Group Theory(1)

Group,Subgroup,Lagrange Theorem, and Cyclic Group

Hengfeng Wei
hengxin0912@gmail.com

Department of Computer Science and Technology, NJU

April 13, 2011

1. Review
   - Concept of Group
     - Subgroup and Lagrange Theorem
   - Cyclic Group

2. Problem Set
   - Homework
   - Concept of Group
   - Subgroup and Lagrange Theorem
   - Cyclic Group

3. Applications and Extension(Optional)
   - Solitaire and Klein 4-group

Outline

From the Particular ···

Figure: Rubik success in twenty-six steps.

Basic Move:

$$L, R, U, D, F, B$$

General Move:
M: any sequence of these 6 basic moves

One Move After Another:
$M_1 * M_2$

Q: Is set of moves under $*$ a group?

From the Particular $\cdots$

Figure: Rubik success in twenty-six steps.

Focus on moves involving D and F:

Q: Is it a subgroup ?
What are its cosets?

Keep Moving:

$$R * R * R * R = \mathbf{I}.$$

Q: Is it a cyclic group ?

More and More $\cdots$
"Group Theory and the Rubik's Cube" by Janet Chen.

... to the general

群论公理:
$(G,*)$为群当且仅当有$e\in G$和G上一元运算(-1)使得

1. $G\neq\emptyset$
2. $(\forall x,y\in G)(x*y\in G)$
3. $(\forall x,y,z\in G)(x*(y*z)=(x*y)*z)$
4. $(\forall x\in G)(x*e=e*x=x)$
5. $(\forall x\in G)(x*x^{-1}=x^{-1}*x=e)$

Examples of Group

重要群举例:

1. $\langle \mathbf{Z}, + \rangle$
2. $\langle \mathbf{Z}_n, \oplus \rangle$
3. $U(m)$关于模m乘法构成群
$U(m) = \{a \in \mathbf{Z}_m \mid (a, m) = 1\}$

(To Problem Set)

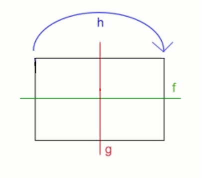
举例:

$m = 10, U(m) = \{1, 3, 7, 9\}$.

$m = 11, U(m) = \{1, 2, \cdots, 9, 10\}$.

Klein 4-group:

$(P_{181}(10.2))$



x	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

Property of Group

G是群,

1. G的单位元唯一
2. G中每个元素的逆元唯一
3. $\forall x \in G, (x^{-1})^{-1} = x.$
4. $\forall x, y \in G, (xy)^{-1} = y^{-1}x^{-1}.$
5. $\forall x \in G, x^n x^m = a^{n+m}.$
6. $\forall x \in G, (a^n)^m = a^{nm}.$
7. 在群中消去律成立
   $\forall a, b, c \in G, ab = ac \vee ba = ca \rightarrow b = c.$

Order of Elements of Group

元素的阶:

$a \in G$, 使得等式$a^k = e$成立的最小正整数k称为a的阶,记为$|a| = k$.

有限群关于阶的概念的重要结论:

1. 有限群中不存在无限阶元。
2. $\forall a \in G, |a| = |a^{-1}|$ $(P_{184}(2))$
   1. 有限群中阶大于2的元素有偶数个。$(a^2 = e \Leftrightarrow a = a^{-1})$
   2. 偶数阶群中阶为2的元素为奇数个。 $(P_{203}(18))$
3. $|a| = n, a^m = e \rightarrow n \mid m$ $(P_{184}(1))$
4. $|ab| = |ba|$ $(|ab| = \infty?)$ $(P_{185}(2))$
5. $|b^{-1}ab| = |a|$. $(P_{185}(1))$

Subgroup

通过局部来认识整体,我们需要研究子群。

$(G, *, e, -1)$为群, $H \subseteq G$, 若

1. $(\forall x, y \in H)(x * y \in H)$ $(Closure)$
2. $e \in H$ $(Indentity)$
3. $(\forall x \in H)(x^{-1} \in H)$ $(Inverses)$

则称$(H, *)$是$(G, *)$的子群.

举例:

- $(\{e\}, *)$,$(G, *)$
- $(b\mathbf{Z}, +) \leq (\mathbf{Z}, +)$
- $C(G) = \{g \in G \mid gx = xg, \forall x \in G\}$ (center)

Subgroup

Q_1: 如何判定某子集是否构成子群?

Q_2: 如何求出某给定群的所有子群?

子群判定定理:

1.
   1. $H \neq \emptyset$
   2. $(\forall a, b \in H)(ab \in H)$
   3. $(\forall a \in H)(a^{-1} \in H)$
2.
   1. $H \neq \emptyset$
   2. $(\forall a, b \in H)(ab^{-1} \in H)$

Coset

陪集:

$H \leq G, a \in G, Ha = \{ha \mid h \in H\}$.
称Ha是子群H在G中的右陪集。

陪集举例:

$(H = \{0, 3\}, \oplus) \leq (Z_6, \oplus)$

$H0 = H = H3$
$H1 = \{1, 4\} = H4$
$H2 = \{2, 5\} = H5$

问题:

- 在什么情况下,H的一个右陪集aH是G的子群?
- 在什么条件下,G的两个不同的元素a和b生成同一个右陪集?

Coset

子群将群分解成陪集。

$H \leq G, a, b \in G:$

1. $a \in Ha.$
2. $Ha = H \Leftrightarrow a \in H.$ (集合相等!)
3. Ha 为子群 $\Leftrightarrow a \in H.$
4. $Ha = Hb \Leftrightarrow a \in Hb \Leftrightarrow b \in Ha \Leftrightarrow ab^{-1} \in H \Leftrightarrow ba^{-1} \in H.$
5. $Ha = Hb \vee Ha \cap Hb = \emptyset.$

举例:

$H = \{3n \mid n \in Z\}, (H, +) \leq (Z, +)$

$Ha = Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow a - b \in H \Leftrightarrow a \equiv b(mod3)$

Lagrange Theorem

子群与陪集之间的阶的关系:

1. $f: Ha \to a^{-1}H$.
2. $|Ha| = |Hb| = |H|$.

Lagrange 定理:
$(G,*)$为有限群,$H \leq G$, 则$|G| = |H| \cdot [G: H]$.

$$[G: H] = r, G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_r$$

Appliaction of Lagrange Theorem

Lagrange定理对分析有限群中元素的阶很有用。

1. 有限群G的子群H的阶数及其它在G中的指数,都是群G的阶数的因子.
2. 有限群G, $a \in G$, $|a| = |\langle a \rangle|$,均是$|G|$的因子.
3. $|G| = n, a \in G, a^n = e$.
4. 设G是素数阶群,则存在$a \in G$, $G = \langle a \rangle$.

Outline

1. Review
   - Concept of Group
     - Subgroup and Lagrange Theorem
   - Cyclic Group
2. Problem Set
   - Homework
   - Concept of Group
   - Subgroup and Lagrange Theorem
   - Cyclic Group
3. Applications and Extension(Optional)
   - Solitaire and Klein 4-group

Cyclic Group

定义:

设G是群，如果存在$a \in G, G = \langle a \rangle$, 则称$G$为循环群。

举例:

- 整数加群$(\mathbf{Z}, +)$是无限循环群。
- 模m整数加群$(\mathbf{Z}_m, \oplus_m)$是m阶循环群。

Structure of Cyclic Group

循环群的结构定理:

1. 如果$G=\langle a\rangle$是无限循环群, 则$G\cong(\mathbf{Z},+)$;

$$G=\{e,a,a^{-1},a^2,a^{-2},a^3,a^{-3},\cdots\}.$$

2. 如果$G=\langle a\rangle$是n阶循环群,则$G\cong(\mathbf{Z}_n,\oplus_n)$.

$$G=\{e,a,a^2,a^3,\cdots,a^{n-1}\}.$$

Q: Where is a^{-1}?

在同构意义下,循环群有且仅有两种!

Generator of Cyclic Group

1. $(\mathbf{Z},+)$恰有两个生成元,即1与-1;
2. $(\mathbf{Z}_n,\oplus_n)$恰有$\varphi(n)$个生成元, $\{i \mid 0 < i \leq n \wedge (i,n) = 1\}$
   例如:
   $$\mathbf{Z}_{12} \text{ 的生成元为: } 1, 5, 7, 11.$$

Subgroup of Cyclic Group

1. $G=\langle a\rangle$是循环群，则G的子群H仍是循环群.
2. $G=\langle a\rangle$是无限循环群，其子群为

$$\{\langle a^d\rangle \mid d=0,1,2,\cdots\}$$

并且除$\{e\}$外，其余子群均为无限循环群.
例如:

$$((Z),+) \text{ 的子群为: } (n\mathbf{Z},+).$$

3. $G=\langle a\rangle$是n阶循环群,其子群为

$$\{\langle a^d\rangle \mid d \text{ 为} n \text{ 的正因子}\}.$$

例如:

$$\mathbf{Z}_{12} \text{ 的子群共6个:} \langle 1\rangle,\langle 2\rangle,\langle 3\rangle,\langle 4\rangle,\langle 6\rangle,\langle 12\rangle.$$

Outline

Homework

本次Homework习题解析已经上传，见“离散数学习题解析第六周(群论(1))”

Outline

$(U(m), \otimes_m)$

试证明:
设m是大于1的正整数,记$U(m) = \{a \in \mathbf{Z}_m \mid (a, m) = 1\}$,
则$U(m)$关于$\otimes_m$的乘法构成群。

举例:

$$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

$(U(m), \otimes_m)$

试证明:

设m是大于1的正整数,记$U(m) = \{a \in \mathbf{Z}_m \mid (a, m) = 1\}$,
则$U(m)$关于$\otimes_m$的乘法构成群。

举例:

$$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

数论知识:

在求元素$a \in U(m)$的逆元时，你可能会用到如下数论知识:
$(a, m) = 1 \Leftrightarrow (\exists u, v \in \mathbf{Z})(au + mv = 1)$. 请说明,$u$即是$a$的逆元.

解答:

$(U(m), \otimes_m)$

试证明:

设m是大于1的正整数,记$U(m) = \{a \in \mathbf{Z}_m \mid (a, m) = 1\}$,
则$U(m)$关于$\otimes_m$的乘法构成群。

举例:

$$U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$$

数论知识:

在求元素$a \in U(m)$的逆元时,你可能会用到如下数论知识:
$(a, m) = 1 \Leftrightarrow (\exists u, v \in \mathbf{Z})(au + mv = 1)$. 请说明,$u$即是$a$的逆元.

解答:

- 运算封闭性
- 结合律
- 单位元$(1 \in U(m))$
- 逆元$(au + mv = 1, a^{-1} = u.)$

3-order Group

试证明:在同构意义下,3阶群只有一种结构，即3阶循环群。

提示:

- 使用群表。
- 使用Lagrange Theorem。

Order of ab

一般不能由a, b的阶直接得到ab的阶。

证明以下命题:

有限群G, $a, b \in G, |a| = n, |b| = m, ab = ba \wedge (n, m) = 1 \Rightarrow |ab| = nm.$

方法:

设$|ab| = r$, 则需证:$(mn)|r$ 和$r|(mn)$, 也即$n|(rm), m|(rn), r|(mn)$.

还记得关于元素阶的那个重要结论吗?

$|a| = n, a^m = e \Leftrightarrow n \mid m$

解答:

Order of ab

一般不能由a, b的阶直接得到ab的阶。

证明以下命题:
有限群G， $a, b \in G, |a| = n, |b| = m, ab = ba \wedge (n, m) = 1 \Rightarrow |ab| = nm.$

方法:
设$|ab| = r$, 则需证:$(mn)|r$ 和$r|(mn)$, 也即$n|(rm), m|(rn), r|(mn).$
还记得关于元素阶的那个重要结论吗?
$|a| = n, a^m = e \Leftrightarrow n \mid m$

解答:

$a^{rm} = a^{rm} \cdot b^{rm} = (ab)^{rm} = e \Rightarrow n|(rm) \Rightarrow n|r.$
$(ab)^{mn} = e.$

-

Outline

1. Review
   - Concept of Group
     - Subgroup and Lagrange Theorem
   - Cyclic Group
2. Problem Set
   - Homework
   - Concept of Group
   - Subgroup and Lagrange Theorem
   - Cyclic Group
3. Applications and Extension(Optional)
   - Solitaire and Klein 4-group

Application of Lagrange Theorem

试证明Fermat小定理:
设p为素数,则对任意一个与p互素的整数a,有$a^{p-1} \equiv 1(\mathrm{mod}\ \mathrm{p})$.

提示:
已证:

$$U(m) = \{a \in \mathbf{Z}_m \mid (a, m) = 1\}$$

关于$\otimes_m$构成群。
请思考: 当m为素数p时, P_{190}推论1意味着什么?

解答:

Application of Lagrange Theorem

试证明Fermat小定理:
设p为素数,则对任意一个与p互素的整数a,有$a^{p-1} \equiv 1(\mathrm{mod\ p})$.

提示:
已证:

$$U(m) = \{a \in \mathbf{Z}_m \mid (a, m) = 1\}$$

关于$\otimes_m$构成群。
请思考: 当m为素数p时, P_{190}推论1意味着什么?

解答:
当$m = p$为素数时, $U(p)$的阶为$p - 1$.
a与p互素,$\therefore a \in U(p) \Rightarrow a^{(p-1)} = e = 1$

Application of Lagrange Theorem

试证明:在同构意义下,四阶群有且仅有两种.
对于每个四阶群$(G,*)$,
$(G,*) \cong (Z_4,+_4)$ 或$(G,*) \cong$ Klein 4-group.

提示:
使用Lagrange Theorem分析每个元素的可能的阶。

解答:

Application of Lagrange Theorem

试证明:在同构意义下,四阶群有且仅有两种.
对于每个四阶群$(G,*)$,
$(G,*)\cong(Z_4,+_4)$ 或$(G,*)\cong$ Klein 4-group.

提示:
使用Lagrange Theorem分析每个元素的可能的阶。

解答:
设$G=\{e,a,b,c\}$.

Case 1: $|a|=4\vee|b|=4\vee|c|=4$
$\Rightarrow G=\langle a\rangle\vee G=\langle b\rangle\vee G=\langle c\rangle.$

Case 2: $|a|\neq 4\vee|b|\neq 4\vee|c|\neq 4\Rightarrow|a|=2\vee|b|=2\vee|c|=2.$

Application of Lagrange Theorem

试证明:在同构意义下,四阶群有且仅有两种.

对于每个四阶群$(G, *)$,

$(G, *) \cong (Z_4, +_4)$ 或$(G, *) \cong$ Klein 4-group.

提示:

使用Lagrange Theorem分析每个元素的可能的阶。

解答:

设$G = \{e, a, b, c\}$.

Case 1: $|a| = 4 \vee |b| = 4 \vee |c| = 4$
$\Rightarrow G = \langle a \rangle \vee G = \langle b \rangle \vee G = \langle c \rangle$.

Case 2: $|a| \neq 4 \vee |b| \neq 4 \vee |c| \neq 4 \Rightarrow |a| = 2 \vee |b| = 2 \vee |c| = 2$.

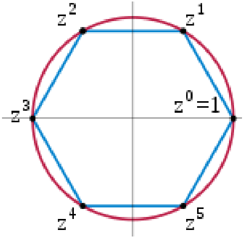
Q: $|G| \leq 6$?

Outline

n-th Root of Unity

试证明:
全体n次单位根组成的集合
$U_n=\{x\in\mathbf{C}\mid x^n=1\}=\{\cos\frac{2k\pi}{n}+\mathbf{i}\sin\frac{2k\pi}{n}\mid k=0,1,2,\cdots,n-1\}$
关于数的乘法构成n阶循环群($P_{202}(6)$).
并求U_n的所有生成元.

解答:



n-th Root of Unity

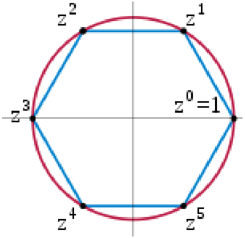
试证明:

全体n次单位根组成的集合

$$U_n = \{x \in \mathbf{C} \mid x^n = 1\} = \{\cos\frac{2k\pi}{n} + \mathbf{i}\sin\frac{2k\pi}{n} \mid k = 0, 1, 2, \cdots, n-1\}$$

关于数的乘法构成n阶循环群($P_{202}(6)$).

并求U_n的所有生成元.



解答:

1. 复数乘法的几何意义.
2. 先说明U_n构成群.
3. 令$\omega = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, 则$U_n = \langle\omega\rangle = \{1, \omega, \omega^2, \cdots, \omega^{n-1}\}$.
4. $(k, n) = 1, \omega^k$为生成元.

Cyclic Groop

设f为群$(G,*)$到群$(H,\circ)$的满同态，
证明：若G为循环群，则H亦为循环群$(P_{204}(27))$。

解答:

Cyclic Groop

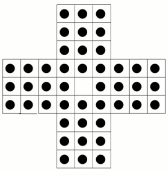
设f为群$(G,*)$到群$(H,\circ)$的满同态，
证明：若G为循环群，则H亦为循环群$(P_{204}(27))$。

解答:
令$G=\langle a\rangle$,则

$$H=f(G)=f(\langle a\rangle)=\{f(a^n)\mid n\in Z\}=\{(f(a))^n\mid n\in Z\}=\langle f(a)\rangle.$$

Outline

The Game of Solitaire



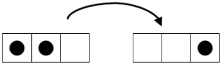
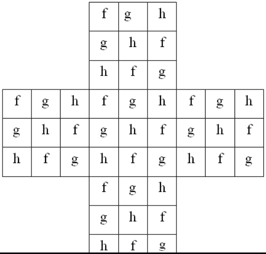


Figure: Is it easier for “Anywhere” than “Center” ?



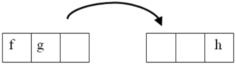
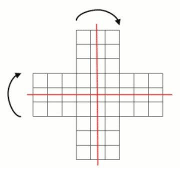
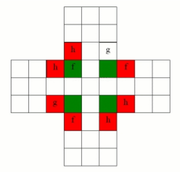
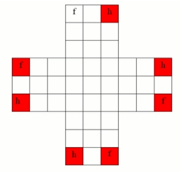


Figure: The value of the board does not change during a move!

The Game of Solitaire







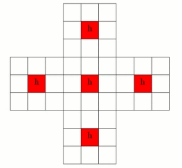


Figure: $f * g = h$, we might as well have jumped into the central hole!

That's the end. Thank you.

Figure: Bring Up a Question