数、对称性与群

by 2501-Evortexio.7

> *Algebra is generous; she often gives more than is asked of her.*
>
> Jean d'Alembert

计数与对称

我们从很小就接触数字和运算．通过**计数**（counting），我们创造出一系列自然数并发现它们有无穷多个．接着我们在自然数中做加法（多次后继）和乘法（多次相同的加法）如 $3+14=17$，$7\times 4=28$ 等，经过推广发现它们的结果总是落在自然数中：[1.]

$$\times:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$$
$$+:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$$

当我们试图寻找某次加法或乘法之前的数——即解一元一次方程——时，我们发现解并不总是落在自然数中．为此，我们又从减法——加法的逆——定义了负数，从除法——乘法的逆——定义了分数，使一元一次方程总是有解．我们把所有这些数叫做**有理数**（rational number）[2.]．接着人们在求解更高次代数方程的过程中发现了一些数，容易证明它们不是有理数，如 $\sqrt{5}$，$\sqrt[7]{6}$，$\sqrt{7+\sqrt{3}}$ 等；在几何学中，我们发现圆周率 π 不是有理数；在微积分中，我们又用级数展开的方法验证了 e 不是有理数．我们把它们统称为**无理数**（irrational number）[3.]．把所有有理数和无理数合在一起，我们验证了它们具有多种运算的完备性，并把它们叫做**实数**（real number）．

16世纪数学家Cardano在《大术》中给出了三次方程的一般解法，却意外得到了 $\sqrt{-121}$ 的"不合理的"结果．Descartes就此发明了**复数**（complex number）．后来 De Moivre 和 Euler 将复数与二维旋转联系起来，极大地扩展了其实际意义．

以上是我们熟知的故事，也大致是我们认识数的历程．

未来学习工科的同学还可能接触到 Hamilton 拓展复数发明的**四元数**（quaternion）[4.]，它们在三维旋转的表示上十分方便．在密码学和抽象代数[5.]中还会遇到**有限域**（finite field）中的元素．此外，对计算机有了解的同学一定很熟悉 $\boldsymbol{p}$ **进数**（p-adic number）．这些都被称为"数"．

著名的 Leonhard Euler 和 Gauss 都曾经研究过一类数字对整数模的代数运算——**模算术**（modular arithmetic）[6.]．它是把**同余**（congurency）作为等价关系的一种新的算术系统．学过竞赛的同学可能知道，我们这里再简单介绍一下．

> *Def* 1.1　同余 同余类 模运算
>
> ---
>
> 设 a, b, m 为整数，若 m 整除 $a-b$，则称 a 与 b 关于模 m 同余．通常记为 $a \equiv b \pmod{m}$．
>
> 关于整数 m 同余的所有整数叫做一个**模-m 同余类**（congurent class modulo m）．
>
> 把取整数 a 除以正整数 m 的余数记作 $a \mod m$，$(a+b) \mod m$ 叫做 a 和 b 关于模 m 的加法，$(a \times b) \mod m$ 叫做 a 和 b 关于模 m 的乘法；求解形如 $a+x \equiv c \pmod{m}$ 的方程的运算叫做模减法，求解形如 $ax \equiv c \pmod{m}$ 的方程的运算叫做模除法；此外还可以类比出模乘方和离散对数．它们统称为**模算术**（modular arithmetic）．

举几个例子就可以简单地说明．

$$-4 \equiv 38 \equiv 31 \equiv 3 \pmod{7}$$

显然它们除以 7 的余数都是 3，或者说它们任意两者的差都是 7 的倍数．

一共有 3 个模-3 同余类，分别是 [7.]：

$$\begin{aligned}
[0]_3 &= 3\mathbb{Z} = \{\dots, -6, -3, 0, 3, 6, \dots\} \\
[1]_3 &= 3\mathbb{Z}+1 = \{\dots, -5, -2, 1, 4, 7, \dots\} \\
[2]_3 &= 3\mathbb{Z}+2 = \{\dots, -4, -1, 2, 5, 8, \dots\}
\end{aligned}$$

同理对于正整数 m，也有 m 个模-m 同余类．

模运算类似于钟表的记时．八点以后七个小时是三点，即 $(8+7) \mod 12 = 3$．试着将钟表的刻度从 12 个改为任意正整数 m 个，便可以类比出模-m 算术．值得注意的是，模算术中除法、负数幂和对数运算并不是对算术数值取余数，而是模意义下的"逆运算"．

$$\begin{aligned}
5+8 \equiv 6 \pmod{7} &\implies (5+8) \mod 7 = 6 \\
3 \times 7 \equiv 1 \pmod{10} &\implies (3 \times 7) \mod 10 = 1 \\
3 \times 11 \equiv 1 \pmod{8} &\implies (1/3) \mod 8 \\
&\quad = 11 \mod 8 \\
&\quad = 3
\end{aligned}$$

注意模-m 算术的结果必须落在集合 $\{0, 1, 2, \ldots, m-1\}$ 中，这个集合我们常常记作 $\mathbb{Z}_m$ ；如果算术结果不在 $\mathbb{Z}_m$ 中，则要对结果关于 m 取余数使它落在该集合中.

再来回顾一下小学时学习的"对称"这个概念.

对称（symmetry）指的是一个对象经过某种操作，其形状与原来相重合的性质．我们在数学课上只学习过轴对称和中心对称两种对称性，但是在结构化学和有机化学中，我们遇到过许多其它的对称性．比如正多面体对称性（想想 $\mathrm{CH_4}$ 和 $\mathrm{SF_6}$ ）、n-重旋转轴（绕轴旋转 $2\pi/n$ 后与原图形重合，图中 $n=7$ ）、镜面对称（想想一对光学对映体）、旋转中心对称（顾名思义，其对称元素通常称作反轴）、平移对称性（想想晶体点阵和晶胞）等，下图（图1-1）展示了它们.

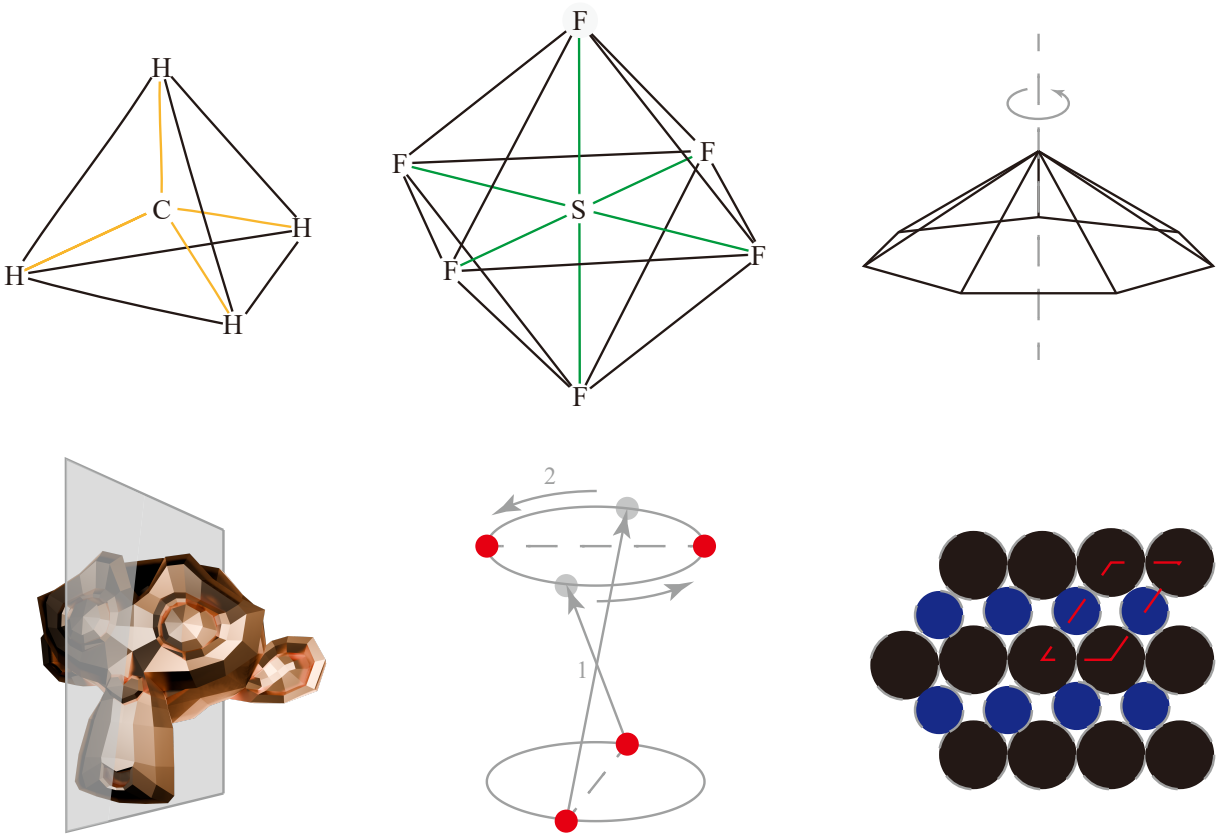


fig_1.1

但是，我们从未系统地研究过它们.

我们不妨从简单的平面正六边形开始．很容易发现它有12种对称操作，分别是（表1-1，图1-2）：

不变	**顺时针旋转** 60°	**顺时针旋转** 120°	**顺时针旋转** 180°	**顺时针旋转** 240°	**顺时针旋转** 300°
翻面	**翻面再顺时针旋转** 60°	**翻面再顺时针旋转** 120°	**翻面再顺时针旋转** 180°	**翻面再顺时针旋转** 240°	**翻面再顺时针旋转** 300°

table_1.1

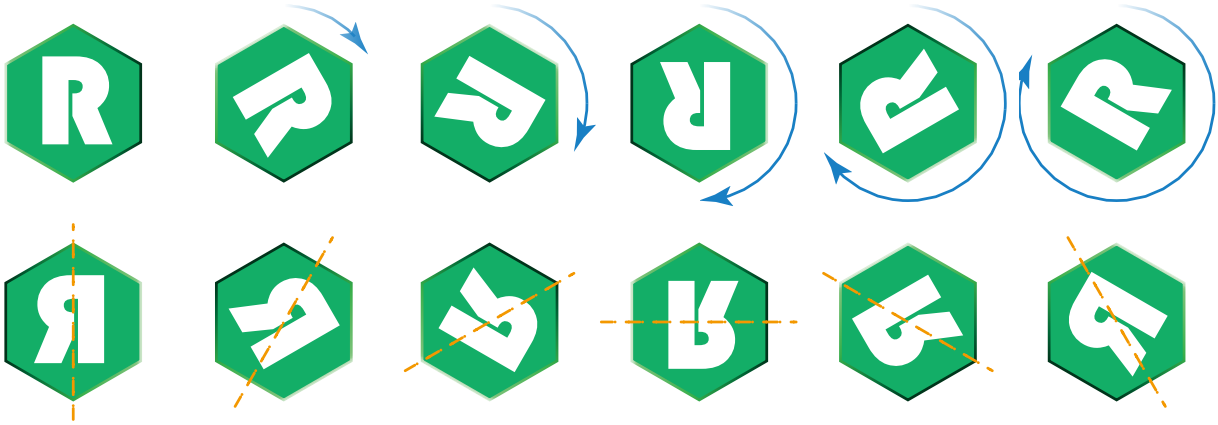


fig_1.2

其中翻面两次相当于不变，顺时针旋转 360° 相当于不变．我们发现，每种对称操作都是由几个“翻面”和“旋转 60° ”复合而成的．而任意两个操作相继进行，结果还是对称操作的一种；每种对称操作都有一个操作可以让它恢复为“不变”．

数与对称都是我们熟悉的东西．但是它们有什么关系呢?

群和它的表示

在解决五次方程通解的过程中，Lagrange 和 Ruffini 等数学家已经意识到了一些朴素的置换群理论的内容．后来在两位英年早逝的天才数学家 Niels Abel [8.] 和 Évariste Galois [9.] 的努力下，群论作为一门数学理论终于得以建立．后来又经过了几代数学家如 Cayley（他发明了后面要讲到的 Cayley 表）、Dedekind（就是这位通过著名的 Dedekind 分割完善了实数理论）、Klein（将群论与几何对称紧密联系）、Sophus Lie（他通过连续群研究微分方程，这类被命名为“Lie 群”的群成为数学和物理学中最重要的元素之一）的研究，群论逐渐完善，并与其他学科如影射几何和拓扑学相结合，筑起了现代数学的大厦．在这个过程中，很多数学家都曾对群提出了自己的定义，而第一个将数论、几何和多项式理论中的群用统一定义表述的是 Klein 的学生 Walther von Dyck，他在1882年首次给出了被认为是“现代的”群的定义．

我们先来给出我们的**群**（group）的定义．这是一种最常见、也相对现代的定义，几乎所有抽象代数的教科书上都使用它来描述群这种数学元素．

Def 2.1　群

群是一个集合 G 和在它上面定义的二元运算 [10.] $\circ$（可称作群乘法）组成的二元组 $(G, \circ)$ 使满足以下公理：

- **封闭性**（closure）：对于任意 $a, b \in G$，$a \circ b \in G$
- **结合律**（associativity）：对于任意 $a, b, c \in G$，$(a \circ b) \circ c = a \circ (b \circ c)$
- **单位元**（identity）：存在 $e \in G$，使对于任意 $a \in G$，有 $e \circ a = a \circ e = a$
- **逆元**（inverse）：对于任意 $a \in G$，都存在一个 $b \in G$ 使得 $a \circ b = e$，它通常记作 a^{-1}

注意这里的群乘法“ $\circ$ ”并不是真正的乘法，而只表示一种**二元运算**（binary operation，$\circ : G \times G \to G$），它可以是数的加减乘除、集合交并差积、函数算子组合等等甚至是全新定义的运算，它并不一定满足交换律．尽管如此，我们在大多数情况下还是把它省略，将 $a \circ b$ 写作 ab，将 $\underbrace{a \circ a \circ \cdots \circ a}_{n}$ 记作 a^n，将 $\underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n}$ 记作 a^{-n}．如果集合 G 上的运算已经在上文中规定，我们常说 G 是群．

上面的定义似乎有些抽象，我们先用自然语言复述一下．首先封闭性保证了无论哪些、多少个元素在这种运算下的结果都落在群内．结合律代表着运算的一种“稳定性” [11.]，它使得如果几个元素在一定顺序下得到 e，那么它们以同样的顺序连续出现在运算中时可以消去．单位元类似于加法中的 0 或乘法中的 1，它与其它任何元素运算都得到元素自身．而逆元的存在保证了群中每一个元素都可以在某种情况下消去．群乘法“ $\circ$ ”不一定满足交换律，如果它满足总是交换律则称这个群为 **Abel 群**（Abelian group） [12.]．

应该承认，这样的定义不是很 reasonable，我们很难从中看出这样做的 motif．但是对于数学中很多比较抽象的概念，我们不可能总是要求在读到它们时就完全理解．不如先记住这些定义，并用它们来检验一些例子和练习．在不断使用的过程中，你会发现你慢慢地理解了这些看似抽象的 definition．下面我们就来看一些常见的群的例子吧~

E.g.　2.1.1　整数集 $\mathbb{Z}$ 在普通加法运算下构成 Abel 群．单位元是 0，逆元是相反数．

E.g.　2.1.2　整数集 $\mathbb{Z}$ 在普通乘法下不构成群，因为没有逆元．

E.g.　2.1.3　所有非零有理数 $\mathbb{Q}^*$ 在普通乘法下构成 Abel 群，单位元是1，逆元是倒数．

E.g.　2.1.4　实数集 $\mathbb{R}$ 和复数集 $\mathbb{C}$ 既构成加法群也构成乘法群，但是要注意乘法群不包含 0．

E.g. 2.1.5 所有 n-维向量在向量加法下构成 Abel 群.

E.g. 2.1.6 “计数与对称”一节中提到的六边形的 12 种对称操作在“相继操作”的二元运算下构成群，但不是 Abel群，称作 12 阶二面体群，记作 D_6 . 顺时针旋转 60° 再翻面相当于翻面再顺时针旋转 300°，显然交换律不成立. 更一般地，所有正 n 面体的全部对称操作都可以各自成群，它们是 $2n$ 阶**二面体群**（dihedral group），记作 D_n .

E.g. 2.1.7 如果你学过线性代数，那么你会发现：所有 $n \times n$ 矩阵（实或复）在矩阵乘法下构成群，我们称之为**一般线性群**（general linear group），记作 $GL(n, \mathbb{F})$ （ $\mathbb{F}$ 是实数集或复数集等数域）；所有行列式为 1 的 $n \times n$ 矩阵（实或复）在矩阵乘法下构成群，我们称之为**特殊线性群**（special linear group），记作 $SL(n, \mathbb{F})$. 它们都是非 Abel 群.

读到这里，你应该已经对群有了一个基本的感受. 群有几条比较重要的基本性质，它们都直接从定义中得出.

> $(a^{-1})^{-1} = a$，即逆元关系是“互为逆元”.
>
> 单位元 e 在群中是唯一的.
>
> **消去律**（cancellation）：如果 $ab = ac$ 或 $ba = ca$，那么 $b = c$.
>
> 逆元 a^{-1} 对群元素 a 是唯一的.
>
> **鞋袜律**（socks-shoes property）：$(ab)^{-1} = b^{-1}a^{-1}$，你可以理解为先穿上袜子再穿鞋再戴鞋套，这一系列行为的反面是先脱掉鞋套再脱掉鞋再脱袜子~

下面证明前三条性质为例. 另外两条性质~~有大托梦给我~~请读者自行尝试证明.

证明 首先证明右消去律. 若 $ba = ca$，则 $baa^{-1} = caa^{-1}$，由结合律 $b(aa^{-1}) = c(aa^{-1})$ 即 $b = be = ce = c$. ■

注意到命题 $(a^{-1})^{-1} = a$ 等价于 $e = a^{-1}a$，已知 $aa^{-1} = e$，可得 $a^{-1}aa^{-1} = a^{-1}e = ea^{-1}$，由右消去律同时消去 a^{-1} 可得 $a^{-1}a = e$ as desired.

由于 $a^{-1}a = e$，与右消去律同理可证得左消去律.

若有两个单位元 e_1 和e_2，则 $a = ae_1 = ae_2$，由消去律 $e_1 = e_2$. $\mathcal{Q.E.D}$ ~

我们把群中元素的个数叫做群的**阶**（order），记作 $|G|$. 我们前面例子中的群，除去表征对称性的二面体群以外，其它群的阶都是 ∞，这样的群叫做**无限群**（infinite group），否则叫做**有限群**（finite group）. 那么是否还有其它有限群呢?

TRIVIALLY!

下面我们来看一看一种特殊但是重要的群——**循环群**（cyclic group）．

在上文模运算的学习中我们认识了一个叫做 $\mathbb{Z}_m$ 的数集，它表示所有小于 m 的自然数，也可以理解为关于 m 的模运算所有可能的结果．容易发现，在模加法下，这个集合满足封闭性的条件；我们可以验证 0 是它的单位元；其它每个元素的逆元都是与它相加等于 m 的那个数（取模后等于零）；显然满足结合律．因此它是一个群．

那么它是什么样的呢？我们让 1 反复和 1 运算如下（可以省略取模符号）：

$$\begin{aligned}
1 &= 1 \\
1+1 &= 2 \\
1+1+1 &= 3 \\
&\cdots \\
\underbrace{1+1+1+\cdots+1}_{m-1} &= m-1 \\
(m-1)+1 &= 0 \\
&\cdots
\end{aligned}$$

接着又从 $1+0=1$ 开始．我们发现，结果总是在 0 到 $m-1$ 之间循环．于是，我们把这种群叫做模-m 加法群（废话），又叫循环群，其中 1 是该群的一个**生成元**（generator）．我们不妨将这个群进一步抽象化：令它的生成元为 a，阶为 k，则我们令 $a^k=e$，循环群可表示为 $\{e, a, a^2, a^3, \ldots, a^{k-1}\}$，其中 a 是一个生成元，也不难发现，对于任何 s 只要 s 与 k 互质，那么 a^s 也是一个生成元．我们来证明一下：

证明　　令 $a^{sr}=e=e^n=a^{kn}$，即 $sr=kn$，化为 $r=\frac{kn}{s}$．因为 k 与 s 互质，所以当且仅当 n 是 s 的整数倍时 r 取整，此时 r 是 k 的整数倍．因此，a^s 每自乘 k 次返回到 e，若自乘的次数小于 k 则不为 e，这意味着这 k 次自乘的结果没有重复．而群中恰好有 k 个元素，说明在 k 次自乘的过程中，a^s 的幂遍历了所有元素．这样，$\{e, a^s, (a^s)^2, (a^s)^3, \ldots, (a^s)^{k-1}\}$ 与原来的群只有元素顺序上的不同了．值得注意的是，这并不是一个语言上规范的证明，只是为了有让读者更清楚直观的体会，不过该证明逻辑上是正确完全的．你可以尝试用反证法等写一个规范的证明作为练习（别骂了别骂了~）．

在建立循环群的概念时，我们将数字抽象为了字母所代表的群元素，将模加法抽象为了群运算（群乘法），这种思想使得我们可以用群论的方法来研究数论问题，et vice versa~ 实际上，这里就用到了在代数中极其常见和重要的一种映射：**同构**（isomorphism）．下面先给出它的定义：

> *Def* 2.2　群同构
>
> 对群而言，同构是一个既是单射又是满射 [<13.>] 的映射 ϕ，从一个群 G 到另一个群 $\overline{G}$ 使它保持群结构，即 $\phi(a)\phi(b)=\phi(ab)$．同构的逆映射也是一个同构，如果两个群之间存在同构映射，那么我们说这两个群是同构的（isomorphic），记作 $G\cong\overline{G}$．

直观来说，群同构就是两个群在代数研究的范围内完全相同 [<14.>]，只是换了不同的名字和外观．它们有完全相同的代数性质，这意味着我们只要研究得到一个群的代数性质，就可以将其应用到所有与它同构的群中．

E.g.　2.2.1　实数加法群与正实数乘法群在 $\phi(x)=2^x$ 下同构．根据函数的单调性及值域可以验证它既是单射又是满射，又因为 $2^a2^b=2^{a+b}$，所以它满足同构的定义．容易找出它的逆映射为 $\phi^{-1}(x)=\log_2 x$，它也是一个同构．

E.g.　2.2.2　集合 $\{0,1,2\}$ 在模-3 运算下与集合 $\{0,n,2n\}$ 在模-$3n$ 运算下形成的群同构．这个例子很简单，请自己尝试运用定义验证一下．

既然有了同构，一个很自然的问题就是我们是否可以用一套统一的系统来表示所有的群．这种想法在后来发展成为了群表示论．这里我们不使用矩阵，也不研究无限群．我们将用置换来完成对有限群的表示．

置换（permutation）是集合 A 到它自身的既是单射又是满射的映射，~~这个定义就像没说一样~~．对于一个没有任何附加的其它数学结构的集合来说，它好像就是恒同映射．然而，对于集合中的每个元素来说，这却是有意义的：置换要么将它映射到它本身，要么映射到集合中的其它元素．这意味着对于任何一个由这个集合中元素生成的数学结构里面，这些元素都进行了一次重新排列．因此，我们通常这样来表示一个有限集的置换（这真的不是矩阵！XD）：

$$\begin{bmatrix} \alpha & \beta & \gamma & \cdots \\ \alpha_1 & \beta_1 & \gamma_1 & \cdots \end{bmatrix}$$

其中上下两行都是集合中的全部元素，只是以不同的顺序排列着．它表示这个置换把第一行的元素换成第二行正下面的元素．举个例子：

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 6 & 3 & 5 & 2 \end{bmatrix}$$

就表示把 2 换成 4，把 4 换成 3，把 3 换成 6，把 6 换成 2．其中 1 和 5 保持不变．

等等……看上面这句，怎么像转了一圈？没错，这就是转了一圈！由于 2 换成了 4，4 就不能再出现，必须要换成别的元素……由于 2 必须出现一次，一定有一个元素换成了 2，这就闭环了．这种情况，我们通常写作 (2436)（当然你可以写成 (6243) 或者别的，只要圆排列不变就行），把这

种表示叫做一个**轮换**（cycle）．比如这个例子中就是一个 4-cycle．有时候，一个置换不止包含一个轮换，比如这个：

$$(2436)(15)=\begin{bmatrix}1&2&3&4&5&6\\5&4&6&3&1&2\end{bmatrix}$$

它就至少写成两个轮换的“乘积”．

还有一点我们可以发现：每个轮换都可以写成几个 2-cycle 的乘积；因为显然，每个置换都可以通过几次两两置换完成．比如上例中的 $(2436)=(26)(46)(36)$，先令 2 和 6 互换，再令 4 和 6 互换，最后令 3 和 6 互换．显然这只是其中一种分解方式，但是它总是有效的：令轮换中的每个元素依照轮换的顺序和其中一个元素互换，从该元素的下一个元素开始．想想为什么？

这种方式下，我们可以把所有置换都写成几个 2-cycle 的乘积，注意不一定满足交换律．事实上，当两个轮换中没有出现相同的元素时，它们满足交换律，比如上面的 $(2436)(15)$ 就等于 $(15)(2436)$，这很容易理解（两个轮换相互毫无关系）．

用 2-cycle 表示置换还有一些有趣的性质，比如恒同置换只能表示为偶数个 2-cycle 的乘积；一个置换若能表示为偶数个 2-cycle 的乘积则只能表示为偶数个 2-cycle 的乘积，若能表示为奇数个 2-cycle 的乘积则只能表示为奇数个 2-cycle 的乘积（英文口诀很好记，“Always even or always odd.”）．我们把分解为偶数个 2-cycle 的置换叫做**偶置换**（even permutation），反之叫做奇置换．由于偶置换的乘积和逆映射也都是偶置换，容易验证，n 个元素间的全部偶置换在置换复合（相继作用）下构成群．我们将这个群叫做 $\boldsymbol{n}$ **元交错群**（alternating group of degree n），记作 A_n．类似地，我们把 n 个元素间所有置换（奇或偶）构成的群叫做 $\boldsymbol{n}$ **元对称群**（symmetric group of degree n），记作 S_n．

下面终于轮到做我们梦寐以求的事情了：用置换表示所有有限群．

> *Theorem* 2.1　Cayley 定理（Cayley's theorem）
>
> 任何有限群同构于一个以置换为元素的群．

这个定理看上去很简洁，但意义重大．它的证明用到了构造的方法，并不困难．对于一个群 G 中的任意元素 $g\in G$，定义 $T_g:x\mapsto gx$ 对于所有 $x\in G$．下证 T_g 是一个置换：

对于任意 $x_1,x_2\in G$，若 $T_g(x_1)=T_g(x_2)$，即 $gx_1=gx_2$，则由消去律 $x_1=x_2$．又因为每个 $T_g(x_i)$ 都存在，所以 T_g 是双射（一一映射）．由群的封闭性，T_g 是从 G 到 G 的映射，即 G 的置换．

令 $\overline{G}=\{T_g\mid g\in G\}$，下证 $\overline{G}$ 是一个群：

对于任意 $g,h\in G$，$T_g(T_h(x))=T_g(hx)=g(hx)=(gh)x=T_{gh}(x)$，由群 G 封闭性 $gh\in G$ 可知 $T_{gh}\in\overline{G}$，$\overline{G}$ 在置换复合下封闭．单位元为恒同置换 $T_e:x\mapsto x$．$T_gT_{g^{-1}}=T_{gg^{-1}}=T_e$，故有 $(T_g)^{-1}=T_{g^{-1}}$，逆元也是良定义的．置换复合本质上是函数复合，故满足结合律．

从 $T_gT_h=T_{gh}$ 中我们已经可以找出同构映射了．令 $\phi:g\mapsto T_g$，容易验证 ϕ 是同构．
Finishing the proof as desired !

这是一个漂亮的定理，意味着所有有限群，无论它的元素是什么样的——数字、点、集合，甚至人名和水果——都可以统一地用置换来代替！上述证明中的 ϕ 称为群 G 的一个**左正则表示**（left regular representation）．如果定义 $T_g:x\mapsto xg$，则得到的 ϕ 为**右正则表示**（right regular representation）．由于 ϕ 是一个同构，它们都是**忠实**（faithful）表示（了解即可）．

在这个定理的基础上发明了一种有用的工具：**Cayley 表**（Cayley table），又叫群乘法表 （group multiplication table）．具体的做法是：把群运算的符号写在左上角，群中所有元素从单位元开始横着向右列举一遍再竖着向下列举一遍，形成一个 $(|G|+1)\times(|G|+1)$ 二维表．在每个格上写出对应的行上左端元素与列上顶端元素的运算结果．如 4 阶循环群 $\mathbb{Z}_4^+$ （更多时候写作 C_4 ）的乘法表如下（表2-1）：

$+\ (\mathrm{mod}\ 4)$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

table_2.1

它是沿对角线轴对称的，这说明它是一个 Abel 群．Cayley 表的每一行每一列都不重不漏地包含了所有群元素，可以看作是群上的一个置换．

群的结构——从子群到同态

在数学中我们经常遇到“子（sub-）”这个前缀，如**子集**（subset）、**子流形**（submanifold）、**拓扑子空间**（topological subspace）等．它通常与集合有关，包含了原对象中的一些元素，并继承了一些性质．研究这些子对象的性质对于研究原对象的性质非常有意义，因为它们通常是原对象中“有秩序且合理”的一块．这有点像解剖学的研究方法：去研究某个器官、组织，并阐明它们之间的联系，便能够还原出来整个机体的生理活动过程了．同样地，群也应当存在它的**子群**（subgroup）．下面我们先给出子群的定义：

> *Def* 3.1　子群
>
> 对于一个群 $(G,\circ)$，如果有 $H\subset G$ 使得 $(H,\circ)$ 也是一个群，那么称 H 是 G 的一个子群，记作 $H\leq G$.

这个定义不难理解，它是说，群中的一部分元素，在完全相同的运算下也构成了一个更小的群．显然它包含单位元，且像任何等价关系和其它序关系那样，具有传递性（我的子群的子群，还是我的子群）．下面通过一些例子来认识它：

E.g.　3.1.1　只含单位元的群 $\{e\}$ 和群本身 G 是 G 的子群，称作**平凡子群**（trivial subgroup）．

E.g.　3.1.2　若 s 是 m 的一个因数，那么 s 阶循环群 $\mathbb{Z}_s^+$ 同构于 m 阶循环群 $\mathbb{Z}_m^+$ 的一个子群．就像是从钟表（可看作 12 阶循环群 $\mathbb{Z}_{12}^+$ ）中挑出来 3 点、 6 点、 9 点和 12 点（它们四个成的群同构于 $\mathbb{Z}_4^+$ ）那样．

E.g.　3.1.3　$2n$ 阶二面体群 D_n 的一个子群是由单位元和反映操作（翻面）组成的 $\{E,F\}$ ，它同构于二阶循环群；另一个子群是由单位元和所有旋转组成的 $\{E,R,R^2,\ldots,R^{n-1}\}$ ，它同构于 n 阶循环群．

E.g.　3.1.4　上文中 Cayley 定理的另一种等价表述：任意 n 阶群同构于 S_n 的一个子群．

E.g.　3.1.5　在普通加法运算下，有 $\mathbb{Z}\leq\mathbb{Q}\leq\mathbb{R}\leq\mathbb{C}$ ；在普通乘法运算下， $\mathbb{Q}^*\leq\mathbb{R}^*\leq\mathbb{C}^*$.

E.g.　3.1.6　当维度 n 和 数域 $\mathbb{F}$ 都相同时，特殊线性群是一般线性群的子群；旋转群（顾名思义）是特殊线性群的子群．

E.g.　3.1.7　若 $H\leq G$ ，对于任意 $g\in G$ ， $gHg^{-1}:=\{ghg^{-1}\mid h\in G\}$ 是 G 的另一个子群，叫做 H 的一个**共轭子群**（conjugate subgroup）． H 的所有共轭子群（包括它本身）之间互为共轭，构成一个**共轭类**（conjugacy class）．

E.g.　3.1.8　所有三维实向量（欧氏空间 $\mathbb{R}^3$ ）在线性加法下构成群，所有过原点的直线和平面都是它的子群．

要判断一个群的子集是它的子群，我们不需要一一代入它的全部四条定义，只需要满足以下两个条件即可判断为真：

- 该子集在群 G 的运算下封闭；
- 子集中每个元素都有逆元在子集中．

其它条件都可以由这两条推出.

如果我们总是在思考各种群的子群，也许还会发现一个有趣的现象．对于任意 $a \in G$，都有 $a^2, a^3, \cdots \in G$（封闭性），因此所有由 a 多次自乘得来的元素构成一个循环群，它是 G 的子群．显然，存在一个整数 $n \leq G$ 使得 $a^n = e$，n 的最小取值即为这个子群的阶数．这个子群我们通常记作 $\langle a \rangle$，其中元素个数（子群的阶）也称为元素 a 在 G 中的阶，记为 $|a|$．由于任意元素都可以这样生成循环群，所以有限群在某种意义上都可以看作是由几个循环群以一定方式"粘合"起来的.

接下来我们研究子群与原群 [15.] 的关联．我们首先定义**陪集**（coset）：

> $Def\ \ 3.2$　陪集
>
> ---
>
> 对于任意 $a \in G$，$H \leq G$．令 $aH := \{ah \mid h \in G\}$，叫做子群 H 在群 G 中的左陪集；令 $Ha := \{ha \mid h \in G\}$，叫做子群 H 在群 G 中的右陪集．其中元素个数记作 $|aH|$ 和 $|Ha|$.

可以发现，它用子群中的元素逐个与 a 运算来建立起一个子群和群中任意一个元素的联系，进而建立起它与整个群的联系．如果 $a \in H$，显然任何 ah 和 ha 都是 H 的元素，并且能遍历到 H 的每一个元素，使 $aH = Ha = H$．而对于 $a \notin H$，它产生的陪集又与子群是什么关系呢？下面我们的讨论都以左陪集为例，得出的这些结论在右陪集中也是适用的.

显然对于 $a \notin H$ 且 $a \in aH$，所以 aH 与 Ha 不可能完全重合．那么它们是否有相交的部分呢？假设存在 $h_1 \in H \cap aH$，那么必然存在 h_2 使得 $h_1 = ah_2 \in H$，又由群中每个元素有逆元，有 $ah_2h_2^{-1} = a \in H$，与假设不符.

这就是说，陪集与子群要么完全重合，要么交集为空！扩展到两个陪集之间：$aH = Ha$ 或 $aH \cap bH = \varnothing$．证明如下：我们将它分成三步来证.

i.**证明：**　对于任意 $a \in G$，都有 $|aH| = |H|$.

对于 $h_1, h_2 \in H$，若 $h_1 = h_2$，则 $ah_1 = ah_2$．$\implies$ 若 $ah_1 \neq ah_2$，则 $h_1 \neq h_2$；若 $ah_1 = ah_2$，则 $h_1 = h_2$．$\implies$ 若 $h_1 \neq h_2$，则 $ah_1 \neq ah_2$．故存在双射 $\phi : H \to aH$，即 $|aH| = |H|$，证明完毕.

ii.**证明：**　$a \in bH \implies aH = bH$.

若 $a \in bH$，则可表示为 $a = bh_1$ 其中 $h_1 \in H$．因此对于任意的 $h_2 \in H$，都有 $ah_2 = bh_1h_2 \in bH$，故 $aH \in bH$．又有 $|aH| = |bH| = |H|$，所以 $aH = bH$，证明完毕.

iii.**证明原命题：**　　设存在 $c \in aH \cap bH$，则 $cH = aH = bH$．■．

其实，证明这个命题并不必须分成这三步，也可以更简单一些．但一来这样每一步都很清晰，二来这几个子命题恰好说明了陪集的重要意义：通过子群和它的陪集，可以将一个群不重（如上）不漏（注意到每个元素都可以生成陪集，如果它不属于已知陪集）地划分为大小相等的几块——陪集可以看作是子群的平移．就像这幅图所展示的：

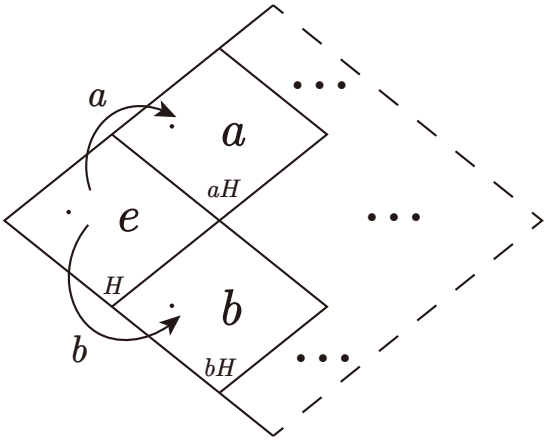


fig_3.1

从几个例子我们可以看得更清楚：

E.g.　3.2.1　　对于线性空间 $\mathbb{R}^3$ 在向量加法下构成的群的一个同胚于 $\mathbb{R}^2$ 子群（即过原点的一个向量平面），所有与它平行但不重合的平面都是它的陪集．对于它的一个同胚于 $\mathbb{R}$ 的子群（即过原点的一条向量直线），所有与它平行但不重合的直线都是它的陪集．

E.g.　3.2.2　　十二阶二面体群 D_6 的一个子群是单位元和所有单纯的旋转（同构于 $\mathbb{Z}_6^+$），它的陪集只有两个，即它本身和所有包含翻面的操作；另一个子群是单位元和翻面，它有六个陪集，分别是它本身和 table_1.1 中它右边的五列．

于是，就有了陪集形式表述的 **Lagrange 定理**（Lagrange's theorem）：

> *Theorem* 3.1　Lagrange 定理
>
> ---
>
> 对于一个有限群 G 和它的子群 H，总有 $|G|$ 整除 $|H|$．

现在来看，这个定理几乎是显然的．尽管当时并没有群、子群、陪集这些概念，Lagrange 还是以他自己的形式发现了这个定理．从中可以轻松得出一些小结论：

- $|G|$ 整除 $|a|$，即元素的阶是群的阶的因数．

证明　注意到 $\langle a\rangle \leq G$.

- $a^{|G|}=e$.

证明　由 $|a|$ 定义得 $a^{|a|}=e$ ，又有 $|G|=k|a|\,(k\in\mathbb{N}^*)$ ，因此 $a^{|G|}=a^{k|a|}=e^k=e$.

以及下面这个在九省联考中出现过的、在竞赛中相当常见、在实际应用中也颇具价值的 **Fermat 小定理**（Fermat's little theorem）：

> *Corollary* 3.1.1　Fermat 小定理
>
> 若 p 为素数，对于任意正整数 a 有 $a^p\equiv a\pmod p$.

证明　构造集合 $\mathbb{Z}_p^*=\{1,2,3,\ldots,p-1\}$ ，该集合在模-p 乘法下封闭，单位元为 1 ，取模前即满足乘法结合律．当且仅当 p 为素数，每个元素都存在逆元，下证逆元的唯一存在性：

设 $a\in\mathbb{Z}_p^*$ 的逆元为 x ，则应满足 $ax\equiv 1\pmod p$ ，这是一个同余方程，等价于 $ax=np+1$ ，根据 Bézout 定理 [16.] ，它一定有解．我们要找出它的全部解．下面的字母全部默认为正整数．将 a 移到右边，即 $x=\frac{np+1}{a}$ ，设一个解为 r ，另一个解为 $r\pm k=\frac{ra}{a}\pm k=\frac{ra\pm ka}{a}$ ，要使分子满足 $np+1$ 的形式，应有 $ka=np$ 使 n 为正整数，$n=\frac{ka}{p}$ ，又因为 p 是质数，所以 k 的解为 $k=sp,s\in\mathbb{N}^*$ ．这意味着原同余方程每相邻 p 有且仅有一解，则在 $\{1,2,\ldots,p\}$ 上有且仅有一解．若解为 p ，代入得 $ap=np+1$，显然对于素数 p 不成立．故原同余方程在 $\{1,2,\ldots,p-1\}$上有且仅有一解．逆元的唯一存在性证毕．（练习：找出一种更简洁的逆元存在性证明．）

则 $\mathbb{Z}_p^*$ 是在模-p 乘法下是群．对于 $0\leq a<p$ ，由于 a 在群中，显然 $a^{p-1}=a^{|\mathbb{Z}_p^*|}=1$ ，即 $a^p\equiv a\pmod p$ ．对于 $a\geq p$ ，令 $a=np+r$ 使 $r\in\mathbb{Z}_p^*$，则 $a^p=(np+r)^p$ ，根据高中所学的二项式定理相关知识，多项式展开后唯一不含因数 p 的项为 r^p ，则 $a^p\equiv r^p\equiv r\pmod p$ ．又因为 $a=np+r\equiv r\pmod p$ ，故 $a^p\equiv a\pmod p$ 成立．原命题得证．

需要注意的是，Lagrange 定理的逆命题并不成立．$|G|$ 的每一个因数并不一定都对应着相应阶数的子群．一个典型的例子是四元交错群 A_4 ，尽管 $|A_4|=\frac{4!}{2}=12$ ，但是它并没有 6 阶子群．另一种判断某个阶数子群存在性的方法是著名的 **Sylow 定理**（Sylow's theorems），但相关的内容较多（其实是因为我跳过了轨道和稳定化子すいません~），这里不做介绍，感兴趣的请自己查阅 textbook 或相关讲义和笔记．

根据 Lagrange 定理，$\frac{|G|}{|H|}$ 是一个整数，我们自然也会想到，它是否也对应着一个子群的阶数．答案是肯定的．从这一想法，我们定义了**商群**（quotient group），又叫**因子群**（factor group）．我并不想像抽象代数的教科书那样直接给出概念；我希望能从头开始一步步地建立它．我们知道 $\frac{|G|}{|H|}$

是 H 陪集的个数，一个显然的想法是将每个陪集作为这个新群的一个元素．为了让它的结构与 G 相似，必须有 $\phi : aH \times bH \mapsto (ab)H$ ，即将这个群保持 G 的运算．自然地，它就有了单位元 $eH = H$ ，以及各个元素的逆元（自分で確認してください）．我们也许会想到使用一个同构 $a \mapsto aH$ ，但是，它并不完备：我们发现对于一个确定的陪集 aH ，其中任何一个元素都可以是 a ，用来表示这个陪集．用数学语言表达就是： $\forall h \in H, aH = (ah)H$ ．假如我们仅仅用 $a \times b \mapsto ab$ 来表示这个群的运算，那么由于任意 ah 也可以用来代替 a ，就等于承认了 $ahb = ab$ ，经过消去律就成了 $h = e$ ，这显然不能符合 H 是非平凡子群的情况．所以我们不得不放弃用某个元素来代替一个陪集的想法．为了让 aH 中的某个元素和 bH 中的每个元素的运算结果都落在 $(ab)H$ 中，需要满足以下陈述：

$$\forall h_1, h_2 \in H, \exists h_3 \in H, ah_1bh_2 = abh_3 \tag{cl3.1}$$

这难住了我们：我们不会处理这样的结构．我们会想：如果这个群是 Abel 群就太好了，因为 $ah_1bh_2 = abh_1h_2 \in (ab)H$ ．但并不是每个子群都是 Abel 群．为了最大限度地适用于更多子群，同时严格地满足上述命题，我们会想到让任意 $hb = bh'$ 即可（注意 h' 不一定等于 h ），这样 $ah_1bh_2 = abh_1'h_2 \in (ab)H$ ．由于要求对所有 $h \in H$ 成立，这等价于 $Hb = bH$ ，即子群 H 关于 b 的左陪集与右陪集相同．为了让任意 $b \in G$ 都满足上述 $(\mathrm{cl}3.1)$ ，要求子群 H 的所有左陪集和右陪集都相同．这就是最早由 Galois 提出的**正规性**（normality）的概念．下面我们给出**正规子群**（normal subgroup）的定义：

> *Def* 3.3　正规子群
>
> ---
>
> 对于一个 $N \leq G$ ，若对于任意 $a \in G$ ，都有 $aH = Ha$ ，则称 N 是 G 的一个正规子群，记作 $N \lhd G$.

不要误以为 H 中的元素都与其它元素可交换，而是 $ah_1 = h_2a$ ，只要 h_1 与 h_2 都在 H 中即可，它们可以相等也可以不等．这是一个比交换律要弱的性质，因此更容易满足，但很多时候"它就像交换律一样好"．

通常我们验证正规子群的方法是验证它的任意一个共轭子群都是它的子集（利用定义就可以发现这与定义是等价的），即：

$$N \lhd G \iff \forall g \in G, x \in N, gxg^{-1} \in N$$

容易验证所有共轭子群的元素个数是一样多的，因此，共轭子群是子群的子集就等于是说这个子群的所有共轭子群都是它本身．此外，对于一些特殊的情况，我们还可以更容易地判断一个子群是否正规：

- 如果相应有限阶数的子群有且仅有一个，那么它是正规子群．

证明　注意到它的共轭子群与它的阶数相等，这意味着它的所有共轭子群都是它本身.

- 如果 $\frac{|G|}{|N|}=2$，那么 $N\lhd G$.

证明　注意到这个子群的非平凡左陪集和右陪集都是 G 中去掉 N 以后所有元素的集合.

简单地举几个例子吧.

E.g.　3.3.1　平凡子群是正规的.

E.g.　3.3.2　如果子群是 Abel 群，那么它是正规的．我们定义群的**中心**（center，或者德语 Zentrum）为 $Z(G):=\{a\in G\mid \forall g\in G,\,ag=ga\}$，它是群中最大的 Abel 子群，包含了所有与其它元素交换的元素.

E.g.　3.3.3　当 n 与 $\mathbb{F}$ 一致时，特殊线性群 $SL(n,\mathbb{F})\lhd GL(n,\mathbb{F})$，这可以直接由行列式的线性性得出（$\det(A)\ \det(B)=\det(AB)$）.

基于此，我们便可以给出 well defined 的商群定义了.

> *Def*　3.4　商群（因子群）
>
> ---
>
> 对于一个群 G 和它的正规子群 $N\lhd G$，记 $G/N:=\{aH\mid a\in G\}$，即 H 所有左陪集（或右陪集）的集族．它是一个群，称为 G 关于 H 的商群（因子群），其群乘法为 $aHbH=(ab)H$.

商群也有一些基本性质，比如循环群的商群都是循环群，Abel 群的商群都是 Abel 群等．其中有一个比较有趣，你可以尝试证明一下：如果 $G/Z(G)$ 是循环群，那么 G 是 Abel 群.

我们观察一个群和它的商群，它们之间保持了运算，但是其中元素的对应关系并不像同构那样严格．这种关系比同构要弱许多，我们称之为**同态**（homomorphism）.

> *Def*　3.5　群同态
>
> ---
>
> 对群而言，同态是一个映射 τ，从一个群 G_1 到另一个群 G_2 使它保持群运算，即 $\tau(a)\tau(b)=\tau(ab)$.

对比同构的概念，我们发现：首先它既不要求单射，即可以把好几个元素映射到一个；也不要求满射，也就是说可以只把 G_1 映射到 G_2 的一部分上，或者说 G_1 的同态像 $\tau(G_1)$（也可以记作 $\operatorname{Im}\tau$）只要是 G_2 的子集即可．如果一个同态是单射，我们就把它叫做单同态；如果一个同态是

满射，我们就把它叫做满同态；如果一个同态既是单射又是满射，那么它是一个同构．我们注意到一个群到它的商群存在一个满同态 $\tau_1 : a \mapsto aH$ ，这个同态看起来如此自然且典范~（其实并不只是因为"看起来"，更深层次的原因请自行探索）以至于我们把它叫做**自然同态**（natural homomorphism）或**典范同态**（canonical homomorphism）．

在一个同态中，有一些元素被映射为 G_2 中的单位元 e' ，这些元素的集合叫做同态 τ 的**核**（kernel），记作 $\operatorname{Ker}\tau := \{g \mid g \in G_1, \tau(g) = e'\}$ ．单同态的核是 G_1 中的单位元．下面这幅图形象地展示了同态、满同态、单同态和同构．

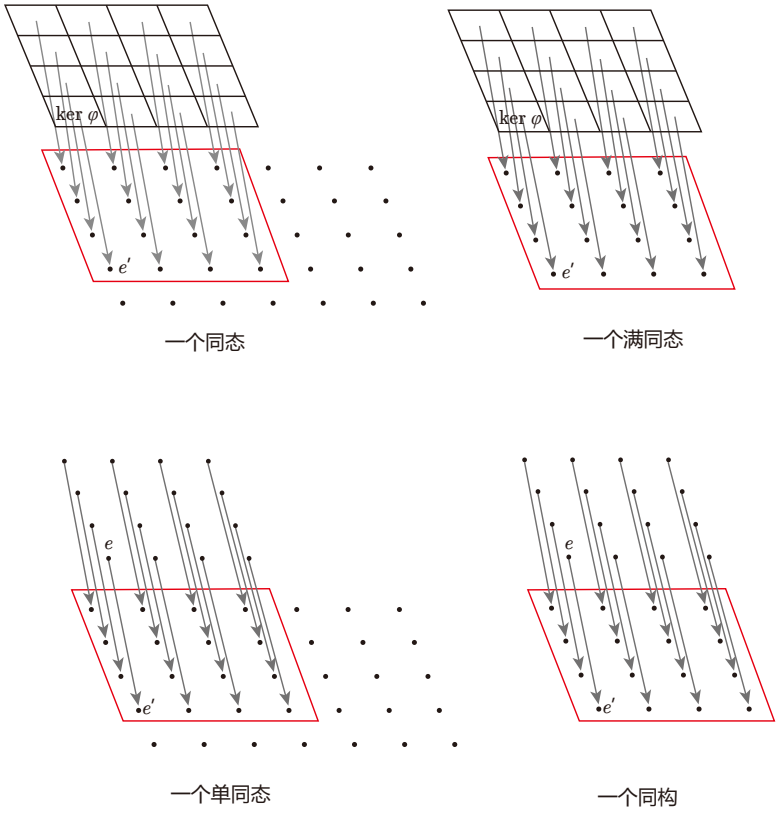


fig_3.2

同态只能说明两个群在结构上有一定的相似之处，它们相互只能部分地反映对方的特征．但是，由于容易满足，同态的应用十分广泛，尤其是在群表示论中．下面有一个我个人认为非常有趣的例子：

E.g. 3.5.1 所有实系数多项式的集合 [17.] 记作 $\mathbb{R}[x]$ ，它在加法运算下是一个 Abel 群．则求导是它到自身的一个同态，其同态核为整数加法群 $\mathbb{Z}$ ．

既然群到商群的映射是同态，那么反过来同态是否都具有类似于群到商群映射的结构呢？这个问题最初由 Jordan 研究，后来 Emmy Noether [18.] 在她的论文 *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern* 中第一次给出了广泛性的（适用于多种代数结构）答

案：是的．在这篇论文中，Noether 总结出了一系列有关同态中的同构的定理，被后人称为 Noether's isomorphism theorems，它们成为了现代代数学的最重要基础之一．我们介绍其中最基础的**群同态基本定理**（fundamental homomorphism theorem，FHT），又叫做**群的第一同构定理**（the first isomorphism theorem for groups）．

> *Theorem* 3.2　群同态基本定理
>
> 若 $\phi : G \to G'$ 是一个同态，则有 $\mathrm{Ker}\ \phi \lhd G$ 且 $G/\mathrm{Ker}\ \phi \cong \phi(G)$.

证明　记 G' 中单位元为 e'，首先证明 $\mathrm{Ker}\ \phi \lhd G$．先证 $\mathrm{Ker}\ \phi \leq G$ 如下：

显然 $\mathrm{Ker}\ \phi \subseteq G$．由上文子群的判定条件需证封闭性及逆元存在．对于任意 $e_1, e_2 \in \mathrm{Ker}\ \phi$，有 $\phi(e_1e_2) = \phi(e_1)\phi(e_2) = e'$，即 $e_1e_2 \in \mathrm{Ker}\ \phi$（**封闭性**）．对于 G 的单位元 e，对任意 $a \in G$，有 $\phi(a) = \phi(ae) = \phi(a)\phi(e)$，由消去律 $\phi(e) = e'$，可得 $e \in \mathrm{Ker}\ \phi$．对于任意 $e_1 \in \mathrm{Ker}\ \phi$，总有 $\phi(e_1)\phi(e_1^{-1}) = \phi(e_1e_1^{-1}) = \phi(e)$，即 $\phi(e_1^{-1}) = e'$，可得 $e_1^{-1} \in \mathrm{Ker}\ \phi$（**逆元**）．

综上所述，有 $\mathrm{Ker}\ \phi \leq G$ 成立．对任意 $e_1 \in \mathrm{Ker}\ \phi$ 且 $a \in G$，总有 $\phi(ae_1a^{-1}) = \phi(a)\phi(e_1)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e'$，即 $ae_1a^{-1} \in \mathrm{Ker}\ \phi$．由上文正规子群的判断条件可得 $\mathrm{Ker}\ \phi \lhd G$.

写出 $G/\mathrm{Ker}\ \phi = \{a\mathrm{Ker}\ \phi \mid a \in G\}$，$\phi(G) = \{\phi(a) \mid a \in G\}$．构造映射 $\sigma : G/\mathrm{Ker}\ \phi \to \phi(G), a\mathrm{Ker}\ \phi \mapsto \phi(a)$．但是，它其实并不一定是一个映射：因为陪集的 a 可以是陪集中的任意元素，它们的同态像相同并不是显然的，这里必须要验证 σ 是良定义的映射，即将每个陪集只映射到 $\phi(G)$ 中的唯一确定元素：

若 $a\mathrm{Ker}\ \phi = b\mathrm{Ker}\ \phi$，有 $b \in a\mathrm{Ker}\ \phi$，可以将 b 唯一地表示为 ae_3 其中 $e_3 \in \mathrm{Ker}\ \phi$．那么一定有 $a^{-1}b = e_3 \in \mathrm{Ker}\ \phi$，即 $\phi(a^{-1}b) = \phi(a^{-1})\phi(b) = e'$．要处理这个结构，我们注意到 $\phi(a^{-1})\phi(a) = \phi(aa^{-1}) = e'$，则 $\forall a \in G$ 有 $\phi(a^{-1}) = \phi(a)^{-1}$．代入得 $\phi(a^{-1})\phi(b) = \phi(a)^{-1}\phi(b) = e' = \phi(a)^{-1}\phi(a)$，由消去律得 $\phi(a) = \phi(b)$．这就证明了 σ 是一个映射：对于每个确定的陪集，它只将它映射到唯一确定的 $\phi(a)$.

然后我们就开始证明它是同构：首先它是个同态，因为 $\sigma(a\mathrm{Ker}\ \phi\, b\mathrm{Ker}\ \phi) = \sigma(ab\mathrm{Ker}\ \phi) = \phi(ab) = \phi(a)\phi(b) = \sigma(a\mathrm{Ker}\ \phi)\sigma(b\mathrm{Ker}\ \phi)$；其次它是个单射，假设存在 $\sigma(a\mathrm{Ker}\ \phi) = \sigma(b\mathrm{Ker}\ \phi) = \phi(a)$，那么 $\phi(a) = \phi(b)$，两边一起左乘 $\phi(a^{-1})$，得到 $\phi(a^{-1}b) = e'$，即 $a^{-1}b \in \mathrm{Ker}\ \phi$．记 $b = ag$ 则 $a^{-1}ag = g \in \mathrm{Ker}\ \phi$，即 $b \in a\mathrm{Ker}\ \phi$，也就是说 $a\mathrm{Ker}\ \phi = b\mathrm{Ker}\ \phi$．最后证明它是一个满射，对于每个 $\phi(a)$，它都由某个 a 映射得到，它一定属于一个陪集 $a\mathrm{Ker}\ \phi$，因此它是满射．综上所述，它是一个同构．

至此，原命题就证明完毕了（这可能就是某些教材省略的"繁而不难"的证明吧#$...%@~）

如果你学过线性代数（再次），你可能会想到**秩-零化度定理**（rank nullity theorem），即线性变换的秩和零化度（零空间的维度）的和总是等于原像的维度，看起来非常直观．它就是同态基本定理在线性空间的表现形式．

至此，我们的文章主体部分就要告一段落了．我们从简单的模运算和对称性开始，构建起了一系列概念，最终得到了如此美妙的结果．这可能就是数学的 charme 所在吧．

探索仍在继续...

如果你完完整整地读到了这里，并且理解了上面所说的全部，那么恭喜你，你对代数的感觉真的很好；即使你未能完全理解，能读下来也颇为不易：如果感兴趣不妨再多读几遍，花些时间多想一想（作者学会这些内容也差不多花了整一个月）．事实上，群论只是抽象代数的一个相对不那么现代的小小分支——离入门抽象代数这门学科，你还差得很远．但是，在读完上面所有内容以后，你已经有了阅读一些代数书籍和论文的能力，并掌握了一些常用的代数研究方法．如果你真的想系统性地学习更多群论和抽象代数，这里推荐几本我用过的教材：

入门级别（前两本书差不多，挑一个）：

- Dummit 的 *Abstract Algebra, 3rd.ed.*（那个合著者经常被忘记bs，还有据说出第四版了）
- Gallian 的 *Contemporary Abstract Algebra, 10th.ed.*（有十分详细的前置知识，甚至不要求之前认识复数和最大公约数）
- Nathan Carter 的 *Visual Group Theory*，好看，但是内容只包括群论，可以作为早期学习阶段的辅助用书．有在线的网页可交互学习资源，好像需要梯子．

物理方向（通俗易懂）：

- 李新征老师的 《〈群论一〉讲义》，是北京大学物理学院内部资料（官网上可直接下载，相当好的简体中文讲义！）．

代数领域综合，有一定深度：

- GTM73 和 GTM211，别的也有评价不错的我没看过，这两本我也没看完，但是经典作品确实是漂亮，从群环域模到表示论一气呵成．如果不知道 GTM 是什么就可以不用考虑了，先入门再说．

其实我再这方面看过的资料也不是很多，大家可以自己探索（或者说，一定要自己探索）．另外，代数是一个非常吃概念的学科，一定要非常重视例子和练习，运用你学到的概念去检验它们，其实也就并没有那么“抽象”了．

法国的布尔巴基学派从公理化集合论出发，把数学研究的对象分为代数结构、序结构和拓扑结构（现在看来并不完备）；抽象代数这门学科研究的核心对象就是代数结构．其实群只是其中最典

型、也相对简单和丰富的一种代数结构，这幅图展示了各种常见的代数结构的关系（图4-1）：

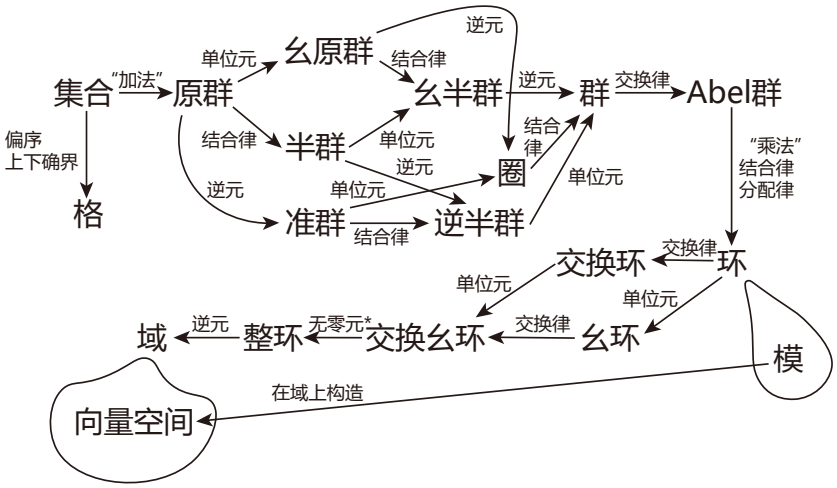


fig_4.1

前面讲历史的时候提到过 **Lie 群**（Lie group），它把数学里面最漂亮的两个东西（别跟我说层、景、钻石、棱镜那一堆抽象的玩意）——群和流形联系在了一起，成为微分几何和代数拓扑的重要研究对象．如果你知道**流形**（manifold）是什么（形象来说其实就是嵌入高维空间里面的一个局部同胚于较低维的欧氏空间的拓扑空间），那么可以来看看这个大家都耳熟能详的Lie群的定义：

> $Def\ \ 4.1$　Lie 群
>
> ---
>
> Lie 群既是流形也是群，满足以下两个条件：
>
> 1. 群乘法是光滑的（无穷阶可导 C^∞）；
> 2. 求逆元的映射 $a \mapsto a^{-1}$ 是光滑的（无穷阶可导 C^∞）．

容易验证，上文说到过的一般线性群和特殊线性群在数域为 $\mathbb{R}$ 或 $\mathbb{C}$ 时都是 Lie 群．实际上所有表示 n-维旋转的矩阵组成的群——**正交群**（orthogonal group） $SO(n)$ 也是一类常见的 Lie 群，此外还有**辛群**（symplectic group）和**酉群**（unitary group），它们分别是辛矩阵和酉矩阵组成的群．

我们前面给出过商群的定义，很自然地会想到，既然有商也应该有一种乘法：事实上我的代数很多书里都是先介绍的**外直积**（external direct product），再介绍的正规性和商群．两个群的外直积类似于集合的笛卡尔积，定义如下：

$$G_1 \oplus G_2 := \{(g_1, g_2) \mid \forall g_1 \in G_1,\, g_2 \in G_2\}$$

它是一个阶数为 $|G_1||G_2|$ 的群，群乘法为 $(g_1, g_2)(g_1' g_2') = (g_1 g_1', g_2 g_2')$ ．它就像把两个群"粘合"起来了．相似地，还有**内直积**（internal direct product），它定义在 G 的两个交集为 $\{e\}$ 的正规子群 N 和 H 间：

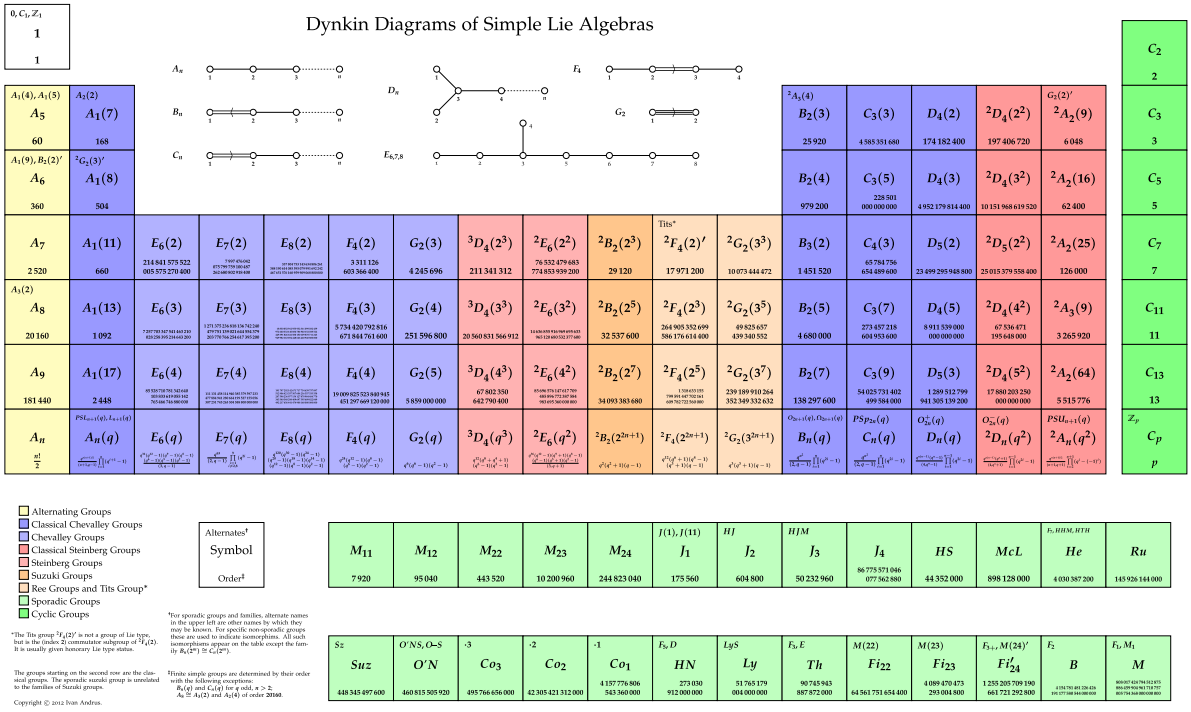
$$N \times H = \{nh \mid \forall n \in N,\, h \in H\}$$

它与 N 和 H 的外直积是同构的．在外直积的基础上，有著名的**有限 Able 群基本定理**（fundamental theorem of finite Abelian groups）．它表述了所有有限 Abel 群的分类和结构：

> *Theorem* 4.1　有限 Abel 群分类定理
>
> 每个有限Abel群都可以被唯一地分解为几个素数幂阶循环群的外直积．即Abel群 $G \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{p_i^{m_i}}^{+}$ ，其中 p_i 是素数， m_i 是整数．

这种分类思想在数学的发展中产生了很大的影响，后来，数学家不仅由此创立了**范畴论**（category theory），而且创建了**有限单群周期表**（the periodic table of finite simple groups）（表4-1）：

The Periodic Table Of Finite Simple Groups



打印出来你当然看不清，里面的字太小了，比如 Lie 群 $E_8(4)$ 的阶数为:

$$
\begin{aligned}
&191\ 797\ 292\ 142\ 671\ 717\ 754\ 639\ 757\ 897\\
&512\ 906\ 421\ 357\ 507\ 604\ 216\ 557\ 533\ 558\\
&287\ 598\ 236\ 977\ 154\ 127\ 870\ 984\ 484\ 770\\
&345\ 340\ 348\ 298\ 409\ 697\ 395\ 609\ 822\ 849\\
&492\ 217\ 656\ 441\ 474\ 908\ 160\ 000\ 000\ 000
\end{aligned}
$$

它的结构图由18个数学家共同绘制，其计算结果，包括所有的信息及表示，其总容量达到了60GB，可以铺满整个曼哈顿岛．不过上面的周期表是开源的，你可以在网上很容易地找到`.pdf`格式的文件放大来看．

所谓**单群**（simple group），就是没有非平凡正规子群的群，也即它的正规子群要么是 $\{e\}$ 要么是它本身．下面两行是无法归类进几大类的一些特殊的单群，称作**散在单群**（sporadic group），其中右下角的 M 是最大的一个，被命名为**魔群**（monster group）．这个群线性既约表示需要的维数从小到大分别是 $1, 196883, 21296876, \ldots$，其前 n 项和恰好等于代数数论模形式中的 j-不变量（一个著名的模函数）的 Fourier 展开形式中规范化后（去掉常数项）第 n 项的系数．基于此，普林斯顿大学的 Conway 和剑桥大学的 Norton 提出了**魔群月光猜想**（Monstrous Moonshine）．该猜想认为可以由魔群构建一个无限维代数结构，通过魔群的不可约线性表示，给出 j-不变量的每个 Fourier 系数，而魔群每个元素在这个代数结构上的作用，都自然给出了与某个群相关的模形式．之所以叫"月光"，是因为这在当时看来实在太不可思议．其内容摘录如下：

> **Conway-Norton's Monstrous Moonshine Conjecture（1979）**: There is a natural infinite dimensional graded representation $V = \bigoplus_{n=0}^{\infty} V_n$ of $\mathbb{M}$, such that for any $g \in \mathbb{M}$, the series $\sum \mathrm{Tr}(g|V_n)q^{n-1}$ is the q-expansion of a modular function $T_g(\tau)$ on the complex upper half-plane $\mathfrak{H}$ that satisfies the following properties:
>
> (1) $T_g(\tau)$ is invariant under a discrete subgroup Γ_g of $SL_2(\mathbb{R})$ that contains $\Gamma_0(12|g|)$.
> (2) $T_g(\tau)$ generates the field of meromorphic functions on the smooth compactification of the quotient Riemann surface $\mathfrak{H}/\Gamma_g$, i.e., $T_g(\tau)$ is a Hauptmodul for Γ_g. In particular, $\mathfrak{H}/\Gamma_g$ is a genus zero complex curve with finitely many punctures.

别说你看不懂，我学完基本的抽代也还是看不懂．这里涉及的知识太深，还有待我们慢慢探索．该问题最终由加州伯克利大学的 Borcherds 借用物理学里面的共形场论和弦论中的方法解决．

代数可能是你面前几道可怕的 IMO 不等式真题；但是任何一门数学学科远不仅仅是技巧的堆砌，真正的美感来源于从看似简单的定义中得到如此丰富的结果；它挑战我们逻辑思维和形式化语言的边界．总之，Algebra 是我认为最美的学科，仅展示如上．

Appendix-i-注释

<1.>两个 $\mathbb{N}$ 之间的乘号是**笛卡尔积**（Cartesian product）又称**直积**（direct product），它生成全部有序元素组的集合．定义为：

$$X \times Y := \{(x, y) \mid x \in X, y \in Y\}$$

<2.>有人认为更好的翻译也许是"比例数"或"可比数"，此处存在争议．

<3.>更详细地，能通过解有理式代数方程得到的数叫做**代数数**（algebraic number），表示为 $\mathbb{A}_R$；而无法用根式表示的那些数，比如 π^n，e^n 与 $\sin 1\ (rad)$，称作**超越数**（transcendental）．

<4.>四元数 $\mathbb{H}$ 表示为 $\alpha + \beta i + \gamma j + \delta k$ 使 $i^2 = j^2 = k^2 = ijk = -1$，它的乘法不总是满足交换律，感兴趣的同学可以自己研究．之后 Cayley（后面还会经常讨论到他）和 Hamilton 的朋友 Graves 各自独立地研究了**八元数**（octonion）$\mathbb{O}$ 的性质．

<5.>其实我们这里讨论的就是抽象代数的基础内容．

<6.>事实上模算数最早起源于古代的中国和印度．

<7.>同余类中任意一个数放在直角括号内可以表示这个同余类．

<8.>尼尔斯·亨利克·阿贝尔（Niels Henrik Abel，1802年8月5日—1829年4月6日），挪威数学家，在很多数学领域做出了开创性的工作．他最著名的一个成果是首次完整地给出了高于四次的一般代数方程没有一般形式的代数解的证明．这个问题是他那个时代最著名的未解决问题之一，悬疑达250多年．他也是椭圆函数领域的开拓者．尽管阿贝尔成就极高，却在生前没有得到认可，他的生活非常贫困．

<9.>埃瓦里斯特·伽罗瓦（Évariste Galois，1811年10月25日—1832年5月31日），法国数学家，群论的创立者．利用群论彻底解决了根式求解代数方程的问题，并由此发展了一整套关于群和域的理论，人们称之为伽罗瓦理论，并把其创造的"群"叫作伽罗瓦群．他因强烈支持共和主义受到保皇势力迫害入狱，20岁时死于一场"爱情和荣誉"的决斗．他的传记很值得一读．

<10.>其实我们将封闭性放在二元运算的定义中，即必须满足封闭性才是二元运算．

<11.>相应地，交换律代表着运算的一种"对称性"，分配律代表着两种运算间的优先级和一种"穿透性"．范畴论的学习可以帮助你加深对它们的体会．idea 来自：交换律、结合律、分配律的本质是什么？ - 知乎用户的回答 - 知乎 https://www.zhihu.com/question/285971671/answer/446968492

<12.>没错就是用那个英年早逝的维京人 Niels Abel 名字命名的．

<13.>既是单射又是满射，就是一一对应的映射．对于每个 x，总有唯一的 $\phi(x)$ 与之对应，反之亦然．

<14.>同构并不是群之间最强的等价关系，在群表示论中有**等价表示**（equivalent representation），要求两个置换群或线性群同为一个对称群或一般线性群的子群且互为共轭（下一章会说到）.

<15.>没见过我这么不严谨的叫法吧哈哈哈，**原群**（magma，hot liquid rock found just below the surface of the earth...但是它真叫这个名字）是带有封闭二元运算的集合，比群的定义要宽松许多．当然这里我指的是"子群所属于的那个我们一开始研究的群".

<16.>Bézout 定理是初等数论中的重要定理，译作裴蜀定理或贝祖定理．表述为设 a, b 是不全为零的整数，对任意整数 x, y，满足 $\gcd(a,b) | ax+b$，且存在整数 x, y，使得 $ax+by=\gcd(a,b)$．其中 $\gcd(a,b)$ 表示 a 与 b 的**最大公约数**（greatest common divider）．其证明可以参考：https://oi-wiki.org/math/number-theory/bezouts/

<17.>它其实是一个整环，叫做**多项式环**（polynomial ring）．它是交换代数和代数几何等学科中十分重要且基础的研究对象.

<18.>艾米·诺特（Emmy Noether，1882年3月23日—1935年4月14日），德国数学家．她彻底改变了环、域和代数的理论；在物理学方面，**Noether 定理**（Noether's theorem）解释了对称性和守恒定律之间的根本联系．她还被称为"现代数学之母"，她允许学者们无条件地使用她的工作成果，也因此被人们尊称为"当代数学文章的合著者"．她的 *Idealtheorie in Ringbereichen*（《环中的理想论》）这篇重要论文标志着抽象代数学真正成为一门数学分支．然而，巨大的声誉并未改善她受到性别歧视的处境，在不合理的制度下，她的生活非常艰苦.

Appendix-ii-练习

练习对于抽象代数这样重视概念和抽象对象的理解的学科而言极其重要．例子可以帮助你构建起对于概念的第一印象，而练习则可以让你真正地将概念理解为你自己的东西．下面给出了几道练习题，当然，这是远远不够的，你必须学会对你遇到的各种结构使用所学去检验，甚至凭借自己想象构造一些结构．下面有些练习难度可能较大，量力而行.

1. 【模运算的计算】计算：

$$\begin{aligned} 100 \mod 7 &= \\ (16 \times 11) \mod 13 &= \\ (2/9) \mod 10 &= \end{aligned}$$

2. 【群的定义的理解】证明 $\mathbb{Z}_n^* := \{x \in \mathbb{Z}_n \mid \gcd(x,n) = 1 \wedge x > 0\}$ 在模-n 乘法下为群.

3. 【群的定义的理解】（如果你学过线性代数）确定 $GL(2, \mathbb{Z}_2)$ 是不是Abel群并给出证明.

4. 【同构的理解】**自同构**（automorphism）指的是一个将群中的每个元素映射到群中元素的同构映射．所有自同构映射的集合记作 $\mathrm{Aut}(G)$ ．**内自同构**（inner automorphism）指的是一个映射将群中每个 $x \in G$ 映射到 axa^{-1} ．所有内自同构的集合记作 $\mathrm{Inn}(G)$ ．证明它们在映射复合运算下为群．如果有能力，证明 $\mathrm{Aut}(\mathbb{Z}_n^+) \cong \mathbb{Z}_n^*$ ．

5. 【置换群的理解】求对称群 S_4 和它的子群 A_4 的阶数．如果对 n 元对称群 S_n 和它的子群 A_n ，它的阶数又该如何求得？试用排列组合的知识解决．

6. 【Cayley 表】画出 $\mathbb{Z}_6^+$ 和 $\mathbb{Z}_7^*$ 的乘法表，观察它们是否同构．

7. 【子群的理解】如果一个子集元素个数有限，最少需要证明几条群公理就能证明它是子群？分别是哪几条？证明你的猜想．

8. 【Fermat 小定理】计算 $17^{97} \mod 13$ ．

9. 【正规性&商群】证明 $G/Z(G) \cong \mathrm{Inn}(G)$ ．

10. 【同态和同态定理】找出合适的群乘法使 $\mathbb{R}/\mathbb{Z} \cong S^1$ 成立并证明．其中 S^1 是一维球面，即圆．

11. 【同态和同态定理】证明第二同构定理：已知 $N \lhd G$ 且 $H \leq G$ ，则 $H/H \cap N \cong HN/N$ ．其中 $HN := \{hn \mid h \in H \wedge n \in N\}$ ．

12. 【外直积与分类】（拓展题）证明任意阶数为 p^2 的群要么同构于 $\mathbb{Z}_{p^2}$ ，要么同构于 $\mathbb{Z}_p \oplus \mathbb{Z}_p$ ．

13. 【计算机技术与应用】把具有部分素数性质的合数叫做**拟素数**（quasi prime number）．用 Python 或其它你熟悉的编程语言写一个程序，找出以 $a = 3, 24, 37$ 的 Fermat 小定理为判据时最小的 3 个拟素数．

14. 【数学与生活】魔方是布达佩斯大学建筑学院的 Ernő Rubik 教授发明的一种益智游戏，自从面世以来广受欢迎（一个标准的三阶魔方如图）．试用置换表示一个二阶魔方的任意操作，思考它们是否构成一个群．查阅相关资料，了解魔方、群论与计算机的关系．你也可以尝试自己解决二阶魔方的一些问题（如：至少需要几步操作可以还原任意一种打乱的二阶魔方？）．

Appendix-iii-参考材料

按照字母顺序：

David S. Dummit & Richard M. Foote, *Abstract Algebra, 3rd*. John Wiley & Sons, 2003.

東雲正樹 (2020, Nov. 30), 群论 (Group Theory) 终极速成 / 物理系零基础火箭级 notes, https://zhuanlan.zhihu.com/p/643534515

J. Conway & S. Norton, *Monstrous Moonshine*. Cambridge, Bull. Lond. Math. Soc., 11:308-339, 1979. DOI: 10.1112.

John M. Lee, *Introduction to Smooth Manifolds, 2nd*. New York, Springer New York, NY, 2012.

Joseph A. Gallian, *Contemporary Abstract Algebra, 10th*. Taylor & Francis Group, LLC, 2021.

J. Stillwell, *Mathematics and Its History, 3rd*. New York, Springer New York, NY, 2010.

J. Voight, *Quaternion Algebras*. Cham, Springer Nature Switzerland AG, 2021.

李新征, 《群论一》讲义. 北京大学物理学院, 2018.

N. Carter, *Visual Group Theory*. Washington, DC, Mathematical Association of America, 2009.

S. Carnahan & S. Urano, *Monstrous Moonshine for Integral Group Rings*, arXiv:2111.09404v2 [math.RT], 2023. DOI: 10.48550.

S. Lang, *Algebra, 3rd.(revised)*. New York, Springer New York, NY, 2002.

S. Roman, *Advanced Linear Algebra, 3rd*. New York, Springer-Verlag New York 2008.

Thomas W. Hungeford, *Algebra*. New York, Springer-Verlag New York, 1974.

V. Tatitscheff, *A short introduction to Monstrous Moonshine*. Strasbourg, arXiv:1902.03118v4 [math.NT], 2021. DOI: 10.48550.