0 引 言

代数学是一个有悠久历史的数学分支。在 19 世纪后期, 德国学派在代数学中系统地建立了一套抽象的语言和方法, 从根本上影响了此后代数学的发展。在 20 世纪中, 这些抽象的语言和方法逐渐被代数领域甚至更广的领域普遍接受。在今天, 至少在数学领域, “代数” 和 “抽象代数” 这两个术语实际上已是同一个意义。

按照 Dieudonné 的观点, 代数学是由代数数论和代数几何两个方面激发的。这是一种通过观察人类文明史而提出的哲学观点, 并非仅指现代代数学 (如同另一些学者指出的, 现代代数学还受到一些其他方面的激发, 例如代数拓扑就起了极其重要的影响)。我们简单地回顾一下代数学的发展史, 就不难理解这些哲学观点。

代数方程 (即多项式方程) 是代数学的一个古老的研究课题, 有广泛的应用背景。而丢番都 (Diophantus) 方程 (即代数方程的整数解问题) 则是代数数论的古老的研究课题。代数方程的研究使代数学逐渐成为一个独立的数学分支。自从 17 世纪 30 年代费马 (Fermat) 和笛卡儿 (Descartes) 建立直角坐标系, 产生了解析几何, 将代数与几何联系了起来, 代数几何就从此发源。从 17 世纪到 19 世纪是代数学蓬勃发展的时期, 研究的对象有代数运算、多项式、线性代数等, 主要还是围绕着代数方程及其应用。

1830 年前后, 伽罗瓦和阿贝尔在代数方程的解的研究中发现了一类新的数学对象 —— 群。伽罗瓦巧妙地把代数方程的可解性问题化为群论的问题, 证明了 5 次以上的方程没有一般的解法 (5 次方程的情形是阿贝尔解决的)。这一工作显示出群论的强大威力。此后人们逐渐认识到群是一种普遍的的存在, 而且又是一种强有力的工具。因此群逐渐成为数学中最重要的基本概念之一, 对此后的数学以至其他科学产生了深远的影响。19 世纪中期, 黎曼所开创的黎曼曲面的研究, 是数学的又一基本课题, 它与分析、代数、几何和数论都有密切的联系。

在这一时期, 代数数论也有很大的发展, 如 Kummer 在研究费马大定理时产生了“理想数” (现在称为理想) 的概念。在 19 世纪后期, 索弗斯 · 李将群论的思想用于研究微分方程, 产生了李群的概念, 而李代数则是代数学的一个新研究课题。

19 世纪后期到 20 世纪初期, 德国学派 (代表人物有阿廷、诺特、希尔伯特等) 将代数学中的基本概念推广, 形成抽象概念如群、环、同态等, 这样也有了很多新的研究课题, 如特征 p 的几何或数论。抽象的语言至少有下面几个好处: 一是有了一套统一高效的语言, 有利于抓住问题的关键; 二是隐含着不同课题之间的类比, 从而对新的研究思路有激励作用; 三是用抽象的眼光观察一些具体的研究对象, 可以理解其在更宽广的领域中的意义。此后, 代数学中的抽象语言逐渐被普遍接受, 以致今天很多作者不再用 “抽象代数” 这个术语而直接称之为 “代数学”。

然而, 抽象的语言也是有缺点的。一个重要的缺点是往往将具体的背景掩埋在抽象的、形式的或 “一般情形” 的定义中, 即使不了解这些背景, 仍可以从这些定义出发推导出很多命题; 但如果完全不顾背景地研究下去, 很难保证会得到有价值的结果, 在极端的情形甚至会成为 “纯粹形式逻辑”。因此, 许多专家都非常强调在代数的学习和研究中随时注意问题的背景。

20 世纪 20 年代以后, 拓扑学逐渐对代数学有了重要影响。起初人们发现, 拓扑学中的同调用群论的语言表述很合适, 这刺激了阿贝尔群的研究, 后来基础群的研究又刺激了自由群的研究。更重要的是同调代数的产生, 它将拓扑学中同调的方法推广到其他领域 (包括几何、代数、数论等), 而且在逻辑上将抽象代数从集合的层次提高到 “范畴” 的层次。

除了代数数论、代数几何和代数拓扑以外, 在 20 世纪对代数学有重要影响的学科还有物理学、组合学、信息科学和其他一些应用学科。代数学本身也有一些经典的研究课题, 如有限单群的分类。

代数学的基本研究对象是有限运算 (即仅涉及有限多个对象的运算), 特别是二元运算 (即两个对象的运算, 例如加、减、乘、除都是二元运算)。与此对照, 在分析中研究的极限则不是有限运算。现代代数学研究的课题很多, 具体地说, 有:

i) 群与半群, 二者都是带有一种二元运算的集合, 但它们的背景很不相同: 群的基本背景是变换, 可以理解为物理意义下的运动; 而半群的基本背景是自同态 (集合到自身的映射)。

ii) 环, 是带有两种二元运算 (一般称为 “加法” 和 “乘法”) 的集合。两种二元运算由 “乘法分配律” 联系在一起。交换环的背景主要是数和函数; 结合环的基本背景是矩阵、微分算子等; 而非结合环 (如李代数、八元数、克利福德代数等) 则各有不同的背景。与环密切联系的一个研究对象是模。

iii) 域论和伽罗瓦理论, 这是最重要的经典课题, 也是现代数学的一类最重要的工具。

iv) 线性代数是一个经典的分支, 但从抽象代数的观点可以拓宽其研究范围, 即研究一般域上的线性代数, 其背景有分析、数论、几何、组合学、计算数学、代数学的若干其他分支以及物理学、化学、计算机科学、信息科学等应用领域。

v) 双线性及多重线性代数 (张量积等), 这是一个不可缺少的基本工具。

vi) 同调代数, 它将拓扑学的方法应用到其他学科以寻求各种 “不变量”, 而不变量在各学科中都是分类学的基础。在各学科中建立了很多种同调, 一个很深入的研究方向是 K-理论, 它在拓扑、代数、数论、微分几何等学科都有重要的应用。另一方面, 在建立一般的同调方法中, 形成了 “范畴” 的语言, 而以往在抽象代数中用的是集合论的语言, 可以说范畴比集合更抽象。

vii) 在群、环、模等代数对象的研究中, 表示是一个根本的方法, 在很多课题中也是主要的研究对象; 而对表示的长期深入的研究, 使表示论逐渐成为一个分支, 而且是数学最强有力的工具之一。

viii) 线性代数群虽属于群论的范围, 但已形成一个独立的分支。

(上面并未列出所有的方向。)

代数学有非常广泛的应用领域, 其中有的学科通常划入代数学的范围, 如代数组合论, 编码和密码学, 数学物理中的代数对象 (如卡茨 - 穆迪代数、量子群等), 数学机械化等。

代数学与拓扑学、微分几何、数论、代数几何、李群、泛函分析、计算数学、应用数学等许多数学学科, 物理学、化学、计算机科学、系统科学、信息科学等其他学科以及很多应用领域有密切联系。

在今天, 由于代数学的内容非常广泛, 在一本教科书中已无法作全面的介绍, 在一个基础教程中更是只能选择几个课题。在本书中仅涉及群论、交换环与模的初等理论、域论和伽罗瓦理论。这些内容基本上都是 “经典的”, 很多是 20 世纪初甚至更早的, 在今天已相当成熟, 而这些内容对于抽象代数的初步学习都是基本的和必需的。在内容的处理上, 本书在有些地方采用了一些较近代的观点, 并介绍了一些应用。

1 群　论

1　群

在几何中经常会遇到对称的图形。所谓对称性, 就是图形经过某种运动后能和自身重合。我们来看几个例子。

例 1.1　平面上的一个正 n 边形 (如图 1.1 中的正六边形) 绕中心旋转角 $\frac{2\pi}{n}$ 的整数倍可与自身重合, 且有 n 条对称轴 (如图 1.1 中的虚线所示)。正多边形对这些对称轴反射后也与自身重合 (反射也可以看作在空间中的翻转)。不难看出, 如果先作一次旋转再作一次反射, 其结果相当于对另一个对称轴作一次反射; 而若对两条对称轴依次作反射, 其结果相当于一个旋转, 而旋转的角度与两个反射的先后次序有关。

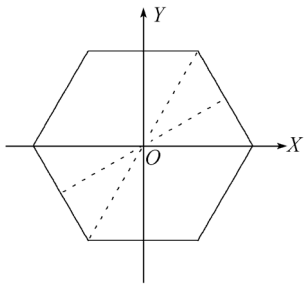

图　1.1

例 1.2　一个正方体 (见图 1.2) 有多个旋转对称轴, 两个相对面中心的连线是一条四次对称轴 $\left(\text{即绕此轴旋转 } \frac{2\pi}{4} \text{ 可与自身重合}\right)$, 而两个相对顶点的连线是一条三次对称轴 $\left(\text{即绕此轴旋转 } \frac{2\pi}{3} \text{ 可与自身重合}\right.$, 如图 1.2 中的短长虚

线所示 $\big)$。此外正方体的中心是一个对称中心, 还有一些反射对称面等。不难验证, 如果先后绕一条三次对称轴和一条四次对称轴作旋转, 其结果相当于另一个旋转, 其旋转轴和旋转的角度都与所作的两个旋转的先后次序有关。由这个例子可见对称性可能是很复杂的。

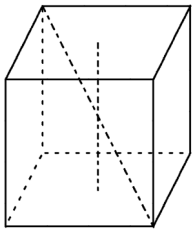

图 1.2

例 1.3 图 1.3 是由边长为 1 的正三角形的顶点铺成的点阵, 称为一个 “格”。这个格沿 X 轴方向平移 1 单位可与自身重合, 绕原点 O 旋转 $\frac{\pi}{3}$ 也可与自身重合。与例 1.1 和例 1.2 不同的一点是, 有无限多种运动能使格移到与自身重合的位置。

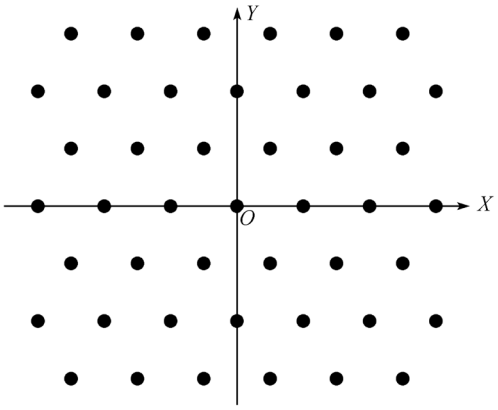

图 1.3

对称性在数论、拓扑、分析、代数等很多其他数学领域也可以遇到, 而且在物理、化学等学科以及很多应用领域也经常遇到。实际上, 对称性在自然界中普遍存在, 而且是研究自然界的一个极为重要的着眼点。

研究对称性的根本工具是群论。我们先给出群的一般定义, 然后再详细解释。

定义 1.1 一个*群*是一个集合 G 带有一个 “二元运算”, 即一个映射 $G\times G\to$

G (称为乘法, $(a,b)\in G\times G$ 在此映射下的像记作 $a\cdot b$ 或 ab, 称为 a 与 b 的积), 满足条件:

i) $(ab)c=a(bc)$ 对任意 $a,b,c\in G$ 成立 (这称为 "乘法结合律");

ii) 存在 (唯一的) $e=e_G\in G$ 使得 $ae=ea=a$ 对任意 $a\in G$ 成立 (e 称作*单位元*);

iii) 对任意 $a\in G$, 存在 (唯一的) $b\in G$ 使得 $ab=ba=e$ (b 称作 a 的*逆元*, 记 $b=a^{-1}$)。

群 G 称为*交换群*或*阿贝尔群*, 如果除上述三个条外还有

iv) $ab=ba$ 对任意 $a,b\in G$ 成立。

(对任两个元 $a,b\in G$, 若 $ab=ba$, 则称 a 与 b *交换*, 条件 iv) 就是说 G 的任意两个元交换。)

上面的定义来源于多方面的背景, 是从多种相距甚远的不同情形中抽象出来的, 因此需要通过多方面的具体情形来理解。我们先举几个例子, 并解释例 1.1∼ 例 1.3 中的图形与群的关系。在以下几节将看到更多的例子。

例 1.4 所有非零有理数的集合 $\mathbb{Q}^*$ 是一个以乘法为二元运算的群。类似地, 所有非零实数的集合 $\mathbb{R}^*$ 和所有非零复数的集合$\mathbb{C}^*$ 也是以乘法为二元运算的群。此外, 所有正有理数的集合 $\mathbb{Q}_{>0}$ 也是一个以乘法为二元运算的群。

注意在例 1.4 中, $\mathbb{Q}^*$ 是 $\mathbb{R}^*$ 的子集, 而且二者的群运算是一致的, 我们说 $\mathbb{Q}^*$ 是 $\mathbb{R}^*$ 的 "子群"。一般地, 如果 G 是一个群, H 是 G 的子集, 且按 G 的乘法运算组成一个群, 则称 H 为 G 的*子群*。

引理 1.1 设 G 为群, H 为 G 的子集, 则 H 为 G 的子群当且仅当下列条件成立:

i) 若 $a,b\in H$ 则 $ab\in H$;

ii) $e\in H$;

iii) 对任意 $a\in H$ 有 $a^{-1}\in H$。

证明很简单, 留给读者作为习题 (习题 1.8)。

在例 1.4 中, $\mathbb{Q}^*$, $\mathbb{R}^*$ 和 $\mathbb{Q}_{>0}$ 都是 $\mathbb{C}^*$ 的子群。对任意群 G, 一元子集 $\{e\}$ 和 G 本身都是 G 的子群。我们将只有一个元的群称为*零群*, 故称 $\{e\}$ 为 G 的*零子群*。

例 1.5 所有整数的集合 $\mathbb{Z}$ 是一个以加法为二元运算的群, 对此我们将定义中的 "乘法" 改称为 "加法", 而称 $\mathbb{Z}$ 为 "加法群"。类似地, 所有有理数的集合

$\mathbb{Q}$, 所有实数的集合 $\mathbb{R}$ 和所有复数的集合$\mathbb{C}$ 也都是加法群。

注意 $\mathbb{Z}$ 是 $\mathbb{Q}$ 的子群。易见在 $\mathbb{Z}$ 中, 所有偶数组成一个 (加法) 子群, 记为 $2\mathbb{Z}$。更一般地, 对任意整数 n, 所有 n 的倍数组成一个 (加法) 子群 $n\mathbb{Z} \subset \mathbb{Z}$。

对任意正整数 n, n 维实向量空间$\mathbb{R}^n$ 和复向量空间 $\mathbb{C}^n$是以加法为二元运算的群。更一般地, 任一实或复线性空间也是以加法为二元运算的群。

注意, 对任一个群我们都可以将乘法改称为 “加法”, 而称之为 “加法群”。此时我们常将乘号改记为加号 “+”, 将单位元记为 0, 称为*零元*, 而将一个元 a 的逆元记为 $-a$, 称为 a 的*负元*。采用不同的术语和记号只是为了方便而已。

例 1.6 设 n 为正整数。两个整数 a, b 称为*模 n 同余的*, 如果它们的差能被 n 整除, 此时记 $a \equiv b \pmod{n}$。易见同余是一等价关系 (即同余关系是自反的, 对称的和传递的), 由此可以按模 n 的同余关系将所有整数分类。详言之, 对任意整数 a, $\bar{a} = a + n\mathbb{Z} = \{a + kn | k \in \mathbb{Z}\}$ 是与 a 同余的所有整数的集合, 它是 $\mathbb{Z}$ 中的一个由相互同余的整数组成的类, 称为一个模 n 的*同余类* (有的文献中称为一个模 n 的*同余数*)。所有模 n 的同余类的集合记为 $\mathbb{Z}/n\mathbb{Z}$, 它显然是一个 n 元集合。易见对任意整数 a, b, $\bar{a}$ 中的任意整数与 $\bar{b}$ 中的任意整数的和在 $\overline{a+b}$ 中, 所以我们可以在 $\mathbb{Z}/n\mathbb{Z}$ 中定义一个 “加法” 运算 $\bar{a} + \bar{b} = \overline{a+b}$; 类似地, 也可以在 $\mathbb{Z}/n\mathbb{Z}$ 中定义一个 “乘法” 运算 $\bar{a} \cdot \bar{b} = \overline{ab}$。不难验证这样定义的加法和乘法满足交换律、结合律、分配律等。

易见 $\mathbb{Z}/n\mathbb{Z}$ 按加法组成一个群, 其中 $\bar{0}$ 为零元, $\bar{a}$ 的负元为 $\overline{-a}$。

我们来回忆一下辗转相除法。设 a, b 为整数, $b > 0$, 令 $r = \left[\dfrac{a}{b}\right]$ $\left(\text{即不大于}\dfrac{a}{b}\text{的最大整数}\right)$, $s = a - rb$, 则 $0 \leqslant s < b$, 即余数小于除数。若 $s \neq 0$, 将 a, b 分别换为 b, s 再继续作除法, 如此继续下去, 这个过程就叫做 “辗转相除”。由于每除一次余数都要减小, 由数学归纳法原理可知经过有限多次辗转相除必将会有一次得到余数 0, 从而辗转相除停止。由归纳法不难看出, 每次除法所得的余数都是形如 $ma + nb$ $(m, n \in \mathbb{Z})$ 的数, 而最后一次除法的除数 d 可以整除各次除法的除数, 从而整除 a 和 b。由此得到$d = \gcd(a, b)$, 并且由此可见任意两个整数 a 和 b 的最大公约数可以表为 $ma + nb$ $(m, n \in \mathbb{Z})$。

令$(\mathbb{Z}/n\mathbb{Z})^*$ 为 $\mathbb{Z}/n\mathbb{Z}$ 中所有与 n 互素的同余类组成的子集 (注意若 $\bar{a}$ 中有一个数与 n 互素, 则其中所有的数都与 n 互素), 则易见 $(\mathbb{Z}/n\mathbb{Z})^*$ 按乘法组成一个群, 其中 $\bar{1}$ 为单位元; 对任意 $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^*$, 由辗转相除法可知存在整数 r, s 使得 $ra + sn = 1$, $\bar{a}$ 的逆元即为 $\bar{r}$。

例 1.4$\sim$ 例 1.6 中的群都是阿贝尔群。下面是几个非交换群的例子。

例 1.7 设 S 是一个集合, S 到自身的一个一一映射称为 S 的一个置换。所有这些置换组成的集合记为 $\mathrm{Per}(S)$。对任意 $\sigma,\tau\in\mathrm{Per}(S)$, 记 $\sigma\circ\tau$ 为 σ 和 τ 的合成, 即

$$\sigma\circ\tau(s)=\sigma(\tau(s))\quad(\forall s\in S)\tag{1}$$

则易见 $\sigma\circ\tau\in\mathrm{Per}(S)$。显然任意 $\sigma\in\mathrm{Per}(S)$ 的逆映射 $\sigma^{-1}\in\mathrm{Per}(S)$, 而 $\mathrm{Per}(S)$ 中有一个 "恒同映射" id_S, 将每个元 $s\in S$ 映到自身。由定义可见, $\mathrm{Per}(S)$ 是一个以 $\circ$ 为乘法的群, 称为 S 的置换群, 其中的单位元为 id_S, 而任意元 σ 的逆元为 σ^{-1} (注意, 合成由定义显然满足结合律, 即 $(\sigma\circ\sigma')\circ\sigma''=\sigma\circ(\sigma'\circ\sigma'')$)。

特别地, $S=\{1,\cdots,n\}$ 的置换群称作 n 次对称群, 记为 $\mathfrak{S}_n$。注意$\mathfrak{S}_n$ 有 $n!$ 个元。

对任意 $\sigma\in\mathfrak{S}_n$, 有

$$\prod_{1\leqslant i<j\leqslant n}(\sigma(j)-\sigma(i))=\pm 2!3!\cdots(n-1)!\tag{2}$$

这是因为每一对 S 中的数恰在左边的一个因子中同时出现 (注意 σ 是一一映射), 所以这些因子的积的绝对值与 σ 无关。若 (2) 中的数为正则称 σ 为偶置换, 否则称 σ 为奇置换。可以证明所有偶置换组成一个群A_n, 称作交错群 (见例 3.6)。

易见 $\mathfrak{S}_n$ 中的一个元 σ 可以表达为一个 2 行 n 列的整数矩阵, 它的第 1 行依次为 1,2,$\cdots$, n, 第 2 行依次为 $\sigma(1),\sigma(2),\cdots,\sigma(n)$。此外还有下面的简单记法。设 $\sigma\in\mathfrak{S}_n$, a_1 为 1 到 n 间的任一整数, 令 $a_2=\sigma(a_1)$, $a_3=\sigma(a_2)$,$\cdots$, 等等, 由于 S 是有限集, 必将有两个正整数 $i<j$ 使得 $a_i=a_j$; 若 $i>1$, 则有 $a_{i-1}=\sigma^{-1}(a_i)=\sigma^{-1}(a_j)=a_{j-1}$, 故由归纳法可知有正整数 r 使得 $a_{r+1}=a_1$。不妨设 r 是这样的整数中最小的一个, 我们说 σ 有一个 r-循环 $(a_1a_2\cdots a_r)$ (即 $\sigma(a_i)=a_{i+1}$ $(1\leqslant i<r)$, $\sigma(a_r)=a_1$)。易见 σ 可以表示为若干个循环的积 (即合成), 可简记为形如 $(a_1a_2\cdots a_r)(b_1b_2\cdots b_s)\cdots$, 其中每个整数至多出现一次 (为简单起见略去所有 1-循环, 而将单位元 id_S 记为 (1))。2-循环也称为对换。

注意置换是一种异于数的数学对象。事实上, 我们所遇到的大多数群都不能看作数集, 因此对群不应仅从数的角度去理解。

若群 G 是有限集, 则称 G 为有限群, 其元素个数称为 G 的阶, 记为 $|G|$。易见 $|\mathbb{Z}/n\mathbb{Z}|=n$, $|A_n|=n!/2$ $(n>1)$。若 G 不是有限群, 则我们说 G 的阶 $|G|=\infty$。

例 1.8 令$GL_n(\mathbb{R})$ 为所有 $n\times n$ 可逆实矩阵的集合, 并取矩阵乘法为它的二元运算。记 I 为 n 阶单位方阵*。由线性代数可知矩阵乘法满足结合律, 且对

* 本书中的矩阵统一用白体表示

任意 $T \in GL_n(\mathbb{R})$ 有 $IT = TI = T$, $T^{-1}T = TT^{-1} = I$。由此即可验证 $GL_n(\mathbb{R})$ 按矩阵乘法为一个群。类似地, 所有 $n \times n$ 可逆复矩阵的集合 $GL_n(\mathbb{C})$ 按矩阵乘法为一个群。$GL_n(\mathbb{R})$ 和 $GL_n(\mathbb{C})$ 分别称为实的和复的*一般线性群*。

令 $SL_n(\mathbb{R})$ 为 $GL_n(\mathbb{R})$ 中所有行列式为 1 的元组成的子集, 则易见 $SL_n(\mathbb{R})$ 是 $GL_n(\mathbb{R})$ 的子群, 称为一个*特殊线性群*。此外, $GL_n(\mathbb{R})$ 中的所有正交阵组成一个子群 $O_n(\mathbb{R})$, 称为一个*正交群*; 而 $GL_n(\mathbb{C})$ 中的所有酉矩阵组成一个子群 $U_n(\mathbb{C})$, 称为一个*酉群*。

对任意正整数 n, $GL_{2n}(\mathbb{R})$ 中的一个矩阵 T 如果满足 ${}^tT \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} T = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ (其中 I 为 n 阶单位阵), 则称为*辛矩阵*。所有辛矩阵组成 $GL_{2n}(\mathbb{R})$ 的一个子群 $Sp_n(\mathbb{R})$, 称为一个*辛群*。

上面这些群都是所谓 "典型群" (详见 3.3 节)。

例 1.9 实线性空间到自身的可逆线性映射称为线性变换。设 V 为实线性空间, 记 $GL(V)$ 为 V 的所有线性变换组成的集合, 它是 $\mathrm{Per}(V)$ 的子集。显然线性变换的合成仍是线性变换, 线性变换的逆也是线性变换, 且恒同映射是线性变换, 故 $GL(V)$ 是 $\mathrm{Per}(V)$ 的子群 (以 $\circ$ 为乘法)。若 $\dim(V) = n$, 我们经常可以将 $GL(V)$ 与例 1.8 中的 $GL_n(\mathbb{R})$ 等同起来 (见下面的例 2.5)。

如果 V 是欧几里得空间, 即定义了一个内积 $\langle , \rangle$, 则易见 $GL(V)$ 中所有保持内积 $\langle , \rangle$ 的线性变换 (就是 $T \in GL(V)$ 使得 $\langle Tv, Tw \rangle = \langle v, w \rangle$ 对任意 $v, w \in V$ 成立, 即正交变换) 组成一个子群 $O_n(V, \langle , \rangle)$ (在没有疑问时可简记为 $O_n(V)$)。例 1.1 和例 1.2 中的旋转和反射都是正交变换, 如果考虑例 1.1 中所有保持正 n 边形的正交变换全体组成的集合 D_n, 则由引理 1.1 易见 D_n是 $O_2(V)$ 的子群, 称为一个*二面体群*。而例 1.2 中所有保持正方体的正交变换全体组成 $O_3(V)$ 的一个子群。

类似地, 若 W 为复线性空间, 记 $GL(W)$ 为 W 的所有复线性变换组成的集合, 则它是一个以 $\circ$ 为乘法的群, 且为 $\mathrm{Per}(W)$ 的子群。如果 W 是埃尔米特空间, 即定义了一个埃尔米特形式 $\langle , \rangle$, 则 $GL(W)$ 中所有保持 $\langle , \rangle$ 的线性变换 (即酉变换) 组成一个子群 $U(W)$。

设 G 为群, $g, h \in G$, 则有 $(gh)^{-1} = h^{-1}g^{-1}$, 这是因为

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = e \tag{3}$$

对任一群 G, 由引理 1.1 易见 G 的任意多个子群的交为子群。对任意子集 $S \subset G$, G 的所有包含 S 的子群的交称为 S *生成*的子群, 记作 $\{S\}$。易见 $\{S\}$ 由所有 S 中的元及其逆元的有限积 (包括 e) 组成, 即

$$\{S\} = \{s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} | n \geqslant 0,\ s_i \in S,\ \epsilon_i = \pm 1 \forall i\} \tag{4}$$

这是因为, 显然 (4) 的右边为一个包含 S 的子群 $H \subset G$, 而任一包含 S 的子群 $H' \subset G$ 显然包含 H, 所以 H 就是所有包含 S 的子群的交。特别地, 若 $\{S\} = G$, 则称 S 为 G 的一组生成元, 此时若 S 为有限集则称 G 为有限生成的; 而若 S 只有一个元 (即 G 由一个元生成), 则称 G 为循环群。一个元 $g \in G$ 生成的子群的阶 (可能为 ∞) 称为 g 的阶。

例如, 在例 1.1 中, 绕中心旋转角 $\frac{2\pi}{n}$ 的运动 ρ 是 $O_2(V)$ 中的 n 阶元, 任一反射是 2 阶元, 而 D_n 可由 ρ 和任一反射生成, 故为有限生成的 (习题 7)。

习题

1.1. 设 G 是一个非空集合, 带有一个满足结合律的二元运算 $(a, b) \mapsto ab$, 使得对任意 $a, b \in G$, 方程 $ax = b$ 和 $xa = b$ (对 x) 都有解。证明 G 是一个 (以此二元运算为乘法的) 群。如果只假定方程 $ax = b$ 有解, 是否仍能保证 G 是一个群?

1.2. 设群 G 由两个元 a, b 生成, 而 a, b 满足 $a^5 = b^3 = a^3 b^2 a^2 b = e$。证明 G 是阿贝尔群。

1.3. 证明当 $n > 2$ 时 $\mathfrak{S}_n$ 不是阿贝尔群, 当 $n > 3$ 时 A_n 也不是阿贝尔群。

1.4. 证明 $\mathfrak{S}_3$ 可以由任意两个不同的 2 阶元生成, 也可以由任意一个 2 阶元和任意一个 3 阶元生成。此外, 任意 2 阶元与 3 阶元不交换, 任两个不同的 2 阶元也不交换。(提示：两个不同的 2 阶元的积是 3 阶元。)

1.5. 设 $a = (123) \in \mathfrak{S}_3$ 而 $b \in \mathfrak{S}_3 - A_3$。试不通过计算证明 $bab^{-1} = a^2$。(提示：参看习题 1.3 和习题 1.4。)

1.6. 设 $m, n \in \mathbb{Z}$, 记 $\bar{m}$ 为 m 在 $\mathbb{Z}/n\mathbb{Z}$ 中的像。证明 $\bar{m}$ 为 n 阶元当且仅当 $\gcd(m, n) = 1$。

1.7. 设 P 是例 1.1 中的正 n 边形, ρ 是绕中心旋转角 $\frac{2\pi}{n}$ 的运动, τ 为对任一对称轴的反射。验证 ρ 和 τ 分别是 D_n 中的 n 阶和 2 阶元, 且 D_n 由 $\{\rho, \tau\}$ 生成。

1.8. 证明引理 1.1。

2 同态

两个群之间的映射如果和群运算相容, 则称为同态。详细说：

定义 2.1 设 G, G' 为群。一个映射 $f : G \to G'$ 称作同态, 如果 $f(ab) =$