自由群以及群的表达

2021 年 12 月 22 日

第一节　引言

循环群是由一个元素生成的群，整数加群与循环群之间存在着紧密的联系. 我们现在想知道，对于多个元素生成的群，是否也能找到一个类似的群来刻画.

第二节　自由群的定义及性质

现在有任意非空集合 S，我们想要由 S 生成群 $F(S)$. 对于一个群而言，其中元素总是由生成元及其逆元通过群上的二元运算运算得到的. 类比由字母生成字的过程，将一串字母串起来可以得到一个字. 于是我们试图将 S 中元素看作字母进行排列，由于 $F(S)$ 需要满足群的结构，我们同时也需要定义每个字母的逆元.

定义 2.1　*$F(S)$ 是满足如下性质的群：*

1. *$F(S)$ 上定义乘法，如果 $w_1 = x_1 \cdots x_n, w_2 = y_1 \cdots y_m$，则 $w_1 \cdot w_2 = x_1 \cdots x_n y_1 \cdots y_m$.*
2. *$F(S)$ 中每个字均有逆元，亦即若 $x_1 \in F(S)$，则 $x_1^{-1} \in F(S)$，并且对于一些 $x_i \in S \cup S^{-1}$，一定有 $x_1 \cdots x_n \in F(S)$.*
3. *$F(S)$ 中有单位元，并且单位元与任意单词 w 的左右乘积依然是 w.*

由上述性质，

$$F(S) = \{e\} \cup \{x_1 x_2 \cdots x_n | x_i \in S \cup S^{-1}, 1 \leq i \leq n\}. \tag{2.1}$$

上述定义存在不完善之处，对于一个形如 $w = \cdots xaa^{-1}y \cdots$ 的字，应该与 $w' = \cdots xy \cdots$ 是同一个字，并且对形如 $\cdots x^{-1}xx^{-1} \cdots$ 的字化简方式也不止一种.

定义 2.2　*字 w 为简化字，如果 w 中没有形如 $a^{-1}a(a \in S \cup S^{-1})$ 的字串.*

性质 2.1　*对于给定的字，有唯一对应的简化字.*

证明　我们对字的长度 n 作数学归纳. 当 $n = 1$ 时，一定是简化字，归纳假设结论对小于 n 的长度均成立，对于长度为 n 且不是简化字的情况，于是至少有一个导致不是简化字的字 xx^{-1}，我们得到由有限步骤构成的消去过程，并且

1. 如果在第 k 步消去字 xx^{-1}，则可以将第 i 步换到第一步进行，于是消去后得到字的长度为 $n-2$，由归纳假设结论成立.
2. 如果在第 k 步消去 x 或 x^{-1} 之中的一个，那么那么一定有另外的 $(x^{-1}x)x^{-1}$ 或者 $x(x^{-1}x)$ 形式被消去，并且两种形式中以不同的方式消去效果一致，归结到前一种情况，结论成立. □

接着我们需要解决之前的定义问题.

定义 2.3 w 与 w' 有关系，即 $w \sim w'$，如果两者有相同的简化形式.

性质 2.2 如果 $w \sim w', u \sim u'$，则 $wu \sim w'u'$.

证明 设 w_0, u_0 分别为 w 与 w'、u 与 u' 的简化字，则由乘法的结合律，wu 经过可能不完全的简化可以得到 w_0u_0，同理 $w'u'$ 也是如此，于是 $wu \sim w'u'$. □

由上述命题我们可以修正 $F(S)$ 的定义

定义 2.4 $S \cup S^{-1}$ 上乘积运算为字符的连接并且化简为简化字，

$$F(S) = \{1\} \cup \{x_1x_2\cdots x^n | x_i \in S \cup S^{-1}\} \tag{2.2}$$

为由 S 生成的自由群. 如果 S 有限，则 $F(S)$ 为有限生成自由群.

我们想要证明每个群都是自由群的群同态像，为此需要先有自由群扩充为群同态.

定理 2.1 (自由群的泛性质) 设 G 为群，S 为非空集合，$f : S \to G$ 为映射，则 f 可以唯一扩充为群同态 $\phi : F(S) \to G$. 特别地，若取 $S \subseteq G$ 为 G 的生成元集，则可以选择 $f(x) = x$ 使 ϕ 为满同态，于是每个群都可看作自由群的同态像，根据群同态基本定理，每个群都可看做自由群的商群 $F(S)/\operatorname{Ker}\phi$.

证明 设 $w = a_1 \cdots a_n, a_i \in S \cup S^{-1}$，为了保持群结构，定义

$$\phi(a_1 \cdots a_n) = \phi(a_1) \cdots \phi(a_n)$$

并且确保 ϕ 的确是由 f 扩充而来的群同态，还需要定义

$$\phi(a_i) = \begin{cases} f(a_i), a_i \in S \\ f(a_i^{-1})^{-1}, a_i \in S^{-1}. \end{cases}$$

上述定义保持群结构并且由映射 f 唯一确定，故 ϕ 是由 f 扩充成的唯一群同态.
当 $S \subseteq G$ 为群的生成元集（注意到集合 G 本身即为群 G 生成元集，故这样的 S 总是存在的）时，我们证明 ϕ 事实上可以为满同态.
$\forall x \in G$，由于 S 是 G 的生成元集，我们有 $x = x_1^{r_1} \cdots x_n^{r_n}, x_1, \cdots, x_n \in S, r_1, \cdots r_n \in \mathbb{N}_+$，于是 $\phi(x) = \phi(x_1^{r_1}) \cdots \phi(x_n^{r_n}) = x_1^{r_1} \cdots x_n^{r_n} = x$.
因此 ϕ 为满射，于是为满同态. □

第三节　群的表达

设 G 为群，由上一节定理，对任意 G 生成元集 $S \subseteq G$，存在群同态 $\phi : F(S) \to G$ 使得

$$G = \operatorname{Im}\phi \cong F(S)/\operatorname{Ker}\phi. \tag{3.1}$$

我们将使得上述同构成立的商群记为 $F(S)/N$.

定义 3.1　如果群 $G \cong F(S)/N$, 则 G 的表达（presentation）记为

$$\langle S | r = e, r \in N \rangle . \tag{3.2}$$

特别地，如果 $R = r_1, \cdots, r_n \subseteq N$ 且包含 R 的最小正规子群为 N，则此时 R 为 N 的生成元集

$$G = \langle S | r_1 = \cdots = r_n = e \rangle . \tag{3.3}$$

S 中的元素为 G 的生成元，N（R）中元素为生成元的生成关系.

至此我们已经能够将任意群表示为自由群对于特定生成关系的商群. 回顾一下，我们先通过群 G 的生成元集 S 以及逆元全体，不经过群 G 的运算，只是按照文字排列的方式生成自由群 $F(S)$，然后寻找 $\phi : F(S) \to G$ 为满同态，通过群同态基本定理，群 $F(S)/\operatorname{Ker}\phi$ 即与群 G 同构，而 $\operatorname{Ker}\phi$ 由 N 中元或其生成元集 R 得到，故实际上群 G 是由其对应的自由群 $F(S)$ 以及对应满同态的核确定的. 形象地看，这里 $F(S)$ 提供了构建群 G 所有可能的组成方式，而 $\operatorname{Ker}\phi$ 通过定义群 G 中等于单位元的元素（亦即 $F(S)$ 中被映射为单位元的元素）决定了群 G 的最终结构.

例 3.1　循环群 $\mathbb{Z}/n\mathbb{Z} \cong \langle a \rangle / \langle a^n \rangle$，从而可以表达为 $\langle a | a^n = 1 \rangle$.

例 3.2　二面体群 D_n 的表现.
设二面体群的旋转变换为 r, 反射变换为 τ，并且 $r^n = e, \tau^2 = e, (\tau r)^2 = e$. 令 $S = r, \tau$，并且通过映射 $S \to D_n$ 诱导满同态 $\phi : F(S) \to D_n$. 并且有 $r^n, \tau^2, (r\tau)^2 \in \operatorname{Ker}\phi$.
再令 K 为包含 $r^n, \tau^2, (r\tau)^2$ 的最小正规子群，则有 $K \subseteq N$，另一方面 $F(S)/K$ 中元素根据商群的定义总是可以写成 $r^i\tau^j (0 \le i \le n-1, 0 \le j \le 1)$ 的形式，于是 $|F(S)/K| \le 2n$，故只能为 $K = N$，此时 $|F(S)/K| = |D_n| = 2n$. 根据前面的定义我们有

$$D_n = \left\langle r, \tau | r^n = \tau^2 = (r\tau)^2 = 1 \right\rangle .$$

参考文献

[1] 欧阳毅, & 叶郁. (n.d.). 近世代数.
Retrieved from http://staff.ustc.edu.cn/~ msheng/references/moderna.pdf