计算机问题求解 – 论题3-16 - 群与拉格朗日定理

2014年12月29日

下面的话是什么意思？

It makes sense to write equations with group elements and group operations. If a and b are two elements in a group G, does there exist an element $x \in G$ such that $ax = b$? If such an x does exist, is it unique? The following proposition answers both of these questions positively.

问题1：什么是一个algebraic structures？

Table 3.1. Multiplication table for $\mathbb{Z}_8$

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

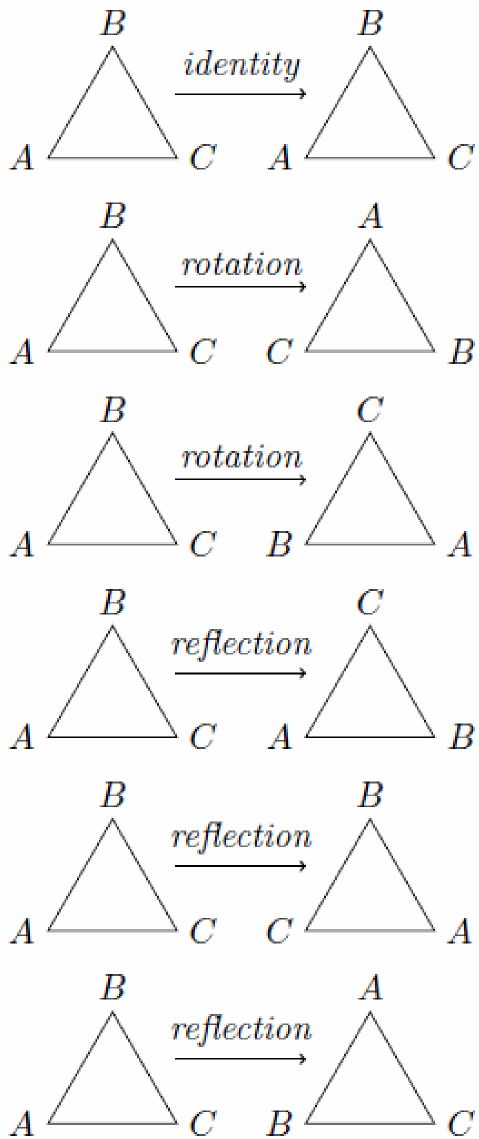
（Z_8，•）

第二例：

Table 3.2. Symmetries of an equilateral triangle

$\circ$	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	id	μ_3	μ_1	μ_2
ρ_2	ρ_2	id	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	id	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	id	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	id

Figure 3.2. Symmetries of a triangle



$$id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$$

$$\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$$

$$\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

$$\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$

Table 3.4. Multiplication table for $U(8)$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

一元一次方程的解

- 什么情况下，ax=b有解？解是否唯一？解是什么？

- (R-{0},×)具有什么性质？

群 – 一种“公理化”的代数系统

- The law of composition is *associative*. That is,

$$(a \circ b) \circ c = a \circ (b \circ c)$$

  for $a, b, c \in G$.

- There exists an element $e \in G$, called the *identity element*, such that for any element $a \in G$

$$e \circ a = a \circ e = a.$$

- For each element $a \in G$, there exists an *inverse element* in G, denoted by a^{-1}, such that

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

注意：对于the integers mod *n*，加法一定构成群，乘法则未必。

问题：

你还熟悉哪些“运算性质”，在群公理中没有提到？

问题：

群中有可能包含“0”吗？

问题:

谈到群，你会联想到程序设计语言中“数据类型”的概念吗？

群方程

Proposition 3.6 *Let G be a group and a and b be any two elements in G. Then the equations $ax = b$ and $xa = b$ have unique solutions in G.*

PROOF. Suppose that $ax = b$. We must show that such an x exists. Multiplying both sides of $ax = b$ by a^{-1}, we have $x = ex = a^{-1}ax = a^{-1}b$.

To show uniqueness, suppose that x_1 and x_2 are both solutions of $ax = b$; then $ax_1 = b = ax_2$. So $x_1 = a^{-1}ax_1 = a^{-1}ax_2 = x_2$. The proof for the existence and uniqueness of the solution of $xa = b$ is similar. □

问题8：

直觉上，你能说说群和对称性研究有什么关联吗？

问题：

假如我们从一个至少两个元素的群中取异于单位元的元素，让它持续的乘自己，你能描述一下情况会怎样吗？

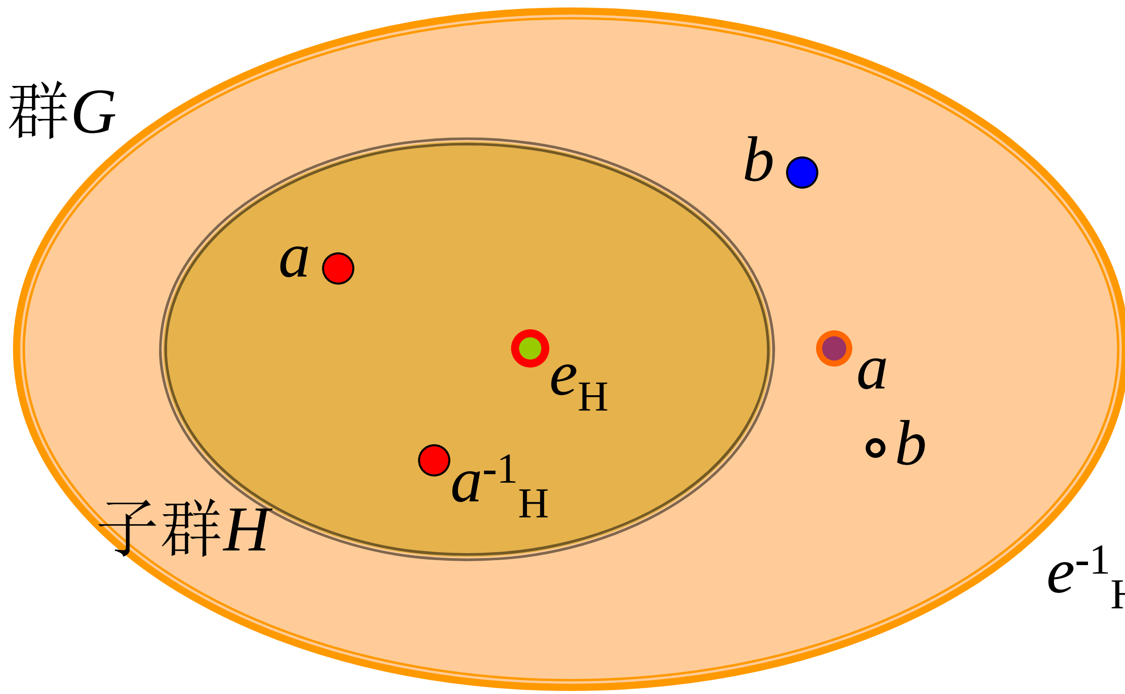
什么是子群?

We define a *subgroup* H of a group G to be a subset H of G such that when the group operation of G is restricted to H, H is a group in its own right.

问题：

乘积在哪里？

问题1：ab应该在哪儿？



问题15-2：

e_H是否一定是e_G?

问题15-3：

$e^{-1}{}_H$是否一定是$e^{-1}{}_G$?

子群的判定

Proposition 3.9 *A subset H of G is a subgroup if and only if it satisfies the following conditions.*

1. *The identity e of G is in H.*
2. *If $h_1, h_2 \in H$, then $h_1 h_2 \in H$.*
3. *If $h \in H$, then $h^{-1} \in H$.*

子群的判定

Proposition 3.10 *Let H be a subset of a group G. Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H.*

PROOF. Let H be a nonempty subset of G. Then H contains some element g. So $gg^{-1} = e$ is in H. If $g \in H$, then $eg^{-1} = g^{-1}$ is also in H. Finally, let $g, h \in H$. We must show that their product is also in H. However, $g(h^{-1})^{-1} = gh \in H$. Hence, H is indeed a subgroup of G. Conversely, if g and h are in H, we want to show that $gh^{-1} \in H$. Since h is in H, its inverse h^{-1} must also be in H. Because of the closure of the group operation, $gh^{-1} \in H$. □

问题：

群中某个元素的所有整数次幂为什么一定构成子群？如果这个子集包含原来群中所有元素，这意味着什么？

子群的判定 – 有限子群

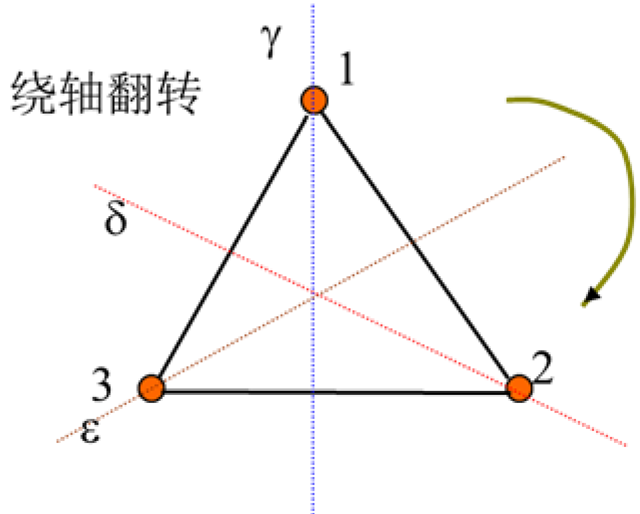
- G是群，H是G的非空有限子集。H是G的子群当且仅当：
  - $\forall a,b \in H,\ ab \in H$
- 证明
  - 必要性显然
  - 充分性：只须证明逆元素性
    - 若H中只含G的单位元，H显然是子群。否则，任取H中异于单位元的元素a, 考虑序列

$$a, a^2, a^3, \ldots$$

注意：该序列中各项均为有限集合H中的元素，因此，必有正整数i,j(j>i), 满足：$a^i=a^j$, 因此：

$$a^{-1}=a^{j-i-1} \in H$$

现在回头再看看
Symmetries of a Triangle



顺时针旋转：
0度：e
120度：α
240度：β

问题：

将Symmetries of a Triangle看作群，元素究竟是什么？

问题：

为什么一个有限集合上所有一一对应的函数一定能构成一个群？

置换群

子群的陪集

Let G be a group and H a subgroup of G. Define a ***left coset*** of H with ***representative*** $g \in G$ to be the set

$$gH = \{gh : h \in H\}.$$

Right cosets can be defined similarly by

$$Hg = \{hg : h \in H\}.$$

Example 1. Let H be the subgroup of $\mathbb{Z}_6$ consisting of the elements 0 and 3. The cosets are

$$\begin{aligned} 0 + H &= 3 + H = \{0, 3\} \\ 1 + H &= 4 + H = \{1, 4\} \\ 2 + H &= 5 + H = \{2, 5\}. \end{aligned}$$

子群的陪集

问题：

H和gH是否肯定“一样大”？

问题：

诸gH中会不会有相同元素？有相同元素意味着什么？

问题：

什么样的元素，它们的陪集是相同的？

陪集划分一个群

Theorem 6.2 *Let H be a subgroup of a group G. Then the left cosets of H in G partition G. That is, the group G is the disjoint union of the left cosets of H in G.*

Proof. Let g_1H and g_2H be two cosets of H in G. We must show that either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose that $g_1H \cap g_2H \neq \emptyset$ and $a \in g_1H \cap g_2H$. Then by the definition of a left coset, $a = g_1h_1 = g_2h_2$ for some elements h_1 and h_2 in H. Hence, $g_1 = g_2h_2h_1^{-1}$ or $g_1 \in g_2H$. By Lemma 6.1, $g_1H = g_2H$. $\square$

问题17：

如果G是有限群，你能得出什么结论吗？

拉格朗日定理

Theorem 6.5 (Lagrange) *Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.*

问题：

为什么元素个数是质数的群一定是循环群？

问题：

为什么不可能有比Symmetries of a Triangle元素个数更少的非交换群？

家庭作业

- TJ pp.51-: 3, 6, 7, 17, 28, 36, 38, 41, 48, 52
- TJ pp.100-: 8，11, 12, 16, 21

$$
\begin{aligned}
271^{321} &\equiv 271^{2^0+2^6+2^8} \pmod{481}\\
&\equiv 271^{2^0}\cdot 271^{2^6}\cdot 271^{2^8} \pmod{481}\\
&\equiv 271\cdot 419\cdot 16 \pmod{481}\\
&\equiv 1,816,784 \pmod{481}\\
&\equiv 47 \pmod{481}.
\end{aligned}
$$

问题：

你能说说这个计算背后的理论根据吗？

问题:

如果我们并不关心集合中究竟是什么东西，那么所谓“结构”中最关键的是什么？

二元运算及其性质

问题：

你能理解为什么“结构”由运算确定吗？