华东师范大学
EAST CHINA NORMAL UNIVERSITY

网络安全数学基础(二)

沈佳辰
jcshen@sei.ecnu.edu.cn

§6.4 陪集和商群

- 定义6.4.1 设H是群G的子群，$a \in G$，则$aH = \{ah|h \in H\}$称为H的**左陪集**；相应的，$Ha = \{ha|h \in H\}$称为H的**右陪集**，a称为该左（右）陪集的**代表元**。如果$aH = Ha$，那么称之为H的**陪集**。

§6.4 陪集和商群

- 定义6.4.1 设H是群G的子群，$a \in G$，则$aH = \{ah|h \in H\}$称为H的**左陪集**；相应的，$Ha = \{ha|h \in H\}$称为H的**右陪集**，a称为该左（右）陪集的**代表元**。如果$aH = Ha$，那么称之为H的**陪集**。

- 若G是阿贝尔群，那么H的所有左（右）陪集都是它的陪集。

华东师范大学 EAST CHINA NORMAL UNIVERSITY

- 定理6.4.1 设H是群G的子群，则

  (i) H的所有左（右）陪集的阶都等于H的阶；

  (ii) 对任意$a \in H$，都有$aH = \{c \in G | c^{-1}a \in H\}$，$Ha = \{c \in G | ac^{-1} \in H\}$；

  (iii) 对任意$a, b \in G$，$aH = bH$的充要条件是$b^{-1}a \in H$，$Ha = Hb$的充要条件是$ab^{-1} \in H$；

  (iv) 对任意$a, b \in G$，$aH \cap bH = \emptyset$的充要条件是$b^{-1}a \notin H$，$Ha \cap Hb = \emptyset$的充要条件是$ab^{-1} \notin H$；

  (v) 对任意$a \in H$，都有$aH = Ha = H$。

证明：这里我们都只证明左陪集的情况，右陪集的情况可类似证明。

证明：这里我们都只证明左陪集的情况，右陪集的情况可类似证明。

(i) 取H的任意左陪集$aH = \{ah|h \in H\}$，其中$a \in G$，显然$|aH| \leq |H|$，下面证明$|aH| \geq |H|$，

证明：这里我们都只证明左陪集的情况，右陪集的情况可类似证明。

(i) 取H的任意左陪集$aH=\{ah|h\in H\}$，其中$a\in G$，显然$|aH|\le|H|$，下面证明$|aH|\ge|H|$，即只需证明对任意$h,h'\in H,h\ne h'$，都有$ah\ne ah'$，否则$ah=ah'$，因此$h=a^{-1}ah=a^{-1}ah'=h'$，与假设矛盾，因此$|aH|=H$。

(ii) 令$H' = \{c \in G | c^{-1}a \in H\}$，我们需要证明$H' \subseteq aH$和$aH \subseteq H'$。

(ii) 令$H' = \{c \in G | c^{-1}a \in H\}$，我们需要证明$H' \subseteq aH$和$aH \subseteq H'$。

先证$H' \subseteq aH$，对任意$h' \in H'$，存在$h \in H$，使得$h'^{-1}a = h$，则$ah^{-1} = eah^{-1} = h'h'^{-1}ah^{-1} = h'hh^{-1} = h'e = h'$，又因为$h \in H$，$H$是$G$的子群，因此$h^{-1} \in H$，所以$h' = ah^{-1} \in aH$，故$H' \subseteq aH$；

(ii) 令$H' = \{c \in G | c^{-1}a \in H\}$，我们需要证明$H' \subseteq aH$和$aH \subseteq H'$。

先证$H' \subseteq aH$，对任意$h' \in H'$，存在$h \in H$，使得$h'^{-1}a = h$，则$ah^{-1} = eah^{-1} = h'h'^{-1}ah^{-1} = h'hh^{-1} = h'e = h'$，又因为$h \in H$，$H$是$G$的子群，因此$h^{-1} \in H$，所以$h' = ah^{-1} \in aH$，故$H' \subseteq aH$；

再证$aH \subseteq H'$，对任意$c \in aH$，存在$h \in H$，使得$c = ah$，则$c^{-1}a = (ah)^{-1}a = h^{-1}a^{-1}a = h^{-1}e = h^{-1} \in H$，因此$c \in H'$，故$aH \subseteq H'$。

(iii) 先证必要性，对任意$g \in aH$，存在$h \in H$，使得$g = ah$，又因为$aH = bH$，因此$g \in bH$，即存在$h' \in H$，使得$g = bh'$，所以$h' = b^{-1}g = b^{-1}ah$，因此$b^{-1}a = h'h^{-1} \in H$，得证。

(iii) 先证必要性，对任意$g \in aH$，存在$h \in H$，使得$g = ah$，又因为$aH = bH$，因此$g \in bH$，即存在$h' \in H$，使得$g = bh'$，所以$h' = b^{-1}g = b^{-1}ah$，因此$b^{-1}a = h'h^{-1} \in H$，得证。

再证充分性，先证$aH \subseteq bH$，对任意$g \in aH$，存在$h \in H$，使得$g = ah$，因为$b^{-1}a \in H$，所以存在$h' \in H$，使得$b^{-1}a = h'$，因此$b^{-1}g = b^{-1}ah = h'h$，所以$g = b(h'h) \in bH$，因此$aH \subseteq bH$；

(iii) 先证必要性，对任意 $g \in aH$，存在 $h \in H$，使得 $g = ah$，又因为$aH = bH$，因此$g \in bH$，即存在$h' \in H$，使得$g = bh'$，所以$h' = b^{-1}g = b^{-1}ah$，因此$b^{-1}a = h'h^{-1} \in H$，得证。

再证充分性，先证$aH \subseteq bH$，对任意$g \in aH$，存在$h \in H$，使得$g = ah$，因为$b^{-1}a \in H$，所以存在$h' \in H$，使得$b^{-1}a = h'$，因此$b^{-1}g = b^{-1}ah = h'h$，所以$g = b(h'h) \in bH$，因此$aH \subseteq bH$；再证$bH \subseteq aH$，对任意$g \in bH$，存在$h \in H$，使得$g = bh$，令$h' = b^{-1}a \in H$，则$g = bh = ebh = aa^{-1}bh = a(b^{-1}a)^{-1}h = ah'^{-1}h \in aH$，因此$bH \subseteq aH$。

(iv) 先证充分性，用反证法，设$g \in aH \cap bH \neq \emptyset$，则存在$h, h' \in H$，使得$g = ah = bh'$，此时$b^{-1}a = b^{-1}gh^{-1} = b^{-1}bh'h^{-1} = eh'h^{-1} = h'h^{-1} \in H$，与$b^{-1}a \notin H$矛盾，因此$aH \cap bH = \emptyset$；

(iv) 先证充分性，用反证法，设$g \in aH \cap bH \neq \emptyset$，则存在$h, h' \in H$，使得$g = ah = bh'$，此时$b^{-1}a = b^{-1}gh^{-1} = b^{-1}bh'h^{-1} = eh'h^{-1} = h'h^{-1} \in H$，与$b^{-1}a \notin H$矛盾，因此$aH \cap bH = \emptyset$；

再证必要性，仍用反证法，设$b^{-1}a \in H$，则存在$h \in H$，使得$b^{-1}a = h$，取$g \in aH$，则存在$h' \in H$，使得$g = ah'$，此时$g = ah' = eah' = bb^{-1}ah' = bhh' \in bH$，所以$g \in aH \cap bH$，与$aH \cap bH = \emptyset$矛盾，所以$b^{-1}a \notin H$，得证。

(v) 因为$a \in H$，且H是群，因此对任意$h \in H$，都有$ah \in H$，所以$aH \subseteq H$，但是由(i)可知$|aH| = |H|$，所以$aH = H$。

- 对于任意$a, b \in G$，我们知道要么$b^{-1}a \in H$，要么$b^{-1}a \notin H$，二者必居其一，则由定理6.4.1的(iii)和(iv)可知aH和bH要么相等，要么不相交，此时我们可根据H将群G表示成若干个不相交的陪集的并。

- 对于任意$a, b \in G$，我们知道要么$b^{-1}a \in H$，要么$b^{-1}a \notin H$，二者必居其一，则由定理6.4.1的(iii)和(iv)可知aH和bH要么相等，要么不相交，此时我们可根据H将群G表示成若干个不相交的陪集的并。

- 定义6.4.2 设H是群G的子群，将H在G中不同陪集组成的新集合$\{aH|a \in G\}$称为H在G中的**商集**，记作G/H，$|\{aH|a \in G\}|$记作$[G: H]$。

- 定理6.4.2 设G是群，若$K \le H \le G$，则
  (i) $|G| = [G: H]|H|$；
  (ii) $[G: K] = [G: H][H: K]$。

- 定理6.4.2 设G是群，若$K \leq H \leq G$，则
  (i) $|G| = [G:H]|H|$；
  (ii) $[G:K] = [G:H][H:K]$。

证明： (i) 令$\{aH|a \in G\} = \{a_1H, a_2H, \dots, a_nH, \dots\} = \{a_iH|i \in I\}$，则显然$|G| = |\bigcup_{i\in I} a_iH| = \sum_{i\in I}|a_iH|$，由定理6.3.1 (i)可知对任意$i \in I$，$|a_iH| = |H|$，因此$|G| = \sum_{i\in I}|a_iH| = |I||H| = [G:H]|H|$。

- 定理6.4.2 设G是群，若$K \leq H \leq G$，则
  (i) $|G| = [G:H]|H|$；
  (ii) $[G:K] = [G:H][H:K]$。

证明： (i) 令$\{aH|a \in G\} = \{a_1H, a_2H, \ldots, a_nH, \ldots\} = \{a_iH|i \in I\}$，则显然$|G| = |\bigcup_{i\in I} a_iH| = \sum_{i\in I}|a_iH|$，由定理6.3.1 (i)可知对任意$i \in I$，$|a_iH| = |H|$，因此$|G| = \sum_{i\in I}|a_iH| = |I||H| = [G:H]|H|$。

(ii) 因为$K \leq H \leq G$，由(i)可知$|G| = [G:H]|H|, |H| = [H:K]|K|, |G| = [G:K]|K|$，因此$[G:K]|K| = |G| = [G:H]|H| = [G:H][H:K]|K|$，所以$[G:K] = [G:H][H:K]$。

- 例 我们知道$Z_6=\{0,1,2,3,4,5\}$关于模6加法构成群，$Z'_6=\{0,2,4\}$显然是Z_6的非空子集，且容易验证Z'_6关于模6加法也构成群，因此Z'_6是Z_6的子群，又显然有$|Z_6|=6, |Z'_6|=3$，可知$[Z_6:Z'_6]=\frac{|Z_6|}{|Z'_6|}=\frac{6}{3}=2$；另一方面容易验证$0+Z'_6=2+Z'_6=4+Z'_6$以及$1+Z'_6=3+Z'_6=5+Z'_6$，所以$[Z_6:Z'_6]=2$成立。

- 对于给定的群G和它的子群H，我们定义了左陪集和右陪集，那么在什么条件下，无论我们怎么取代表元a，左陪集和右陪集都相等，即$aH = Ha$？

- 显然当G是阿贝尔群时，$aH = Ha$都成立。

- 有没有更一般的结论？

- 定义6.4.3 设N是群G的子群，如果对任意$a \in G$，都有$aN = Na$，那么我们称N是G的**正规子群**，记作$N \lhd G$。

- 定义6.4.3 设N是群G的子群，如果对任意$a \in G$，都有$aN = Na$，那么我们称N是G的**正规子群**，记作$N \lhd G$。

- 阿贝尔群的所有子群都是它的正规子群。

- 定理6.4.3 设N是群G的子群，则如下条件是等价的：
  (i) 对任意$a \in G$，都有$aN = Na$；
  (ii) 对任意$a \in G$，都有$aNa^{-1} = \{ana^{-1} | n \in N\} = N$；
  (iii) 对任意$a \in G$，都有$aNa^{-1} \subseteq N$。

证明：要证明$(i),(ii),(iii)$等价，只需证明(i)蕴含(ii)、(ii)蕴含(iii)、(iii)蕴含(i)。

证明：要证明$(i),(ii),(iii)$等价，只需证明(i)蕴含(ii)、(ii)蕴含(iii)、(iii)蕴含(i)。

(1) (i)蕴含(ii)，先证$aNa^{-1} \subseteq N$，对任意$b \in aNa^{-1}$，存在$n \in N$，使得$b = ana^{-1}$，因此$ba = an$，又因为$aN = Na$，所以存在$n' \in N$，使得$n'a = an = ba$，所以$b = be = baa^{-1} = n'aa^{-1} = n' \in N$，因此$aNa^{-1} \subseteq N$；

证明：要证明$(i),(ii),(iii)$等价，只需证明(i)蕴含(ii)、(ii)蕴含(iii)、(iii)蕴含(i)。

(1) (i)蕴含(ii)，先证$aNa^{-1} \subseteq N$，对任意$b \in aNa^{-1}$，存在$n \in N$，使得$b = ana^{-1}$，因此$ba = an$，又因为$aN = Na$，所以存在$n' \in N$，使得$n'a = an = ba$，所以$b = be = baa^{-1} = n'aa^{-1} = n' \in N$，因此$aNa^{-1} \subseteq N$；再证$N \subseteq aNa^{-1}$，对任意$b \in N$，因为$aN = Na$，所以存在$n' \in N$，使得$ba = an'$，因此$b = an'a^{-1} \in aNa^{-1}$，因此$N \subseteq aNa^{-1}$。

(2) (ii)蕴含(iii)显然。

(2) (ii)蕴含(iii)显然。

(3) (iii)蕴含(i)，先证$aN \subseteq Na$，对任意$b \in aN$，存在$n \in N$，使得$b = an$，所以$ba^{-1} = ana^{-1} \in aNa^{-1} \subseteq N$，因此存在$n' \in N$，使得$ba^{-1} = n'$，此时$b = n'a \in Na$，所以$aN \subseteq Na$。

(2) (ii)蕴含(iii)显然。

(3) (iii)蕴含(i)，先证$aN \subseteq Na$，对任意$b \in aN$，存在$n \in N$，使得$b = an$，所以$ba^{-1} = ana^{-1} \in aNa^{-1} \subseteq N$，因此存在$n' \in N$，使得$ba^{-1} = n'$，此时$b = n'a \in Na$，所以$aN \subseteq Na$。再证$Na \subseteq aN$，对任意$b \in Na$，存在$n \in N$，使得$b = na$，又因为$a \in G$，所以$a^{-1} \in G$，由$(iii)$可知$a^{-1}Na = a^{-1}N(a^{-1})^{-1} \subseteq N$，因此$a^{-1}b = a^{-1}na \in a^{-1}Na \subseteq N$，因此存在$h' \in N$，使得$a^{-1}b = h'$，此时$b = ah' \in aN$，所以$Na \subseteq aN$。

- 定理6.4.4 设N是群G的正规子群，G/N是N在G中的所有陪集组成的集合，定义G/N上的运算$\cdot$为：$(aN)(bN) = (ab)N$，则$(G/N,\cdot)$构成一个群，称为G对于N的**商群**。

证明：首先我们证明这样定义的运算是有意义的，即它确实定义了一个映射，也就是说对于同一个陪集，选取不同的代表元所得的运算结果是相同的，即对任意$a' \in aN, b' \in bN$，都有$(a'b')N = (ab)N$。事实上，对任意$g \in (a'b')N$，存在$n \in N$，使得$g = a'b'n$，又因为$a' \in aN, b' \in bN$，所以存$n_1, n_2 \in N$，使得$a' = an_1, b' = bn_2$，因此$g = a'b'n = an_1bn_2n$，因为N是G的正规子群，因此$bN = Nb$，所以存在$n' \in N$，使得$n_1b = bn'$，所以$g = an_1bn_2n = abn'n_2n \in abN$，所以$(a'b')N \subseteq (ab)N$；另一方面，对任意$g \in (ab)N$，存在$n \in N$，使得$g = abn$，又因为$a' \in aN, b' \in bN$，所以存$n_1, n_2 \in N$，使得$a' = an_1, b' = bn_2$，因此$g = abn = a'n_1^{-1}b'n_2^{-1}n$，同样因为$N$是$G$的正规子群，因此$b'N = Nb'$，所以存在$n' \in N$，使得$n_1^{-1}b' = b'n'$，所以$g = a'n_1^{-1}b'n_2^{-1}n = a'b'n'n_2^{-1}n \in a'b'N$，所以$(ab)N \subseteq (a'b')N$。

接下来，我们还需要证明封闭性、结合律、单位元的存在性、逆元的存在性。

接下来，我们还需要证明封闭性、结合律、单位元的存在性、逆元的存在性。

封闭性：对于任意$g, g' \in G/N$，存在$a, b \in G$，使得$g = aN, g' = bN$，显然$ab \in G$，则$gg' = (ab)N \in G/N$。

接下来，我们还需要证明封闭性、结合律、单位元的存在性、逆元的存在性。

封闭性：对于任意$g, g' \in G/N$，存在$a, b \in G$，使得$g = aN, g' = bN$，显然$ab \in G$，则$gg' = (ab)N \in G/N$。

结合律：对于任意$g, g', g'' \in G/N$，存在$a, b, c \in G$，使得$g = aN, g' = bN, g'' = cN$，则$(gg')g'' = \big((aN)(bN)\big)(cN) = \big((ab)N\big)(cN) = \big((ab)c\big)N = \big(a(bc)\big)N = (aN)((bc)N = (aN)\big((bN)(cN)\big) = g(g'g'')$。

单位元：令$e' = eN$，其中e为G的单位元，对于任意$g \in G/N$，存在$a \in G$，使得$g = aN$，因此$ge' = (aN)(eN) = (ae)N = aN = g$，且$e'g = (eN)(aN) = (ea)N = aN = g$，因此$e'$是$G/N$的单位元。

单位元：令$e' = eN$，其中e为G的单位元，对于任意$g \in G/N$，存在$a \in G$，使得$g = aN$，因此$ge' = (aN)(eN) = (ae)N = aN = g$，且$e'g = (eN)(aN) = (ea)N = aN = g$，因此$e'$是$G/N$的单位元。

逆元：对于任意$g \in G/N$，存在$a \in G$，使得$g = aN$，令$g' = a^{-1}N$，则$gg' = (aN)(a^{-1}N) = (aa^{-1})N = eN = e'$，$g'g = (a^{-1}N)(aN) = (a^{-1}a)N = eN = e'$，因此$g'$是$g$的逆元。

- 例 上例中我们验证了$|Z_6| = [Z_6:Z'_6]|Z'_6|$。事实上由于Z_6是阿贝尔群，Z'_6是它的子群，因此Z'_6是它的正规子群，所以Z_6/Z'_6也是一个群，我们知道它仅有两个元素：$0+Z'_6$和$1+Z'_6$。

- 定理6.4.5 （同态基本定理）设 f 是群 H 到群 G 的同态映射，则$\ker(f)$是H的正规子群，且存在群$H/\ker(f)$到群$f(H)$的同构映射f': $a\ker(f) \to f(a)$，其中$a \in H$，且$f = i \cdot f' \cdot s$，其中·表示函数的复合运算，i表示$f(H)$到G的恒等映射，s表示H到$H/\ker(f)$的自然同态。

证明：首先证明$\ker(f)$是H的正规子群，由定理6.3.3，仅需证明对任意$a\in H$，都有$a\ker(f)\,a^{-1}\subseteq\ker(f)$，事实上，对任意$b\in a\ker(f)\,a^{-1}$，存在$e'\in\ker(f)$，使得$b=ae'a^{-1}$，因为$e'\in\ker(f)$，所以$f(e')=e$，其中$e$为$G$的单位元，又因为$f(b)=f(ae'a^{-1})=f(a)f(e')f(a^{-1})=f(a)ef(a)^{-1}=e$，所以$b\in\ker(f)$，所以$a\ker(f)\,a^{-1}\subseteq\ker(f)$。

接下来我们证明f'是同构映射。

接下来我们证明f'是同构映射。

同态性：对于任意$a', b' \in H/\ker(f)$，存在$a, b \in H$，使得$a' = a\ker(f), b' = b\ker(f)$，因此$f'(a')f'(b') = f(a)f(b) = f(ab) = f'\big((ab)\ker(f)\big) = f'(\big(a\ker(f)\big)\big(b\ker(f)\big)) = f'(a'b')$。

接下来我们证明f'是同构映射。

同态性：对于任意$a', b' \in H/\ker(f)$，存在$a, b \in H$，使得$a' = a\ker(f), b' = b\ker(f)$，因此$f'(a')f'(b') = f(a)f(b) = f(ab) = f'\big((ab)\ker(f)\big) = f'(\big(a\ker(f)\big)\big(b\ker(f)\big)) = f'(a'b')$。

单射：若$a', b' \in H/\ker(f)$，使得$f'(a') = f'(b')$，则存在$a, b \in H$，使得$a' = a\ker(f), b' = b\ker(f)$，且$f(a) = f(b)$，因此$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = f(a)f(a)^{-1} = e$，所以$ab^{-1} \in \ker(f)$，由定理6.3.1$(iii)$可知$a\ker(f) = b\ker(f)$，即$a' = b'$，所以$f'$是单射。

接下来我们证明f'是同构映射。

同态性：对于任意$a',b' \in H/\ker(f)$，存在$a,b \in H$，使得$a' = a\ker(f), b' = b\ker(f)$，因此$f'(a')f'(b') = f(a)f(b) = f(ab) = f'\big((ab)\ker(f)\big) = f'\big(\big(a\ker(f)\big)\big(b\ker(f)\big)\big) = f'(a'b')$ 。

单射：若$a',b' \in H/\ker(f)$，使得$f'(a') = f'(b')$，则存在$a,b \in H$，使得$a' = a\ker(f), b' = b\ker(f)$，且$f(a) = f(b)$，因此$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = f(a)f(a)^{-1} = e$，所以$ab^{-1} \in \ker(f)$，由定理6.3.1$(iii)$可知$a\ker(f) = b\ker(f)$，即$a' = b'$，所以$f'$是单射。

满射：对任意$g \in f(H)$，由$f(H)$定义可知，存在$h \in H$，使得$g = f(h)$，令$h' = h\ker(f)$，则$f(h') = f(h) = g$，因此f'是满射。

容易验证$f = i \cdot f' \cdot s$。

容易验证$f = i \cdot f' \cdot s$。

- 例 上例中我们证明了Z'_6是Z_6的正规子群，所以Z_6/Z'_6也是一个群，它的阶为2，仅包含两个元素$0 + Z'_6$和$1 + Z'_6$。从另一个角度来看，如果我们定义Z_6到Z_2的映射：$f: a \to a \; mod \; 2$，则$\ker(f) = Z'_6$，$f(Z_6) = Z_2$，由定理6.4.5可知存在群Z_6/Z'_6到Z_2的同构：$f': a + Z'_6 \to f(a) = a \; mod \; 2$，即$Z_6/Z'_6 \cong Z_2$。因为$Z'_6 \cong Z_3$，有时我们会写成$Z_6 = Z_3 \times Z_2$。

§6.5 循环群

- 定义6.5.1 设G是一个群，如果存在$a \in G$，对任意$g \in G$，存在$n \in Z$，使得$g = a^n$，则称G是一个**循环群**。

§6.5 循环群

- 定义6.5.1 设G是一个群，如果存在$a \in G$，对任意$g \in G$，存在$n \in Z$，使得$g = a^n$，则称G是一个**循环群**。

- 例 Z_6关于模加运算构成一个群，且对于任意$n \in N$，都有$n = n\,1$，因此Z_6是一个循环群。

- 定理6.5.1 设G是一个群，$\{H_i|i \in I\}$是G的一组子群，则$\bigcap_{i\in I} H_i$也是G的子群。

- 定理6.5.1 设G是一个群，$\{H_i | i \in I\}$是G的一组子群，则$\bigcap_{i\in I} H_i$也是G的子群。

证明：显然$\bigcap_{i\in I} H_i$非空，对任意$a,b \in \bigcap_{i\in I} H_i$，显然对每个$i \in I$，都有$a,b \in H_i$，所以$ab^{-1} \in H_i$，因此$ab^{-1} \in \bigcap_{i\in I} H_i$，由定理6.2.6可知$\bigcap_{i\in I} H_i$也是一个群。

- 定义6.5.2 设G是一个群，$X \subseteq G$，设$\{H_i|i \in I\}$是G的所有包含X的子群，则$\bigcap_{i\in I} H_i$称为X**生成的子群**，记为$< X >$。如果$|X|$有限，则称$< X >$是**有限生成**的，特别的，如果$X = \{x\}$，则称$\bigcap_{i\in I} H_i$ 为x生成的群。

- 定理6.5.2 设G是一个群，$X \subseteq G, X \neq \emptyset$，则$< X > = \left\{a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} | t \in Z^+, a_i \in X, n_i \in Z, 1 \leq i \leq t\right\}$，特别的，对任意$a \in G$，有$< a > = \{a^n | n \in Z\}$。

- 定理6.5.2 设G是一个群，$X \subseteq G, X \neq \emptyset$，则$< X > = \left\{a_1^{n_1} a_2^{n_2} \cdots a_t^{n_t} | t \in Z^+, a_i \in X, n_i \in Z, 1 \leq i \leq t\right\}$，特别的，对任意$a \in G$，有$< a > = \{a^n | n \in Z\}$。

- 显然$< a >$是循环群。

- 例 整数集Z关于加法构成一个群，0是其单位元。设$H \leq Z$，则H是循环群，且$H =< 0 > = \{0\}$或$H =< m > = mZ$，其中$m \in Z^{+}$，进一步当$H =< 0 >$时，它是有限群，当$H = < m >$时，他是无限群。

- 例 整数集Z关于加法构成一个群，0是其单位元。设$H \leq Z$，则H是循环群，且$H =< 0 > = \{0\}$或$H =< m > = mZ$，其中$m \in Z^+$，进一步当$H =< 0 >$时，它是有限群，当$H = < m >$时，他是无限群。

证明：若H是由0生成的，则$H =< 0 > = \{0\}$，否则，存在$a \in H, a \neq 0$，因为$H \leq Z$，所以a的逆元$-a \in H$，所以H中有正整数，设m为H中最小的正整数，则$H =< m >$，如若不然，则存在$a \in H \subseteq Z$，且$m \nmid a$，所以存在$q, r \in Z, 0 < r < m$，使得$a = qm + r$，由群的性质可知$r \in H$，与m为H中最小的正整数矛盾，因此$H =< m >= mZ$。

显然$< 0 >$的阶为1，所以$< 0 >$是有限群，而mZ中有无限个元素，因此它是无限群。

- 定理6.5.3 设G是一个循环群，则存在$g \in G$，使得$G = \{g^n | n \in N\}$。进一步，如果G是有限群，令$m = |G|$，则$G = \{g^n | n = 0,1,\ldots,m-1\}$，如果$G$是无限群，则对任意$n, n' \in N, n \neq n'$，都有$g^n \neq g^{n'}$。

证明：因为G是循环群，因此存在$g \in G$，对任意$a \in G$，存在$n \in N$，使得$a = g^n$，令$H = \{g^n | n \in N\}$，显然$G \subseteq H$，现在证明$H \subseteq G$，对任意$b \in H$，存在$n \in N$，使得$b = g^n$，又因为$g \in G$且G是群，因此$g^n \in G$，即$b \in G$，因此$H \subseteq G$，所以$G = H$。

如果G是有限群，$m = |G|$，令$H = \{g^n | n = 0,1,\ldots,m-1\}$，由于$g \in G$且$G$是群，因此对$n = 0,1,\ldots,m-1$，都有$g^n \in G$，因此$H \subseteq G$。现在我们证明$g^n$两两不同，其中$n = 0,1,\ldots,m-1$，如果存在$0 \le n < n' \le m-1$，使得$g^n = g^{n'}$，则$g^{n'-n} = e$，其中$e$为$G$的单位元，且$0 < n'-n \le m-1$，此时对任意$a \in G$，存在$i \in N$，使得$a = g^i$，则存在$q, r \in N, 0 \le r < n'-n \le m-1$，使得$i = q(n'-n)+r$，此时$a = g^i = g^{q(n'-n)+r} = (g^{n'-n})^q g^r = e^q g^r = g^r$，$G \subseteq \{g^n | n = 0,1,\ldots,m-2\}$，与$|G| = m$矛盾，所以$|H| = m = |G|$，因此$H = G$。

如果 G 是无限群，如果存在 $n, n' \in N, n \neq n'$，使得 $g^n = g^{n'}$，不妨设$n' > n$，则$g^{n'-n} = e$，其中e为G的单位元，此时对任意$a \in G$，存在$i \in N$，使得$a = g^i$，则存在$q, r \in N, 0 \leq r < n' - n$，使得$i = q(n' - n) + r$，此时$a = g^i = g^{q(n'-n)+r} = (g^{n'-n})^q g^r = e^q g^r = g^r$，$G \subseteq \{g^n | n = 0,1, \ldots, n' - n - 1\}$，与$G$是无限群矛盾，得证。

- 事实上，如果G是有限群，$m = |G|$，则$g^m = e$，否则存在$1 \leq n \leq m-1$，使得$g^m = g^n$，则$g^{m-n} = e$，类似定理证明，可知$G \subseteq \{g^n | n = 0,1,\ldots,m-n-1\}$，与$|G| = m$矛盾。

- 定理6.5.4 设 G 是一个循环群，如果它是无限群，则 $G \cong Z$ ，否则令$m = |G|$，则$G \cong Z/mZ$。

- 定理6.5.4 设 G 是一个循环群，如果它是无限群，则 $G \cong Z$ ，否则令$m = |G|$，则$G \cong Z/mZ$。

证明：因为G是循环群，所以存在$g \in G$，对任意$a \in G$，存在$n \in Z$，使得$a = g^n$。定义Z到G的映射：$f: n \to g^n$，则对任意$n, n' \in Z$，因为G是循环群，因此$g^n, g^{n'} \in G$，此时有$f(n + n') = g^{n+n'} = g^n g^{n'} = f(n)f(n')$，因此 f 是同态映射；又因为对任意$a \in G$，存在$n \in Z$，使得$a = g^n$，因此存在$n \in Z$，使得$f(n) = g^n = a$，所以$f(Z) = G$，由定理6.3.5可知$G = f(Z) \cong Z/\ker(f)$，

- 定理6.5.4 设 G 是一个循环群，如果它是无限群，则 $G \cong Z$，否则令$m = |G|$，则$G \cong Z/mZ$。

证明：因为G是循环群，所以存在$g \in G$，对任意$a \in G$，存在$n \in Z$，使得$a = g^n$。定义Z到G的映射：$f: n \to g^n$，则对任意$n, n' \in Z$，因为G是循环群，因此$g^n, g^{n'} \in G$，此时有$f(n + n') = g^{n+n'} = g^n g^{n'} = f(n)f(n')$，因此 f 是同态映射；又因为对任意$a \in G$，存在$n \in Z$，使得$a = g^n$，因此存在$n \in Z$，使得$f(n) = g^n = a$，所以$f(Z) = G$，由定理6.3.5可知$G = f(Z) \cong Z/\ker(f)$，如果$|G| = m$，则由定理6.4.3可知$\ker(f) = mZ$，因此$G \cong Z/\ker(f) = Z/mZ$；如果G是无线群，则由定理6.4.3可知$\ker(f) = \{0\}$，因此$G \cong Z/\ker(f) = Z/\{0\} \cong Z$。

- 定理6.5.5 循环群的子群仍是循环群。

- 定理6.5.6 设G是一个循环群，a是它的生成元。如果G是无限群，则a和a^{-1}是它的所有生成元；如果G是有限群，则a^k是它的生成元当且仅当$(k,m)=1$，其中$m=|G|$。

§6.6 置换群

- 定义6.6.1 设$S=\{1,2,\dots,n\}$，称S到其自身的映射σ是一个**置换**或n元**置换**，如果σ是双射，即
$$\begin{array}{cccc} \sigma: & S & \rightarrow & S \\ & k & \mapsto & i_k \end{array}$$
且对任意$1\le k<k'\le n$，都有$i_k\neq i_{k'}$。

§6.6 置换群

- 定义6.6.1 设$S=\{1,2,\dots,n\}$，称S到其自身的映射σ是一个**置换**或n**元置换**，如果σ是双射，即
$$\begin{array}{cccc} \sigma: & S & \to & S \\ & k & \mapsto & i_k \end{array}$$
且对任意$1\le k<k'\le n$，都有$i_k\neq i_{k'}$。

- 通常将n元置换置换σ写成$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$的形式。

- 例 $\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 2 & 1 & 3\end{pmatrix}$是$S=\{1,2,3,4,5,6\}$上的一个置换，也可以写成$\begin{pmatrix}5 & 6 & 4 & 2 & 3 & 1\\ 1 & 3 & 2 & 5 & 4 & 6\end{pmatrix}$的形式。

- 置换的乘法：设σ和σ'是S上两个置换，则它们的乘积$\sigma\sigma'$也是一个置换，且$(\sigma\sigma')(i) = \sigma(\sigma'(i))$。

- 置换的乘法：设σ和σ'是S上两个置换，则它们的乘积$\sigma\sigma'$也是一个置换，且$(\sigma\sigma')(i) = \sigma(\sigma'(i))$。

- 如果把置换看作S到自身的函数，则置换乘法就是函数复合运算。

- 例 令$\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}$和$\sigma'=\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}$是$S=\{1,2,3,4,5,6\}$上的置换，则$\sigma\sigma'=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}=\begin{pmatrix}5&6&4&2&3&1\\1&3&2&5&4&6\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\1&3&2&5&4&6\end{pmatrix}$。

- 置换的逆变换：设$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$，则其逆变换为$\sigma^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ 1 & 2 & \cdots & n\end{pmatrix}$。

- 置换的逆变换：设$\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(n)\end{pmatrix}$，则其逆变换为$\sigma^{-1}=\begin{pmatrix}\sigma(1) & \sigma(2) & \cdots & \sigma(n)\\ 1 & 2 & \cdots & n\end{pmatrix}$。

- 例 $\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 6 & 5 & 4 & 2 & 1 & 3\end{pmatrix}$是$S=\{1,2,3,4,5,6\}$上的一个置换，它的逆变换$\sigma^{-1}=\begin{pmatrix}6 & 5 & 4 & 2 & 1 & 3\\ 1 & 2 & 3 & 4 & 5 & 6\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 5 & 4 & 6 & 3 & 2 & 1\end{pmatrix}$。

- 定理6.6.1 n元置换全体组成的集合S_n关于置换乘法构成一个群，其阶为$n!$。

- 定理6.6.1 n元置换全体组成的集合S_n关于置换乘法构成一个群，其阶为$n!$。

证明：两个n元置换的乘积仍是n元置换，因此S_n关于置换乘法封闭。又由函数复合满足结合律易知S_n关于置换乘法满足结合律。易验证恒等置换$\begin{pmatrix}1 & 2 & \cdots & n\\1 & 2 & \cdots & n\end{pmatrix}$为其单位元，对任意$n$元置换$\sigma$，其逆变换$\sigma^{-1}$为其逆元。因此$S_n$关于置换乘法构成一个群。又因为$(1,2,\cdots,n)$在置换$\sigma$下的像$(\sigma(1),\sigma(2),\cdots,\sigma(n))$是$(1,2,\cdots,n)$的一个排列，这样的排列共有$n!$个，因此$|S_n|=n!$。

- 定义6.6.2 设σ是一个n元置换，如果存在$I = \{i_1, i_2, \dots, i_k\} \subseteq \{1,2, \dots n\}$，使得$\sigma(i_j) = i_{j+1}, \sigma(i_k) = i_1$，其中$j = 1,2, \dots, k-1$，并且对任意$j \in \{1,2, \dots n\} \backslash \mathrm{I}$，都有$\sigma(j) = j$，那么称$\sigma$是一个$k$-**轮换**，记作$(i_1, i_2, \dots, i_k)$。

- 定理6.6.2 任意置换都可以表示为不相交的轮换的乘积，且在不考虑乘法顺序的情况下，该表示是唯一的。

证明：对任意n元置换σ，取序列$i_1 = 1, \sigma(1), \sigma\big(\sigma(1)\big), \ldots$，由于$\sigma$是$n$元置换，则存在非负整数$k$，使得$\sigma^k(1) = 1$，令$k_1$是最小的这样的$k$，则$1, \sigma(1), \sigma\big(\sigma(1)\big), \ldots, \sigma^{k_1-1}(1)$各不相同，且$\sigma_1 = \Big(1, \sigma(1), \sigma\big(\sigma(1)\big), \ldots, \sigma^{k_1-1}(1)\Big)$是一个$k_1$-轮换，任取$i_2 \in \{1,2, \ldots n\}\backslash\{1, \sigma(1), \sigma\big(\sigma(1)\big), \ldots, \sigma^{k_1-1}(1)\}$，取序列$i_2, \sigma(i_2), \sigma\big(\sigma(i_2)\big), \ldots$，同样的，存在非负整数$k$，使得$\sigma^k(i_2) = i_2$，令$k_2$是最小的这样的$k$，则$i_2, \sigma(i_2), \sigma\big(\sigma(i_2)\big), \ldots, \sigma^{k_2-1}(i_2)$各不相同，且$\sigma_2 = \Big(i_2, \sigma(i_2), \sigma\big(\sigma(i_2)\big), \ldots, \sigma^{k_2-1}(i_2)\Big)$是一个$k_2$-轮换，如此继续，直至$\{1,2, \ldots n\}$中所有元素都在某一个轮换中出现，设最后一个得到的轮换为 $\sigma_j = \Big(i_j, \sigma(i_j), \sigma\left(\sigma(i_j)\right), \ldots, \sigma^{k_j-1}(i_j)\Big)$，是一个$k_j$-轮换，

显然这样得到的轮换两两不交，所以它们之间的乘法满足交换律，且$\{1,2,\ldots,n\} = \sigma_1\sigma_2\cdots\sigma_j$。

若存在轮换的乘积$\tau_1\tau_2\cdots\tau_l = \sigma$，则存在$k_1 \in \{1,2,\ldots,l\}$，使得$\tau_{k_1}(1) = \sigma(1) = \sigma_1(1)$，此时易得$\tau_{k_1} = \sigma_1$，所以$\prod_{i=1,i\neq k_1}^{l}\tau_i = \prod_{i=2}^{j}\sigma_i$，则存在$k_2 \in \{1,2,\ldots,l\}\backslash\{k_1\}$，使得$\tau_{k_2}(i_2) = \sigma(i_2) = \sigma_2(i_2)$，此时易得$\tau_{k_2} = \sigma_2$,所以$\prod_{i=1,i\neq k_1,i\neq k_2}^{l}\tau_i = \prod_{i=3}^{j}\sigma_i$，如此继续，最终可得$l = j$，且存在$1,2,\ldots,j$的一个排列$k_1,k_2,\ldots,k_j$，使得$\tau_{k_i} = \sigma_i$对所有的$i \in \{1,2,\ldots,j\}$都成立，即在不计乘法顺序的情况下，该表示唯一。

- 例 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&1&2&4&3\end{pmatrix}$是$S=\{1,2,3,4,5,6\}$上的一个置换，可表示为两个轮换的乘积，即$\begin{pmatrix}1&2&3&4&5&6\\6&5&1&2&4&3\end{pmatrix}=(1,6,3)(2,5,4)$。

- 定义6.6.3 设$i_1, i_2, \dots, i_n$是一个n元排列，则(i_k, i_l)称为该排列的一个逆序，如果$i_k > i_l$，其中$1 \leq k < l \leq n$。排列中逆序的个数称为该排列的逆序数，记为$[i_1, i_2, \dots, i_n]$。

- 定义6.6.3 设$i_1, i_2, \ldots, i_n$是一个n元排列，则(i_k, i_l)称为该排列的一个逆序，如果$i_k > i_l$，其中$1 \leq k < l \leq n$。排列中逆序的个数称为该排列的逆序数，记为$[i_1, i_2, \ldots, i_n]$。

- 定理6.6.3 设σ是一个n元置换，则它可以表示成若干个对换（2-轮换）的乘积，且对换个数的奇偶性与σ的逆序数$[\sigma(1), \sigma(2), \cdots, \sigma(n)]$的奇偶性相同。

- 定义6.6.4 置换σ称为偶置换，如果它可以表示为偶数个对换的乘积；σ称为奇置换，如果它可以表示为奇数个对换的乘积。

- 定义6.6.4 置换σ称为偶置换，如果它可以表示为偶数个对换的乘积；σ称为奇置换，如果它可以表示为奇数个对换的乘积。

- 定理6.6.4 n元偶置换全体关于置换的乘法构成一个群，它的阶为$n!/2$。