模意义下乘法群性质

huhao

June 30, 2022

定义

- 代数系统 $(A, O_1, O_2, \ldots, O_m)$：若干元素组成的集合 A，以及若干元素间的运算 O_i，满足定义域是 A^k，值域是 A。
- 半群 $(A, \cdot)$：代数系统；$\cdot : A^2 \to A$，且 $x(yz) = (xy)z$。
- 群的积：$(A, \cdot) \times (B, \cdot) = \{A \times B, \cdot\}$，且 $(u, v) \cdot (a, b) = (u \cdot a, v \cdot b)$。
- 含幺半群 $(A, \cdot)$：半群；$\exists e, xe = x$。可以发现，$ex = x$。
- 群 $(A, \cdot)$：含幺半群；$\forall x, \exists y, yx = e$。可以证明，只要任意一个元素存在左逆元，那么它就有唯一的逆元。
- Abel 群 $(A, \cdot)$：群；$xy = yx$。Abel 群一个很重要的性质是 $a^k b^k = (ab)^k$。
- 循环群 $(A, \cdot)$：群；$\exists x, \forall y, \exists k, x = y^k$，不难发现，循环群是 Abel 群。
- 置换群 $(A, \cdot)$：A 中所有元素均为函数，由 $1 \sim n$ 的排列 p 所确定：$f_p(i) = p_i$，且若 $xy = z$ 则 $f_y(f_x(i)) = f_z(i)$，不难发现，这是群。

同构与同态

若 $f\colon A \to B$，$(A,\cdot),(B,\cdot)$ 是代数系统，且 $f(a)+f(b)=f(ab)$ 则称（f 是）A,B（的）同态。

如果 f 是双射，则称为同构。

容易验证，所有 n 维循环群是模 n 意义下加法群（下面简记为 Z_n）的同构。

容易证明，同态与同构会保留上一页中代数系统的性质。

生成元

在群中，定义 $\langle a\rangle = \{x|x = a^k\}$，$O\langle a\rangle = |\langle a\rangle|$ 称为 a 的阶，若 $O\langle x\rangle = |A|$，则称 x 为 A 的生成元。

不难发现。

- $x \in Z_n, O\langle x\rangle | n$。
- $O\langle x\rangle = O\langle -x\rangle$。

Abel 群的性质

所有有限 Abel 群 $(A, \cdot)$ 与 $Z_{i_1} \times Z_{i_2} \times \ldots Z_{i_n}$（若干循环群的积）同构。

记 $|A| = n$，取 $O\langle x\rangle$ 最大的 x，则 $\langle x\rangle$ 构成子群，且可以找出 $n/O\langle x\rangle$ 个大小为 $O\langle x\rangle$ 集合，使得集合中所有元素乘上 $\langle x\rangle$ 中的元素依然在这个集合中（这可以不断找一个元素 u，然后生成集合 $\{u^k\}$，这样不同集合肯定是不交的）。

若 $O\langle x\rangle \neq n$，则有多个集合，若将这些集合间的乘运算规定为各取一个元素相乘，得到的结果在的集合。则这些集合和乘法也构成群 $(B, \cdot)$。

假如 $(B, \cdot)$ 与 $C = Z_{i_1} \times Z_{i_2} \times \ldots Z_{i_n}$ 同构，若能证明 A 与 $C \times Z_{O\langle x\rangle}$ 同构，则可根据归纳法证明。

不妨把 B 中的元素（一个集合），通过同构的函数映射至 C 中的元素，通过 $(j_1, j_2, \ldots j_n), 0 \leq j_k < i_k$ 表示。

续

对于群乘积的每一维 Z_{i_k}，可以在 $(0,0,\ldots,1,\ldots 0)$ 对应集合 t_k 中（第 k 位为 1）（暂时）任取一个元素 u_k 作为这个群的代表，假定 $u_k^{i_k} = e_A$（否则下面将在 t_k 中找到一个代替这个 u_k 的元素），因为后续证明需要用到这一点。

如果 $u_k^{i_k} \neq e_A$，那么有 $u_k^{i_k} = x^y$，则（下式用到了 $u_k^r = e_A \Rightarrow i_k | r$，这个可以是根据 t_k 的定义得到的）：

$$O\langle u_k x^l \rangle = i_k \frac{O\langle x \rangle}{(y + l i_k, O\langle x \rangle)}$$

根据 x 的定义，有：$i_k \leq (y + l i_k, O\langle x \rangle)$

取 $l = \lfloor \frac{y}{i_k} \rfloor$ 即可得到 $i_k | y$。

则 $u'_k = u_k x^{-\frac{y}{i_k}}$ 满足 $u_k'^{i_k} = e_A$，用 u'_k 代替任取的 u_k 即可。

续

对于集合 $(j_1, \ldots j_n)$，不妨用 $r_{j_1,\ldots j_n} = \prod_k u_k^{j_k}$ 代表（根据定义，则个元素一定在集合内）。

所以 $(\{r\}, \cdot)$ 对运算封闭，它是一个群。可以将 A 中的元素表示为 $(u, v), u \in \{r\}, v \in \langle x \rangle$，这样可以唯一的表示出 $|A| = |\{r\}| O\langle x \rangle$ 个元素，如果将这样的一一对应关系记为函数 f，则 f 是 $(A, \cdot)$ 与 $(\{r\}, \cdot) \times (\langle x \rangle, \cdot)$ 的同构。

所以 A 与 $C \times Z_{O\langle x \rangle}$ 同构（这里没有证明 $\{r\}$ 与 C 同构，可以尝试自行证明。同时可以发现此部分可以不证明，因为已经可以归纳地找到与 r 同构的若干循环群的积了），证明完毕。

续

更进一步，我们知道了 A 与 $\prod_j Z_{i_j}$ 同构，则有：$|Z_{i_j}| \mid |A|$。

则对于 A 中的元素 x，通过同构映射至 $\prod_j Z_{i_j}$ 中的元素 $(x_1 \dots x_k)$，则 $x^{|A|}$ 可以映射至 $(x_1 \dots x_k)^{|A|} = (x_1^{|A|} \dots x_k^{|A|}) = (e_1 \dots e_k)$，即 $x^{|A|} = e$。

将 Abel 群分解为循环群

和证明中的构造方式一致：

不妨记要分解的 Abel 群为 A，遍历 A 中元素，找到 $O\langle x\rangle$ 最大的 x，提出所有 x^k。

然后将 A 划分为 $\dfrac{|A|}{O\langle x\rangle}$ 个集合，递归的将这些集合划分为循环群。

然后找出每个集合的代表元，这些代表元组成集合 B，就将 A 划分为了 $B\times\langle x\rangle$，B 划分为循环群方式在上一步已经计算出来了。

这样每一次都会使要划分为循环群的元素个数除以 2，这样就可以 $O(n\log n)$ 的时间复杂度内划分开。

循环群性质

Z_{xy} 与 $Z_x \times Z_y$ 同构，其中 $(x, y) = 1$。

如果令 1_A 为 A 的生成元，则：

- $1_{xy} = (1_x, 1_y)$
- $(1_x, 1_y) = (1_{xy}^y, 1_{xy}^x)$

上面分别给出了双向的构造。

循环群 Z_n 生成元个数为 $\varphi(n)$。

考虑一个生成元 g，则可以将其它元素写成 g^k 的形式，$O\langle g^k \rangle = \dfrac{n}{(n, k)}$，

则满足 $(n, k) = 1$ 的 g^k 是生成元，则一共是 $\varphi(n)$ 个。

模意义下乘法（半）群

对于模 n 意义下的乘法半群，如果仅考虑 $Z_n^* = \{x|(n,x)=1\}$，那么这就是一个 Able 群（可以通过裴蜀定理证明），可以用 $\varphi(n)$ 来表示出它的元素个数。

由 Abel 群的性质可知：$(n,x)=1 \Rightarrow x^{\varphi(n)}=1$。

对于奇质数 p，$Z_p^* = ([1, p-1], \times)$ 是 Abel 群。在这个群中，$f(x) = a_n x^n + \cdots + a_0 = 0$ 的解的个数不超过 n:

若 x_n 是方程的解，那么 $f(x) = (x - x_n)g(x)$，而 $g(x)$ 最多有 $n-1$ 个解不在这 $1 + (n-1)$ 个解中的元素 y 这会使 $(y - x_n)$ 和 $g(y)$ 都不是 0。

根据这个定理（拉格朗日定理），可以证明上述群是循环群:

根据 Abel 群与若干循环群之积同构，可以得到：对于任意 $x \in [1, p-1]$，有 $O\langle x\rangle | p-1$，因为 $O\langle x\rangle$ 等于在每一个循环群上阶的最小公倍数。

所以不妨令 $S_d = \{x | O\langle x\rangle = d\}$，于是若 d 不是 $p-1$ 的约数，一定有 $S_d = \emptyset$。

又如果有 $O\langle x\rangle = d$，那么 $x^k = 1$ 就是 $x^d = 1$ 的解，根据拉格朗日定理，这 d 个数就是唯 d 解，如果 $(k, d) = 1$，那么 $O\langle x^k\rangle = d$，即 $|S_d| = \varphi(d)$。

续

于是有 $S_d = 0$ 或 $S_d = \varphi(d)$（前者是上一页中把红色的字换成“没有”的情况），又有：

$$p - 1 = \sum_i |S_i| \leq \sum_{d|p-1} \varphi(d) = p - 1$$

所以 $|S_d| = \varphi(d)[d|p-1]$。所以 $S_{p-1} \neq \emptyset$，于是就证明了上面讨论的群是循环群。称原根为满足 $O\langle x\rangle = p - 1$ 的 x，即这个群的生成元。

不妨再看看模 p^2 下的情况，现在我们要证明的是存在 $x \in Z_{p^2}^*, O\langle x\rangle = (p-1)p = \varphi(p^2)$。

不妨考虑 p 的原根 g，对于 $g+ip, i \in Z^+$，有：$\varphi(p)|O\langle g+ip\rangle, O\langle g+ip\rangle|\varphi(p^2)$，所以 $O\langle g+ip\rangle \in \{\varphi(p), \varphi(p^2)\}$。

假如 $Z_{p^2}^*$ 不是循环群，则 $O\langle g\rangle = O\langle g+p\rangle = \varphi(p)$，则：

$$1 = (g+p)^{\phi(p)} = \sum_{i=0}^{p-1} \binom{p-1}{i} p^i g^{p-1-i} =$$

$$1 + g^{-1}p(p-1) + 0 + \cdots + 0 = 1 - g^{-1}p$$

则 $p|g^{-1}$，矛盾，所以 $g, g+p$ 一定有一个阶为 $\varphi(p^2)$。

考虑 g 为 $Z_{p^2}^*$ 的原根，则可以通过归纳法：假设 g 为 $Z_{p^{c-1}}^*$ 的原根，则在 $Z_{p^c}^*$ 中有 $O\langle g\rangle \in \{\varphi(p^{c-1}), \varphi(p^c)\}$，不妨设：

$$g^{\varphi(p^{c-2})} = g^{(p-1)p^{c-3}} = 1 + p^{c-2}k \neq 1$$

则：

$$g^{\varphi(p^{c-1})} = (1 + p^{c-2}k)^p = 1 + p^{c-1}k$$

由于 $k \neq 0$，也就是说 $g^{\varphi(p^{c-1})} \neq 1$，所以 $O\langle g\rangle = \varphi(p^c)$

类似的，考虑一下 $Z^*_{2p^c}$，不难证明：$f(x) = x \bmod p^c$ 是 $Z^*_{2p^c}$ 到 $Z^*_{p^c}$ 的同构映射，所以它的性质和 $Z^*_{p^c}$ 一样。

总结

对于奇质数 p，$Z_{p^c}^*, Z_{2p^c}^*$ 都是循环群，即有原根，且恰有 $\varphi(\varphi(p^c))$ 个。

不难验证，Z_2^*, Z_4^* 都有原根，分别是 $1; 1, 3$。

上述群中元素可以用一个正整数来代表，乘法操作就可以变为 $Z_{\varphi(p^c)}$ 上的加操作。

对于其它的整数 n，Z_n^* 是 Abel 群，可以划分为若干循环群之积。群中元素可以用一个数组代表，乘法操作也可以变为若干循环群积上的加操作。

例

给定 n, a, b，满足 $n \leq 10^6, (b, n) = 1$，求下式解的个数：

$$x^a \bmod n = b$$

加强版：没有 $(b, n) = 1$ 的限制。