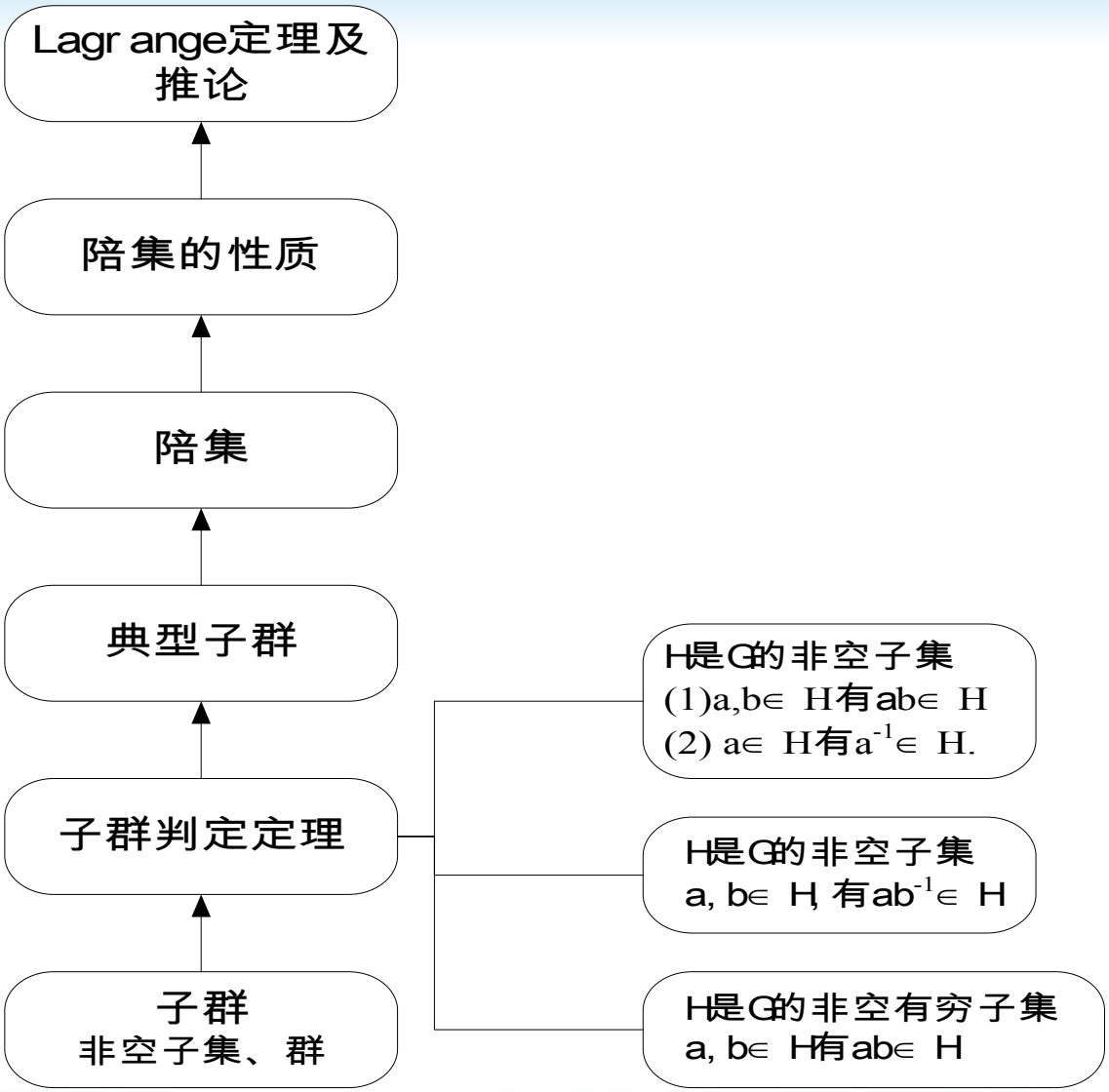
上节复习



北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

阿贝尔群、循环群、置换群：各种不同的群。

8.3 特殊的群——阿贝尔群、循环群和置换群

- 什么是阿贝尔群
  - 若群 <G, •> 的运算•适合交换律，则称 <G, •> 为阿贝尔群（ Abelian Group ）或交换群。
- 在一个阿贝尔群 <G, •> 中，一个乘积可以任意颠倒因子的次序而求其值。
- 在阿贝尔群中，易见有如下指数律成立
  - $(a•b)^m=a^m•b^m$ ， m 为任意整数

北京科技大学 University of Science and Technology Beijing

知识回顾

- 生成子群

设 G 为群 , $a \in G$,

$$<a>=\{a^k \mid k \in Z\}$$

即 a 的所有的幂构成的集合，为 G 的子群，称为由 a 生成的子群 .

8.3 特殊的群——阿贝尔群、循环群和置换群

循环群的定义

定义 8.10 设 G 是群，若存在 $a \in G$ 使得

$$G=\{a^k \mid k \in \mathbf{Z}\}$$

则称 G 是**循环群**，记作 $G=\langle a \rangle$，称 a 为 G 的生成元.

循环群的分类：n **阶循环群**和**无限循环群**.

设 $G=\langle a \rangle$ 是循环群，若 a 是 n 阶元，则

$$G = \{ a^0=e, a^1, a^2, \ldots, a^{n-1} \}$$

那么 $|G| = n$，称 G 为 n 阶循环群.

若 a 是无限阶元，则

$$G = \{ a^0=e, a^{\pm 1}, a^{\pm 2}, \ldots \}$$

称 G 为无限循环群.

实例：$\langle \mathbf{Z}, + \rangle$ 为无限循环群

$\langle Z_n, \oplus \rangle$ 为 n 阶循环群

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

循环群的生成元

定理 8.13 设 $G=\langle a\rangle$ 是循环群 .

(1) 若 G 是无限循环群，则 G 只有两个生成元，即 a 和 a^{-1}.

(2) 若 G 是 n 阶循环群，则 G 含有 $\phi(n)$ 个生成元 . 对于任何小于 n 且与 n 互质的数 $r\in\{0,1,\ldots,n-1\}$, a^r 是 G 的生成元 .

$\phi(n)$ 称为欧拉函数，例如 $n=12$ ，小于或等于 12 且与 12 互素的正整数有 4 个：

$$1, 5, 7, 11 \ ,$$

所以 $\phi(12)=4$.

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

定理 8.13 设 $G=\langle a\rangle$ 是循环群.

(1) 若 G 是无限循环群，则 G 只有两个生成元，即 a 和 a^{-1}.

证 (1) 显然 $\langle a^{-1}\rangle \subseteq G$. $\forall a^k \in G$ ，

$$a^k=(a^{-1})^{-k} \in \langle a^{-1}\rangle \ ,$$

因此 $G \subseteq \langle a^{-1}\rangle$ ， a^{-1} 是 G 的生成元.

再证明 G 只有 a 和 a^{-1} 这两个生成元. 假设 b 也是 G 的生成元，

则 $G=\langle b\rangle$. 由 $a \in G$ 可知存在整数 t 使得 $a = b^t$. 由 $b \in G = \langle a\rangle$

知存在整数 m 使得 $b = a^m$. 从而得到

$$a = b^t = (a^m)^t = a^{mt}$$

由 G 中的消去律得

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

因为 G 是无限群，必有 $mt-1 = 0$. 从而证明了 $m = t = 1$ 或 $m = t = -1$ ，即 $b = a$ 或 $b = a^{-1}$

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

定理 8.13 设 $G=\langle a\rangle$ 是循环群.

(2) 若 G 是 n 阶循环群，则 G 含有 $\phi(n)$ 个生成元. 对于任何小于 n 且与 n 互质的数 $r\in\{0,1,\ldots,n-1\}$, a^r 是 G 的生成元.

(2) 只须证明：对任何正整数 r ($r\le n$) ，

a^r 是 G 的生成元 $\Leftrightarrow$ n 与 r 互质.

充分性. 设 r 与 n 互质，且 $r\le n$ ，那么存在整数 u 和 v 使得

$$ur + vn = 1$$

从而 $$a = a^{ur+vn} = (a^r)^u(a^n)^v = (a^r)^u$$

这就推出$\forall\, a^k\in G$ ， $a^k = (a^r)^{uk}\in\langle a^r\rangle$ ，即 $G\subseteq\langle a^r\rangle$.

另一方面，显然有 $\langle a^r\rangle\subseteq G$. 从而 $G = \langle a^r\rangle$.

必要性. 设 a^r 是 G 的生成元，则 $|a^r| = n$. 又因为 $|a| = n$ ， $|a^r| = n/(n,r)$ ，所以 $(n,r)=1$

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

实例

例 10

(1) 设 $G=\{e, a, \ldots, a^{11}\}$ 是 12 阶循环群，则 $\phi(12)=4$.

小于 12 且与 12 互素的数是 1, 5, 7, 11, 由定理 8.13 可知 a, a^5, a^7 和 a^{11} 是 G 的生成元 .

(2) 设 $G=<Z_9,\oplus>$ 是模 9 的整数加群，则 $\phi(9)=6$.

小于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理 8.13 ， G 的生成元是 1, 2, 4, 5, 7 和 8.

(3) 设 $G=3Z=\{3z \mid z\in Z\}$, G 上的运算是普通加法 . 那么 G 只有两个生成元 : 3 和– 3.

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

循环群的子群

定理 8.14 设 $G=\langle a\rangle$ 是循环群 .

(1) G 的子群仍是循环群 .

(2) 若 $G=\langle a\rangle$ 是无限循环群，则 G 的子群除 $\{e\}$ 以外都是无限循环群 .

(3) 若 $G=\langle a\rangle$ 是 n 阶循环群，则对 n 的每个正因子 d ， G 恰好含有一个 d 阶子群 .

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

定理 8.14 设 $G=\langle a\rangle$ 是循环群.

(1) G 的子群仍是循环群.

证 (1) 设 H 是 $G=\langle a\rangle$ 的子群，若 $H=\{e\}$，显然 H 是循环群，

否则取 H 中的最小正方幂元 a^m，下面证明 $H=\langle a^m\rangle$.

易见 $\langle a^m\rangle \subseteq H$.

下面证明 $H\subseteq\langle a^m\rangle$.

为此，只需证明 H 中任何元素都可表成 a^m 的整数次幂.

任取 $a^l\in H$，由除法可知存在整数 q 和 r，使得

$$l = qm+r \quad , \quad \text{其中} \quad 0\le r\le m-1$$

$$a^r = a^{l-qm} = a^l(a^m)^{-q}$$

由 $a^l, a^m\in H$ 且 H 是 G 的子群可知 $a^r\in H$.

因为 a^m 是 H 中最小正方幂元，必有 $r=0$. 这就推出 $a^l=(a^m)^q\in\langle a^m\rangle$

定理 8.14 设 G=<a> 是循环群 .

(2) 若 G=<a> 是无限循环群，则 G 的子群除 {e} 以外都是无限循环群 .

(3) 若 G=<a> 是 n 阶循环群，则对 n 的每个正因子 d ， G 恰好含有一个 d 阶子群 .

(2) 设 $G=\langle a\rangle$ 是无限循环群， H 是 G 的子群 .

若 $H\neq\{e\}$ 可知 $H=\langle a^m\rangle$ ，其中 a^m 为 H 中最小正方幂元 .

假若 $|H|=t$ ，则 $|a^m|=t$ ，从而得到 $a^{mt}=e$. 这与 a 为无限阶元矛盾 .

(3) 设 $G=\langle a\rangle$ 是 n 阶循环群，则 $G=\{a^0=e, a^1, \ldots, a^{n-1}\}$

下面证明对于 n 的每个正因子 d 都存在一个 d 阶子群 .

易见 $H=\langle a^{n/d}\rangle$ 是 G 的 d 阶子群 .

假设 $H_1=\langle a^m\rangle$ 也是 G 的 d 阶子群，其中 a^m 为 H_1 中的最小正方幂元 . 则由 $(a^m)^d=e$ 可知 n 整除 md ，即 n/d 整除 m.

令 $m=(n/d)\cdot l$ ， l 是整数，则有

$$a^m=(a^{n/d})^l\in H$$

这就推出 $H_1\subseteq H$. 又由于 $|H_1|=|H|=d$ ，得 $H_1=H$.

8.3 特殊的群——阿贝尔群、循环群和置换群

实例

例 11

(1) $G=\langle Z,+\rangle$ 是无限循环群，其生成元为 1 和– 1.

对于自然数 $m\in N$ ， 1 的 m 次幂是 m ， m 生成的子群是 mZ ， $m\in N$. 即

$$\langle 0\rangle = \{0\} = 0Z$$

$$\langle m\rangle = \{mz \mid z\in Z\} = mZ \quad , \quad m>0$$

(2) $G=Z_{12}$ 是 12 阶循环群 . 12 正因子是 1,2,3,4,6 和 12 ， G 的子群 :

1 阶子群 $\langle 12\rangle=\langle 0\rangle=\{0\}$

2 阶子群 $\langle 6\rangle=\{0,6\}$

3 阶子群 $\langle 4\rangle=\{0,4,8\}$

4 阶子群 $\langle 3\rangle=\{0,3,6,9\}$

6 阶子群 $\langle 2\rangle=\{0,2,4,6,8,10\}$

12 阶子群 $\langle 1\rangle=Z_{12}$

北京科技大学 University of Science and Technology Beijing

练习

设 G=<a> 是 12 阶循环群。

1 ）求出 G 的所有生成元；

2 ）求出 G 的所有子群

北京科技大学 University of Science and Technology Beijing

作业

- **补充习题 8.3**

设 G=<a> 是 15 阶循环群。

1) 求出 G 的所有生成元；

2) 求出 G 的所有子群

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

n 元置换及乘法

定义 8.11 设 $S=\{1, 2, \ldots, n\}$, S 上的任何双射函数

$\sigma: S \to S$ 称为 S 上的 **n 元置换**.

例如 $S=\{1, 2, 3, 4, 5\}$, 下述为 5 元置换

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

定义 8.12 设 σ, τ 是 n 元置换, σ 和 τ 的复合 $\sigma \circ \tau$ 也是 n 元置换, 称为 **σ 与 τ 的乘积**, 记作 $\sigma\tau$.

例如

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$$

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

k 阶轮换

定义 8.13 设 σ 是 $S = \{1, 2, \ldots, n\}$ 上的 n 元置换，若 $\sigma(i_1)=i_2, \sigma(i_2)=i_3, \ldots, \sigma(i_{k-1})=i_k, \sigma(i_k)=i_1$，且保持 S 中的其他元素不变，则称 σ 为 S 上的 **k 阶轮换**，记为 $(i_1,i_2,\ldots,i_k)$.

若 k=2，则称 σ 为 S 上的**对换**.

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

n 元置换的轮换表示

设 $S=\{1, 2, \ldots, n\}$，对于任何 S 上的 n 元置换 σ，存在着一个有限序列 $i_1, i_2, \ldots, i_k$, $k \geq 1$, (可以取 $i_1=1$) 使得

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

令 $\sigma_1=(i_1\ i_2 \ldots i_k)$, 是 σ 分解的第一个轮换．将 σ 写作 $\sigma_1\sigma'$,

继续对 σ' 分解．由于 S 只有 n 个元素，经过有限步得到

$$\sigma=\sigma_1\sigma_2 \ldots \sigma_t$$

轮换分解式的特征

轮换的不交性（以上任何两个轮换都作用于不同的元素上）

分解的惟一性： 若 $\sigma=\sigma_1\sigma_2 \ldots \sigma_t$ 和 $\sigma=\tau_1\tau_2 \ldots \tau_s$ 是σ的两个轮换表示式，则有

$$\{\sigma_1, \sigma_2, \ldots, \sigma_t\}=\{\tau_1, \tau_2, \ldots, \tau_s\}$$

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

实例

例 12 设 $S = \{1, 2, \dots, 8\}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 2 & 6 & 7 & 5 & 3 \end{pmatrix}$$

则 轮换分解式为：

□ $\sigma = (1\ 5\ 2\ 3\ 6)\ (4)\ (7\ 8) = (1\ 5\ 2\ 3\ 6)\ (7\ 8)$

$\tau = (1\ 8\ 3\ 4\ 2)\ (5\ 6\ 7)$

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

置换的对换分解

设 $S=\{1,2,\ldots,n\}$ ，$\sigma=(i_1\ i_2\ \ldots\ i_k)$ 是 S 上的 k 阶轮换， σ 可以进一步表成对换之积，即

$$(i_1\ i_2\ \ldots\ i_k)=(i_1\ i_2)\ (i_1\ i_3)\ \ldots\ (i_1\ i_k)$$

任何 n 元置换表成轮换之积，然后将每个轮换表成对换之积 .

例如 8 元置换

$\sigma=(1\ 5\ 2\ 3\ 6)\ (7\ 8)=(1\ 5)\ (1\ 2)\ (1\ 3)\ (1\ 6)\ (7\ 8)$

$\tau=(1\ 8\ 3\ 4\ 2)\ (5\ 6\ 7)=(1\ 8)\ (1\ 3)\ (1\ 4)\ (1\ 2)\ (5\ 6)\ (5\ 7)$

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

对换分解的特征

对换分解式中对换之间可以有交，分解式也不惟一 .

例如 4 元置换

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

可以有下面不同的对换表示：

$\sigma = (1\ 2)\ (1\ 3)$ ， $\sigma = (1\ 4)\ (2\ 4)\ (3\ 4)\ (1\ 4)$

表示式中所含对换个数的奇偶性是不变的 .

如果 n 元置换σ 可以表示成奇数个对换之积，则称σ为**奇置换**，否则称为**偶置换**，不难证明奇置换和偶置换各有 $n!/2$ 个 .

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

n 元置换群

所有的 n 元置换构成的集合 S_n 关于置换乘法构成群，称为 **n 元对称群**．其中恒等置换是它的单位元（又称**幺置换**）。n 元对称群的子群称为 **n 元置换群**。

例 13 设 $S=\{1, 2, 3\}$ ，

3 元对称群 $S_3=\{ (1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$

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

北京科技大学 University of Science and Technology Beijing

8.3 特殊的群——阿贝尔群、循环群和置换群

S_n 的子群

设 A_n 是所有的 n 元偶置换的集合．则 A_n 是 S_n 的子群，称为 n 元交错群。

证 恒等置换 (1) 是偶置换，所以 A_n 非空．

根据判定定理三，只需证明封闭性：

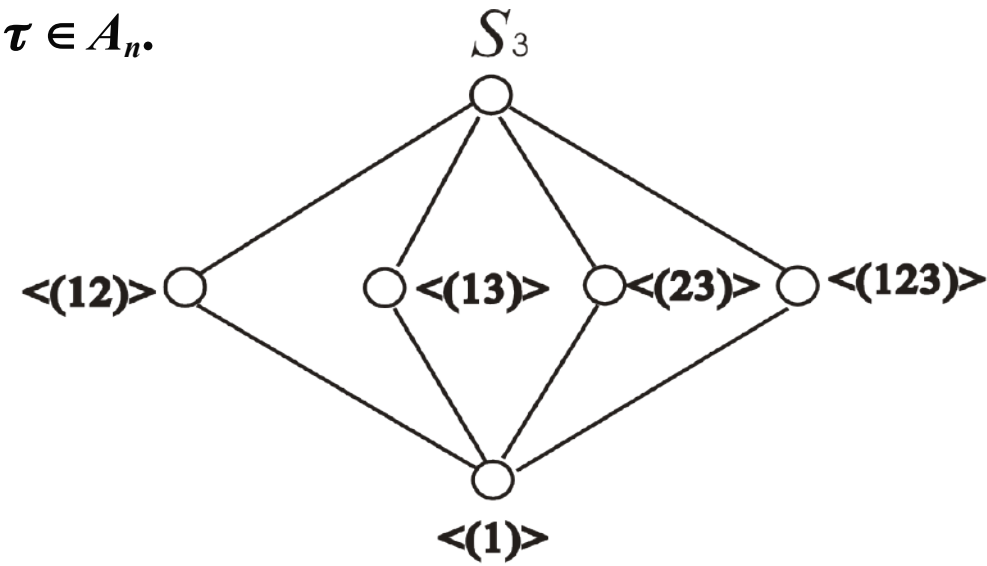
任取$\sigma,\tau\in A_n$，σ，τ 都可以表成偶数个对换之积，那么$\sigma\tau$

也可以表成偶数个对换之积，所以$\sigma\tau\in A_n$.

实例：S_3 的子群格

S_3={(1), (12), (13), (23),
(123), (132)},

A_3={(1), (123), (132)},
{(1)},
{(1), (12)}, {(1), (13)},
{(1), (23)}.



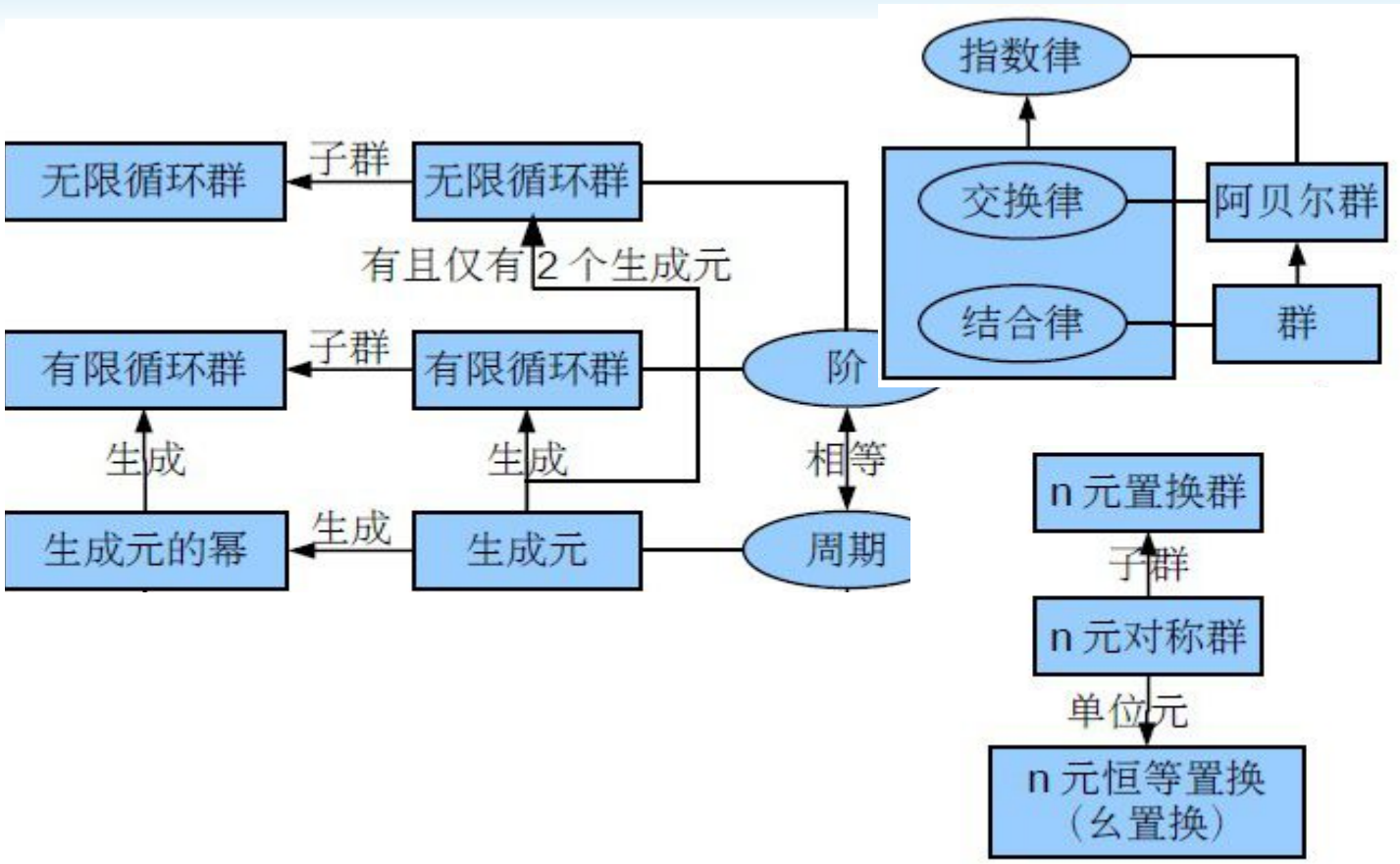
北京科技大学 University of Science and Technology Beijing

小结

- 适合交换律的群称为阿贝尔群，阿贝尔群适合指数律。
- 由一个元素的幂构成的群称为循环群，循环群中各元素的的阶是循环群的重要性质。
- 由 n 元置换的集合和置换的复合构成的群称为 n 元置换群，特别地，由全部 n 元置换构成的群称为 n 元对称群。

北京科技大学 University of Science and Technology Beijing

小结



北京科技大学
University of Science and Technology Beijing