Group Theory(2)

Normal Subgroup,Homomorphism,and Permutation Group

Hengfeng Wei
hengxin0912@gmail.com

Department of Computer Science and Technology, NJU

April 26, 2011

Outline

Permutation Group

概念之间的关系辨析:

For $X \neq \emptyset$:

- 对称群(*Symmetric group*): 非空集合X上的一一变换关于合成运算所构成的群S_X.
- 变换群(*Transformation group*): S_X的任一子群.

For $|X| = n$:

- n阶置换(*Permutation*): X上的一一变换
- n次对称群: S_n
- 置换群(*Permutation group*): S_n的子群.

Cayley Theorem

(Cayley Theorem, 1854)
每一个群都同构于一个变换群.

每一个有限群都同构与一个置换群.

证明要点:

1. $a \in G$, $\phi_a : \phi_a(x) = ax, \forall x \in G$. ϕ_a is a function.
2. $G_l = \{\phi_a \mid a \in G.\}$ 关于变换的合成构成S_G的子群.
3. $\rho : G \cong G_l . a \mapsto \phi_a, \forall a \in G$.

Cayley Theorem

(Cayley Theorem, 1854)
每一个群都同构于一个变换群.

每一个有限群都同构与一个置换群.

证明要点:

1. $a \in G$, $\phi_a : \phi_a(x) = ax, \forall x \in G$. ϕ_a is a function.
2. $G_l = \{\phi_a \mid a \in G.\}$ 关于变换的合成构成S_G的子群.
3. $\rho : G \cong G_l . a \mapsto \phi_a, \forall a \in G$.

重要意义:

> *"Cayley's theorem puts all groups on the same footing, by considering any group (including infinite groups such as* $(\mathbf{R}, +)$*) as a permutation group of some underlying set.*
> *Thus, theorems which are true for permutation groups are true for groups in general."*

Cayley Theorem

$$a \in G, \phi_a : \phi_a(x) = ax, \forall x \in G.$$

*Cayley*定理在运算表中的体现:

*	e	a	b	c	d	f	permutation
e	e	a	b	c	d	f	e
a	a	e	d	f	b	c	(12)(35)(46)
b	b	f	e	d	c	a	(13)(26)(45)
c	c	d	f	e	a	b	(14)(25)(36)
d	d	c	a	b	f	e	(156)(243)
f	f	b	c	a	e	d	(165)(234)

Figure: Cayley Theorem for S_3

Permutation

置换:
X为非空集合，且$|X|=n$，则其上定义的双射称为X上的n元置换。

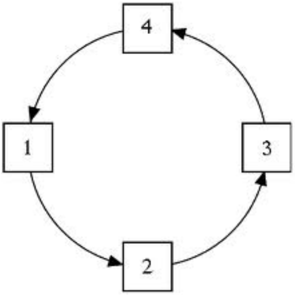
$$e=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad \alpha=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad \beta=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$
$$\gamma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad \delta=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\quad \varepsilon=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

Q: S_3 是最小的非交换群?

Cycle

轮换:

$$\sigma = (i_1 i_2 \cdots i_r).$$



Cycle

轮换的性质:

$$\sigma,\tau \text{ 为轮换且不相交,则} \sigma\tau = \tau\sigma.$$

Figure: $\sigma\tau = \tau\sigma$

Remember: 轮换也是函数！要证明两个函数相等，可考虑他们对于每个元素的作用是相同的。通常，需要对元素进行适当分类。

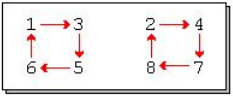
Permutation $\to$ Cycle

用轮换表示置换:

(1) 每一个置换可表为一些不相交的轮换的乘积.

(2) n阶置换的轮换分解式在不计次序的情况下是唯一的.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 7 & 6 & 8 \\ 3 & 4 & 5 & 7 & 6 & 8 & 1 & 2 \end{pmatrix} = (1356)(2478)$$



Permutation → Transposition

对换:
每一置换都可表为对换的乘积.

$$\sigma = (i_1 i_2 \cdots i_r) = (i_1 i_2)(i_1 i_3)\cdots(i_1 i_r).$$

Q: 置换的对换表示是唯一的吗?
如果不唯一,在不同的表示方式中有什么性质是保持不变的(不变式!!!)吗?

Permutation $\to$ Transposition

Parity of Permutation

每一个置换表为对换的乘积，所用对换个数的奇偶性是唯一的.

证明要点:

Insight: σ的对换表示中对换个数与排列$i_1, i_2, \cdots, i_n$的逆序数同奇偶(唯一).

群同态:

$$\mathrm{sgn} : S_n \to \{-1, 1\}.$$

Permutation → Transposition

计数:

$n \geq 2$阶置换中，偶置换与奇置换各有$\frac{n!}{2}$个.

- $f : A_n \to B_n : p \in A_n, f(p) = (a_1, a_2)p.$
- $g : B_n \to A_n : p \in B_n, g(p) = (a_1, a_2)p.$

n次交错群(Alternating group)

在S_n中，全体偶置换构成S_n的子群,称为n次交错群.

举例:

$$A_3 = \{(1), (123), (132)\}.$$

Q: 为什么不研究全体奇置换的集合?

Outline

1. Review
   - Permutation Group
   - Normal Subgroup and Quotient Group
   - Fundamental Theorem over Homomorphism
2. Problem Set
   - Permutation Group
   - Normal Subgroup and Quotient Group
   - Fundamental Theorem over Homomorphism
3. Applications and Extension(Optional)
   - Permutation Group Behind 15-Puzzle

Normal Subgroup

正规子群:

$(H,*) \lhd (G,*) : (H,*) \leq (G,*), (\forall a \in G)(aH = Ha).$

特别提醒:$\forall h \in H, \exists h' \in H, gh = h'g (g \in G).$

举例:

- 平凡群$(\{e\},*)$和G是正规子群。$((\forall a \in G)(aG = G = Ga).)$
- 交换群G的一切子群都是G的正规子群。
- 群G的中心C是G的正规子群。
  $(C = \{a \mid a \in G \wedge \forall x \in G(ax = xa)\}.)$

Normal Subgroup

正规子群判定定理:
G为群，H为G的子群，则:

$$H \lhd G \Leftrightarrow (\forall g \in G, \forall h \in H)(ghg^{-1} \in H).$$

Quotient Group

商群:

设G是群，H是G的正规子群，则H的所有陪集组成的集合

$$G/H = \{Ha \mid a \in G\}.$$

关于陪集的乘法运算$(Ha) \cdot (Hb) = H(ab)$构成群，称为G关于H的商群。

正规子群的陪集集合提供了看待群的一种视角。一种视角就是一种抽象。它与普通子群的抽象的区别在于它保持了运算。

Quotient Group

商群:

设G是群，H是G的正规子群，则H的所有陪集组成的集合

$$G/H = \{Ha \mid a \in G\}.$$

关于陪集的乘法运算$(Ha)\cdot(Hb) = H(ab)$构成群，称为G关于H的商群。

正规子群的陪集集合提供了看待群的一种视角。一种视角就是一种抽象。它与普通子群的抽象的区别在于它保持了运算。

证明:

1. 运算的封闭性($Ha \cdot Hb = H(ab) \in G/H$.)
2. 结合律($(Ha \cdot Hb)\cdot Hc = Ha \cdot (Hb \cdot Hc)$.)
3. 单位元($He = H$.)
4. 逆元($(Ha)^{-1} = Ha^{-1}$.)

Quotient Group

商群:
设G是群，H是G的正规子群，则H的所有陪集组成的集合

$$G/H = \{Ha \mid a \in G\}.$$

关于陪集的乘法运算$(Ha) \cdot (Hb) = H(ab)$构成群，称为G关于H的商群。

正规子群的陪集集合提供了看待群的一种视角。一种视角就是一种抽象。它与普通子群的抽象的区别在于它保持了运算。

证明:

1. 运算的封闭性$(Ha \cdot Hb = H(ab) \in G/H.)$
2. 结合律$((Ha \cdot Hb) \cdot Hc = Ha \cdot (Hb \cdot Hc).)$
3. 单位元$(He = H.)$
4. 逆元$((Ha)^{-1} = Ha^{-1}.)$

Q: 此证明哪里体现了正规子群的必要性?
如果没有，为什么只考虑在正规子群之上定义商群呢?

Quotient Group

良定义(well-defined)的运算:

$$(Ha)\cdot(Hb)=H(ab).$$

要求: H的任意两个陪集Ha, Hb的乘积是唯一确定的,与陪集代表元的选取无关

$Ha'=Ha, Hb'=Hb,$

$Ha'\cdot Hb'=H(a'b')=(Ha')b'=(Ha)b'=(aH)b'$

$=a(Hb')=a(Hb)=(aH)b=(Ha)b=H(ab)=(Ha)\cdot(Hb).$

Quotient Group

良定义(well-defined)的运算:

$$(Ha)\cdot(Hb) = H(ab).$$

要求: H的任意两个陪集Ha, Hb的乘积是唯一确定的,与陪集代表元的选取无关

$Ha' = Ha, Hb' = Hb,$

$Ha' \cdot Hb' = H(a'b') = (Ha')b' = (Ha)b' = (aH)b'$

$= a(Hb') = a(Hb) = (aH)b = (Ha)b = H(ab) = (Ha)\cdot(Hb).$

举例:

在群S_3中, $H = \{(1), (1,2)\}.$

$H(1,3) = \{(1,3), (1,3,2)\} = H(1,3,2).$

$H(2,3) = \{(2,3), (1,2,3)\} = H(1,2,3).$

然而, $H(1,3)\cdot H(2,3) = H(1,2,3).$

$H(1,3,2)\cdot H(1,2,3) = H(1).$

Outline

1. Review
   - Permutation Group
   - Normal Subgroup and Quotient Group
   - Fundamental Theorem over Homomorphism
2. Problem Set
   - Permutation Group
   - Normal Subgroup and Quotient Group
   - Fundamental Theorem over Homomorphism
3. Applications and Extension(Optional)
   - Permutation Group Behind 15-Puzzle

Homomorphism

同态:

$\phi : G \to G'$:

$$\phi(ab) = \phi(a)\phi(b).$$

同态保持了群双方的运算性质. 同态是一种抽象过程, 忽略了等价类中个体之差异, 只考虑共有之特性.

$$\begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix} \Rightarrow -1 \qquad \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} \Rightarrow +1$$

$$\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix} \Rightarrow -1 \qquad \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} \Rightarrow +1$$

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix} \Rightarrow -1 \qquad \begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} \Rightarrow +1$$

Homomorphism

G为群，H为G的正规子群,定义自然同态：

$$\sigma : G \to G/H.(a \mapsto Ha.)$$

$$\sigma : G \to G'.H \leq G, K \leq G'.$$

1. $\sigma(H)$是G'的子群.
2. $\sigma^{-1}(K)$是G的子群.
3. 如果H是G的正规子群，则$\sigma(H)$是$\sigma(G)$的正规子群.
4. 如果K是G'的正规子群，则$\sigma^{-1}(K)$是G的正规子群.
5. $Ker\sigma$是G的正规子群.

Fundamental Thorem over Homomorphism

群同态基本定理:
设σ是群G到群G'的满同态， $K = Ker\sigma$, 则

$$G/K \cong G'.$$

- 从同构的观点看，群的同态像就是群的商群.
- 同态核可以看作是群与其同态像之间相似度的一个度量.

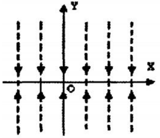
Fundamental Thorem over Homomorphism

两个简单的例子:

$$G = \{\alpha = (a, b) \mid a, b \in R\},$$
$$\bar{G} = \{a \mid a \in R\}.$$
$$\phi : (a, b) \mapsto a, \forall (a, b) \in G.$$

$\mathrm{Ker}\varphi = \{(0, y) | y \in R\} = N$ (即 Y 轴上的所有点).

$G/\mathrm{Ker}\varphi = \{(a, 0) + N | a \in R\} = \{[0], [a], [b], [c], \cdots\}$



$$\phi : Z \to Z_n;$$
$$a \mapsto \bar{a}.$$
$$Z/\langle n\rangle \cong Z_n.$$

Fundamental Thorem over Homomorphism

利用群同态基本定理证明商群同构:

(1) 第一同构定理:

设ϕ是群G到G'的同态.则

$$G/\mathrm{Ker}\phi \cong \phi(G).$$

(2) 第二同构定理:

设$H \leq G, K \lhd G$, 则

$$HK/K \cong H/(H \cap K).$$

(3) 第三同构定理:

设$H \lhd G, K \lhd G, K \subseteq H$, 则

$$G/H \cong (G/K)/(H/K).$$

Outline

Permutation Group

试证明:

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}.$$

则对任一n阶置换σ,有

$$\sigma^{-1}\tau\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(k_1) & \sigma(k_2) & \cdots & \sigma(k_n) \end{pmatrix}.$$

解答: 置换是函数。如何证明函数相等?

Permutation Group

试证明:

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}.$$

则对任一n阶置换σ,有

$$\sigma^{-1}\tau\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(k_1) & \sigma(k_2) & \cdots & \sigma(k_n) \end{pmatrix}.$$

解答: 置换是函数。如何证明函数相等?

Q: What if $\tau = (a_1, a_2, \cdots, a_k)$?

Permuation Group

试验证:

$(i_k a \cdots b), (i_n c \cdots d)$不相交,则

$$(i_k, i_n)(i_k, a, \cdots, b)(i_n, c, \cdots, d) = (i_k, a, \cdots, b, i_n, c, \cdots, d).$$

$$(i_k, i_n)(i_k, a, \cdots, b, i_n, c, \cdots, d) = (i_k, a, \cdots, b)(i_n, c, \cdots, d).$$

Permuation Group

试验证:

$(i_k a\cdots b), (i_n c\cdots d)$不相交,则

$$(i_k,i_n)(i_k,a,\cdots,b)(i_n,c,\cdots,d)=(i_k,a,\cdots,b,i_n,c,\cdots,d).$$

$$(i_k,i_n)(i_k,a,\cdots,b,i_n,c,\cdots,d)=(i_k,a,\cdots,b)(i_n,c,\cdots,d).$$

简单介绍另一种“置换可表为不相交轮换之积”的证明方法。

Permutation Group

已知$\sigma^3 = (1,4,3,7,5,6,2)$,求$\sigma$.

解答:

Permutation Group

已知$\sigma^3 = (1,4,3,7,5,6,2)$,求$\sigma$.

解答:

$\sigma = (1,6,7,4,2,5,3)$.

Outline

Normal Subgroup

请证明:

在S_4中，令

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

K是S_4的正规子群.

提示:

$$\sigma^{-1}\tau\sigma = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ \sigma(k_1) & \sigma(k_2) & \cdots & \sigma(k_n) \end{pmatrix}.$$

Normal Subgroup

请证明:

设H, K都是G的子群。如果$H \lhd G$且$H \subseteq K$, 则$H \lhd K$。

Normal Subgroup

请证明:

$$\sigma : G \to G', \text{为同态映射}, H \le G, K \le G'.$$

1. $\sigma(H)$是G'的子群.
2. $\sigma^{-1}(K)$是G的子群.
3. 如果H是G的正规子群，则$\sigma(H)$是$\sigma(G)$的正规子群.
4. 如果K是G'的正规子群，则$\sigma^{-1}(K)$是G的正规子群.
5. $Ker\sigma$是G的正规子群.

Normal Subgroup

请证明:

设G为群，H_1, H_2为G的正规子群。则$H_1 \cap H_2, H_1 H_2$ 都是G的正规子群。

Q: 如果$H, K \leq G, \neg(H, K \lhd G)$?

Outline

Fundamental Theorem over Homomorphism

应用(*apply*)群同态基本定理证明与商群相关的同构关系的例题，请参见文件《离散数学习题解析第八周》。该文件已上传至教学网站。

Outline

1. Review
   - Permutation Group
   - Normal Subgroup and Quotient Group
   - Fundamental Theorem over Homomorphism
2. Problem Set
   - Permutation Group
   - Normal Subgroup and Quotient Group
   - Fundamental Theorem over Homomorphism
3. Applications and Extension(Optional)
   - Permutation Group Behind 15-Puzzle

Permutation Group Behind 15-Puzzle

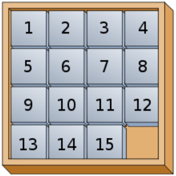


Figure: The starting position for the 15-puzzle.

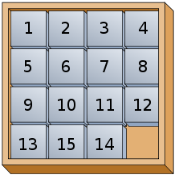


Figure: The unsolvable case for the 15-puzzle.

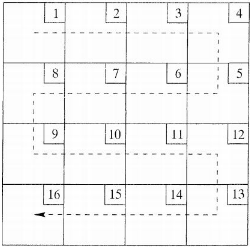


Figure: The dashed line and the numbers indicate a special ordering of the cells.

Permutation Group Behind 15-Puzzle

使用置换群建模:

Placement: blocks $\rightarrow$ cells.

Problem: placements 变化繁多.

More Insight: "以不变应万变"

Slot:

block i 在cell j处:

如果blank 在cell $k > j$处，则称"block i is in slot j";

否则，称"block i is in slot $(j-1)$".

Configuration:

$$[a_1, a_2, \cdots, a_{15}].$$

Q: Where is the blank block in the config.?

Permutation Group Behind 15-Puzzle

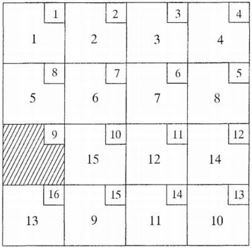


Figure: An example for configuration.

$$C = [1, 2, 3, 4, 8, 7, 6, 5, 14, 12, 13, 10, 15, 11, 9].$$

考察基本元素：Moves

$$
\begin{aligned}
\sigma_{1,8} &= (1, 2, 3, 4, 5, 6, 7) \\
\sigma_{2,7} &= (2, 3, 4, 5, 6) \\
\sigma_{3,6} &= (3, 4, 5) \\
\sigma_{5,12} &= (5, 6, 7, 8, 9, 10, 11) \\
\sigma_{6,11} &= (6, 7, 8, 9, 10) \\
\sigma_{7,10} &= (7, 8, 9) \\
\sigma_{9,16} &= (9, 10, 11, 12, 13, 14, 15) \\
\sigma_{10,15} &= (10, 11, 12, 13, 14) \\
\sigma_{11,14} &= (11, 12, 13) \\
\sigma_{n,n+1} &= id, n = 1, 2, \ldots, 15 \\
\sigma_{i,j} &= \sigma_{j,i}^{-1} \quad \text{for all relevant } i > j
\end{aligned}
$$

Figure: Moving the blank from cell i to j effects the permutation $\sigma_{i,j}$.

Permutation Group Behind 15-Puzzle

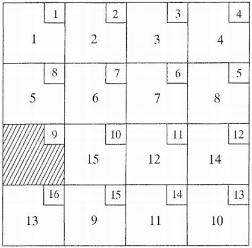


Figure: An example for configuration.

$$C = [1, 2, 3, 4, 8, 7, 6, 5, 14, 12, 13, 10, 15, 11, 9].$$

考察基本元素：Moves

$$
\begin{aligned}
\sigma_{1,8} &= (1,2,3,4,5,6,7)\\
\sigma_{2,7} &= (2,3,4,5,6)\\
\sigma_{3,6} &= (3,4,5)\\
\sigma_{5,12} &= (5,6,7,8,9,10,11)\\
\sigma_{6,11} &= (6,7,8,9,10)\\
\sigma_{7,10} &= (7,8,9)\\
\sigma_{9,16} &= (9,10,11,12,13,14,15)\\
\sigma_{10,15} &= (10,11,12,13,14)\\
\sigma_{11,14} &= (11,12,13)\\
\sigma_{n,n+1} &= id,\ n = 1,2,\ldots,15\\
\sigma_{i,j} &= \sigma_{j,i}^{-1} \quad \text{for all relevant } i > j
\end{aligned}
$$

Figure: Moving the blank from cell i to j effects the permutation $\sigma_{i,j}$.

Identifying the subgroup of S_{15} generated by these 18 cycles!

Permutation Group Behind 15-Puzzle

It is actually A_{15}!

非完全严格证明:

1. The 18 cycles generate all *consecutive* 3-cycles in S_{15}.
2. The *consecutive* 3-cycles generate all cycles in $S_n (n \geq 3)$.
3. The 3-cycles generate $A_n (n \geq 3)$.

$(1,2,\ldots,7)^{-n}(3,4,5)(1,2,\ldots,7)^{n}$ yields $(1,2,3),\ldots,(5,6,7)$;

$(5,6,\ldots,11)^{-n}(7,8,9)(5,6,\ldots,11)^{n}$ yields $(5,6,7),\ldots,(9,10,11)$ ar

$(9,10,\ldots,15)^{-n}(11,12,13)(9,10,\ldots,15)^{n}$ yields $(9,10,11),\ldots,(13,14,$

$$(a,b)(c,d) = (a,b,c)(a,d,c) \qquad (1)$$
$$(a,b)(b,c) = (a,c,b) \qquad (2)$$
$$(a,b)(a,b) = Id \qquad (3)$$

That's the end. Thank you.

Figure: Bring Up a Question