Group Theory

Hengfeng Wei
hengxin0912@gmail.com

Department of Computer Science and Technology, NJU

April 27, 2011

Outline

集合运算律

1: 请证明补集之唯一性(Optional)。

Theorem:

令A, B为E的任意子集，则$B = \sim A \Leftrightarrow A \cup B = E \& A \cap B = \emptyset$

tips:

$$B = B \cap E = B \cap (A \cup \sim A) = (B \cap A) \cup (B \cap \sim A)$$
$$= \emptyset \cup (B \cap \sim A) = (A \cap \sim A) \cap (B \cap \sim A)$$
$$= \sim A \cap (A \cup B) = \sim A \cap E = \sim A.$$

集合运算律

2: 请证明以下命题等价:

1. $A \subseteq B$
2. $A \cup B = B$
3. $A \cap B = A$
4. $A - B = \emptyset$

Q: 为什么可以采用循环证明?

A: $\Leftrightarrow$ is an equivalence relation.

集合运算律

3: 请证明∩关于−是可分配的:

Theorem:

$$A \cap (B - C) = (A \cap B) - (A \cap C)$$

tip: 换个方向，化繁为简更容易。

练习:

请问∪关于−是可分配的吗?

集合运算律

4: 请证明$\cap$关于$\oplus$是可分配的:

Theorem:

$$A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C)$$

tips:

- $B \oplus C = (B - C) \cup (C - B)$
- $A \cap (B - C) = (A \cap B) - (A \cap C)$

练习:

请问$\cup$关于$\oplus$是可分配的吗?

集合运算律

5: 请解答如下与幂集相关的题目:

tip:
概念清晰, 区分$\in, \subseteq$。

1. $A \subseteq B \Leftrightarrow P(A) \subseteq P(B)$ (课本P_{100}第36题& P_{101}第44题)
2. $P(A) \cap P(B) = P(A \cap B)$ (课本P_{101}第45(1)题)
3. 字母集合$|A| = n$,自然数集合$|B| = m$,求$P(A) \cap P(B)$ (课本P_{98}第12(1)题)
4. $P(\bigcap A_i) = \bigcap P(A_i)$ (2010年期中测试题)

Outline

容斥原理

6: 求Euler函数ϕ: Review

(P_{91}例6.6,2001年期中测试题)

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

$$\phi(n) = n \prod_{i=1}^{k} (1 - \frac{1}{p_k}).$$

Outline

有序对

7: 如何定义三元组(Optional)?

We have:

$$\langle x, y\rangle = \{\{x\}, \{x, y\}\}$$

then:

$$\langle x, y, z\rangle = \{\{x\}, \{x, y\}, \{x, y, z\}\}$$

Q: Is the definition OK?

Tips: Consider $\langle x, y, x\rangle$ *and* $\langle x, y, y\rangle$

A: $\langle x_1, x_2, x_3\rangle = \langle\langle x_1, x_2\rangle, x_3\rangle$.

Operation over Binary Relation

8: 请证明如下运算性质：

$R_1 \subseteq A \times B, R_2 \subseteq A \times B$

1. $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$ (P_{132} 第20(1)题)
2. $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$ (P_{132} 第20(2)题)
3. $(\sim R)^{-1} = \sim (R^{-1})$
4. $(R_1 - R_2)^{-1} = R_1^{-1} - R_2^{-1}$

Properties of Binary Relation

9: 请证明如下命题: (P_{118}表7.2)

R, S are symmetric, so are $R^{-1}, R\cap S, R\cup S,$ and $R-S$.

tips:

- R is symmetric $\Leftrightarrow R = R^{-1}$.
- $(\sim R)^{-1} = \sim(R^{-1})$.
- $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$.

Equivalence Relation

10: 请证明如下定义的关系为等价关系，并给出商群。

1. $\langle a, b\rangle \sim \langle c, d\rangle \Leftrightarrow a+d=b+c$
   (where $a<b, a, b \in N$)(P_{133}第36题,作业补充题)

2. $\langle a, b\rangle \sim \langle c, d\rangle \Leftrightarrow ad=bc$

3. $A=P(X), C \subseteq X, \forall x, y \in A, xRy \Leftrightarrow x \oplus y \subseteq C$ (P_{133}第32(5)题)

Equivalence Relation

11: Counting partitions on a set with n elements(Optional)

try:

- $\left\{ {n \atop 0} \right\} = 0$
- $\left\{ {n \atop 1} \right\} = 1$
- $\left\{ {n \atop 2} \right\} = 2^{n-1} - 1$
- $\left\{ {n \atop n-1} \right\} = \binom{n}{2}$
- $\left\{ {n \atop n} \right\} = 1$

Recurrence relation:

$$\left\{ {n \atop r} \right\} = r\left\{ {n-1 \atop r} \right\} + \left\{ {n-1 \atop r-1} \right\}$$

Bell number:

$$B_n = \sum_{r=0}^{n} \left\{ {n \atop r} \right\} (n \geq 1)$$

Closure

复合闭包:

证明: A is finite set,$R \subseteq A \times A \Rightarrow rt(R) = tr(R)$.

提示:

$(I_A \cup R)^n = I_A \cup R \cup R^2 \cup \cdots \cup R^n = I_A \cup (\cup_{i=1}^n R^i)$

解答:

$$
\begin{aligned}
tr(R) &= t(I_A \cup R) \\
&= \cup_{i=1}^n (I_A \cup R)^i \\
&= (I_A \cup R) \cup (I_A \cup R)^2 \cup \cdots \cup (I_A \cup R)^n \\
&= (I_A \cup R) \cup (I_A \cup (\cup_{i=1}^2 R^i)) \cup \cdots \cup (I_A \cup (\cup_{i=1}^n R^i)) \\
&= I_A \cup R \cup R^2 \cup \cdots \cup R^n \\
&= I_A \cup (\cup_{i=1}^n R^i) \\
&= I_A \cup t(R) \\
&= r(t(R)) \\
&= rt(R)
\end{aligned}
$$

Closure

复合闭包:

证明: $R \subseteq A \times A \Rightarrow st(R) \subseteq ts(R)$.

解答:

$$\begin{aligned} R \subseteq s(R) &\Rightarrow t(R) \subseteq t(s(R)) \\ &\Rightarrow st(R) \subseteq sts(R) = ts(R) \end{aligned}$$

$s(R)[sym] \Rightarrow ts(R)[sym] \Rightarrow sts(R) = ts(R)$.

Outline

Function

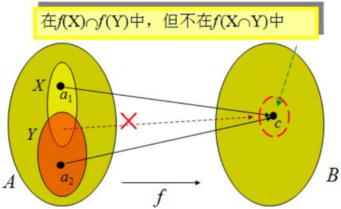
概念辨析:

1. $A = \emptyset, B = \emptyset \Rightarrow B^A = \emptyset^{\emptyset} = \{\emptyset\}$
2. $A = \emptyset, B \neq \emptyset \Rightarrow B^A = B^{\emptyset} = \{\emptyset\}$
3. $A \neq \emptyset, B = \emptyset \Rightarrow B^A = \emptyset^A = \emptyset$

Function

交集与并集的函数像:

1. P_{162} 第12题 说明 $f(A \cap B) = f(A) \cap f(B)$ 不是永远为真的。
2. 设 $f : A \to B, B_1 \subseteq B$. 试证明: $f(A \cap f^{-1}(B_1)) = f(A) \cap B_1$.



Function

企图证明$f(A \cap B) = f(A) \cap f(B)$:

$y \in f(A \cap B)$

$\Leftrightarrow \exists x(x \in A \wedge x \in B \wedge xfy)$

$\Leftrightarrow \exists x(x \in A \wedge xfy \wedge x \in B \wedge xfy)$

$\Leftrightarrow \exists x(x \in A \wedge xfy) \wedge (x \in B \wedge xfy)$

$\Leftrightarrow y \in f(A) \wedge y \in f(B)$

$\Leftrightarrow y \in (f(A) \cap f(B))$

$$f(A \cap f^{-1}(B_1)) = f(A) \cap B_1.$$

任取y,

$y \in f(A \cap f^{-1}(B_1)) \Leftrightarrow \exists x(x \in A \cap f^{-1}(B_1) \wedge xfy)$

$\Leftrightarrow \exists x(x \in A \wedge \underline{x \in f^{-1}(B_1)} \wedge xfy) \Leftrightarrow \exists x(x \in A \wedge \underline{f(x) \in B_1} \wedge xfy)$

$\Leftrightarrow \exists x(x \in A \wedge y \in B_1 \wedge xfy) \Leftrightarrow \exists x(x \in A \wedge xfy) \wedge y \in B_1$

$\Leftrightarrow y \in f(A) \wedge y \in B_1 \Leftrightarrow y \in f(A) \cap B_1$ $\square$

Outline

Homomorphism and Isomorphism

P_{180} **第18题**

$V_1 = \langle Z, +, \cdot \rangle$, $V_2 = \langle Z_n, \oplus, \otimes \rangle$.

令$f : Z \to Z_n, f(x) = (x) \bmod n$.

证明,f为V_1到V_2的满同态映射。

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:

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

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$(1 \in U(m))$

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:

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

–

Outline

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:
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:

figure/6root.png

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:
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

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

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

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

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:

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

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$H \triangleleft G$且$H \subseteq K$，则$H \triangleleft K$。

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。