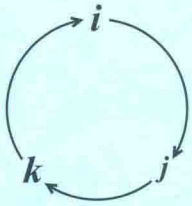
南京大学百门优质课程系列教材

近世代数

MODERN ALGEBRA

孙智伟　编著

$$ij=k \quad jk=i \quad ki=j$$
$$ji=-k \quad kj=-i \quad ik=-j$$



$$x^5-4x+2=0$$

$$S_n'=A_n$$

$$[G:H]|H|=|G|$$

$$K/(H\cap K)\cong HK/H$$

$$G/\mathrm{Ker}(\sigma)\cong \mathrm{Im}(\sigma)$$

$$R/(A_1\cap\cdots\cap A_n)\cong R/A_1\oplus\cdots\oplus R/A_n$$

$$I_0\subseteq I_1\subseteq I_2\subseteq\cdots$$

$$x^q-x=\prod_{a\in\mathbb{F}_q}(x-a)$$

$$\mathrm{Gal}(M/K)\cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M)$$

南京大学出版社

南京大学百门优质课程系列教材

近世代数

MODERN ALGEBRA

孙智伟 编著

特配电子资源

微信扫码

· 网络课程

· 拓展阅读

· 互动交流

南京大学出版社

图书在版编目(CIP)数据

近世代数 / 孙智伟编著. —南京：南京大学出版社，2022.8

ISBN 978-7-305-25945-6

Ⅰ. ①近… Ⅱ. ①孙… Ⅲ. ①抽象代数 Ⅳ. ①O153

中国版本图书馆 CIP 数据核字(2022)第 131274 号

出版发行 南京大学出版社
社　　址 南京市汉口路 22 号　　邮编 210093
出 版 人 金鑫荣

书　　名 近世代数
编　　著 孙智伟
责任编辑 刘　飞　　编辑热线 025-83592146

照　　排 南京开卷文化传媒有限公司
印　　刷 南京人民印刷厂有限责任公司
开　　本 787 mm×1092 mm　1/16　印张 11.25　字数 255 千
版　　次 2022 年 8 月第 1 版　2022 年 8 月第 1 次印刷
ISBN 978-7-305-25945-6
定　　价 39.00 元

网　　址：http://www.njupco.com
官方微博：http://weibo.com/njupco
微信服务号：njuyuexue
销售咨询热线：(025)83594756

前言

“近世代数”是数学系本科生的重要专业课，讲解群、环、域这三个重要代数结构的基础知识. 编者从1999年开始为南京大学数学系本科生讲授此课，经过二十多年的教学实践积累了更适于初学者的特色讲稿. 本教材正是基于这些讲稿编写的.

南京大学数学系2002级的一位同学曾在南京大学小百合论坛上发帖谈他学习近世代数的感受，在帖子中他写道：“在我最困难的日子里，人生的乐趣已消失殆尽. 唯独每周一次的近世代数课宛若寒冷冬夜中的一丝火光，给我一点慰藉. 倘若所有的课程都如近世代数课一般，那也许不仅对我，也是数学系广大芸芸学子的福音了. 至少，我从近世代数课中发现了数学的精华和美妙.”相信有更多的同学从编者二十多年的近世代数课教学中体会到群、环、域理论的美妙. 感谢上过编者此课的同学们，给他们的讲授也让编者一次又一次温习近世代数之美.

2012年，超星电子图书馆派人来全程拍摄编者讲授的“近世代数”. 讲课视频上网后，已被很多大学生观看学习，产生了较广泛的影响. 2018年，编者负责的“近世代数”入选南京大学“百”层次优质课程.

编者负责的“近世代数”慕课于2020年在中国大学MOOC平台正式上线，其慕课讲稿均由本人编写. 这是与本教材相配套的在线资源，网址为https://www.icourse163.org/NJU-1462062161. 编者感谢南京大学数学系刘公祥教授、陈柯与胡昊宇副教授共同参与慕课的讲解，特别感谢陈柯老师与胡昊宇老师分别为慕课大纲与习题的安排献计献策.

本书需要极少的预备知识，学过线性代数的本科二年级以上的大学生或研究生都可以阅读. 关于所需的集合论与初等数论方面的基础知识，读者可参看本书参考书目中Enderton的书《Elements of Set Theory》与编者的书《基础数论入门》. 参考书目中还列了几本近世代数方面有价值的教材与习题集供读者参考.

本书中的定理、引理、推论、例子与公式的编号都含有所在节号，但没有所在章号. 引用别的章结果时，会写明用的是第几章中结论. 本书每章留有20道习题，难度是合适的，个别较难点的题被分解成几小步或加了提示.

对近世代数中常用的数学概念，首次引入时本书标注英文名称，这便于读者进一步阅读有关英文书籍。为增加趣味性，本书还扼要介绍了一些重要数学家

的生平事迹, 也提到一些有趣的未解决猜测.

本书内容适用于一学期每周四节的近世代数课程, 进度紧张时有些部分(包括第3章的定理1.5、定理2.2、定理2.4以及第6章的定理6.1与6.2)证明可以略去不讲.

本书初稿完成后征询了一些同行专家的意见, 首都师范大学的徐飞教授、北京大学的袁新意教授、南方科技大学的胡勇老师、南京大学的朱富海教授与南京邮电大学的伍海亮博士都对初稿提出了宝贵的修改建议, 在此对他们表示衷心的感谢! 编者的在读研究生夏伟、汪涵与任宸凯协助进行了书稿的校对, 对他们的辛勤付出一并表示感谢。

感谢南京大学出版社蔡文彬主任、胡豪老师以及钱梦菊编辑鼓励支持本书的出版, 也感谢刘飞编辑认真细致的编辑工作.

编者相信, 本教材的出版将有益于近世代数的初学者.

孙智伟 (南京大学数学系)

写于2022年8月

本书常用记号说明

自然数集：$\mathbb{N}=\{0,1,2,\cdots\}$.

正整数集: $\mathbb{Z}^+=\{1,2,3,\cdots\}$.

整数环：$\mathbb{Z}$.

a 整除 b: $a\mid b$.

模正整数m的剩余类环：$\mathbb{Z}_m=\mathbb{Z}/m\mathbb{Z}=\{\bar{a}=a+m\mathbb{Z}:\ a\in\mathbb{Z}\}$.

有理数域：$\mathbb{Q}$.

实数域：$\mathbb{R}$.

实数α的整数部分: $\lfloor\alpha\rfloor$.

复数域：$\mathbb{C}$.

虚数单位: i.

立方根$\frac{-1+\sqrt{-3}}{2}$: ω.

集合A的基数：$|A|$.

置换 σ 的符号：$\mathrm{sign}(\sigma)$.

$\{1,\cdots,n\}$上的对称群：S_n.

$\{1,\cdots,n\}$上的交错群：A_n.

群(或者幺半群、域)的单位元：e.

群中元素a的阶：$o(a)$.

n 阶循环群: C_n.

群G的中心：$Z(G)=\{x\in G:\ \forall g\in G\,(gx=xg)\}$.

群G的导群 (换位子群)：$G'=\langle x^{-1}y^{-1}xy:\ x,y\in G\rangle$.

群G的 n 阶导群: $G^{(n)}$.

有限群G的幂指数: $\exp(G)=\min\{n\in\mathbb{Z}^+:\ \forall x\in G\,(x^n=e)\}$.

H为群G的子群：$H\leqslant G$.

子群H在群G中的指标：$[G:H]$.

H为群G的正规子群：$H\trianglelefteq G$.

群G按其正规子群H作成的商群：$G/H=\{gH:\ g\in G\}$.

子群H在群G中的正规核：$H_G=\bigcap\limits_{g\in G}gHg^{-1}$.

子群H在群G中的正规化子：$N_G(H)=\{g\in G:\ gH=Hg\}$.

同态 σ 的同态核：$\mathrm{Ker}(\sigma)$.

同态 σ 的同态像：$\mathrm{Im}(\sigma)$.

群G的自同构群：$\mathrm{Aut}(G)$.

群G的内自同构群：$\mathrm{Inn}(G)$.

群G作用在集合X上时，$x \in X$所在的轨道：$O_x = \{g \circ x : g \in G\}$.

群G作用在集合X上时，$x \in X$的稳定化子：$\mathrm{Stab}(x) = \{g \in G : g \circ x = x\}$.

群G作用在集合X上时的作用核：$\mathrm{Ker}(X) = \{g \in G : \forall x \in X\,(g \circ x = x)\}$.

群G作用在集合X上时的不动点集合：$\mathrm{Fix}(G) = \{x \in X : \forall g \in G\,(g \circ x = x)\}$.

群$G_1, \cdots, G_n$的直积：$G_1 \times \cdots \times G_n$.

I为环R的理想：$I \trianglelefteq R$.

环R按其理想I作成的商环：$R/I = \{a + I : a \in R\}$.

幺环R的单位群：$U(R)$.

环$R_1, \cdots, R_n$的直和：$R_1 \oplus \cdots \oplus R_n$.

域F的特征：$\mathrm{ch}(F)$.

q元域：$\mathbb{F}_q$.

K为域L的子域：$K \leqslant L$.

域扩张L/K的次数：$[L : K]$.

域F的自同构群：$\mathrm{Aut}(F)$.

域扩张L/K的Galois群：$\mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) : \forall a \in K\,(\sigma(a) = a)\}$.

目 录

第1章 群论基础

§1.1 代数方程发展史与群论起源

代数学最初的主要任务是解代数方程. 早在古巴比伦的文字泥板中就给出了实系数一元二次方程的解法.

对于一元二次方程$ax^2+bx+c=0$ (其中$a\neq 0$), 让$\Delta=b^2-4ac$, 则

$$\begin{aligned} & ax^2+bx+c=0 \\ \Longleftrightarrow\ & x^2+\frac{b}{a}x+\frac{c}{a}=0 \\ \Longleftrightarrow\ & \left(x+\frac{b}{2a}\right)^2=\frac{\Delta}{4a^2} \\ \Longleftrightarrow\ & x=\frac{-b\pm\sqrt{\Delta}}{2a}. \end{aligned}$$

对于一元n次多项式

$$P(x)=x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n,$$

令$x=y+t$ (其中参数t待定) 则依二项式定理知

$$P(x)=(y+t)^n+a_1(y+t)^{n-1}+\sum_{1<k\leqslant n}a_k(y+t)^{n-k}=y^n+(nt+a_1)y^{n-1}+Q(y),$$

这里$Q(y)$是关于y的次数小于$n-1$的多项式. 取$t=\frac{a_1}{n}$, 则$y=x-\frac{a_1}{n}$, 而且

$$P(x)=0\iff y^n+Q(y)=0.$$

因此, 解一元n次方程$P(x)=0$等价于解不含次高项(即y^{n-1}项)的一元n次方程$y^n+Q(y)=0$.

例如: 对于一元二次方程$x^2+bx+c=0$, 作根的平移$x=y-b/2$便得到关于y的不含一次项的方程$y^2=(b^2-4c)/4$, 由此可得

$$x=y-\frac{b}{2}=\pm\frac{\sqrt{b^2-4c}}{2}-\frac{b}{2}=\frac{-b\pm\sqrt{b^2-4c}}{2}.$$

一元三次方程的解法源于意大利数学家N. Fontana (丰坦纳, 1499–1557), G. Cardano (卡尔丹诺, 1501–1576) 在其1545年出版的书中发表了一元三次方程解法.

我们不妨只考虑不含次高项的一元三次方程

$$x^3+px=q.$$

写$x=a+b$ (其中a,b待定), 则原方程化为

$$(a+b)^3+p(a+b)=q,\ \text{即}\ (p+3ab)(a+b)=q-(a^3+b^3).$$

选取a,b使得

$$\begin{cases}3ab=-p,\\ a^3+b^3=q,\end{cases}$$

则$x=a+b$为原方程的根.

如果$3ab=-p$且$a^3+b^3=q$, 则

$$(a^3-b^3)^2=(a^3+b^3)^2-4(ab)^3=q^2-4\left(-\frac{p}{3}\right)^3=4\Delta$$

(其中$\Delta=\frac{q^2}{4}+\frac{p^3}{27}$), 从而$a^3-b^3=\pm2\sqrt{\Delta}$,

$$a^3=\frac{q}{2}\pm\sqrt{\Delta}\ \text{且}\ b^3=\frac{q}{2}\mp\sqrt{\Delta}.$$

由于$x^3-1=(x-1)(x^2+x+1)$, 三个立方根为

$$1,\ \omega=\frac{-1+\sqrt{-3}}{2},\ \bar{\omega}=\omega^2=\frac{-1-\sqrt{-3}}{2}.$$

选定a,b使得

$$\begin{cases}a^3=\frac{q}{2}+\sqrt{\Delta},\\ b^3=\frac{q}{2}-\sqrt{\Delta}.\end{cases}$$

考虑到

$$\begin{cases}(a\omega)^3=(a\omega^2)^3=a^3,\\ (b\omega)^3=(b\omega^2)^3=b^3,\\ (a\omega)(b\omega^2)=ab=(a\omega^2)(b\omega),\end{cases}$$

三个数

$$x_1=a+b,\ x_2=a\omega+b\omega^2,\ x_3=a\omega^2+b\omega$$

都是原方程$x^3+px=q$的根. 注意

$$x_1+x_2+x_3=a(1+\omega+\omega^2)+b(1+\omega+\omega^2)=a\times 0+b\times 0=0,$$

$$x_1x_2+x_1x_3+x_2x_3=x_1(x_2+x_3)+x_2x_3=(a+b)(-a-b)+(a^2-ab+b^2)=-3ab=p,$$

而且

$$x_1(x_2x_3)=(a+b)(a^2-ab+b^2)=a^3+b^3=q.$$

因此

$$\begin{aligned}&(x-x_1)(x-x_2)(x-x_3)\\=&x^3-(x_1+x_2+x_3)x^2+(x_1x_2+x_1x_3+x_2x_3)x-x_1x_2x_3\\=&x^3+px-q,\end{aligned}$$

即x_1,x_2,x_3为方程$x^3+px=q$的全部三个根.

1540年, Cardano的学生L. Ferrari (费拉里, 1522–1565) 找到了求解一元四次方程的办法.

我们不妨只考虑不含立方项的一元四次方程

$$x^4+px^2+qx+r=0.$$

引入待定参数t并考虑到$(x^2+t)^2=x^4+2tx^2+t^2$, 原方程等价于

$$(x^2+t)^2=(2t-p)x^2-qx+(t^2-r).$$

选择t使右边二次式的判别式为0, 即让t满足三次方程

$$(-q)^2-4(2t-p)(t^2-r)=0.$$

于是原方程等价于

$$(x^2+t)^2=(2t-p)\left(x-\frac{q}{2(2t-p)}\right)^2.$$

解两个一元二次方程

$$x^2+t=\sqrt{2t-p}\left(x-\frac{q}{2(2t-p)}\right)$$

与

$$x^2+t=-\sqrt{2t-p}\left(x-\frac{q}{2(2t-p)}\right),$$

即可得到原四次方程的四个根.

1796年, 19岁的C. F. Gauss (高斯, 1777–1855)证明了正十七边形可用圆规与直尺作出(古希腊留下的难题). 方程$x^{17}=1$的解(即17次单位根)为

$$\mathrm{e}^{2\pi i\frac{r}{17}}=\left(\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17}\right)^r\ (r=0,\cdots,16).$$

Gauss证明了用圆规与直尺可作出长为$\cos\frac{2\pi}{17}$的线段(从而可作出角度$\frac{2\pi}{17}$), 因为$16\cos\frac{2\pi}{17}$等于

$$-1+\sqrt{17}+\sqrt{34-2\sqrt{17}}+2\sqrt{17+3\sqrt{17}-\sqrt{34-2\sqrt{17}}-2\sqrt{34+2\sqrt{17}}}.$$

J. L. Lagrange (拉格朗日, 1736–1813) 认为三次、四次代数方程求根公式的发现多少带点偶然性, 他力图用统一的观点来求解二、三、四次代数方程. 1770年, Lagrange发表了长篇论文《关于代数方程解法的思考》, 通过引入Lagrange 预解方程他找到了统一求解二、三、四次代数方程的办法.

设

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=(x-x_1)\cdots(x-x_n).$$

令$t(\rho)=x_1+\rho x_2+\cdots+\rho^{n-1}x_n$, 则$1\leqslant k\leqslant n$时

$$\begin{aligned}\frac{1}{n}\sum_{\rho^n=1}\rho^{1-k}t(\rho)=&\frac{1}{n}\sum_{\rho^n=1}\rho^{1-k}\sum_{j=1}^{n}\rho^{j-1}x_j=\sum_{j=1}^{n}\frac{x_j}{n}\sum_{\rho^n=1}\rho^{j-k}\\=&\sum_{j=1}^{n}\frac{x_j}{n}\sum_{r=0}^{n-1}\mathrm{e}^{2\pi i\frac{j-k}{n}r}=x_k.\end{aligned}$$

最后一步是因为$z^n=1$但$z\neq1$时, $\sum\limits_{r=0}^{n-1}z^r=\frac{z^n-1}{z-1}=0$. 故对任何$n$次单位根$\rho$求出$t(\rho)$后, 就可求出$n$个根$x_1,\cdots,x_n$. 因此Lagrange建议先解预解方程

$$\prod_{i_1,\cdots,i_n}\left(x-(x_{i_1}+\rho x_{i_2}+\cdots+\rho^{n-1}x_{i_n})\right)=0,$$

其中ρ为n次单位根, 乘积过$1,\cdots,n$的所有全排列$i_1,\cdots,i_n$.

上面这个预解方程的系数是关于$x_1,\cdots,x_n$的对称多项式, 从而可用$x_1,\cdots,x_n$的初等对称多项式

$$\sigma_1=x_1+\cdots+x_n,\quad \sigma_r=\sum_{1\leqslant i_1<i_2<\cdots<i_r\leqslant n}x_{i_1}x_{i_2}\cdots x_{i_r}\ (r=2,\cdots,n)$$

来表示, 因而可用原方程系数$a_1, \cdots, a_n$表示出来.

对于一元二次方程$x^2+bx+c=0$, 设其根为x_1与x_2. 相应的Lagrange预解方程为

$$(x-(x_1+x_2))(x-(x_2+x_1))=(x-(x_1+x_2))^2=0$$

与

$$(x-(x_1-x_2))(x-(x_2-x_1))=x^2-(x_1-x_2)^2=0.$$

对称多项式$(x_1-x_2)^2$可用基本对称多项式表示出来, 事实上

$$(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2.$$

由于$x_1+x_2=-b$且$x_1x_2=c$, 两个预解方程容易解出, 因而可解出原方程$x^2+bx+c=0$.

三次方程$x^3+px=q$的预解方程是六次的, 但为关于x^3的二次方程. 四次方程

$$x^4+px^2+qx+r=0$$

的预解方程形如

$$((x^2-t_1^2)(x^2-t_2^2)(x^2-t_3^2))^4=0,$$

这可化为关于x^2的三次方程.

但Lagrange吃惊地发现他的统一方法对高于四次的一元代数方程失效. 例如: 不含次高项的一元五次方程

$$x^5+ax^3+bx^2+cx+d=0$$

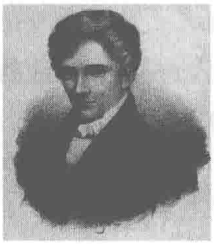
的预解方程是关于x^5的24次方程(注意$1,2,3,4,5$的全排列总个数为$5!=120=5\times 24$), 比原来的五次方程更难! Lagrange 认为五次或更高次方程的求解是上帝向人类智慧的挑战.

到了十九世纪二十年代, 挪威数学家N. H. Abel (阿贝尔, 1802–1829) 尝试求解一元五次方程, 最后却出人意料地证明了下述否定性结果:

定理1.1 (Abel定理). *对整数$n\geqslant 5$, 复数域上字母系数的n次多项式方程*

$$x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$$

不是根式可解的, 即使用复数与该方程的系数$a_1, \cdots, a_n$进行加减乘除与开方运算不可能得到该方程的所有根.



N. H. Abel

E. Galois

法国天才数学家E. Galois (伽罗瓦, 1811–1832) 创造性地引入“群(group)”这个伟大概念, 把代数方程的根式可解性与相应的Galois群是否为可解群联系起来, 彻底解决了一元代数方程是否根式可解的判别问题. 例如: Galois指出方程$x^5 - 4x + 2 = 0$就不是根式可解的.

【历史注记】**Galois与群论**

Galois一生经历坎坷, 21岁时死于因爱情纠纷引发的决斗. 1832年5月29日, 他在决斗前夕给友人的遗书中概述了自己在代数方程根式可解性方面的工作. 他写道:“我相信最终会有人发现, 将这一堆东西解释清楚对他们是有益的.”

Galois生前几次向法国科学院提交论文”关于代数方程论的研究报告”, 但没得到承认. Galois的遗稿到达J. Liouville (刘维尔, 1809–1882)手中后, 他看懂了这篇划时代的论文, 并于1846年在他主编的杂志上发表了Galois 的论文.

Galois的工作不仅标志着经典代数方程论的结束,也促使代数转向研究“群”这样抽象的结构.

E. Picard (皮卡, 1856–1941) 评价说:“在开创性和概念的深邃方面无人能及.”另一位数学家评论说:“Galois的洞察力简直可以说是个奇迹, 在科学史上即使再伟大的发现通常都可追溯到当时流行的东西, 只是由谁来发现的问题. 但Galois的理论与Einstein的广义相对论是仅有的例外.”

Galois洞察到代数方程根式可解的条件就是它具有某种特定类型的Galois群. Galois研究的群实际上是现在所说的置换群. 1854年, A. Cayley (凯莱, 1821–1895) 引入抽象群的概念, 但在当时没有引起注意.

受Galois工作的启发, 挪威数学家S. Lie (索菲斯·李, 1842–1899) 在1873–1874年引入连续群(现称Lie群)用以研究微分方程及相关分析.

除了数学上的应用外, 群论在量子力学、分子结构、分子振动、晶体对称、规范场论等方面也有重要的应用.

§1.2 半群与群的概念

设X是个非空集合.假如对任何的$x, y \in X$有唯一的X中元$x \circ y$与之对应, 则称$\circ$为X上一个二元运算, 并说X对运算$\circ$**封闭**. 如果运算$\circ$满足结合律,即对任何的$x, y, z \in X$有

$$(x \circ y) \circ z = x \circ (y \circ z),$$

则说X按运算$\circ$形成一个**半群**(semigroup), 也称$\langle X, \circ \rangle$ 为半群结构. 为方便起见, 我们称运算$\circ$为"乘法", 并常把$x \circ y$简写成xy.

设M是个半群. 如果e为M中元,且对任何的$a \in M$都有$ea = a = ae$, 则称e为半群M的**单位元**(identity) 或者**幺元**. 有单位元的半群叫做**幺半群**(monoid).

如果e_1, e_2都是幺半群M的单位元, 那么显然有$e_1 = e_1 e_2 = e_2$. 因此幺半群M的单位元唯一, 我们记之为e.

对于幺半群M中元a, 假如有$b \in M$使得$ab = e = ba$, 则说a可逆, b为a的**逆元**(inverse).

设M为幺半群. 如果$b, c \in M$都是$a \in M$的逆元, 那么

$$b = be = b(ac) = (ba)c = ec = c.$$

对M中可逆元a, 我们用a^{-1}表示a唯一的逆元. 当$a \in M$可逆时, a^{-1}也可逆且$(a^{-1})^{-1} = a$.

幺半群M中可逆元a与b的乘积也可逆,而且$(ab)^{-1} = b^{-1}a^{-1}$. 事实上,

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = e,$$

而且

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = e.$$

【例2.1】正整数集$\mathbb{Z}^+ = \{1, 2, 3, \cdots\}$按数的乘法形成幺半群, 其中数1为乘法单位元. 自然数集$\mathbb{N} = \{0, 1, 2, \cdots\}$依数的加法形成幺半群, 其中0为加法单位元(简称零元).

【例2.2】集合X的全体子集构成的集合$\mathcal{P}(X)$叫做X的**幂集**(power set). 易见$\mathcal{P}(X)$按集合的并运算形成幺半群, 空集$\emptyset$ 为其单位元. $\mathcal{P}(X)$按集合的交运算也形成幺半群, 全集X为其单位元.

【例2.3】全体n阶实方阵按矩阵乘法构成幺半群$M_n(\mathbb{R})$, 其单位元为n 阶单位方阵I_n. $M_n(\mathbb{R})$中元A可逆时, 其逆元A^{-1}正是A的逆矩阵. 对于$M_n(\mathbb{R})$中可逆矩阵A与B, 我们有$(AB)^{-1} = B^{-1}A^{-1}$.

【例2.4】任给整数d, 集合

$$S_d = \{x^2 + dy^2 : x, y \in \mathbb{Z}\}$$

按整数的乘法形成幺半群. 注意S_d对乘法封闭, 因为

$$\begin{aligned}&(u^2+dv^2)(x^2+dy^2)\\&=(ux)^2+(dvy)^2+d((vx)^2+(uy)^2)\\&=(ux\pm dvy)^2+d(vx\mp uy)^2.\end{aligned}$$

【例2.5】对于实数列$(a_n)_{n\geqslant 0}$与$(b_n)_{n\geqslant 0}$, 它们的卷积定义为

$$(a_n)_{n\geqslant 0}*(b_n)_{n\geqslant 0}=(c_n)_{n\geqslant 0},$$

这里

$$c_n=\sum_{k=0}^{n}a_kb_{n-k}.$$

易证$M=\{$实数列$(x_n)_{n\geqslant 0}\}$按卷积运算形成幺半群, 其卷积单位元为序列$(1,0,0,\cdots)$.

对于半群中元素a,b,c,d, 依此顺序作它们的乘积有多种方式:

$$((ab)c)d,\ (a(bc))d,\ a((bc)d),\ (ab)(cd),\ a(b(cd));$$

利用结合律可知它们算出的结果是相同的, 简记为$abcd$.

定理2.1. 设M为半群. 对于$a_1,\cdots,a_n\in M$, 依此顺序做成的这n个元素的乘积$a_1\cdots a_n$与括号的添加方式无关.

证明: 对n进行归纳. 当$n\leqslant 2$时, 结论显然.

现设$n>2$, 且少于n个的M中元的乘积都与括号的添加方式无关. 任给$a_1,\cdots,a_n\in M$及$m\in\{2,\cdots,n-1\}$, 易见

$$\begin{aligned}&(a_1\cdots a_m)(a_{m+1}\cdots a_n)\\&=(a_1(a_2\cdots a_m))(a_{m+1}\cdots a_n)\\&=a_1((a_2\cdots a_m)(a_{m+1}\cdots a_n))\\&=a_1(a_2\cdots a_n).\end{aligned}$$

这表明乘积$a_1\cdots a_n$总取值$a_1(a_2\cdots a_n)$, 它与括号添加方式无关.

类似地, 利用数学归纳法易证下述结果.

定理2.2. 设半群M满足交换律(即对任何$a,b\in M$有$ab=ba$). 任给$a_1,\cdots,a_n\in M$, 它们的乘积与因子排列顺序无关, 亦即$i_1,\cdots,i_n$为$1,\cdots,n$的全排列时

$$a_{i_1}a_{i_2}\cdots a_{i_n}=a_1a_2\cdots a_n.$$