抽象代数入门

罗雨屏

清华大学　交叉信息研究院

2014 年 5 月 3 日

FAQ

- 问：抽象代数是什么？
- 答：其实它是一类树形数据结构，叫做臭翔袋，所以一般称之为臭翔袋树，简称为抽象代数。
- 问：这货很有用吗？会不会很难写啊？
- 答：请参考 LCT 的发展趋势。
- 问：那你抽象代数学的怎么样？成绩多少啊？
- 答：不谈成绩我们还是好朋友。（捂脸）

群

- 定义在一个集合 S 上的运算 $\times$ 满足下列四种性质，即构成一个群
  1. 封闭性：$\forall a, b \in S, a \times b \in S$
  2. 结合律：$\forall a, b, c \in S, (a \times b) \times c = a \times (b \times c)$
  3. 存在单位元：$\exists e \in S, s.t. \forall a \in S, e \times a = a \times e = a$
  4. 存在逆元：$\forall a \in S, \exists b \in S, s.t. a \times b = b \times a = 1$，记作 $b = a^{-1}$
- Abel 群
  - $\times$ 满足交换律：$\forall a, b \in S, a \times b = b \times a$
- 定义

$$a^k = \begin{cases} e & \text{if } k = 0 \\ a \times a^{k-1} & \text{otherwise.} \end{cases}$$

- 在不引起歧义的前提下，$a \times b$ 可以记作 ab

群举例

- $\mathbb{R}$ 上的 $+$
- $\mathbb{R}\backslash\{0\}$ 上的 $\times$
- p 为素数，则 $\mod p$ 下的 $\{1, \ldots, p-1\}$
- xor 群
- $\forall n \in \mathbb{N}$, 令 $S = \{1 \le x \le n : x \in \mathbb{N}, (x, n) = 1\}$, 乘法为对 n 取模
- 非 Abel 群
  - $\{1, 2, \ldots, n\}$ 的所有置换
  - 矩阵群

群的基本性质

- 单位元唯一：若 e, e' 均为单位元，则 $e' = ee' = e$
- 每个元素的逆元唯一：若 a 有两个逆元 x, y ，则 $x = xay = y$
- $(a^{-1})^{-1} = a$
- 消去律：若 $au = bu$ ，则 $a = b$ ；若 $ua = ub$ ，则 $a = b$

结合律（2013 年集训队互测）

- 给定一个定义在 $\{0, 1, \ldots, n-1\}$ 的运算，如何判断其满足结合律？

结合律（2013 年集训队互测）

- 给定一个定义在 $\{0, 1, \ldots, n-1\}$ 的运算，如何判断其满足结合律？
-

结合律（2013 年集训队互测）

- 给定一个定义在 $\{0, 1, \ldots, n-1\}$ 的运算，如何判断其满足结合律？
-
- Light's associativity test

结合律（2013 年集训队互测）

- 给定一个定义在 $\{0, 1, \ldots, n-1\}$ 的运算，如何判断其满足结合律？
-
- Light's associativity test
- Monte Carlo method

结合律（2013 年集训队互测）

- 给定一个定义在 $\{0, 1, \ldots, n-1\}$ 的运算，如何判断其满足结合律？
-
- Light's associativity test
- Monte Carlo method
  - 随机选择两个 0/1 多项式，检验是否存在

结合律（2013 年集训队互测）

- 给定一个定义在 $\{0, 1, \ldots, n-1\}$ 的运算，如何判断其满足结合律？
-
- Light's associativity test
- Monte Carlo method
  - 随机选择两个 0/1 多项式，检验是否存在
  - 位运算：32 倍速

JSOI 2007 群的计数

- 给定一个 n，求 n 阶群的数目

JSOI 2007 群的计数

- 给定一个 n，求 n 阶群的数目
- $n \le 3000$

JSOI 2007 群的计数

- 给定一个 n ，求 n 阶群的数目
- $n \leq 3000$
-

JSOI 2007 群的计数

- 给定一个 n，求 n 阶群的数目
- $n \leq 3000$
-
- 其实我也不会做

JSOI 2007 群的计数

- 给定一个 n ，求 n 阶群的数目
- $n \leq 3000$
-
- 其实我也不会做
- 你看看人家 Mathematica 都不会做

JSOI 2007 群的计数

- 给定一个 n ，求 n 阶群的数目
- $n \le 3000$
-
- 其实我也不会做
- 你看看人家 Mathematica 都不会做
- 所以大家可以放弃治疗了

JSOI 2007 群的计数

- 给定一个 n ，求 n 阶群的数目
- $n \leq 3000$
-
- 其实我也不会做
- 你看看人家 Mathematica 都不会做
- 所以大家可以放弃治疗了
- @Seter：打表 + OEIS，没有超过 2k 的数据

相关概念

- 子群：若 G 为群且 $H \subset G$ ，且 $(H, \times)$ 构成群，则称 H 是 G 的一个子群，记作 $H \leq G$
- 陪集：令 $H \leq G$ ，则 $\forall a \in G$, 记

$$Ha = \{ha : h \in H\}, aH = \{ah : h \in H\}$$

  分别称之为 H 的右陪集、左陪集
  - $Ha = Hb$ 充要条件是 $ab^{-1} \in H$
  - $|Ha| = |Hb|$
  - 若 $Ha \neq Hb$ ，则 $Ha \cap Hb = \emptyset$
  - G 中 H 的所有右陪集构成 G 的一个划分，划分的每一部分大小相等
- Lagrange Theorem
  - 若 $H \leq G$ 且 $|G|$ 有限，则 $|H|$ 是 $|G|$ 的因子

相关概念

- 生成子群：一个集合 S 的生成子群被定义为

$$\bigcap_{S\subseteq G} G$$

- 循环群：若 G 可以由一个元素生成，即存在一个元素 a 满足

$$G=\{a^k : k\in\mathbb{Z}\},$$

  则称 G 是循环群，a 是 G 的一个生成元
- 周期（阶）：对于 $a\in G$ ，定义

$$o(a)=\min\{n\in\mathbb{N} : n>0, a^n=e\},$$

  如果不存在，则记 $o(a)=0$
  - 推论：若 $|G|$ 有限，则 $o(a)||G|$ （Lagrange 定理）
- 若 $|G|=p$ 且 p 为素数，则 G 为循环群
  - 考虑 G 中任意一个元素 a 的阶：$o(a)|p$

数论中的欧拉定理

- $\forall n \in \mathbb{N}, (a, n) = 1$, 有
$$a^{\phi(n)} = 1$$
- $\{a : a \in \mathbb{N}, (a, n) = 1\}$ 构成一个群，群大小为 $\phi(n)$
- 由 $o(a) \mid |G|$ 直接可以推出来

群对集合的作用

- G 为一个群，S 为一个集合，一个 $G \times S \to S$ 的映射 $(g, s) \to g * s$ 满足
  - $\forall x \in S, e * x = x$
  - $\forall a, b \in G, x \in S, (ab) * x = a * (b * x)$
- 则称 G 在 S 上定义了一个左作用
- 若 G 是有限集 S 上的置换群，且 $g * x = gx$ 则群对集合的作用即为置换群对集合的作用
- 在不引起歧义的情况下，$g * x$ 可以被记为 gx 或者 x^g

轨道公式

- 轨道：$\forall x \in S$，定义 x 的轨道为

$$Gx = \{gx : g \in G\}$$

  即在 G 作用下，x 所有可能的结果

- 稳定化子：$\forall x \in S$，定义 x 的稳定化子为

$$\mathsf{Stab}\ x = \{g \in G : gx = x\}$$

  即在 G 中所有保持 x 不动的元素的集合

- 轨道公式：

$$|Gx| = [G : \mathsf{Stab}\ x]$$

BURNSIDE 定理

- 令 G 为一有限群，S 为一个有限 G- 集合，n 为 S 上 G 作用后的不同的轨道数目，则
$$n = \frac{1}{|G|}\sum_{g\in G} S_g$$
其中 $S_g = \{x \in S : gx = x\}$
- 证明：
$$n = \sum_{x\in S}\frac{1}{|Gx|} = \sum_{x\in S}\frac{\mathsf{Stab}\ x}{|G|}$$
- 每一对满足 $gx = x$ 的 (g, x) 都给等式两边贡献 $\frac{1}{|G|}$

置换群

- 轮换分解与对换分解
- 为何置换群如此重要

Theorem (Cayley Theorem)

任何一个群 G 都同构于 G 上置换群的一个子群。

Proof of Cayley Theorem.

定义函数 $\phi : G \to \mathrm{Sym}(G)$，且

$$\phi_g(x) = gx, \forall x \in G,$$

易证 ϕ 为单射，$\mathrm{Im}\ \phi$ 为群同构，而 $\mathrm{Im}\ \phi \leq \mathrm{Sym}(G)$，证毕。 $\square$

SGU 539 Multiswap Sorting

- 给定一个 $(1, 2, \ldots, n)$ 的置换 P
- 每次可以选择不相交的若干对数 $(x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k)$ 然后同时交换 x_i, y_i 在序列中的位置
- 求至少要多少次才能使整个排列有序
- 要求输出一组方案
-
- $n \leq 10^3$

SGU 539 Multiswap Sorting

- 答案至多是 2
- 只需考虑每个轮换就好了
- 对于大小为 2 的排列：只需一次
- 对于大小大于 2 的排列：$(2, 3, \ldots, n, 1)$
  - 第一次：$(3, n), (4, n-1), \ldots$
    - 交换后变成 $(2, 1, n, n-1, \ldots, 3)$
  - 第二次：直接交换
  - 证明：分奇偶讨论即可
    - $(2, 3, 4, 1) \to (2, 1, 4, 3) \to (1, 2, 3, 4)$
    - $(2, 3, 4, 5, 1) \to (2, 1, 5, 4, 3) \to (1, 2, 3, 4, 5)$

HDU 4702 问题描述

- 给定 m 个 $1, \ldots, n$ 的排列 $\sigma_1, \sigma_2, \ldots, \sigma_m$
- 求其生成子群大小
-
- $n, m \leq 50$

Stabilizer

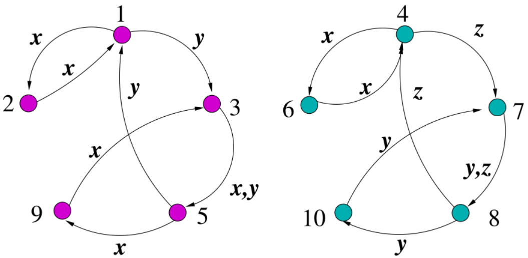
- 令 G 为最后的生成子群
- 维护 n 个排列 ω_x 表示：G 中是否存在一个排列 τ 满足

$$\tau(x) = 1$$

  - 如果存在，定义 $\omega_x = \tau$
  - 规定 $\omega_1 = e$

Orbit

- 令 $G = \langle x, y, z \rangle$
  - $x = (1,2)(3,5,9)$
  - $y = (1,3,5)(7,8,10)$
  - $z = (4,7,8)$



- 其轨道为 $\Delta_1 = \{1,2,3,5,9\}, \Delta_2 = \{4,6,7,8,10\}$
- $\omega_1 = e, \omega_2 = (1,2)(3,5,9), \omega_3 = (1,5,3)(7,10,8)$

判定性问题

- 如果得到了 G 的 ω，如何判断一个置换 σ 是否在 G 中？
- 考虑 $x = \sigma(1)$
  - 如果不存在 ω_x，则 $\sigma \notin G$
  - 否则考虑 $\sigma' = \omega_x \sigma$
    - $\sigma \in G \Leftrightarrow \sigma' \in G$
    - σ' 的好性质：$\sigma'(1) = 1$
- σ' 的意义：都只需判断一个置换 σ' 是否在 Stab 1 中，且 $\sigma'(1) = 1$
  - 考虑 $\sigma'(2)$
  - 递归处理！

判定性问题

- 令 $G = \langle (1,2,3,4,5,6),(2,6)(3,5) \rangle$
- 如何判断 $g = (1,4)(2,3)(5,6)$ 是否在 G 中
- $g(1) = 4, \omega_4 = (1,4)(2,5)(3,6)$
- 所以只需要判断 $\omega_4 g$ 是否在 G 中即可
  - 其实只要判断是否在 Stab 1 中即可
  - Stab $1 = \langle (2,6)(3,5) \rangle$
- $\omega_4 g = (2,6)(3,5)$ 在 G 中
  - g 在 G 中

ω 的意义

- 轨道公式：$|Gx| = [G : \text{Stab } x]$
  - 如果知道 $|Gx|$ 和 $|\text{Stab } x|$ 那么就知道 $|G|$ 了
- $|G1|$ 的意义：有多少个 ω_y 存在
- $|\text{Stab } 1|$ 是 G 的一个子群
  - 再建立一个相同的数据结构维护 Stab 1
- 算法：维护 ω 和 $|\text{Stab } 1|$ 并对 Stab 1 建立相同的数据结构
  - 答案即为每个数据结构的 $|\omega|$ 的乘积

ω 的维护

- 考虑每次添加一个 σ ，我们需要知道两件事
  1. 能得到哪些新的 ω_x
  2. Stab 1 会增加哪些元素
- 对于第一个问题：BFS/DFS
- 对于第二个问题，由于一次添加可能使得 Stab 1 增加很多个元素，所以一个一个添加是不行的
  - 每次添加一个大小有界的集合 X ，满足 Stab $1_{new} = \langle X \cup \text{Stab } 1_{old} \rangle$
  - 这又是一个递归的问题
  - 如何找到的 X ？

Schreier's Lemma

Definition (Transversal)

令 $H \le G$，称 R 为 H 的一个 right transversal 当且仅当 $|R| = [G : H]$ 且

$$\{Hr : r \in R\} = \{Hg : g \in G\},$$

即对于 $g \in G$，存在且仅存在一个 r 满足 $gr^{-1} \in H$，并且这里我们定义 $\overline{g}$ 为这个 r。

Theorem (Schreier's lemma)

令 $H \le G = \langle S \rangle$，$|S| < \infty$，则 H 由以下集合生成：

$$X_H = \{rs(\overline{rs})^{-1} : r \in R, s \in S\}$$

SCHREIER'S LEMMA 的应用

- 维护的 ω 就是 Stab 1 的一个 right transversal
- 由于置换的特殊性：可以快速找到 g 对应的 r，即 $\overline{g}$
- 还需要维护 G 的生成集合 S
  - 在这个数据结构中加一个数组维护即可
- 观察每次添加一个元素后，R 的变化和 X_G 的变化
  - R 的变化：即 ω 的变化
  - X_G 的变化：增加了一个元素

Pseudocode

Algorithm 1 updR(σ, G)

if $\sigma \in G$ **then**
    return
end if
insert σ into X_G
for ω_x in current ω **do**
    updX($\omega_x \sigma$, G)
end for

Algorithm 2 updX(σ, G)

$x \leftarrow \sigma(1)$
if $\omega_x = \emptyset$ **then**
    $\omega_x \leftarrow \sigma$
    for τ in current X_G **do**
        updX($\sigma\tau$, G)
    end for
else
    updR($\omega_x \sigma$, Stab 1)
end if

- 该算法即为著名的 Schreier-Sims algorithm
- 复杂度还是多项式时间的

如何构造数据

- 交错群 A_n 的生成集合

$$\{(1,2,3),(1,2,3),\ldots,(1,2,n)\}$$

- 置换群 S_n 的生成集合

$$\{(1,2),(1,2,\ldots,n)\}$$

- 把 $\{1,2,\ldots,n\}$ 分成若干个集合，不存在一个置换 σ 满足 $\sigma x = y$ 且 x, y 在不同集合

BASE AND STRONG GENERATING SET （BSGS）

- 令 G 为一置换群
- $B = (\beta_1, \beta_2, \ldots, \beta_k)$ 被成为是 G 的一组 base 当且仅当 $\forall g \in G$，g 能被 $(g\beta_1, g\beta_2, \ldots, g\beta_k)$ 唯一确定。
- 对于一组 B，定义 $G^{(0)} = G, G^{(i)} = \{g \in G^{(i-1)} : g\beta_i = \beta_i\}$，即 $G^{(i)}$ 为 $G^{(i-1)}$ 中的 Stab β_i
- S 为一个集合，S 被称为 strong generating set 当且仅当 $\forall 0 \le i \le k, G^{(i)} = \langle S \cap G^{(i)} \rangle$
- Schreier-Sims 算法实际上是求在 BSGS
  - 思考：前面讲的算法中，求出的 BSGS 是什么？

- 令 $G = \langle X \rangle$
- $(B = (\beta_1, \beta_2, \ldots, \beta_k), S)$ 被称为 G 的一组 partial BSGS 当且仅当
  - $X \subseteq S$
  - S 在逆运算下封闭：$\forall x \in S, x^{-1} \in S$
  - 不存在一个元素 $x \in S$，满足 $\forall \beta_i \in B, x\beta_i = \beta_i$
- 如何求任意一组 partial BSGS
  - 初始时令 $S = X \backslash \{e\}, B = \emptyset$
  - $\forall x \in S$，将 x^{-1} 添加进入 S
  - $\forall x \in S$，如果 $xB = B$，则选择一个 β 满足 $x\beta \neq \beta$ 并将 β 添加进 B

Randomization

Algorithm 3 Randomized version of Schreier-Sim Algorithm

$(B, S) \leftarrow$ a partial base and strong generating set
while needn't stop **do**
  $g \leftarrow$ random element in G
  $\bar{g} \leftarrow$ the residue of stripping g w.r.t (B, S)
  if $g \neq e$ **then**
    add $\bar{g}$ and $\bar{g}^{-1}$ to S
    if $B^{\bar{g}} = B$ **then**
      add a point not fixed by $\bar{g}$ to B
    end if
  end if
end while

Stripping

- stripping ？
  - 给定一个 partial BSGS 以及任意一个置换 g ，可以求得 g 不在哪一个 $G^{(i)}$
- 如何随机选择 G 中一个元素
  - 如果已知 BSGS ，那么可以从每个 transversal 里面选择随机选择一个元素，再乘起来
    - 可是 BSGS 还没有求出来
  - product-replacement algorithm

PRODUCT-REPLACEMENT ALGORITHM

Algorithm 4 product-replacement algorithm

$D = (g_1, g_2, \ldots, g_m)$ is a global variable, $g_i \in G$
$i, j \leftarrow$ 2 different integers in $\{1, 2, \ldots, m\}$
if `random()` > 0.5 **then**
    $g \leftarrow g_i g_j$
else
    $g \leftarrow g_j g_i$
end if
$g_i = g$
return g

PRODUCT-REPLACEMENT ALGORITHM

- 这个算法没有 uniformly randomness 的保证
  - Experimentation has shown them to be good.
- m 的大小：有人建议 $m = \max(10, 2n+1)$
- D 的初始化：前面 n 个是 G 的生成集合 X ，后面的为 e
- 随机防卡的一般方法：抛弃前 K 次随机
  - 有人建议 $K \geq 60$

A NEW FIELD

- Computational Group Theory 在等着你们
  - Schreier-Sims algorithm：求 BSGS
  - Todd-Coxeter algorithm：枚举所有陪集
  - product-replacement algorithm：求群里面一个随机元素

域

- 定义在一个集合 S 上的两种运算 $(+,\times)$ 满足
  - $(S,+)$ 构成 Abel 群
  - $(S\backslash\{0\},\times)$ 构成 Abel 群
  - 分配率：$\forall a,b,c\in S,(a+b)\times c=a\times c+b\times c,a\times(b+c)=a\times b+a\times c$
- 则称 $(S,+,\times)$ 构成一个域
  - $(\mathbb{R},+,\times)$ 和 $(\mathbb{C},+,\times)$
  - 若 p 为素数，则 $\mod p$ 构成一个域

域的性质

- 若域 F 的大小有限，则 $|F| = p^k$ ，其中 p 为素数，k 为整数
  - 如何构造大小为 9 的域？
    - 域的扩张
- 任何一个域 F 的乘法群的有限子群 G 是循环群
  - 考虑 $f(x) = x^m - 1$ 在 F 中的根的数目，其中 $m = |F|$
    - 至多为 m 个根
    - $\forall a \in G, a^{|G|} = 1 \Rightarrow$ 至少有 m 个根
- 对于有限域 F ，其中任意元素 a 均满足 $a^{|F|} = a$

Wilson's Theorem

Theorem (Wilson's Theorem)

若 p 为素数，则 $(p-1)! \equiv -1 \mod p$

Wilson's Theorem

Theorem (Wilson's Theorem)

若 p 为素数，则 $(p-1)! \equiv -1 \mod p$

Proof.

□

Wilson's Theorem

Theorem (Wilson's Theorem)

若 p 为素数，则 $(p-1)! \equiv -1 \mod p$

Proof.

- 可以用逆元来证明

$\square$

Wilson's Theorem

Theorem (Wilson's Theorem)

若 p 为素数，则 $(p-1)! \equiv -1 \mod p$

Proof.

- 可以用逆元来证明
- 考虑

$$x^{p-1} - 1$$

在 F_p 上面的根

□

Wilson's Theorem

Theorem (Wilson's Theorem)

若 p 为素数，则 $(p-1)! \equiv -1 \mod p$

Proof.

- 可以用逆元来证明
- 考虑

$$x^{p-1} - 1$$

在 F_p 上面的根

  - 韦达定理

$\square$

ENDING

- 谢谢大家