。令$f : G \to H$为一个同构

1. 证明若$a \in G$是无限阶，则$f(a)$也是无限阶的。若a是有限阶的，证明$f(a)$也是有限阶的，并由此推出若一个G的元素的阶为n但H没有阶为n的元素，则 $G \ncong H$

2. 证明若$G \cong H$，则对每个$\mid G \mid$的因子k，G和H两者具有相同数量的阶为k的元素。

证明1： 由于$f : G \to H$是一个同构，所以f是一个双射。我们假设a是无限阶的，但$f(a) \in H$为n阶，则由同构有$f(a)^n = 1$，然后我们在两边乘上f^{-1}得到$f^{-1}(f(a)^n) = a^n$这意味着a是有限阶的。这是一个矛盾，因此若a是无限阶的则$f(a)$是无限阶的。

若a是有限阶的，则由$G \cong H$可知$f(a^n) = f(a)^n$对任意$n \in Z$成立，所以也是有限阶的。

我们设群G有n阶的元素但H不存在阶为n的元素。由于$f : G \to H$是一个同构。不妨取$a \in G$有$a^n = 1$，那么由于f是同构我们能够得到$f(1) = f(a^n) = f(a)^n = 1$，但$f(a)^n$这样子的元素不存在，所以它甚至不是一个同态。所以$f$不是一个同构，即$G \ncong H$

证明2： G,H同构，我们假设$a\in G$的阶为m，而$a^m=1$，设$f(a)^n=1$，那么因为同构，则满足$f(a^m)=f(a)^m\neq 1$，因为同构的逆也是同构，则$f^{-1}(1)=f^{-1}(f(a)^n)=a^n\neq a^m$矛盾，因此若$G\cong H$，则含有相同数量的阶为$k$的元素。

> 证明任意两个$2n$阶的二面体群同构

证明： 设G,H是两个二面体群，其中$g_a,g_b\in G$和$h_a,h_b\in H$为n阶和2阶元素。并且有$g_a^{-1}=g_bg_ag_b$成立。并且G的元素都有形如$g_a^kg_b^m$其中$0\leq k\leq n-1$,$0\leq m\leq 1$。

现在定义映射$f:G\to H$由函数$f(g_a^kg_b^m)=h_a^kh_b^m$给出。由于两个群具备同样的元素，我们假设f不是同构，则存在相同的元素有$f(g_a^kg_b^m)=f(g_a^tg_b^s)$其中$0\leq t<n,s=0,1$且$k\neq t,m\neq s$由定义可知$f(g_a^kg_b^m)=h_a^kh_b^m$和$f(g_a^tg_b^s)=h_a^th_b^s$满足$h_a^kh_b^m=h_a^th_b^s$矛盾，因此$f$是双射，所以$G\cong H$

> 证明若H是子群且$bH=Hb=\{hb:h\in H\}$对每个$b\in G$成立，则H是正规子群，

证明： 由于$bH=Hb$，则有$H=bHb^{-1}=\{bhb^{-1}:h\in H\}$。所以$H$是由所有共轭元组成的集合，说明$H$是正规子群。

> 令G为有限的乘法群，证明若$|\ G\ |$是奇数的，则每个$x\in G$有唯一的平方根。也就是说恰好存在一个$g\in G$有$g^2=x$

证明： 在证明之前，首先引入一个习题：

习题a： 设G是有限群，G中的每个元素x都有一个平方根，即：对每个$x\in G$有$y\in G$使得$y^2=x$。则G中的每个元素都有唯一的平方根。

证明： 令$f:G\to G$由函数$f(x)=x^2$定义。由题设可知f是一个满射。即存在x使得$f(x)=x^2\in G$成立。若f不是单射，则存在$x=y$有$x^2\neq y^2$，

但$f(x) = f(y)$得到矛盾。因此f是单射。由于f是满的且是单射，所以f是双射，则G中的元素都有唯一的平方根。

现在回到题目的证明上来。利用习题a，我们知道恰好存在一个群G满足这种条件。即存在一个$g \in G$有$x = g^2 \in G$，在上面的证明中我们看到g, x是俩俩配对出现的，因为f是一个双射。但1是特殊的运算，$1^2 = 1$，所以$\mid G \mid = \mid$ 所有$g^2 + 1 \mid$是奇数的。