## 对称群与置换的符号:一个更初等的构造

**约定 1.** 设  $n \in \mathbb{Z}_+$ . 记  $N := \{1, \dots, n\}$ .

**定义 1.** 所有 N 到 N 的双射构成一个有限集,在此集合上赋予映射的复合运算就得到一个 n! 阶有限群,记为对称群  $\mathcal{S}_n$ .

对称群是非常重要的一类群,它的元素叫做置换. 可以用"符号"刻画一个置换的基本性质: 我们希望找到一个非平凡的群同态  $\rho: \mathcal{S}_n \to \mathbb{Z}/2\mathbb{Z}$ ,因为商群  $\mathcal{S}_n/\ker(\rho) \cong \mathbb{Z}/2\mathbb{Z}$  的元素等势,它将  $\mathcal{S}_n$  分为数量相等的两类. 注意,对于一般的群 G,这样的同态  $G \to \mathbb{Z}/2\mathbb{Z}$  可能不唯一,考虑  $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  即可. 当然我们将证明在二阶以上对称群情形下此同态存在且唯一.

约定 2. 我们指出加法群  $\mathbb{Z}/2\mathbb{Z}$  与乘法群  $\{\pm 1\}$  存在唯一同构,以下将不区分二者.

## 第一种构造

笔者初学时,对符号的定义方式是从置换的循环分解入手的. 命循环  $(a_1 \cdots a_n)$  之 "长度"为 n-1,对于置换  $\tau$ ,将其表为循环之积,它的长度  $l(\tau)$  等于各循环长度之和. 取符号  $\rho(\tau) = (-1)^{l(\tau)}$ . 由于循环型的唯一性,该映射良定. 通过将循环进一步分解为对换,容易验证它满足线性.

对于这种虽然较繁琐但可称经典的定义,我们不做过多讨论.写作本文的动机源于学习另一种较为简洁的方法时的一些困惑.

## 第二种构造

李文威老师在《代数学方法:卷一》中采取如下进路(这里稍作无伤大雅的改动):

考虑  $\mathcal{S}_n$  对  $\mathbb{Z}^n$  的作用  $\sigma(x_1,\cdots,x_n)=(x_{\sigma(1)},\cdots,x_{\sigma(n)})$ . 由于  $x\in\mathbb{Z}^n$  本质上是映射  $x\colon N\to Z$ ,  $i\mapsto x_i$ ,所以我们有简洁的表述  $\sigma(x)=x\circ\sigma$ .结合律表为  $\sigma(\tau(x))=x\circ\tau\circ\sigma=x\circ(\tau\sigma)$ ,所以这其实是个右乘作用.

考虑函数

$$\Delta \colon \mathbb{Z}^n \to \mathbb{Z},$$
 
$$(x_1, \cdots, x_n) \mapsto \prod_{1 \le i < j \le n} (x_i - x_j),$$

我们断言(原文作"易见")存在  $\rho(\sigma) = \pm 1$  使得  $\Delta \circ \sigma = \rho(\sigma)\Delta$ ,于是线性可顺理成章推出. 问题在于,是否真的显然? 确实, $\sigma$  的作用相当于调换了某些  $x_i$  与  $x_j$  在减号两边的位置,然而这就足够么?若要严格证明,似乎要用上归纳法了. 甚至,为什么能对这个由未定元组成的表达式进行一系列操作,也是一个有待商榷的问题.

一番冥思苦想后发现, $\Delta$  其实是个 n 元反对称多项式,可看作 n 元多项式环  $\mathbb{Z}(X_1,\dots,X_n)$  中的元素, $\sigma$  自然地作用在此环上. 由于多项式环上的运算律继承自  $\mathbb{Z}$ ,我们现在可以"逐项提取"负号从而把  $\sigma(\Delta)$  整理为形如  $(-1)^m\Delta$  的形式(我们最后给出的构造就受到这个 m 的启发). 最后,由于多项式环的整性(这也继承自  $\mathbb{Z}$ ), $(-1)^m\Delta=(-1)^{m'}\Delta$  蕴含  $(-1)^m=(-1)^{m'}$ ,于是符号映射良定.

多项式环的引入已经超出了群论的范围,它的性质也绝非显然的.因此,希望在不牺牲以上构造简明性的基础上,使用较为初等(实际上只用到集合论)的语言给出一套对于符号的定义.

## 第三种构造

这种构造是我自己想出来的,但前人应该早已提出过了.想法其实很朴素,某种意义上说是上述两种思路的融合;严格证明却不大轻松.

K与 K' 显然不交. 方便起见,我们说 K 中的序偶是正序的,而 K' 中序偶是 倒序的.

约定 4. 设  $\mathcal{P}(N)$  是 N 的幂集. 命  $\mathcal{P}(N)$  中全部二元集构成 Q.

显然 Q 的元素形如  $\{i, j\}$   $(i \neq j)$ .

定义 2. 称  $\iota: K \cup K' \to Q$ ,  $(i, j) \mapsto \{i, j\}$  为遗忘映射.

我们不难注意到  $\iota$  是满射, 且它在 K 或 K' 上的限制都是双射.

定义 3. 称  $\theta$ :  $Q \to K$ ,  $\{i, j\} \mapsto (i, j)$  (i < j) 为排序映射.

容易验证  $\theta$  是  $\iota|_{\kappa}$  的逆.

**定义 4.** 对于  $\sigma \in \mathcal{S}_n$ , 它自然诱导出映射

$$\overline{\sigma}: K \cup K' \to K \cup K', \quad (i, j) \mapsto (\sigma(i), \sigma(j))$$

 $\sigma$  是双射,因为  $\overline{\sigma^{-1}}$  是它的逆.

现在进入正题. 我们仍需定义许多顺手的记号.

约定 5. 对于 
$$\sigma \in \mathcal{S}_n$$
,记  $A_\sigma \coloneqq \overline{\sigma}(K) \cap K$ ,  $B_\sigma \coloneqq \overline{\sigma}(K) \cap K'$ ,  $C_\sigma \coloneqq \overline{\sigma^{-1}}(B_\sigma)$ .

换言之, $B_{\sigma}$ 就是  $\sigma$  作用在 K 上之后,"因相对位置遭到扰动而溢出 K 的那些序偶". 现在回顾  $\Delta$  的结构,可知  $|B_{\sigma}|$  就是"被调换先后顺序的项的数目",我们由此作出正式的定义.

定义 5.  $\rho: \sigma \mapsto (-1)^{|B_{\sigma}|}$  是  $S_n$  到  $\{\pm 1\}$  的映射,  $\rho(\sigma)$  称为  $\sigma$  的符号.

采用此进路的好处是  $|B_{\sigma}|$  当然是一个完全唯一确定的值,于是自然良定. 棘手之处在于验证群同态的线性.

以下用到一些简单的集合运算律,如  $f(A \cup B) = f(A) \cup f(B)$ ,  $(A \cap B)^c = A^c \cup B^c$ . 当 f 为双射时还有  $f(A \cap B) = f(A) \cap f(B)$ .

**引理.** 对于  $\sigma$ ,  $\tau \in \mathcal{S}_n$ , 有  $|B_{\sigma\tau}| \equiv |B_{\sigma}| + |B_{\tau}| \mod 2$ .

证明. 考察集合  $B_{\sigma\tau} = \overline{\sigma\tau}(K) \cap K'$ .

在等式两侧作用双射  $\overline{\sigma^{-1}}$  得到

$$\overline{\sigma^{-1}}(B_{\sigma\tau}) = \overline{\tau}(K) \cap \overline{\sigma^{-1}}(K'),$$

命  $D \coloneqq \overline{\sigma^{-1}}(K')$ . 将  $\overline{\tau}(K)$  写为不交并  $\overline{\tau}(K) = A_{\tau} + B_{\tau}$  得到

$$\overline{\sigma^{-1}}(B_{\sigma\tau}) = A_{\tau} \cap D + B_{\tau} \cap D.$$

对于  $A_{\tau} \cap D = A_{\tau} \cap (K \cap D)$ , 注意到

$$C_{\sigma} = \overline{\sigma^{-1}}(\overline{\sigma}(K) \cap K') = K \cap \overline{\sigma^{-1}}(K') = K \cap D,$$

于是有  $A_{\tau} \cap D = A_{\tau} \cap C_{\sigma}$ .

对于  $B_{\tau} \cap D = B_{\tau} \cap (K' \cap D)$ ,利用双射  $\iota' := \iota|_{K'}$  将其嵌入 Q 得到

$$\iota'(B_\tau\cap (K'\cap D))=\iota'(B_\tau)\cap \iota'(K'\cap \overline{\sigma^{-1}}(K')).$$

命  $\varphi := \overline{\sigma^{-1}}$ . 今断言:

$$E'\coloneqq \iota|_{K'}(K'\cap\varphi(K'))=\iota|_K(K\cap\varphi(K))\eqqcolon E,$$

这是因为 E' 中元素都形如  $(j,i) \in K'$  在  $\iota' \circ \varphi$  下的像  $x = \{\sigma^{-1}(j), \sigma^{-1}(i)\}$  (尽管不是所有的像都在 E' 中),其中 j > i 且  $\sigma^{-1}(j) > \sigma^{-1}(i)$ .

显而易见 i < j 且  $\sigma^{-1}(i) < \sigma^{-1}(j)$ ,则  $\varphi(i,j) \in K$ ,于是 x 也是  $(i,j) \in K$  在  $\iota|_K \circ \varphi$  下的像,证得  $E' \subset E$ ,反向包含同理.

于是我们得到

$$\iota'(B_\tau\cap (K'\cap D))=\iota'(B_\tau)\cap \iota|_K(K\cap \overline{\sigma^{-1}}(K)),$$

继续在两侧作用双射  $\theta$  就将 K' 嵌入到 K 中(这实际上是一个取"镜像"的过程),记  $B_{\tau}$  的"镜像"为  $\hat{B}_{\tau} \coloneqq \theta(\iota'(B_{\tau}))$ ,得到

$$\theta \circ \iota'(B_\tau \cap (K' \cap D)) = \hat{B_\tau} \cap \overline{\sigma^{-1}}(K).$$

不难验证不交并分解  $K+K'=\overline{\sigma^{-1}}(K)+\overline{\sigma^{-1}}(K')$ ,故  $D^c=\overline{\sigma^{-1}}(K')^c=\overline{\sigma^{-1}}(K)$ . 现在考虑  $C_\sigma$  于 K+K' 中的补集

$$C^c_\sigma=(K\cap D)^c=K'\cup\overline{\sigma^{-1}}(K),$$

所以

$$\hat{B_\tau} \cap \overline{\sigma^{-1}}(K) = \hat{B_\tau} \cap (K' \cup \overline{\sigma^{-1}}(K)) = \hat{B_\tau} \cap C_\sigma^c = \hat{B_\tau} \backslash C_\sigma.$$

最后,我们来证明有不交并分解  $K=A_{\tau}+\hat{B}_{\tau}$ . 考虑  $\iota$  在  $\tau(K)=A_{\tau}+B_{\tau}$  上的限制  $\iota_{\tau}$ ,不难验证  $\tau\circ\theta$  是它的逆,故它是双射, $\iota_{\tau}(A_{\tau})+\iota_{\tau}(B_{\tau})=Q$ . 在等式两侧作用双射  $\theta$  即为所求.

现在收尾. 因双射不改变集合的基数,不交并的基数保持加法,基于以上结果写出连等式

$$|B_{\sigma\tau}| = |\overline{\sigma^{-1}}(B_{\sigma\tau})| = |A_{\tau} \cap C_{\sigma}| + |B_{\tau} \cap D|,$$

我们分别计算:

$$\begin{split} |A_{\tau} \cap C_{\sigma}| &= |(K \backslash \hat{B}_{\tau}) \cap C_{\sigma}| = |C_{\sigma} \backslash \hat{B}_{\tau}| = |C_{\sigma}| - |\hat{B}_{\tau} \cap C_{\sigma}|, \\ |B_{\tau} \cap D| &= |\theta \circ \iota'(B_{\tau} \cap D)| = |\hat{B}_{\tau} \backslash \overline{\sigma^{-1}}(K)| = |\hat{B}_{\tau} \backslash C_{\sigma}| = |\hat{B}_{\tau}| - |\hat{B}_{\tau} \cap C_{\sigma}|. \end{split}$$

易知  $|C_{\sigma}| = |B_{\sigma}|, |\hat{B}_{\tau}| = |B_{\tau}|,$  两式相加立得

$$|B_{\sigma\tau}|=|B_{\sigma}|+|B_{\tau}|-2|\hat{B_{\tau}}\cap C_{\sigma}|\equiv |B_{\sigma}|+|B_{\tau}|\mod 2.$$

证毕.

以上引理说明  $\rho$  确实是群同态. n=1 时,它只能是平凡的.  $n \geq 2$  时,设对换  $\pi=(1 \ 2) \in \mathcal{S}_n$ ,算得  $B_{\pi}=\{(2,1)\}, \ \rho(\pi)=-1$ ,故  $\rho$  非平凡.

我们还须说明唯一性. 这必须先证得对称群由对换生成, 而对换都是共轭的, 这些铺垫在此略去.

**定理.**  $n \ge 2$  时,非平凡同态  $\rho: \mathcal{S}_n \to \{\pm 1\}$  存在且唯一.

证明. 存在性已证.

我们知道对换  $\tau_i = (i \quad i+1) \ (1 \le i < n)$  共轭,借由群  $\{\pm 1\}$  的交换性有

$$\rho(\tau_i) = \rho(\sigma_i \pi \sigma_i^{-1}) = \rho(\sigma_i) \rho(\pi) \rho(\sigma_i)^{-1} = \rho(\pi).$$

由于  $\mathcal{S}_n$  由对换  $\tau_i$  生成,则任取置换  $\sigma$ ,它可表为  $\sigma=\tau_{i_1}\cdots\tau_{i_{l(\sigma)}}$ ,从而

$$\rho(\sigma) = \rho(\tau_{i_1} \cdots \tau_{i_{l(\sigma)}}) = (\rho(\pi))^{l(\sigma)}.$$

故  $\rho$  完全由  $\rho(\pi)$  刻画. 若  $\rho(\pi)=1$  这无非是平凡同态; 当  $\rho(\pi)=-1$  时这就是我们构造的同态.

注意这里不需要提前证明  $l(\sigma)$  的奇偶性是确定的,相反,这是此定理的直接推论.