群作用

2023 年 8 月 30 日

目录

1 前言

置换群的出现将我们引向了抽象的群，而凯莱给出了下面的这些结果：展示了抽象群和置换的关系并没有那么远。

2 正文

2.1 定理：凯莱

每个群G（同构于）是对称群S_G的一个子群。特别的，若$|\ G\ | = n$，则G同构于S_n的一个子群。

证明：对每个$a \in G$，定义“变换” $\tau_a : G \to G$由$\tau_a(x) = ax$定义。其中每个$x \in G$（若$a \neq 1$，则τ_a不是同态。）。对$a, b \in G$，$(\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x)) = \tau_a(bx) = abx = \tau_{ab}(x)$。由结合律我们就得到

$$\tau_a\tau_b = \tau_{ab}$$

这说明每个τ_a都是双射。它的逆为$\tau_{a^{-1}}$，有：

$$\tau_a\tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_1 = 1_G$$

且$\tau_a \in S_G$[1]

再定义一个映射$\varphi : G \to S_G$由函数$\varphi(a) = \tau_a$给出，那么

$$\varphi(a)\varphi(b) = \tau_a\tau_b = \tau_{ab} = \varphi(ab)$$

所以φ是一个同态，而且是单射，若$\varphi(a) = \varphi(b)$，则$\tau_a = \tau_b$而有$\tau_a(x) = \tau_b(x)$对所有$x \in G$，我们令$x = 1$就得到$a = b$。这就是我们想要的。其次，若表$|\ X\ | = n$，我们很容易的知道$S_X \cong S_G$。[2]

[1] 可以注意到每个映射都是把一个元素映射成另一个元素，这是由群的封闭性决定的。所以可以看成是一个置换。

[2] 因为对于有限集合来讲，单射等价满射等价于双射。

2.2 定理：陪集表示定理

设G是群，并且令H是G中阶为n的子群。则存在一个同态$\varphi : G \to S_n$，其中$\ker \varphi \leq H$

证明：即使H不是正规子群，我们仍然可以把H在G中的陪集记为G/H。

对每个$a \in G$，定义“变换”$\tau_a : G/H \to G/H$由函数$\tau_a(xH) = axH$给出，其中每个$x \in G$，且$a, b \in G$

$$\tau_a \circ \tau_b(xH) = \tau_a(\tau_b(xH)) = abxH = \tau_{ab}(xH)$$

是结合的，因此

$$\tau_a \tau_b = \tau_{ab}$$

这意味着每个τ_a都是双射，存在逆$\tau_{a^{-1}}$：

$$\tau_a \tau_{a^{-1}} = 1_G$$

并且$\tau_a \in S_{G/H}$，定义$\varphi : G \to S_{G/H}$由$\varphi(a) = \tau_a$给出，重写函数有

$$\varphi(a)\varphi(b) = \tau_a \tau_b = \tau_{ab} = \varphi(ab)$$

所以φ是同态。最后，若$a \in \ker \varphi$，则$\varphi(a) = 1_{G/H}$，那么$\tau_a(xH) = xH$对每个$x \in G$成立。特别的，当$x = 1$，那么$aH = H$有$a \in H$。最后，若$|G/H| = n$，则$S_{G/H} \cong S_n$

当$H = \{1\}$的时候，这正是我们的凯莱定理。

2.2.1 引理：

每个阶为4的群G同构于I_4或者四元群V。更多的，I_4不同构于V。

证明：利用拉格朗日定理，每个G中的元素要么阶是1，要么是2或者4。若阶为4，那么G是循环群。另一方面，对所有$x \in G$有$x^2 = 1$的话。那么G是阿贝尔群。[3]

若不同的元素x, y对G封闭，也不为1，那么$xy \notin \{1, x, y\}$，因此

$$G = \{1, x, y, xy\}$$

[3]若$x^2 = 1$对G中的元素都成立，不妨取任意的两个元素x, y，那么$(xy)^2 = xyxy = 1$，若$yx \neq xy$，则$xyx \neq y$得到$xyxy \neq 1$，是个矛盾。因此$xy = yx$可知G中元素都是交换的。

我们可以看到存在一个双射$f: G \to V$由函数$f(1) = 1. f(x) = (1\,2)(3\,4), f(y) = (1\,3)(2\,4), f(xy) = (1\,4)(2\,3)$是一个同构。对于$I_4 \ncong V$的证明会在练习中给出。

2.2.2 引理：

若G是阶为6的群，则G同构于I_6或者S_3。而$I_6 \ncong S_3$，更多的，I_6也不和S_3同构。

证明：由拉格朗日定理，元素可能的阶有$2, 3$或者6。当然，$G \cong I_6$只有当G有阶为6的元素会发生。

并且对阶为偶数的群，都包含2阶元素。我们记这个元素为t，令$T = \langle t \rangle$[4]

那么$[G : T] = 3$，那么T的陪集是同态$\rho : G \to S_{G/T} \cong S_3$，其中$\ker \rho \leq T$，因此$\ker \rho = \{1\}$或者$\ker \rho = T$，在第一种情况，$\rho$是单射，所以是一个同构。对$| G | = 6 = | S_3 |$。对于第二种，若$\ker \rho = T$，那么$T \lhd G$[5]且定义商群$G/T$。$G/T$也是循环群，且$| G/T | = 3$。所以$a \in G$且$G/T = \{T, aT, a^2T\}$，更多的，其实$\rho_t$是一个置换，其中

$$\rho = \begin{pmatrix} T & aT & a^2T \\ tT & taT & ta^2T \end{pmatrix}$$

由于$t \in T = \ker \rho$，那么ρ_t实际是恒等运算。特别的，$aT = \rho_t(aT) = taT$。因此$a^{-1}ta \in T = \{1, t\}$，但$a^{-1}ta \neq 1$，那么$a^{-1}ta = t$。因此$ta = at$。现在，$a$的阶或许是3，或者是6.$G$的阶是6，若$a$的阶是3，则$at$的阶就是6[6]。因此，$G$是阶为6的循环群，有$G \cong I_6$。若$a$的阶是6，则$\langle a \rangle = G$可知同构。

2.3 定义：作用

若X是集合并且G是一个群，则G作用在X指的是存在一个函数$\alpha : G \times X \to X$，我们把这个叫一个作用，由此可得：

1. 对$g, h \in G$，则$\alpha_g \circ \alpha_h = \alpha_{gh}$
2. $\alpha_1 = 1_X$是一个单位函数。

[4]我们设$| G | = 2n$，而$x^2 = 1$可知$x^{-1} = x$，去掉1后，设剩下的元素都非二阶，但由于G包含元和其逆，此时剩下$2n - 1$个元素，明显不满足配对。矛盾，所以偶数阶的群一定包含二阶元素。

[5]阶为2的子群一定是正规子群

[6]若$(m, n) = 1$，则阶分别为m, n的元素乘积的阶恰好就是mn

这是在说，对每个$x \in X$应用函数得到$\alpha(x,y) = \alpha_x(y)$。

若G作用在X上，可以用gx来代替$\alpha_g(x)$，在这个符号上，公理1看作$g(hx) = (gh)x$

当然，每个子群$G \leq S_X$作用在X上。更一般的，G在集合X上的作用符合同构$G \to S_X$。

2.3.1 引理：

若$\alpha : G \times X \to X$是$G$在$X$上的作用，则$g \to \alpha_g$定义了同态$G \to S_X$。反过来，若$B : G \to S_X$是一个同态，那么$\beta : G \times X \to X$由$\beta(g,x) = B(g)(x)$定义，且是作用。

证明： 若$\alpha : G \times X \to X$是作用，我们说每个$\alpha_g$都是$X$上的置换。很容易验证它的逆是$\alpha_{g^{-1}}$，因为$\alpha_g \alpha_{g^{-1}} = 1_X$，有$A : G \to S_X$由$A(g) = \alpha_g$定义。这是一个被我们指定目标了的函数，那么$A$很容易证明是同态，由公理1我们有

$$A(gh) = \alpha_{gh} = \alpha_g \circ \alpha_h = A(g) \circ A(h)$$

反过来，$\beta : G \times X \to X$由同构$B : G \to S_X$定义，其中$\beta(g,x)w = B(g)(x)$是作用。根据我们刚才定义的符号，即$\beta_g = B(g)$。因此，公理1只是在说$B(g) \circ B(h) = B(gh)$，由于B是个同构，所以这是真的。所以我们就有$B(1) = 1_X$成立，因为同态会把单位元映射到单位元上。

凯莱定理指的是：群G通过变换在自己身上的作用。而推广到更一般的形式就是陪集表示定理，指的是G通过变换在子群H的陪集族上的作用。

例1：共轭作用

我们证明G通过共轭在自己身上作用。因此，对每个$g \in G$，通过

$$\alpha_g(x) = gxg^{-1}$$

定义$\alpha_g : G \to G$，现在验证公理1.对每个$x \in G$，有：

$$\begin{aligned}(\alpha_g \circ \alpha_h)(x) =& \alpha_g(\alpha_h(x)) \\ =& \alpha_g(hxh^{-1}) \\ =& g(hxh^{-1})g^{-1} \\ =& \alpha_{gh}(x)\end{aligned}$$

满足公理1。
注意对每个$x \in G$，我们有
$\alpha_1(x) = 1x1^{-1} = x$，所以$\alpha_1$是单位置换，即$\alpha_1 = 1_G$

2.4 定义：轨道&稳定子群

若G作用于X上且$x \in X$，则x的**轨道**我们记作$\mathcal{O}(x)$，它是X的子集：

$$\mathcal{O}(x) = \{gx : g \in G\} \subseteq X$$

x的稳定子群记为G_x，它是G中的子群:

$$G_x = \{g \in x : gx = x\} \leq G$$

例2

- 凯莱定理说G通过变换$\tau_a : x \to ax$作用自身。若$x \in G$，则轨道(orbit)$\mathcal{O}(x) = G$，如果$x = \tau_a(x) = ax$，则$g = (gx^{-1})x$，x的稳定子群G_x其实是1，若$x = \tau_a(x) = ax$，则$a = 1$，当存在某些$x \in X$和$\mathcal{O}(x) = X$时，我们说这是G在X上可迁的作用
- 当G通过变换$\tau_a : xH \to axH$作用于G/H上，则$\mathcal{O}(xH) = G/H$。这是因为若$g \in G$和$a = gx^{-1}$，则$\tau_a(xH) \to gH$。因此G通过可迁作用在G/H上。则xH稳定子群G_{xH}是xHx^{-1}，对$axH = xH$当且仅当$x^{-1}ax \in H$，也仅当$a \in xHx^{-1}$

让我们看看一些其他的例子：

共轭作用： 令群G通过共轭作用于自身上，若$x \in G$，则

$$\mathcal{O}(x) = \{y \in G : y = axa^{-1} \text{对某些} a \in G\}$$

我们把$\mathcal{O}(x)$叫做x的共轭类，并记为x^G。例如：若$\alpha \in S_n$，则α的共轭类由S_n中具备相同的循环结构的置换组成。

若$x \in G$，则x的稳定子群G_x是：

$$C_G(x) = \{g \in G : gxg^{-1} = x\}$$

这意味着对于这子群，它是由所有$g \in G$且与x交换的元素组成，我们也叫做x在G中的中心化子。

循环群上的作用： 令$X = \{1, 2, \cdots, n\}$。设$\sigma \in S_n$。注意循环群$G = \langle\sigma\rangle$是X上的作用，若$i \in X$，则

$$\mathcal{O}(i) = \{\sigma^k(i) : k \in Z\}$$

现在，设σ有一个完全分解$\beta_1 \cdots \beta_{t(\sigma)}$。并且$i = i_0$被$\sigma$移动。若含有$i_0$的置换是$\beta_j = \{i_0, i_1, \cdots, i_{r-1}\}$，那么就存在某个元素$i_k = \sigma^k(i_0)$对所有$k < r - 1$，因此。

$$\mathcal{O}(i) = \{i_0, i_1, \cdots, i_{r-1}\}$$

其中$i = i_0$，于是$| \mathcal{O}(i) = r |$，而σ固定l的符号l的稳定子群G_l是G，若σ移动l则是G的真子群。

2.4.1 引理：

若G作用于集合X上，则X的轨道是无相交的，若X是有限的，则

$$| X | = \sum_l | \mathcal{O}(x_i) |$$

其中x_i是选择自每个轨道中的

证明： 群G在集合X上的作用构成一个X上的等价关系，定义为

$$x \equiv y \text{若存在} g \in G \text{且} y = gx$$

若$x \in X$，则$1_x = x$，其中$1 \in G$，那么$x \equiv x$，因此$\equiv$是自反的。

若$x \equiv y$，那么$y = gx$则

$$g^{-1}y = g^{-1}gx = 1_x = x$$

那么$x = g^{-1}y$得到$y \equiv x$。因此，$\equiv$是对称的。若$x \equiv y$和$y \equiv z$，那么存在$g, h \in G$和$y = gx$且$z = hy$。有$z = h(gx) = (hg)x$，得到$x \equiv z$，因此$\equiv$是传递的，因此这是一个等价关系。它的轨道定义为

$$[x] = \{y \in X : y \equiv x\} = \{gx : g \in G\} = \mathcal{O}(x)$$

由于轨道构成X的一个分类，我们可以很轻松的得到命题的结果，因为分类是一个划分，所以不存在有元素相交和被重复计算。

2.5　定理：

若G作用在集合X上且$x \in X$，则

$$| \mathcal{O}(x) | = [G : G_x]$$

是稳定子群G_x在G中的指数。

证明：　令G/G_x是所有G中G_x的陪集组成的群族。我们来证明$\varphi : \mathcal{O}(x) \to G/G_x$是双射。由拉格朗日可得：$| G/G_x | = [G : G_x]$。若$y \in \mathcal{O}(x)$，则$y = gx$对某个$g \in G$成立。定义$\varphi(y) = gG_x$，$\varphi$是定义良好的函数。若$y = hx$对某个$h \in G$成立。则$h^{-1}gx = x$得到$h^{-1}g \in G_x$，那么$hG_x = gG_x$。为了得到$\varphi$是单射。假设$\varphi(y) = \varphi(z)$，则对于$g, h \in G$有$y = gx$和$z = hx$那么就有$gG_x = hG_x$。那么$h^{-1}g \in G_x$。这说明$y = z$。最后我们证明$\varphi$是满射。若$gG_x \in G/G_x$，注意函数$\varphi(y) = gx$，则有$y = gx \in \mathcal{O}(x)$。

例如，我们在二面体群D_8上，对于顶点v_0的轨道，$| \mathcal{O}(x) | = 4$，这是因为存在四个旋转。容易验证每个旋转的结果都包含在顶点的表中。而$| G_{v_0} | = 2$ 因为对于正方形来说当我们沿着对角线折叠的时候有2个元素是不变的。而这种折叠有两个所以是2。那么$[G : G_{v_0}] = 8/4 = 4$。

2.5.1　推论：

若有限群G作用在集合X上，则则任意轨道中的元素个数是$| G |$的因子。

证明：　利用定理2.5以及拉格朗日定理，我们就有$| \mathcal{O}(x) |$是G_x在G中的指数，而$| G_x | || G | \Rightarrow | \mathcal{O}(x) || G |$。证毕。

2.5.2　推论：

若x在有限群G中，则x的共轭个数是其中心化子的个数;

$$| x^G |= [G : C_G(x)]$$

并因此可知其是$| G |$的因子。

证明：　在**共轭作用**中我们提到$\mathcal{O}(x)$是共轭类，记作X^G。并且对于每个中心化子$C_G(x)$都是自身的稳定化子G_x，再利用定理2.5即可证明完毕。

2.5.3　推论：

若$\alpha \in S_n$，则S_n中和α具备相同循环结构的置换数量被$n!$整除

证明：　对置换来说，具备相同的循环结构意味着包含共轭元$\gamma\alpha\gamma^{-1} \in S_n$，刚好，$| S_n |= n!$。那么利用推论2.5.2即可得到结果。

2.6　定理：柯西

若G是有限群，阶可被素数p整除，则G包含一个阶为p的元素。

证明：　我们通过对$| G |$运用归纳来证明定理。当$| G |= 1$时成立，因为1没素因子。若$x \in G$，则x的共轭类的数量为$| x^G |= [G : C_G(x)]$，其中$C_G(x)$指的是x在G中的中心化子。若$x \notin Z(G)$，则x^G有多个元素（至少两个），所以$| C_G(x) |<| G |$。若$p \mid | C_G(x) |$对某个非中心元素x成立。则由归纳假设可知在$C_G(x) \leq G$存在p阶元素，则证明完毕。

所以，我们假设对所有非中心元素$x \in G$有$p \nmid | C_G(x) |$。由于$| G |= [G : C_G(x)] \mid C_G(x) |$，由欧拉定理我们有：

$$p \mid [G : C_G(x)]$$

而$Z(G)$由所有$x \in G$和$| x^G |= 1$的元素组成。利用引理2.4.1，则

$$| G |=| Z(G) | + \sum_i [G : C_G(x_i)]$$

x_i是从其中具备多个元素的共轭类中选的。因此$| G |$和所有$[G : C_G(x)]$整除p，这暗示$| Z(G) |$好像整除p。而由于$Z(G)$是阿贝尔群，每个被$| Z(G) |$整除的素因子具备一个这样子的元素。

2.7 定义：类方程

一个关于群G的类方程指的是

$$|G|=|Z(G)|+\sum_i [G:C_G(x_i)]$$

其中x_i选择自每个拥有多于一个元素的共轭类。

2.8 定义：p群

若p是素数，则一个p群是阶为p^n的群，其中$n \geq 0$

2.9 推论：

若p是素数并设G是p群且G至少含有2个元素，则$Z(G) \neq \{1\}$

证明： 考虑类方程

$$|G|=|Z(G)|+\sum_i [G:C_G(x_i)]$$

其中每个$C_G(x_i)$是G的真子群，且$x_i \notin Z(G)$。由于G是p群，$[G:C_G(x_i)]$是$|G|$的因子。并且是p次幂的。因此，p整除除了$|Z(G)|$之外的每一项。一样的，由于$p \mid\mid |G|$和中心化子那么$p \mid\mid |Z(G)|$意味着$Z(G) \neq \{1\}$。

2.10 推论：

若p是素数，则每个阶为p^2的群G都是阿贝尔的。

证明： 若G是非阿贝尔的，则其中心$Z(G)$是真子群，由拉格朗日定理，$|Z(G)|=1$或者是p，但推论2.9告诉我们$Z(G) \neq \{1\}$的，所以$|Z(G)|=p$，并且中心永远是正规子群，所以商群$G/Z(G)$是可被定义的。它的阶也是p。但这是一个矛盾。我们引入如下习题：

> 若$G/Z(G)$循环且$Z(G)$是中心，则G是阿贝尔群。即$G=Z(G)$反之不成立。

它的证明[7]很简单。而我们证明的命题和这个命题矛盾。

[7] $G/Z(G)$循环，则有$G/Z(G)=\langle gZ(G)\rangle$对某个$g \in G$成立，现在取$a=g^iz, b=g^kw$，其中$g \in G, z, w \in Z(G)$。有$ab=g^izg^kw=g^kwg^iz=ba$成立。

例3

对素数p，这里存在阶为p^3的非阿贝尔群。定义$UT(3,p)$是$\mathrm{GL}(3,I_p)$中的所有迹是1的上三角矩阵组成的子群，有如下定义：

$$UT(3,p)=\left\{A=\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}:a,b,c\in I_p\right\}$$

这里很容易看出$UT(3,p)$是$\mathrm{GL}(3,I_p)$的子群。因为I_p是具有p个元素的类，并且a,b,c都具有p个选择，所以一共可以生成p^3个元素。容易验证上三角矩阵的乘积依然是上三角。

2.11 命题：

若G是阶为$|\ G\ |=p^e$的群，则G存在一个阶为p^k的正规子群，其中$k\leq e$

证明： 我们通过对$e\geq 0$归纳来证明。第一步显然的，我们现在继续归纳。由推论2.9，G的中心是非平凡的，即$Z(G)\neq\{1\}$，若$Z(G)=G$，则G是阿贝尔群，这是在重复的证明对于阿贝尔群的阶的任意一个因子都存在一个对应的群。因此，我们假设$Z(G)$是G的真子群，那么$Z(G)\lhd G$，我们有阶严格小于$|\ G\ |$的p群$G/Z(G)$，不妨假设$|\ Z(G)\ |=p^c$，若$k\leq c$，因为$Z(G)$是阿贝尔群，所以$Z(G)$存在阶为p^k的正规子群。因而我们知道G也含有p^k的正规子群。若$k>c$，则$G/Z(G)$包含正规子群S^*，其阶为p^{k-c}，利用对应定理。对正规子群S,G和

$$Z(G)\leq S\leq G$$

有$S/Z(G)\cong S^*$，因此

$$|\ S\ |=|\ S^*\ ||\ Z(G)\ |-p^{k-c}p^c=p^k$$

2.12 定义：

一个群G被称为简单群，若$G\neq\{1\}$且G除了自身和$\{1\}$意外没有任何正规子群。

2.12.1 命题：

一个阿贝尔群G是简单群当且仅当它有限且阶是素数。

证明： 若G是有限的且阶为素数p，则G除了$\{1\}$和自身外不存在任意子群，因此G是简单群。

反过来，我们假设G是简单的，由于G是阿贝尔群，对每个子群都正规，那么G除了$\{1\}$和G之外不存在子群。选择$x \in G$且$x \neq 1$。由于$\langle x\rangle$是子群，我们有$\langle x\rangle = G$。若x是无限阶，则x的所有阶都是不相同的，因此$\langle x^2\rangle < \langle x\rangle$是一个$\langle x\rangle$中一个子群，这矛盾。因此，每个$x \in G$都应该是有限阶的，我们记为$m$。若$m$是复合的，即$m = kl$。且$\langle x^k\rangle$是$\langle x\rangle$的真非平凡子群。但这矛盾，因为$|\ G\ |$是简单的。因此$G = \langle x\rangle$是素数阶的，Q.E.D

我们现在要证明A^5是一非阿贝尔简单群。设一个元$x \in G$存在k个共轭：

$$|\ x^G\ | = |\ \{gxg^{-1} : g \in G\}\ | = k$$

若这里子群$H \leq G$且$x \in H \leq G$

那么到底有多少x在H中的共轭元。由于

$$x^H = \{hxh^{-1:h\in H}\} \subseteq \{gxg^{-1} : g \in G\} = x^G$$

我们就得到$|\ x^H\ | \leq |\ x^G\ |$，也许可以从这里面找到严格不等式$|\ x^H\ | \leq |\ x^G\ |$。

例如，我们可以取$G = S_3$，$x = (1\ 2)$并令$H = \langle x\rangle$，而$|\ x^G\ | = 3$（因为其所有的所有置换是共轭元），其中有$|\ x^H\ | = 1$(因为H是阿贝尔群。)

现在让我们考虑问题，特别的，对$G = S_5$，$x = (1\ 2\ 3)$，且令$H = A_5$

2.13 引理：

所有A^5中的3循环是共轭元。

证明： 令$G = S_5$，$\alpha = (1\ 2\ 3)$和$H = A_5$，可以知道$|\ \alpha^{S_5}\ | = 20$，即S_5存在20个3循环。[8]，利用定理2.5，$|\ C_{S_5(\alpha)}\ | = 6$[9]。那么存在6个交换元在$S_5$中，即：

$$(1),\ (1\ 2\ 3),\ (1\ 3\ 2),\ (4\ 5), (4\ 5)(1\ 2\ 3),\ (4\ 5)(1\ 3\ 2)$$

[8] 一些简单的排列组合，在置换的练习题有具体方法。

[9] $5! = 120$，那么就是 $120/20 = 6$

由于后三个是奇置换，那么$|\ C_{A_5}(\alpha)\ | = 3$，那么这三个都在$A_5$中，所以所有3循环在$A_5$都表现为共轭。

2.14　引理：

所有A_5中的元素要么是3循环要么是3循环的乘积。

证明：　若$\alpha \in A_5$，则α是一些偶数个变换的乘积$\alpha = \tau_1\tau_2\cdots\tau_{2n}$，所以这些变换成对出现，不妨考虑变换$\tau, \tau'$，若$\tau = (i\ j), \tau' = (i\ k)$，那么$\tau\tau' = (i\ k\ j)$，若不相交，则$\tau\tau' = (i\ j)(k\ l) = (i\ j)(j\ k)(j\ k)(k\ l) = (i\ j\ k)(j\ k\ l)$

2.15　定理：

A_5是简单群

证明：　我们要证明的是：若H是A_5的正规子群且$H \neq \{1\}$，则$H = A_5$。现在，若H包含3循环，则H也应包含所有它的共轭类。再利用引理2.14，我们知道$H = A_5$

对$H \neq \{1\}$，它包含某个$\sigma \neq (1)$，我们假设再某些重新排列后，$\sigma = (1\ 2\ 3)$，或者$\sigma = (1\ 2)(3\ 4)$，或者$\sigma = (1\ 2\ 3\ 4\ 5)$，当σ为3循环，那么我们就结束了证明。

若$\sigma = (1\ 2)(3\ 4)$，它的一个共轭为$\beta\sigma\beta^{-1} = (1\ 2)(4\ 5)$，那么我们可以得到$\beta = (3\ 4\ 5) \in H$，因此$\sigma\sigma^{-1} \in H$

若$\sigma = (1\,2\,3\,4\,5)$，通过$\gamma = (1\,2\,3)$得到共轭元$\gamma\sigma\gamma^{-1} = \sigma'' = (2\,3\,1\,4\,5) \in H$。因此，$\sigma''\sigma^{-1} = (2\ 3\ 1\ 4\ 5)(5\ 4\ 3\ 2\ 1) = (1\ 2\ 4) \in H$，所以$\gamma\sigma\gamma^{-1}\sigma^{-1} \in H$所以$H$包含所有2个3循环的乘积。所以，在所有的情况中，$H$都包含3循环，所以这个在$A_5$的正规子群就是$A_5$自身。所以$A_5$是简单群。

2.16　引理：

A_6是简单群

证明：　令$H \neq \{(1)\}$但是A_6的正规子群。我们来证明$H = A_6$，设某些$\alpha \in H$但$\alpha \neq (1)$固定某个i，其中$1 \leq i \leq 6$，定义：

$$F = \{\sigma \in A_6 : \sigma(i) = i\}$$

现在$\alpha \in H \cap F$，所以$H \cap F \neq \{(1)\}$，利用第二同构定理我们有$H \cap F \lhd F$，但F是简单群。由于$F \cong A_5$，所以F的正规子群只有$\{1\}$和F，由于$H \cap F \neq \{(1)\}$，因此$H \cap F = F$，有$F \leq H$，所以H含有3循环，得到$H = A_6$

我们现在假设这里不存在$\alpha \in H$且$\alpha \neq (1)$固定某个i，$1 \leq i \leq 6$。我们考虑A_6中一些循环的置换。任何α应当考虑类似$(1\,2)(3\,4\,5\,6)$或者$(1\,2\,3)(4\,5\,6)$的循环结构。第一种情况，$a^2 \in H$是非平凡置换并固定1，矛盾。在第二种情况H含有$\alpha(\beta\alpha^{-1}\beta^{-1})$，其中$\beta = (2\,3\,4)$这也是一个不平凡置换并固定6。也是一个矛盾，因此$H$不存在可知$A_5$是单群。

2.17　定理：

A_n对$n \geq 5$都是单群。

证明：　若H是A_n的非平凡正规子群，即$H \neq (1)$。我们需要证明H含有3循环即可。若$\beta \in H$是非平凡的则存在某些i让β移动，即$\beta(i) = j \neq i$，现在选择一个固定某个i并移动j的3循环α。而α, β是不交换的，那么$\beta(\alpha(i)) = \beta(i) = j$，$\alpha\beta(j) \neq i$。于是，$\gamma = (\alpha\beta\alpha^{-1}\beta^{-1})$是$H$的非平凡元素。而$\beta\alpha^{-1}\beta^{-1}$是3循环。所以$\gamma$是两个3循环置换的积，因此$\gamma$至多移动6个符号，设为$i_1, \cdots, i_6$

定义：

$$F = \{\sigma \in A_n : \sigma \text{fixes all} i \neq i_1 \cdots i_6\}$$

$F \cong A_6$，且$\gamma \in H \cap F$，所以$H \cap F$是F的非平凡正规子群，但F是与A_6同构的单群，所以$H \cap F = F$有$F \leq H$，所以H含有3循环，有$H = A_n$