表现

2025 年 1 月 3 日

目录

很快啊，跳过射影幺模群来到表现着章节。

所以，我们如何描述一个群，利用凯莱定理，有限群G同构于S_n的一个子群，其中$n = \mid G \mid$，从而群G可以定义为某种置换生成的S_n的子群。这种构造的一例出现在卡迈克尔的群论书中的练习中：

设G是由下面置换生成的S_{16}的子群：

$$
\begin{aligned}
&(a\,c)(b\,d),(e\,g)(f\,h),\\
&(i\,k)(j\,l),\\
&(m\,o)(n\,p)(a\,c)(e\,g)(i\,k)\\
&(a\,b)(c\,d)(m\,o),(e\,f)(g\,h)(m\,n)(o\,p),(i\,j)(k\,l)
\end{aligned}
$$

$\mid G \mid = 256$，$\mid G' \mid = 16$ 其中$a = (i\,k)(j\,l)(m\,o)(n\,p) \in G'$，但$a$不是换位子。

描述群的第二种方法是，对某个$n \geq 2$和某个域k，用$\mathrm{GL}(n,k)$代替S_n，因为一切$n \times n$置换矩阵形成$\mathrm{GL}(n,k)$同构于S_n的子群。从而每个n阶群都可嵌入$\mathrm{GL}(n,k)$。

之前定义过4元群Q，我们来试试一种新的方法，我们把群描述为受制于某种关系的元素生成的，例如二面体群D_{2n}可以描述为$a^n = 1$和$bab^{-1} = a^{-1}$的两个元素a和b生成的，考虑下面的定义：

0.1 定义：广义四元群

广义四元数群Q_n，其中$n \geq 3$，是指由满足

$$a^{2^{n-1}} = 1, bab^{-1} = a^{-1}, b^2 = a^{2^{n-2}}$$

当$n = 3$，就是阶为8的群Q，但这定义有一个明显的缺陷，就是我们不能判断是否有这么一些群，例如，该定义下是否存在一个阶为16的群，注意的是，我们并不是只要找到一个这样的群是仅仅不够的。

为了使这种描述更加的严格，迪克(W.von Dyck) 在19世纪80年代给出了自由群的定义：

0.2 定义：自由群

若X是F的子集，对每个群G和每个函数$f : X \to G$，存在唯一的同态$\varphi : F \to G$使得对一切$x \in X$，$\varphi(x) = f(x)$

$$
\begin{tikzcd}
F \arrow[dr, dotted, "\varphi"] & \\
X \arrow[u] \arrow[r, "f"'] & G
\end{tikzcd}
$$

则说F是以X为基的自由群

该定义模仿了线性映射的定义，这就是为什么可以用矩阵来描述线性变换的理由：

0.3 定理：线性映射

令$X = v_1, \cdots, v_n$是向量空间V的基。若W是向量空间且$u_1, \cdots, u_n$是W中的表。则这里存在一个唯一的线性映射$T : V \to W$使得$T(v_i) = u_i$对所有i成立

注意到给出W的向量表$u_1, \cdots, u_n$和给定映射$f : X \to W$，其中$f(v_i) = u_i$是同一件事情。毕竟一个函数$f : X \to W$由它在$v_i \in X$上的值决定。所以我们可以画出这个定理的图：

$$
\begin{tikzcd}
V \arrow[dr, dotted, "\gamma"] & \\
X \arrow[u] \arrow[r, "f"'] & W
\end{tikzcd}
$$

若我们知道自由群是存在的，则我们可以由如下定义Q_n，令F是基为$X = \{x, y\}$的自由群，再令R是F由$\{x^{2^{n-1}}, yxy^{-1}x, y^{-2}x^{2^{n-2}}\}$生成的正规子群。接着定义$Q_n = F/R$，它很清楚的解释了，$F/R$是由$xR$和$yR$生成的。但不清楚的是$F/R$的阶是否为$2^n$。这需要证明。

第一个问题是，我们证明检验自由群是否存在，构造的思路简单，但检查细节是繁琐的，我们首先看看自由群是什么构成的。

令X是非空集合，再令X^{-1}是X的不相交的复制，也就是说X和X^{-1}不相交，且存在双射$X \to X^{-1}$，可以表示为$x \to x^{-1}$。定义X上的字母表为

$$X \cup X^{-1}$$

若n是正整数，我们定义X上长度$n \geq 1$的字为函数$w : \{1, 2, \cdots, n\} \to X \cup X^{-1}$，实际应用中，我们安如下方式给出一个长度为$n$的字$w$，若$w(i) = X_i^{e_i}$，则

$$w = X_1^{e_1} \cdots X_n^{e_n}$$

其中$x_i \in X$且$e_i = \pm 1$，我们将字的长度表示为$\mid w \mid$。例如：$\mid xx^{-1} \mid = 2$。空字我们记为1，它的长度是0。

函数相等的定义如下：若$u = x_1^{e_1} \cdots x_n^{e_n}$，$v = y_r^{e_r} \cdots y_s^{e_s}$是字，其中对所有$i, y$有$x_, y_j \in X$，则$u = v$当且仅当$m = n$有$x_i = y_i$，且$d_i = e_i$对所有$i$成立。因此，每个字都有独立的拼写。

0.4 定义：子字

一个字$w = x_1^{e_1} \cdots x_n^{e_n}$的子字不是空字，就是形如$u = x_r^{e_r} \cdots x_s^{e_s}$，其中$1 \leq r \leq s \leq n$，$w$的逆定义为$w^{-1} = x_1^{-e_1} \cdots x_n^{-e_n}$，因此对每个字$(w^{-1})^{-1} = w$

0.5 定义：既约

X上的字w是既约的，若$w = 1$或者w不存在任何形如xx^{-1}或者$x^{-1}x$的子字，其中$x \in X$

任意两个X上的字是可相乘的。

0.6 定义：并置

令$u = x_1^{e_1} \cdots x_n^{e_n}$，$v = y_1^{e_1} \cdots y_m^{e_m}$是$X$上的字，则并置指的是：

$$uv = x_1^{e_1} \cdots x_n^{e_n} y_1^{e_1} \cdots y_m^{e_m}$$

若1是空字，则$1v = v$ 且$u1 = u$

我们试着定义自由群是集合X上所有字的集合，且群上运算是并置。其单位元定义为空字1,且逆运算如定义0.4上一样。但有一个问题，若$x \in X$，$x^{-1}x = 1$要怎么处理，这有个矛盾，$x^{-1}x$的长度为2，而1是0.一个简单的方

法是，限制X上的字都是既约字，但u, v是既约字，而uv可能不是。可以用消去把uv变成既约字，但这时候证明结合性则会开始棘手。所以我们这样解决这个问题：因为像$zx^{-1}xyzx^{-1}$和$zyzx^{-1}$这样的字必须恒等，则我们利用X上一切字的集合上的一个等价关系是有意义的。若我们定义F的元素是等价类，则结合性就好证明多了，且在每个等价类中有唯一的既约字，所以可以把F的元素看做既约字，且把两个元素的乘积当做并置然后约化。

注意： 这是一个不严谨的说法，但是容易接受的。我们将默认自由群是以上面描述的形式存在。

现在，对每个集合X，存在一个自由群以X为基，且我们把X上的自由群F元素看做是约化字，运算是并置接着约化，并把元素$[w]$简单记为w

我们刚刚构造的以X为基的自由群F是X生成的，那么一个显然的问题是：任意两个以X为基的自由群是否同构？

0.7 命题：

1. 令X_1是自由群F_1的基和X_2是自由群F_2的基。若这里有一双射$f : X_1 \to X_2$，则有一个扩张了f的同构$\varphi : F_1 \to F_2$
2. 若F是以X为基的自由群，则F由X生成

证明： 命题1可以描述成下述的图：

$$\begin{tikzcd} F_1 \arrow[r, shift left, "\varphi_1"] & F_2 \arrow[l, shift left, "\varphi_2"] \\ X_1 \arrow[u] \arrow[r, shift left, "f"] & X_2 \arrow[u] \arrow[l, shift left, "f^{-1}"] \end{tikzcd}$$

我们可以认为f最终映射到F_2上，因为$X_2 \subseteq F_2$，由于F_1是以X_1为基的自由群，那么就应该存在一个拓展f的同态，$\varphi_1 : F_1 \to F_2$。类似的讨论可以得到$\varphi_2 : F_2 \to F_1$拓展了映射f^{-1}。那么复合映射$\varphi_2\varphi_1 : F_1 \to F_1$拓展了$1_X$。但$1_{F_1}$也扩张了$f$，利用扩张的唯一性，则$\varphi_2\varphi_1 = 1_{F_1}$。同样的讨论使我们得到$\varphi_2\varphi_1 = 1_{F_2}$。所以$\varphi_1$是一个同构

证明2： 设对某个集合X_1有双射$f : X_1 \to X$。若F_1是由X_1为基的自由群，令其运算为等价类上关系就有X_1生成F_1，利用命题1，那么就有一个同构$\varphi : F_1 \to F$使得$\varphi(X_1) = X$。但$\varphi(X_1)$生成$\mathrm{im}\varphi$，因此X生成F

自由群也有等级的概念，但我们首先来检查自由群中的所有基是否具有相同数量的元素。

0.8 引理

若F是以$X = x_1, \cdots, x_n$为基的自由群，则F/F'是以$X' = x_1F', \cdots, x_nF'$为基的自由阿贝尔群。其中$F'$是$F$的交换子群

证明： 注意X'生成F/F'，注意换位子子群F'是F的正规群且F/F'是阿贝尔群。我们利用如下定理证明F/F'是以X'为基的自由阿贝尔群[1]

> 令A是包含集合$X = \{x_1, \cdots, x_n\}$的阿贝尔群，再使A是满足自由群定义且以X为基的自由阿贝尔群：即对每个阿贝尔群G和每个函数$\gamma : X \to G$存在唯一的同态$g : A \to G$使得$g(x_i) = \gamma(x_i)$对所有x_i成立。则$A \cong \mathbb{Z}^n$，因此，我们说A是秩为n的自由阿贝尔群：

考虑下图：

$$\begin{tikzcd}
F \arrow[rr, "\pi"] \arrow[dr, dotted, "g"'] & & F/F' \arrow[dl, dotted, "g'"'] \\
& G & \\
X \arrow[uu, "p"] \arrow[ur, "\gamma v"'] \arrow[rr, "v"'] & & X' \arrow[uu, "p'"'] \arrow[ul, "\gamma"]
\end{tikzcd}$$

图中的G是任意阿贝尔群，p, p'是嵌入映射(inclusions)，π是自然映射，$v : x \to xF'$，$\gamma : X \to G$是函数。令$g : F \to G$是自由群定义给出的唯一同态，且$gp = \gamma v$，并定义$g' : F/F' \to G$为$wF' \to g(w)$，注意g'是well-defined的，因为G是阿贝尔群使得$F' \leq \ker g$成立。

[1] 自由阿贝尔群是以准素循环群做直积得到的

注意现在$g'p'=\gamma$，则

$$g'p'v=g'\pi p=gp=\gamma v$$

由于v是满射的，就有$g'p'=\gamma$，最后，g'是唯一存在的映射，若存在一个g''满足$g''p'=\gamma$，则g',g''生成集合X'，所以他们是等价的。

0.9 命题：

令F是基为X的自由群。若$|X|=n$，则每个F的基都有n个元素

证明： 利用上述引理，F/F'是秩为n的自由阿贝尔群，另一方面，若$y_1,\cdots,y_m$是另一组基，则F/F'也是秩为m的阿贝尔群，最后$F/F'\cong Z^n\cong Z^m$有$n=m$。

0.10 定义：秩

自由群F的秩记为$\mathrm{rank}(F)$，指的是基的元素个数。

于是，命题0.7可以描述为：两个有限自由群是同构的当且仅当它们具有相同的秩

0.11 命题：

每个群G都是一个自由群的商群。

证明： 令X是集合，且存在一个双射$f:X\to G$。（例如，我们可以取X为底集和$f=1_G$），并设F是以X为基的自由群，则存在扩张f的同态$\varphi:F\to G$，由于f是满的，所以φ也是满的。利用引理0.8和第一同构定理，$G\cong F/\ker\varphi$

我们继续描述群

0.12 定义：表现

群G的表现是有序对

$$G = (X \mid R)$$

其中X是一个集合，R是X上的字的集合。且$G = F/N$，其中F是以X为基的自由群且N是由R生成的正规子群：即R中元素的一切共轭生成的子群，并把集合X称为生成元，集合R为关系。

0.13 定义：有限表现

群G是有限生成的，若他有表现$(X \mid R)$，其中X是有限的。群G称为有限表现，若其有一个表现$(X \mid R)$，其中X和R是有限的。

0.13.1 例子

一个群有很多表现，例如$G = \mathbb{I}_6$，就有表现

$$(x \mid x^6)$$

和

$$(a, b \mid a^3, b^2, aba^{-1}b^{-1})$$

虽然我们可以给出两个不同的表现，但根据不同的表现是否能给出同构群，可证明不存在这种算法。

0.13.2 例子2

以X为基的自由群有如下表现：

$$(X \mid \emptyset)$$

自由群的名称正是来源自有一个与无关系的表现。

另一方面，关于记号，我们经常把表现中的关系写作等式，于是I_6中第二个表现的关系

$$a^3, b^2, aba^{-1}b^{-1}$$

可以写为

$$a^3 = 1, b^2 = 1, ab = ba$$

若r是$x_1, \cdots, x_n$上的字，我们可以记$r = r(x_1, \cdots, x_n)$，若H是群且$h_1, \cdots, h_n \in H$，则$r(h_1, \cdots, h_n)$表示吧每个x_i换做h_i得到H中的元素

0.14 定理：von Dyck 定理

设群G有表现

$$G = (x_1, \cdots, x_n \mid r_j, j \in J)$$

即$G = F/N$，其中F是$\{x_1, \cdots, x_n\}$上的自由群，而N是由$r_j = r_j(x_1, \cdots, x_n)$生成的$F$的正规子群，若$H = (h_1, \cdots, h_n)$是群且在$H$中对一切$j \in J$有$r_j(h_1, \cdots, h_n) = 1$，则对一切$i$存在满足$x_i N \to H$的满同态$G \to H$

证明： 若F是以$\{x_1, \cdots, x_n\}$为基的自由群，则存在同态$\varphi : F \to H$使得对一切i有$\varphi(x_i) = h_i$，因为$r_j(h_1, \cdots, h_n) = 1$，从而对所有$j \in J$有$r_j \leq \ker \varphi$。从而$\varphi$可以导出一个合理定义的同态$F/N \to H$为$x_i N \to h_i$

0.15 例子

我们先来构造一个具体的矩阵群

我们构造一个群H_n，它是定义0.1的广义四元群Q_n的一个候选者，其中$n \geq 3$，考虑复数矩阵

$$A = \begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix} \quad 和 \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

其中w是2^{n-1}次单位原根，并设$H_n = \langle A, B \rangle \leq \mathrm{GL}(2, \mathbb{C})$，我们假定$A, B$满足广义四元群定义中的关系，对一切$i \geq 1$，

$$A^{2^i} = \begin{pmatrix} w^{2^i} & 0 \\ 0 & w^{-2^i} \end{pmatrix}$$

从而$A^{2^{n-1}} = I$，实际上A确实是阶为2^{n-1}。更多的

$$B^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A^{2^{n-2}}, \ BAB^{-1} = \begin{pmatrix} w^{-1} & 0 \\ 0 & w \end{pmatrix} = A^{-1}$$

注意A, B不能交换，所以$B \notin \langle A \rangle$，因此陪集$\langle A \rangle$和$B \langle A \rangle$是不同的。由于$A$的阶为$2^{n-1}$，由此推出

$$\mid H_n \mid \geq \mid \langle A \rangle \cup B \langle A \rangle \mid = 2^{n-1} + 2^{n-1} = 2^n$$

在下一个定理我们将证明每个这样的H_n阶为2^n

0.16 命题：

对$n \geq 3$，广义四元数群Q_n存在

证明： 令G是下述定义的表现

$$(a, b \mid a^{2^{n-1}}, bab^{-1} = a^{-1}, b^2 = a^{2^{n-2}})$$

G_n满足广义四元数定义中的所有要求，但有一个例外，它的阶是否都是2^n。利用von Dyck's定理，存在一个满射同态$G_n \to H_n$，其中H_n是上边例子构造的群，那么$\mid G_n \mid \geq 2^n$

另一方面，G_n中的循环群$\langle a \rangle$阶至多为2^{n-1}，因为$a^{2^{n-1}} = 1$，反射$bab^{-1} = a^{-1}$可知$\langle a \rangle \lhd G_n = \langle a, b \rangle$，那么$G_n / \langle a \rangle$是由$b$的象生成的，最后，由于$b^2 = a^{2^{n-2}}$，那么$\mid G_n / \langle a \rangle \leq 2$就有

$$\mid G_n \mid \leq \mid \langle a \rangle \mid\mid G_n / \langle a \rangle \mid \leq 2^{n-1} \cdot 2 = 2^n$$

因此$\mid G_n \mid = 2^n$且$G_n \cong Q_n$

这表明了上述例子的群$H_n \cong Q_n$

注： 二面体群D_{2n}也可以由上面那样证明，表现也是一样的

0.17 命题：

二面体群D_{2n}也有表现：

$$D_{2n} = (a, b \mid a^n = 1, b^2 = 1, bab = a^{-1})$$

证明： 利用von Dyck's定理，构造满射同态$f : C_{2n} \to D_{2n}$，就有$\mid C_{2n} \mid \geq 2_n$。接着为了证明$f$是同构。只需要像命题0.16一样即可。其循环群$\langle a \rangle \in C_{2n}$阶至多为n，因为$a^n = 1$，由于$bab^{-1} = a^{-1}$，则$\langle a \rangle \lhd C_{2n} = \langle a, b \rangle$。因此$C_{2n} / \langle a \rangle$是$b$的像生成的。最后，$b^2 = 1$，则$\mid C_{2n} / \langle a \rangle \mid \leq 2$，有

$$\mid C_{2n} \mid \leq \mid \langle a \rangle \mid\mid C_{2n} / \langle a \rangle \mid \leq 2n$$

因此$\mid C_{2n} \mid = 2n$且$C_{2n} \cong D_{2n}$

现在，我们给出一个定理更简单的证明：

0.18 命题

每个阶为6的非阿贝尔群G同构于S_3

证明： G首先得包含2阶和3阶的元素a, b。因为$\langle a\rangle = 2$，那么$\langle a\rangle \lhd G$就有$bab^{-1} = a$或者$bab^{-1} = a^{-1}$。但第一种情况不可能发生。因为G不是阿贝尔群，现在G满足$D_6 \cong S_3$的表示条件。那么就有一个映射$D_6 \to G$由于两个群阶一样，所以是同构。

最后，我们对8阶的群进行分类

0.19 定理：

每个阶为8的群都同构于：

$$D_8, Q, \mathbb{I}_8, \mathbb{I}_4 \oplus \mathbb{I}_2, \text{or } \mathbb{I}_2 \oplus \mathbb{I}_2 \oplus \mathbb{I}_2$$

中的某一个，这些群俩俩之间不同构

证明： 若G是阿贝尔群，由基定理，G自身就是循环群的直和，而基本定理证明这种群只有列出的这些，因此我们假定G是非阿贝尔群。

首先，G不可能有8阶元素，否则其是循环群。因此就是阿贝尔群。此外每个非单位元都可以为2阶的。为避免G变阿贝尔群，则G有一4阶元素a。所以$< a >$的指数为2。所以这是一个极大子群，从而$G =< a, b >$，由于$G/ < a >$是2阶的，所以$b^2 \in < a >$从而$b^2 = a^i$，其中$0 \leq i \leq 3$。注意不可能有$b^2 = a$或者$b^2 = a^3 = a^{-1}$，否则b的阶是8.所以

$$b^2 = a^2, b^2 = 1$$

有这么两种情况，其次，利用b的正规性，$bab^{-1} \in < a >$，从而$bab^{-1} = a$或者$bab^{-1} = a^{-1}$。由于a, b可交换。这意味着G是阿贝尔群，所以只有$bab^{-1} = a^{-1}$。所以只有两种可能性

$$a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}$$

或

$$a^4 = 1, b^2 = 1, bab^{-1} = a^{-1}$$

利用命题0.16，当$n = 3$的时候是8阶群，正好是第一种表现，命题0.17给出第二种表现。利用von Dyck定理，则存在满同态$Q \to G$或者$D_8 \to G$，然而$| G |= 8$，所以这是个同态。

最后，Q和D_8是不同构的，Q的2阶元唯一，而D_8有好几个2阶元素