第九章 群的结构
2015年10月12日

信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

对群的结构、运算、生成元的思考

1. 一个群能否用最少的元素来表述? 举例说明.
2. 循环群的生成元是惟一的吗? 有多少个? 举例说明.
3. 循环群的子群是循环群吗? 举例说明.
4. 如何找群的生成元? 举例说明.
5. 置换群的运算形式是什么? 并举例说明.
6. 置换是否可以用一系列对换来表示? 对换个数的奇偶性是确定的吗? 并举例说明.

§9.1.1 循环群

本节将运用同态分解定理8.3.3 和加群$\mathbf{Z}$, 以及模m 加群$\mathbf{Z}/m\mathbf{Z}$ 的性质来研究循环群.

首先, 讨论加群$\mathbf{Z}$ 及其子群.

定理9.1.1 加群$\mathbf{Z}$ 的每个子群H 是循环群. 并且有$H =< 0 >$ 或$H =< m >= m\mathbf{Z}$, 其中m 是H 中的最小正整数. 如果$H \neq < 0 >$, 则H 是无限的.

证 如果H 是零子群$\{0\}$, 结论显然成立.

如果H 是非零子群, 则存在非零整数$a \in H$. 因为H 是子群, 所以$-a \in H$. 这说明H 中有正整数. 设H 中的最小正整数为m. 则一定有$H =< m >= m\mathbf{Z}$. 事实上, 对任意的$a \in H$,不妨设$a > 0$ (否则, 考虑$-a = q \cdot m$, 从而, $a = q \cdot (-m)$), 根据定理1.10 (欧几里得除法), 存在整数正整数q, 以及整数r 使得

$$a = q \cdot m + r, \quad 0 \leq r < m.$$

如果$r \neq 0$, 则$r = a + q(-m) \in H$, 这与m 的最小性矛盾. 因此, $r = 0$, $a = q \cdot m \in m\mathbf{Z}$. 故$H \subset m\mathbf{Z}$. 但显然有$m\mathbf{Z} \subset H$. 因此, $H = m\mathbf{Z}$. 证毕

定理9.1.2 每个无限循环群同构于加群$\mathbf{Z}$. 每个阶为m 的有限循环群同构于加群$\mathbf{Z}/m\mathbf{Z}$.

证 设循环群$G =< a >= \{a^n \mid n \in \mathbf{Z}\}$. 考虑加群$\mathbf{Z}$ 到G 的映射:

$$\begin{aligned} f: \mathbf{Z} &\longrightarrow G \\ n &\longmapsto a^n \end{aligned}$$

因为$f(n+k) = a^{n+k} = a^n a^k = f(n)f(k)$, 所以$f$ 是$\mathbf{Z}$ 到G 的同态, 而且是满的. 根据同态分解定理(定理8.3.3 , 群G 同构于商群$\mathbf{Z}/\ker(f)$. 根据定理9.1.1 , $\ker(f) =< 0 >$ 或$\ker(f) = m\mathbf{Z}$. 前者对应于无限循环群, 后者对应于m 阶有限循环群. 证毕

定义9.1.1 设G是一个群, $a \in G$. 则子群$< a >$ 的阶称为元素a 的阶, 记为$\mathrm{ord}(a)$.

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院

定理9.1.3 设G 是一个群, $a \in G$. 则

当a 是无限阶时,有

(i) $a^k = e$ 当且仅当$k = 0$.

(ii) 元素a^k $(k \in \mathbf{Z})$ 两两不同.

当a 是有限阶$m > 0$, 有

(iii) m 是使得$a^m = e$ 的最小正整数.

(iv) $a^k = e$ 当且仅当$m \mid k$.

(v) $a^r = a^k$ 当且仅当$r \equiv k \pmod m$.

(vi) 元素a^k $(k \in \mathbf{Z}/m\mathbf{Z})$ 两两不同.

(vii) $< a >= \{a, a^2, \ldots, a^{m-1}, a^m = e\}$

(viii) 对任意整数$1 \le d \le m$, 有$\mathrm{ord}(a^d) = \dfrac{m}{(d, m)}$.

证 考虑加群$\mathbf{Z}$ 到群G 的映射f :

$$f:\ n \longmapsto a^n.$$

f 是同态映射. 根据定理8.3.3 , 我们有

$$\mathbf{Z}/\ker f \ \cong < a > .$$

情形I. 因为a 是无限阶元等价于$\ker f$, 后者说明f 是一对一的. 因此, (i) 和(ii) 成立.

情形II. 如果a 是有限阶m, 则$\ker f = m\mathbf{Z}$. 因此, 我们有:

(iii) m 是使得$a^m = e$ 的最小正整数.

(iv) $a^k = e$ 等价于$k \in \ker f$, 等价于$m \mid k$.

(v) $a^r = a^k$ 等价于$r - k \in \ker f$, 等价于$r \equiv k \pmod m$.

(vi) 元素a^k 对应于$\mathbf{Z}/\ker f$ 中不同元素, 两两不同.

(vii) $< a >= \{a, a^2, \ldots, a^{m-1}, a^m = e\}$ 与$\mathbf{Z}/\ker f$ 中最小正剩余系相对应.

(viii) 对任意整数$1 \le d \le m$, 有$\mathrm{ord}(a^d) = \dfrac{m}{(d,m)}$.

$(a^d)^k = e$ 等价于$dk \in \ker f$, 等价于$m \mid dk$, 等价于$\dfrac{m}{(d,m)} \mid \dfrac{d}{(d,m)}k$, 等价于$\dfrac{m}{(d,m)} \mid k$.

因此, $\mathrm{ord}(a^d) = \dfrac{m}{(d,m)}$. 证毕

定理9.1.4 循环群的子群是循环群.

证 考虑加群**Z** 到循环群$G =< a >$ 的映射f :

$$f:\ n \longmapsto a^n.$$

f 是同态映射. 根据定理8.3.1 , 对于G 的子群H, 我们有$K = f^{-1}(H)$ 是**Z** 的子群. 根据定理9.1.3 , K 是循环群, 所以$H = f(K)$ 是循环群. **证毕**

定理9.1.5 设G 是循环群.

i) 如果G 是无限的, 则G 的生成元为a 和a^{-1}.

ii) 如果G 是有限阶m, 则a^k 是G 的生成元为当且仅当$(k, m) = 1$.

证 考虑加群$\mathbf{Z}$ 到循环群G 的映射f :

$$f: \ n \longmapsto a^n.$$

f 是同态映射. 根据定理8.3.3 , 我们有

$$\mathbf{Z}/\ker f \cong G.$$

因为G 中的生成元对应于$\mathbf{Z}/\ker f$ 中的生成元, 所以

i) 当G 是无限阶, 即$\ker f = 0$ 时, $\mathbf{Z}/\ker f$ 的生成元是1 和-1. 这时, G 的生成元是a 和a^{-1}.

ii)当G 是有限阶, 即$\ker f = m\mathbf{Z}$, $m > 0$ 时, $\mathbf{Z}/\ker f$ 的生成元是k, $(k, m) = 1$. 这时, G 的生成元是a^k, $(k, m) = 1$. 定理成立. 证毕

下面从生成元的阶来讨论有限群的生成元构造. 为此, 先引进几个引理.

引理9.1.1 设G是有限交换群. 对任意元素$a, b \in G$, 若$(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 则

$$\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b).$$

证 因为

$$a^{\mathrm{ord}(a\cdot b)\cdot \mathrm{ord}(b)} = a^{\mathrm{ord}(a\cdot b)\cdot \mathrm{ord}(b)} \cdot (b^{\mathrm{ord}(b)})^{\mathrm{ord}(a\cdot b)} = ((a \cdot b)^{\mathrm{ord}(a\cdot b)})^{\mathrm{ord}(b)} = 1,$$

根据定理9.1.3 (iv), 有$\mathrm{ord}(a) \mid \mathrm{ord}(a\cdot b)\cdot\mathrm{ord}(b)$. 因为$(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 所以$\mathrm{ord}(a) \mid \mathrm{ord}(a \cdot b)$.

同理, $\mathrm{ord}(b) \mid \mathrm{ord}(a \cdot b)$. 再由$(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, 得到

$$\mathrm{ord}(a) \cdot \mathrm{ord}(b) \mid \mathrm{ord}(a \cdot b).$$

此外, 显然有 $\mathrm{ord}(a \cdot b) \mid \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

故 $\mathrm{ord}(a \cdot b) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$. 证毕

引理9.1.2 设G 是有限交换群. 对任意元素$a, b \in G$, 存在$c \in G$ 使得

$$\mathrm{ord}(c) = [\mathrm{ord}(a), \mathrm{ord}(b)].$$

证 根据定理1.6.6, 对于整数$\mathrm{ord}(a)$ 和$\mathrm{ord}(b)$, 存在整数u, v 满足:

$$u \mid \mathrm{ord}(a), \quad v \mid \mathrm{ord}(b), \quad (u, v) = 1$$

使得 $[\mathrm{ord}(a),\ \mathrm{ord}(b)] = u \cdot v.$
现在令 $s = \frac{\mathrm{ord}(a)}{u}, \quad t = \frac{\mathrm{ord}(b)}{v},$
根据定理9.1.3 (viii), 我们有

$$\mathrm{ord}(a^s) = \frac{\mathrm{ord}(a)}{(s, \mathrm{ord}(a))} = u, \quad \mathrm{ord}(b^t) = v.$$

再根据引理9.1.1, 得到

$$\mathrm{ord}(a^s \cdot b^t) = \mathrm{ord}(a^s) \cdot \mathrm{ord}(b^t) = u \cdot v = [\mathrm{ord}(a),\ \mathrm{ord}(b)].$$

因此, 取$c = a^s \cdot b^t$. 即为所求. 证毕

定理9.1.6 设G是有限交换群, 则G中存在元素$a_1,\ a_2,\ \ldots,\ a_s$满足

$$\mathrm{ord}(a_{i+1}) \mid \mathrm{ord}(a_i),\ 1 \le i \le s-1,$$

并且使得

$$G =< a_1, a_2, \cdots, a_s > .$$

证 设$G = \{b_1,\ b_2,\ \ldots,\ b_n\},\ n = |G|$. 根据引理9.1.2, 存在元素$a_1$使得

$$\mathrm{ord}(a_1) = [\mathrm{ord}(b_1), \ldots, \mathrm{ord}(b_n)].$$

若$G \ne < a_1 >$, 设

$$G- < a_1 >= \{b_{11}, \ldots, b_{1n_1}\},$$

根据引理9.1.2, 存在元素$a_2 \in G\backslash < a_1 >$使得

$$\mathrm{ord}(a_2) = [\mathrm{ord}(b_{11}), \ldots, \mathrm{ord}(b_{1n_1})], \quad \mathrm{ord}(a_2) \mid \mathrm{ord}(a_1).$$

否则, 可找到c_2使得$\mathrm{ord}(c_2) = [\mathrm{ord}(a_1), \mathrm{ord}(a_2)] > \mathrm{ord}(a_1)$, 矛盾.

若$G \neq < a_1, a_2 >$, 设

$$G - < a_1, a_2 > = \{b_{21}, \ldots, b_{2n_2}\},$$

根据引理9.1.2, 存在元素$a_3 \in G \backslash < a_1, a_2 >$ 使得

$$\mathrm{ord}(a_3) = [\mathrm{ord}(b_{21}), \ldots, \mathrm{ord}(b_{2n_2})], \quad \mathrm{ord}(a_3) \mid \mathrm{ord}(a_2).$$

否则, 可找到c_3 使得$\mathrm{ord}(c_3) = [\mathrm{ord}(a_2), \mathrm{ord}(a_3)] > \mathrm{ord}(a_2)$, 矛盾.
如此下去,可找到$a_4, \ldots, a_s$, 使得

$$G = < a_1, a_2, \cdots, a_s >, \quad \mathrm{ord}(a_{i+1}) \mid \mathrm{ord}(a_i), \ 1 \leq i \leq s-1.$$

证毕

例9.1.1 设$n = 5 \cdot 7 \cdot 13 = 455$. $G = (\mathbf{Z}/n\mathbf{Z})^*$. 因为

$$\varphi(n) = (5-1)(7-1)(13-1) = 288,$$

$$[\varphi(5), \varphi(7), \varphi(13)] = [5-1, 7-1, 13-1] = 12,$$

所以G 中元素的阶都是12 的因子.

取$a_1 = 2$, 有$\mathrm{order}_n(a_1) = 12$, 及

$$H_1 =< a_1 >= \{1, 2, 4, 8, 16, 32, 64, 128, 256, 57, 114, 228\}.$$

再取$a_2 = 3$, 有$\mathrm{order}_n(a_2) = 12$, 及

$$H_2 =< a_2 >= \{1, 3, 9, 27, 81, 243, 274, 367, 191, 118, 354, 152\}.$$

这时, H_1 与 H_2 的乘积 H_1H_2 为

$a_1^i a_2^j$	a_2^0	a_2^1	a_2^2	a_2^3	a_2^4	a_2^5	a_2^6	a_2^7	a_2^8	a_2^9	a_2^{10}	a_2^{11}
a_1^0	1	3	9	27	81	243	274	367	191	118	354	152
a_1^1	2	6	18	54	162	31	93	279	382	236	253	304
a_1^2	4	12	36	108	324	62	186	103	309	17	51	153
a_1^3	8	24	72	216	193	124	372	206	163	34	102	306
a_1^4	16	48	144	432	386	248	289	412	326	68	204	157
a_1^5	32	96	288	409	317	41	123	369	197	136	408	314
a_1^6	64	192	121	363	179	82	246	283	394	272	361	173
a_1^7	128	384	242	271	358	164	37	111	333	89	267	346
a_1^8	256	313	29	87	261	328	74	222	211	178	79	237
a_1^9	57	171	58	174	67	201	148	444	422	356	158	19
a_1^{10}	114	342	116	348	134	402	296	433	389	257	316	38
a_1^{11}	228	229	232	241	268	349	137	411	323	59	177	76

.

或

$$\begin{aligned} H_1H_2 \ = \ & \{1,2,3,4,6,8,9,12,16,17,18,19,24,27,29,31,32,34,36,37,38,41,48,\\ & 51,54,57,58,59,62,64,67,68,72,74,76,79,81,82,87,89,93,96,102,\\ & 103,108,111,114,116,118,121,123,124,128,134,136,137,144,148,\\ & 152,153,157,158,162,163,164,171,173,174,177,178,179,186,191,\\ & 192,193,197,201,204,206,211,216,222,228,229,232,236,237,241,\\ & 242,243,246,248,253,256,257,261,267,268,271,272,274,279,283,\\ & 288,289,296,304,306,309,313,314,316,317,323,324,326,328,333,\\ & 342,346,348,349,354,356,358,361,363,367,369,372,382,384,386,\\ & 389,394,402,408,409,411,412,422,432,433,444\} \end{aligned}$$

最后取$a_3 = 11$, 有$\mathrm{order}_n(a_3) = 12$, 及

$$H_3 =< a_3 >= \{1,11,121,421,81,436,246,431,191,281,361,331\}.$$

故

$$G = H_1H_2H_3 =< a_1, a_2, a_3 >$$

9.2 有限生成交换群

在线性空间中, 有一组向量叫做基底, 其具有性质:
(i) 该组向量是生成元, 所有向量都是该组向量的线性组合,
(ii) 该组向量线性无关.
我们希望有限交换群中也有这样一组元素.

乘法交换群G 的一个子集X 叫做G 的**基底**, 如果X 是G 的最小生成元,
即(i) $G =< X >$;
(ii) X 中的任意不同的元素$x_1, x_2, \ldots, x_k$ **乘性无关**,
即不存在不全为零的整数$n_1, n_2, \ldots, n_k$ 使得

$$x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} = e.$$

加法交换群G 的一个子集X 叫做G 的基底, 如果X 是G 的最小生成元, 即
(i) $G =< X >$;
(ii) X 中的任意不同的元素$x_1, x_2, \ldots, x_k$ 在$\mathbf{Z}$ 上**线性无关**,
即不存在不全为零的整数$n_1, n_2, \ldots, n_k$ 使得

$$n_1 x_1 + n_2 x_2 + \cdots + n_k x_k = 0.$$

设$H_1,\ldots,H_k$ 是交换乘群G 的k 个子群. 我们称$H_1\cdots H_k$ 是$H_1,\ldots,H_k$ 的**直积**, 如果

$$(H_1\cdots H_{i-1}H_{i+1}\cdots H_k)\cap H_i=\{e\},\ \ 1\le i\le k.$$

记作$H_1\otimes\cdots\otimes H_k$.

设$H_1,\ldots,H_k$ 是交换加群G 的k 个子群. 我们称$H_1+\cdots+H_k$ 是$H_1,\ldots,H_k$ 的**直和**, 如果

$$(H_1+\cdots+H_{i-1}+H_{i+1}+\cdots+H_k)\cap H_i=\{0\},\ \ 1\le i\le k.$$

记作$H_1\oplus\cdots\oplus H_k$.

定理9.2.1 设交换加群(对应地交换乘群) G 有一组非空基底, 则G 是一组循环群的直和(对应地直积).

证 设$X = \{x_i \mid i \in I\}$ 是G 的非空基底. 根据基底的定义, $G = \sum_{i \in I} < x_i >$.
现在只需证明: 对任意$x_i \in X$,

$$< x_i > \cap (\sum_{j \in I, j \neq i} < x_j >) = \{0\}.$$

设$y \in < x_i > \cap (\sum_{j \in I, j \neq i} < x_j >)$, 则存在$n \in Z$及$n_1, \ldots, n_{i-1}, n_{i+1}, \ldots, n_k \in$ **Z** 使得

$$y = nx_i = n_1 x_1 + \cdots + n_{i-1} x_{i-1} + n_{i+1} x_{i+1} + \cdots + n_k x_k.$$

从而

$$n_1 x_1 + \cdots + n_{i-1} x_{i-1} + (-n) x_i + n_{i+1} x_{i+1} + \cdots + n_k x_k = 0.$$

因为$x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_k$ 是基底, 所以

$$-n = n_1 = \cdots = n_k = 0.$$

因此, $y = nx = 0$. 定理成立. **证毕**
定理9.2.1 中的群叫做**自由交换群**.

定理9.2.2 自由交换群的任意两个基底所含元素个数相同.
这里我们仅考虑基底所含元素个数为有限的情形.
设$G =< x_1, x_2, \ldots, x_k >=< y_1, y_2, \ldots, y_m >$. 考虑子群$H = 2G =< 2x_1, 2x_2, \ldots, 2x_k >$, 则商群

$$G/H = \{(n_1x_1 + n_2x_2 + \cdots + n_kx_k)H \mid n_i \in \mathbf{Z}/2\mathbf{Z}, 1 \le i \le k.\}$$

因此, $[G : H] = 2^k$. 又有$H =< 2y_1, 2y_2, \ldots, 2y_m >$, 同样有$[G : H] = 2^m$. 故$k = m$. 证毕

自由交换群G 的基底的元素个数叫做群G **的秩**.

定理9.2.3 每个交换群G 都是一个秩为$|X|$ 的自由交换群的同态象子群, 其中X 为G 的生成元集.

证 设G 的生成元集$X = \{x_1,\ x_2,\ \ldots\} = \{x_i\}_{i\in I}$. 考虑集合

$$\mathbf{Z}^I = \{(n_1, n_2, \ldots, n_i, \ldots) \mid n_i \in \mathbf{Z},\ i \in I.\}$$

易知, $\mathbf{Z}^I$ 是秩为$|I| = |X|$ 的自由交换群, 且映射

$$f :\ (n_1, n_2, \ldots, n_k, \ldots) \longmapsto n_1x_1 + n_2x_2 + \cdots + n_kx_k$$

是$\mathbf{Z}^I$ 到G 的满同态. 所以$G = f(\mathbf{Z}^I)$. 证毕

注 表达式$(n_1, n_2, \ldots, n_i, \ldots)$ 中只有有限项不为零.

9.3 置换群

本节我们进一步研究对称群 S_n.

设$S = \{1,\ 2,\ \ldots,\ n-1,\ n\}$, σ 是S 上的一个置换, 即σ 是S 到自身的一一对应的映射:

$$\begin{array}{rccc} \sigma: & S & \longrightarrow & S \\ & k & \longmapsto & \sigma(k) = i_k \end{array}$$

因为k 在σ 下的象是i_k, 所以我们可以显示地将σ 表示成

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ i_1 & i_2 & \ldots & i_{n-1} & i_n \end{pmatrix}.$$

σ 当然可写成

$$\sigma = \begin{pmatrix} n & n-1 & \ldots & 2 & 1 \\ i_n & i_{n-1} & \ldots & i_2 & i_1 \end{pmatrix} = \begin{pmatrix} j_1 & j_2 & \ldots & j_{n-1} & j_n \\ i_{j_1} & i_{j_2} & \ldots & i_{j_{n-1}} & i_{j_n} \end{pmatrix},$$

其中$j_1,\ j_2,\ \ldots,\ j_{n-1},\ j_n$ 是$1,\ 2,\ \ldots,\ n-1,\ n$ 的一个排列.

σ 的逆元为: $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \ldots & i_{n-1} & i_n \\ 1 & 2 & \ldots & n-1 & n \end{pmatrix}.$

例9.3.1 设$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}$.

计算$\sigma\tau$, $\tau\sigma$, σ^{-1}.

解 将τ 的像作为σ 的像源, 并依次对应, 有

$$
\begin{aligned}
\sigma \cdot \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 5 & 6 & 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix}.
\end{aligned}
$$

$$
\tau \cdot \sigma = \begin{pmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}.
$$

$$
\sigma^{-1} = \begin{pmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}.
$$

定理9.3.1 n 元置换全体组成的集合S_n 对置换的乘法构成一个群，其阶是$n!$.

证 因为一一对应的映射的乘积仍是一一对应的，且该乘积满足结合律，所以置换的乘法满足结合律.

又n 元恒等置换$e = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 1 & 2 & \ldots & n-1 & n \end{pmatrix}$ 是单位元.

置换$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ i_1 & i_2 & \ldots & i_{n-1} & i_n \end{pmatrix}$ 有逆元

$$\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \ldots & i_{n-1} & i_n \\ 1 & 2 & \ldots & n-1 & n \end{pmatrix}.$$

因此，S_n 对置换的乘法构成一个群.

因为$(1,\ 2,\ \ldots,\ n-1,\ n)$ 在置换σ 下的象$(\sigma(1),\ \sigma(2),\ \ldots,\ \sigma(n-1),\ \sigma(n))$ 是$(1,\ 2,\ \ldots,\ n-1,\ n)$ 的一个排列，这样的排列共有$n!$ 个，所以S_n 的阶为$n!$. 证毕

为了更好地研究置换, 我们先考虑特殊的置换.

如果n 元置换σ 使得$\{1,\ 2,\ \ldots,\ n-1,\ n\}$ 中的一部分元素$\{i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k\}$ 满足$\sigma(i_1)=i_2,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1,$ 又使得余下的元素保持不变, 则称该置换为$k-$**轮换**, 简称轮换, 记作$\sigma=(i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k)$. 如下图:

$$i_1 \to i_2 \to \ldots \to i_{k-1} \to i_k \to i_1$$

k 称为轮换的长度. $k=1$时, 1-轮换为恒等置换; $k=2$ 时, 2-轮换(i_1,i_2)叫做**对换**.

两个轮换$\sigma=(i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k),\ \tau=(j_1,\ j_2,\ \ldots,\ j_{l-1},\ j_l)$ 叫做不相交, 如果$k+l$ 个元素都是不同的.

定理9.3.2 任意一个置换都可以表示为一些不相交轮换的乘积. 在不考虑乘积次序的情况下, 该表达式是惟一的.

证 设σ 是$S = \{1, 2, \ldots, n-1, n\}$ 上的一个置换. 在S 中任取一个元素, 设为$i_1^{(1)}$. 因为$n+1$ 个元素

$$i_1^{(1)}, \sigma^1(i_1^{(1)}), \ldots, \sigma^n(i_1^{(1)}), \sigma^n(i_1^{(1)})$$

都落在n 元集S 中, 必有$k \neq l$ 使得

$$\sigma^k(i_1^{(1)}) = \sigma^l(i_1^{(1)}).$$

不妨设$k > l$, 在上式两端同乘$(\varphi^{-1})^l$, 得到

$$\sigma^{k-l}(i_1^{(1)}) = i_1^{(1)}.$$

取$k_1 \leq n$ 为使得$\sigma^{k_1}(i_1^{(1)}) = i_1^{(1)}$ 的最小正整数, 并令

$$i_2^{(1)} = \sigma^1(i_1^{(1)}), \ldots, i_{k_1}^{(1)} = \sigma^{k_1-1}(i_1^{(1)}).$$

则$\sigma_1 = (i_1^{(1)}, i_2^{(1)}, \ldots, i_{k_1}^{(1)})$ 就是一个k_1−轮换.

如果$k_1 = n$, 则$\sigma = \sigma_1$. 结论成立. 如果$k_1 < n$, 在$S - \{i_1^{(1)}, i_2^{(1)}, \ldots, i_{k_1}^{(1)}\}$中任取一个元素, 设为$i_1^{(2)}$. 取$k_2 \leq n$为使得$\sigma^{k_2}(i_1^{(2)}) = i_1^{(2)}$的最小正整数, 并令

$$i_2^{(2)} = \sigma^1(i_1^{(2)}), \ldots, i_{k_2}^{(2)} = \sigma^{k_2-1}(i_1^{(2)}).$$

则$\sigma_2 = (i_1^{(2)}, i_2^{(2)}, \ldots, i_{k_2}^{(1)})$是一个与$\sigma_1$不相交的$k_2-$轮换. 如此下去,..., 可找到与$\sigma_1, \ldots, \sigma_{r-1}$不相交的$k_r-$轮换$\sigma_r$使得$k_1 + k_2 + \cdots + k_r = n$. 因为对任意$i \in S$, 有

$$(\sigma_1\sigma_2\cdots\sigma_r)(i) = \sigma(i),$$

所以定理成立. 证毕

例9.3.2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix} = (2,5,4)(1,6,3).$

下面考虑轮换与对换的关系.

对于轮换$\sigma = (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k)$, 有

$$\sigma = (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k) = (i_1, i_k)(i_1, i_{k-1})\cdots(i_1, i_3)(i_1, i_2).$$

例9.3.3

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix}. \\ &= (2,5,4)(1,6,3) = (2,4)(2,5)(1,3)(1,6)\end{aligned}$$

定义9.3.1 n 元排列$i_1,\ \ldots,\ i_k,\ \ldots,\ i_l,\ \ldots,\ i_n$ 的一对有序元素$(i_k,\ i_l)$ 叫做**逆序**, 如果$k < l$ 时, $i_k > i_l$. 排列中逆序的个数叫做该排列的**逆序数**, 记为$[i_1,\ \ldots,\ i_n]$.

定理9.3.3 任意一个置换σ 都可以表示为一些对换的乘积, 且对换个数的奇偶性与排列的逆序数$[\sigma(1),\ \ldots,\ \sigma(n)]$ 的奇偶性相同.

证明 设对换$\tau = (\sigma(k),\ \sigma(l))$, 其对排列

$$\sigma(1),\ \ldots,\ \sigma(k),\ \ldots,\ \sigma(l),\ \ldots,\ \sigma(n)$$

作用得到新排列

$$\sigma(1),\ \ldots,\ \sigma(l),\ \ldots,\ \sigma(k),\ \ldots,\ \sigma(n)$$

则发生改变的有序对为

$$\underbrace{(\sigma(k),\ \sigma(k+1)),\ \ldots,\ (\sigma(k),\ \sigma(l))}_{l-k\ \text{对}},\ \underbrace{(\sigma(k+1),\ \sigma(l)),\ \ldots,\ (\sigma(l-1),\ \sigma(l))}_{l-k-1\ \text{对}},$$

$$(\sigma(k),\ \sigma(k+1)),\ \ldots,\ (\sigma(k),\ \sigma(l)),\ (\sigma(k+1),\ \sigma(l)),\ \ldots,\ (\sigma(l-1),\ \sigma(l)),$$

共2(l-k)-1 对. 因此, 对换改变排列的逆序数$[\sigma(1),\ldots,\sigma(n)]$ 的奇偶性.

再设置换$\sigma = \tau_m\cdots\tau_1$ 为m 个对换的乘积, 那么排列$1,\ldots,n$ 经过m 个对换变为排列$\sigma(1),\ldots,\sigma(n)$. 因此, 逆序数$[\sigma(1),\ldots,\sigma(n)]$ 的奇偶性与$[1,\ldots,n]+m=m$ 的奇偶性相同. 证毕

定义9.3.2 一个置换σ 叫做**偶置换**, 如果它可以表示为偶数个对换的乘积; σ 叫做**奇置换**, 如果它可以表示为奇数个对换的乘积.

根据定理9.3.3, 我们有

$$
\begin{array}{rcl}
\hline
\text{偶置换} * \text{偶置换} & = & \text{偶置换} \\
\text{偶置换} * \text{奇置换} = \text{奇置换} * \text{偶置换} & = & \text{奇置换} \\
\hline
\end{array}
$$

记A_n 为n 元偶置换全体组成的集合.

定理9.3.4 A_n 对置换的乘法构成一个群, 其阶是$n!/2$.

证 因为偶置换与偶置换的乘积是偶置换, 恒等置换是偶置换, 偶置换的逆置换是偶置换, 所以A_n 对置换的乘法构成一个群.

因为奇置换与偶置换的乘积是奇置换, 所以n 元奇置换全体组成的集合为$\tau A_n = \{\tau\sigma \mid \sigma \in A_n\}$, 其中$\tau$ 是任一给定的奇置换. 因此, 取定一个奇置换τ, 我们有

$$S_n = A_n \cup \tau A_n$$

以及

$$|S_n| = |A_n| + |\tau A_n| = 2|A_n|.$$

故$|A_n| = n!/2$. 证毕

A_n 叫做交错群.

由n 元置换构成的群叫做n 元置换群.

例9.3.4 设$\sigma = (1,\ 2,\ 3)$. 则循环群

$$G =< \sigma >= \{e,\ (1,\ 2,\ 3),\ (1,\ 3,\ 2)\}$$

是3 元置换群.

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

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

例9.3.5 设$\sigma_1 = (1,\ 2,\ 3,\ 4),\ \sigma_2 = (1,\ 3,\ 2,\ 4)$. 则循环群

$$G_1 =< \sigma_1 >= \{e,\ (1,\ 2,\ 3,\ 4), (1,\ 3)(2,\ 4),\ (1,\ 4,\ 3,\ 2)\}$$

和

$$G_2 =< \sigma_2 >= \{e,\ (1,\ 3,\ 2,\ 4),\ (1,\ 2)(3,\ 4),\ (1,\ 4,\ 2,\ 3)\}$$

都是4 元置换群.

定理9.3.5 设G 是一个n 元群. 则G 同构一个n 元置换群.

证 任取$a \in G$, 作G 到自身的映射:

$$\tau_a : x \longmapsto ax \quad (x \in G),$$

易知τ_a 在G 上是一一对应的, 因此τ_a 是G 元素的一个置换. 令τ_a 组成的集合为

$$G' = \{\tau_a \mid a \in G\}.$$

则G' 是一个群. 事实上, 对任意τ_a, $\tau_b \in G'$, 有

$$(\tau_a)(\tau_b)(x) = \tau_a(bx) = a(bx) = (ab)(x) = \tau_{ab}(x), \quad x \in G$$

因此, $\tau_a\tau_b = \tau_{ab} \in G'$. 此外, 有结合律: $\tau_a(\tau_b\tau_c) = \tau_{a(bc)} = \tau_{(ab)c} = (\tau_a\tau_b)\tau_c$; 有单位元$\tau_e$; 元素τ_a 有逆元: $(\tau_a)^{-1} = \tau_{a^{-1}}$.

又G 到G' 的映射:

$$\varphi : a \longmapsto \tau_a$$

是一一对应的. 且$\varphi(ab) = \tau_{ab} = \tau_a\tau_b = \varphi(a)\varphi(b)$, 故$G$ 同构于G'. 证毕

访问主页
标题页
目录页
第 33 页 共 52 页
返回
全屏显示
关闭
退出

下面我们研究4 元对称群S_4.

例9.3.6 研究4 对称群S_4 及其子群.

解 以像为点可以得到如下Cayley 图. 箭头表示在置换下σ_i 下元素与其像的对应关系.

有3 个4 元循环群.

$$
\begin{aligned}
H_{1234} &= \{\sigma_1 = (1,2,3,4), \sigma_1^2 = (1,3)(2,4), \sigma_1^3 = (1,4,3,2), \sigma_1^4 = (1)(2)(3)(4)\} \\
&= H_{1432} \\
H_{1243} &= \{\sigma_2 = (1,2,4,3), \sigma_2^2 = (1,4)(2,3), \sigma_2^3 = (1,3,4,2), \sigma_2^4 = (1)(2)(3)(4)\} \\
&= H_{1342} \\
H_{1324} &= \{\sigma_3 = (1,3,2,4), \sigma_3^2 = (1,2)(3,4), \sigma_3^3 = (1,4,2,3), \sigma_3^4 = (1)(2)(3)(4)\} \\
&= H_{1423}
\end{aligned}
$$

$$
\sigma_1^2 = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1,\ 3)(2,\ 4)
$$

$$
\sigma_1^3 = \begin{pmatrix} 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}
$$

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY
信息安全工程学院

有1 个非单位元为2 阶元的4 元群.

$H_4 = \{\tau_1 = (1,\ 2)(3,\ 4),\ \tau_2 = (1,\ 3)(2,\ 4),\ \tau_3 = (1,\ 4)(2,\ 3),\ id = (1)(2)(3)(4)\}$

有4 个3 元循环群.

$$
\begin{aligned}
H_{123} &= \{\sigma_4 = (1,\ 2,\ 3)(4),\ \sigma_4^2 = (1,\ 3,\ 2)(4),\ \sigma_4^3 = (1)(2)(3)(4)\} &= H_{132}\\
H_{124} &= \{\sigma_5 = (1,\ 2,\ 4)(3),\ \sigma_5^2 = (1,\ 4,\ 2)(3),\ \sigma_5^3 = (1)(2)(3)(4)\} &= H_{142}\\
H_{134} &= \{\sigma_6 = (1,\ 3,\ 4)(2),\ \sigma_6^2 = (1,\ 4,\ 3)(2),\ \sigma_6^3 = (1)(2)(3)(4)\} &= H_{143}\\
H_{234} &= \{\sigma_7 = (2,\ 3,\ 4)(1),\ \sigma_7^2 = (2,\ 4,\ 3)(1),\ \sigma_7^3 = (1)(2)(3)(4)\} &= H_{243}
\end{aligned}
$$