群的初步知识

这篇笔记里，我们介绍群论的基本知识。在第一部分里，我们从变换群的角度去重新表述仿射变换中已经提到的一些现象，而把有关概念的抽象定义留给第二部分。在第二部分里，我们介绍抽象群论的一些标准术语和基本例子。建议把两部分参照起来阅读。

对于仿射变换的观察

考虑空间仿射变换全体构成的集合$\mathrm{Aff}(E^3)$。它的元素都是平面仿射变换$\phi: E^3 \to E^3$，而且复合是这个集合上一个天然的二目运算，即对任意$\phi, \psi \in \mathrm{Aff}(E^3)$，总有$\phi \circ \psi \in \mathrm{Aff}(E^3)$。我们知道：复合运算有结合律，即对于任意$\phi_1, \phi_2, \phi_3 \in \mathrm{Aff}(E^3)$，满足$\phi_1 \circ (\phi_2 \circ \phi_3) = (\phi_1 \circ \phi_2) \circ \phi_3$；空间的恒同变换属于$\mathrm{Aff}(E^3)$；任何空间仿射变换的逆变换也属于$\mathrm{Aff}(E^3)$。根据上述几条性质，我们就说集合$\mathrm{Aff}(E^3)$关于其复合运算构成一个群，而且它（作为仿射变换）作用在空间E^3上。这是一般的抽象群和群作用的一个具体例子。按群论的一般记号，以下我们也把复合记号$\circ$省去不写。

从空间仿射变换群$\mathrm{Aff}(E^3)$出发，我们可以获得一些新的变换群：

(1) 考虑保距变换全体构成的子集$\mathrm{Isom}(E^3)$。它在复合运算下封闭，依然包含恒同和取逆的运算。于是，我们说它是$\mathrm{Aff}(E^3)$的一个子群。

(2) 空间中全体平移变换也构成空间仿射变换群$\mathrm{Aff}(E^3)$的一个子群，本篇中记作$\mathrm{Transl}(E^3)$。它是$\mathrm{Aff}(E^3)$的一个*正规子群*，这就是说，对于任意的$\phi \in \mathrm{Transl}(E^3)$和任意的$\psi \in \mathrm{Aff}(E^3)$，总有$\psi^{-1}\phi\psi \in \mathrm{Aff}(E^3)$。它本身还是一个*交换群*，这就是说，对于任意$\phi, \psi \in \mathrm{Transl}(E^3)$，总有$\phi\psi = \psi\phi$。（请自行验证，并说明$\mathrm{Isom}(E^3)$既不是$\mathrm{Aff}(E^3)$的正规子群，其本身也不是交换群。）

(3) 给定任何空间图形$X \subset E^3$，我们介绍过它的保距对称群
$$\mathrm{Isom}_{E^3}(X) = \{\phi \in \mathrm{Isom}(E^3) : \phi(X) = X\}$$
类似地，我们还可以引进它的仿射对称群
$$\mathrm{Aff}_{E^3}(X) = \{\phi \in \mathrm{Aff}(E^3) : \phi(X) = X\}$$
后者当然包含前者，但它们一般不相等。用一般群作用的术语，它们也相应地被称为X在$\mathrm{Isom}(E^3)$和$\mathrm{Aff}(E^3)$中的*稳定化子群*。

(4) 在（3）中把X取作单点O，这时的$\mathrm{Aff}_{E^3}(O)$和$\mathrm{Isom}_{E^3}(O)$也称为点O处的（仿射或保距的）迷向子群（isotropy subgroup）。我们可以选取单位正交标架$(O; \boldsymbol{e}_1, \boldsymbol{e}_2, \boldsymbol{e}_3)$，通过仿射坐标，任何$\phi \in \mathrm{Aff}_{E^3}(O)$可以唯一地表示成一个三阶可逆实方阵$A_\phi \in \mathrm{GL}(3, \mathbb{R})$，而任何$\phi \in \mathrm{Isom}_{E^3}(O)$进一步要求方阵正交，即$A_\phi \in \mathrm{O}(3)$。实际上，上述表示给出了（由标架选取决定的）群同构$\mathrm{Aff}_{E^3}(O) \cong \mathrm{GL}(3, \mathbb{R})$和$\mathrm{Isom}_{E^3}(O) \cong \mathrm{O}(3)$。

对于空间仿射变换$\phi: E^3 \to E^3$，我们有诱导的变换$\phi_*: V(E^3) \to V(E^3)$。（后者把任何有向线段$AB$映作有向线段$\phi(A)\phi(B)$，从而把向量映作相应的向量。）我们验证过$\phi_*$是良定义的可逆线性变换。由于向量空间$V(E^3)$的全体线性变换关于复合构成群，记作$\mathrm{GL}\big(V(E^3)\big)$，进行诱导的操作就给出一个映射：
$$\mathrm{Aff}(E^3) \to \mathrm{GL}\big(V(E^3)\big), \qquad \phi \mapsto \phi_*$$

它保持复合运算的形式不变，即满足$(\phi\psi)_* = \phi_*\psi_*$。于是，我们说这个映射是一个*群同态*。它是一个满同态，而它的核（即恒同线性变换的原像）恰好是平移组成的正规子群$\mathrm{Transl}(E^3)$。

现在，任取E^3中单点O。我们注意到$\mathrm{Aff}_{E^3}(O)$与$\mathrm{Transl}(E^3)$交集只包含恒同变换。于是诱导同态限制在$\mathrm{Aff}_{E^3}(O)$是单同态，但它仍然映满整个$\mathrm{GL}\big(V(E^3)\big)$。于是任何$\phi \in \mathrm{Aff}(E^3)$可以唯一地分解成复合$\phi = \tau\psi$，其中，$\tau \in \mathrm{Transl}(E^3)$，$\psi \in \mathrm{Aff}_{E^3}(O)$。关于这个分解，变换的复合是相对容易理解的：如果$\phi = \tau\psi$，$\phi' = \tau'\psi'$，那么$\phi\phi' = \tau\sigma_\psi(\tau')\psi\psi'$，其中$\sigma_\psi(\tau') = \psi\tau'\psi^{-1}$。换言之，复合变换$\phi\phi'$的平移部分由$\tau\sigma_\psi(\tau')$给出，而迷向部分由$\psi\psi'$给出。与此相比，我们也讨论过用反射复合产生保距变换，但在那里复合的规律并不容易把握。

这是群的*半直积*分解的具体例子。由此，我们说空间仿射变换群是它的平移正规子群与它的（任何一个）仿射迷向子群的半直积。上述半直积分解的描述固然告诉了我们单个仿射变换是如何由较熟悉的变换复合而成的，但它更多地着眼于空间仿射变换群在群结构层次上的分解。后一种看法在各种更一般的群论中有着广泛的运用。

群论的几个基本概念

定义　我们所谓的集合G上的一个*群结构*，包括如下信息：（1）一个特定的元素$e \in G$，称为*恒等元*；（2）一个二目运算$G \times G \to G$ 称作*乘法*，记作$(g,h) \mapsto gh$；（3）以及一个单目运算$G \to G$称作*取逆*，记作: $g \mapsto g^{-1}$。而且，它们被要求满足：（1）恒等元是乘法的左右单位，即对于任意$g \in G$，有$eg = ge = g$；（2）乘法满足结合律，即对于任意$g,h,k \in G$，有 $(gh)k = g(hk)$；(3)取逆运算给出乘法的左右逆元，即对于任意$g \in G$，有 $g^{-1}g = gg^{-1} = e$。指定了群结构的集合G就称为一个抽象的*群*。

练习　验证就任何群而言，其乘法的左右单位必须唯一，其乘法的左右逆元必须唯一，乘积的取逆等于取逆的反序乘积，取逆再取逆等于恒同。

例　设X是一个集合，则全体可逆映射$\sigma: X \to X$组成一个群 $\mathrm{Perm}(X)$，即X的*置换群*（group of permutations）：恒同变换是其恒等元，映射的复合是其乘法，映射的取逆是取逆运算。特别地，有限集合$\{1,2\cdots,n\}$的置换群称为*n元对称群*（symmetric group on n elements），通常记作S_n。（我们之前也定义过度量空间中的图形的保距对称群，由于上下文完全不同，但愿不至于混淆。）S_n中的元素常常记作

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

的形式，下边行是上边行的一个排列，意思是$\sigma(k) = i_k$。因为我们的映射遵循左式记号，即$(\sigma\tau)(k) = \sigma(\tau(k))$，所以，记号的乘法形如：

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$$

例　设X是一个集合，A是其子集，则所有保持A不变的置换（即满足$\sigma(A) = A$者）构成也一个群，称为置换群 $\mathrm{Perm}(X)$的关于A的*稳定化子群*（stabilizer）。这个构造给出置换群的许多子群的例子，但不是全部。比如*轮换*（rotation）

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 2 & 3 & \cdots & n & 1 \end{pmatrix}$$

生成的群实际上由置换$\mathrm{id}, \tau, \tau^2, \cdots, \tau^{n-1}$构成，它却没有非平凡的不变子集合。和它同构的群

称为n阶*循环群*（cyclic group of order n），通常记作C_n。（就有限群而言，其作为集合的元素个数即称为这个群的阶。）

定义　两个群G、H之间的一个*同态*就是一个保持乘法的映射$\phi: G \to H$，即对于任意$g, g' \in G$，有$\phi(gg') = \phi(g)\phi(g')$。

练习　验证群同态把恒等元映到恒等元，互逆元素映到互逆元素。

例　设G是一个群，X是一个集合。群G在X上的一个*作用*（action）是这样的一个映射$\alpha: G \times X \to X$，写作$(g, x) \mapsto \alpha_g(x)$，要求满足$\alpha_e(x) = x$和$\alpha_{gh}(x) = \alpha_g(\alpha_h(x))$。群在集合上的每个作用可以等价地刻画为一个同态$\phi: G \to \mathrm{Perm}(X)$：给定群作用，我们可以定义置换$\phi(g): X \to X$为$x \mapsto \alpha_g(x)$；反过来，任何同态$\phi: G \to \mathrm{Perm}(X)$也唯一地给出群作用$(g, x) \mapsto \phi(g)(x)$。这个两个过程是自然而且互逆的。

例　设G是一个群。它在自己上有三个自然的作用：*左作用*$L_h(g) = hg$，*右作用*$R_h(g) = gh^{-1}$，以及*共轭作用*$\sigma_h(g) = hgh^{-1}$（conjugation）。但是，注意$R_h^*(g) = gh$给出的并非我们所谓的作用，因为它在复合下是反变的：$R_{hk}^*(g) = R_k^*\big(R_h^*(g)\big)$。

练习　对于任意群同态$\phi: G \to H$，验证它的核

$$\mathrm{Ker}(\phi) \coloneqq \{g \in G: \phi(g) = e \in H\}$$

构成一个群，且它在共轭作用下不变，即对于任意$\mathrm{g} \in \mathrm{G}$，有$\sigma_{\mathrm{g}}\big(\mathrm{Ker}(\phi)\big) = \mathrm{Ker}(\phi)$；它的像

$$\mathrm{Im}(\phi) \coloneqq \{\phi(g) \in H: g \in G\}$$

也构成一个群。

定义　给定群G的一个*子群*H是一个在乘法和取逆下封闭的子集合，并由此而具有继承的群结构。如果群G有一个子群H，则H的一个*左陪集*是群G关于等价关系$g \sim g' \Leftrightarrow \exists h \in H: g = g'h$的等价类，它们形如子集$gH = \{gh \in G: h \in H\}$。*右陪集*的定义类似，形如$Hg = \{hg \in G: h \in H\}$。

定义　如果G的一个子群N在G的共轭作用下不变，就称之为一个*正规子群*。设N是G的正规子群，则N-*陪集*（coset）的集合

$$G/N \coloneqq \{gN \subset G: g \in G\}$$

关于诱导的乘法$(gN)(hN) = (gh)N$构成的群称为G模N的*商群*。

练习　验证正规子群的左陪集都是同样代表元素的右陪集。

练习　验证商群的乘法定义是合理的，即与陪集代表元选取无关。

于是下述定理无非是前边练习的重新概括：

定理　设N是G的正规子群，则存在自然的群同态*短正合列*（short exact sequence）

$$\{e\} \longrightarrow N \xrightarrow{\iota} G \xrightarrow{\pi} G/N \longrightarrow \{\mathrm{e}\}$$

这里的意思是，在每一个同态接合处，前一同态的像都等于后一同态的核。具体来讲，即ι是

单同态（放入），π是满同态（取模），并且$\mathrm{Im}(\iota) = \mathrm{Ker}(\pi)$。

一般来说，如果知道了给定群的一个正规子群和它的相应商群，我们还不完全知道原来群的结构。比如，如果一个群有一个正规子群同构于C_4，其商群又同构于C_2，那么这个群可能是C_8，也可能是$C_4 \times C_2$，或者二面体群D_4（平面上正方形的保距对称群）。这里，我们遇到了所谓的扩张问题。

一种比较简单的情形是，如果G还有一个子群H，它在模N的商同态下被同构地映满G/N。这时H的元素作为代表元恰好不重复不遗漏地枚举N的陪集，所以G中元素都可以唯一地写成$g = nh$的形式，其中$n \in N, h \in H$。这样，我们说G是一个*半直积*（semi-direct product），写作$N \rtimes H$。作为集合，G可以等同为集合的直积$N \times H$，但等同之下乘法并非对应分量相乘。实际上，容易验证，

$$(n, h)(n', h') = (n\sigma_h(n'), hh')$$

这表明N分量的乘法要经受H的一次共轭作用。

注记　更一般地，任给群N, H，以及同态$\alpha: H \to \mathrm{Aut}(N)$，我们可以定义抽象的半直积$N \rtimes_\alpha H$为集合$N \times H$并赋予乘积$(n, h)(n', h') = (n\alpha_h(n'), hh')$。比如，$C_4$的自同构只有两个，一个是恒同，另一个非平凡的α刚好是C_4的取逆，它们定义的抽象的半直积分别同构于直积$C_4 \times C_2$和二面体群D_4。

[本稿由原作者刘毅修订于 2017-10-31]