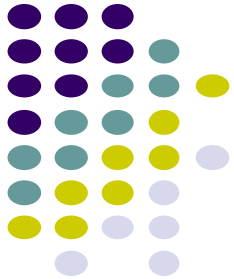
代数结构-群与环
习题课及作业

2024, 5, 6

南京大学计算机科学与技术系

内容提要- 半群与独异点



半群的定义

定义 13.1.1 设 $V=\langle S,\circ\rangle$ 是一个具有二元运算的代数系统，如果运算 $\circ$ 满足结合律，那么称 V 为**半群**.

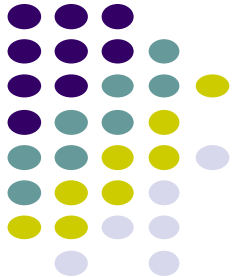
独异点的定义

定义 13.1.2 如果半群 $V=\langle S,\circ\rangle$ 中关于 $\circ$ 运算存在单位元 $e\in S$，那么称 V 是**幺半群**，也称作**独异点**，记作 $V=\langle S,\circ,e\rangle$.

半群与独异点的幂运算

$$a^0=e(\text{只对独异点成立}).$$
$$a^1=a.$$
$$a^{n+1}=a^n a.$$
$$a^m a^n=a^{m+n}.$$
$$(a^m)^n=a^{mn}.$$

内容提要-群的定义及实例



群的定义

定义 13.1.3 设 G 是非空集合，$\circ$ 是 G 上的二元运算，若下述条件被满足：

(1) 结合律，即对 $\forall a,b,c \in G$，有 $(a \circ b) \circ c = a \circ (b \circ c)$；

(2) 单位元，即 $\exists e \in G$ 使得对 $\forall a \in G$，有 $e \circ a = a = a \circ e$；

(3) 逆元，即对 $\forall a \in G, \exists a^{-1} \in G$ 使得 $a \circ a^{-1} = e = a^{-1} \circ a$；

则称 G 是一个群.

定义 13.1.4

(1) 若群 G 是有穷集，则称 G 是有限群，否则称作无限群. G 的基数称为群 G 的阶.

(2) 只含单位元的群称作平凡群.

(3) 若群 G 中的二元运算是可交换的，则称 G 为交换群或阿贝尔(Abel)群.

群的实例

整数加群 $\langle \mathbb{Z}, + \rangle$，实数加群 $\langle \mathbb{R}, + \rangle$，有理数加群 $\langle \mathbb{Q}, + \rangle$，复数加群 $\langle \mathbb{C}, + \rangle$，模 n 整数加群 $\langle \mathbb{Z}_n, \oplus \rangle$，$n$ 阶实矩阵的加群 $\langle \boldsymbol{M}_n(\mathbb{R}), + \rangle$，Klein 四元群 $G = \{e, a, b, c\}$，平凡群 $\{e\}$，循环群 $\langle a \rangle$，n 元置换群，其中，$\langle \mathbb{Z}, + \rangle$，$\langle \mathbb{R}, + \rangle$，$\langle \mathbb{Q}, + \rangle$，$\langle \mathbb{C}, + \rangle$，$\langle \boldsymbol{M}_n(\mathbb{R}), + \rangle$ 都是无限阶交换群，循环群 $\langle a \rangle$ 是(有限阶或无限阶)交换群，Klein 四元群是有限阶非交换群，n 元置换群是有限阶(交换或非交换)群.

元素的幂

定义 13.1.5 设 G 是群，$a \in G, n \in \mathbb{Z}$，则 a 的 n 次幂定义为

$$a^n = \begin{cases} e, & n = 0, \\ a^{n-1}a, & n > 0, \\ (a^{-1})^{-n}, & n < 0. \end{cases}$$

元素的阶

定义 13.1.6 设 G 是群，$a \in G$，使得等式 $a^k = e$ 成立的最小正整数 k 称为 a 的阶，记作 $|a| = k$，这时也称 a 为 k 阶元. 若不存在这样的正整数 k，则称 a 为无限阶元.

内容提要-群的基本性质

定理 13.1.1 (群的幂运算规则) 设 G 为群，则

(1) $\forall a \in G, (a^{-1})^{-1} = a$.

(2) $\forall a, b \in G, (ab)^{-1} = b^{-1}a^{-1}$. 推广形式为 $(a_1 a_2 \cdots a_{m-1} a_m)^{-1} = a_m^{-1} a_{m-1}^{-1} \cdots a_2^{-1} a_1^{-1}$.

(3) $\forall a \in G, a^n a^m = a^{n+m}, n, m \in \mathbb{Z}$.

(4) $\forall a \in G, (a^n)^m = a^{nm}, n, m \in \mathbb{Z}$.

(5) 若 G 为交换群，则 $(ab)^n = a^n b^n$.

定理 13.1.2 设 G 为群，则 G 中满足消去律，即对任意 $a, b, c \in G$ 有

(1) 若 $ab = ac$，则 $b = c$.

(2) 若 $ba = ca$，则 $b = c$.

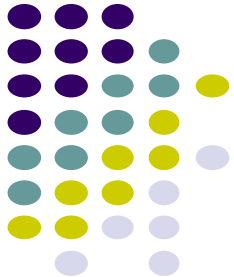
定理 13.1.3 设 G 为群，$a \in G$，且 $|a| = r$. 则

(1) 对任意 $k \in \mathbb{Z}, a^k = e$ 当且仅当 $r \mid k$，即 r 整除 k.

(2) $|a^{-1}| = |a|$.

(3) $|a^t| = \dfrac{r}{(t, r)}$，这里 $t \in \mathbb{Z}, (t, r)$ 是 t 与 r 的最大公因数 $\gcd(t, r)$.

子群



子群的定义

定义 13.1.7 设 G 是群，H 是 G 的非空子集，如果 H 关于 G 中的运算构成群，那么称 H 是 G 的子群，记作 $H \leqslant G$.

若 H 是 G 的子群，且 $H \subset G$，则 H 是 G 的真子群，记作 $H < G$.

判定定理

定理 13.1.4 (判定定理一) 设 G 为群，H 是 G 的非空子集，则 $H \leqslant G$ 当且仅当下面的条件成立.

(1) $\forall a, b \in H$ 有 $ab \in H$;

(2) $\forall a \in H$ 有 $a^{-1} \in H$.

定理 13.1.5 (判定定理二) 设 G 为群，H 是 G 的非空子集，则 $H \leqslant G$ 当且仅当 $\forall a, b \in H$ 有 $ab^{-1} \in H$.

定理 13.1.6 (判定定理三) 设 G 为群，$\varnothing \neq H \subseteq G$，如果 H 是有穷集，则 $H \leqslant G$ 当且仅当 $\forall a, b \in H$ 有 $ab \in H$.

子群实例

设 G 为群，设 $a \in G$，令

$$H = \{a^k | k \in \mathbb{Z}\},$$

即 a 的所有幂构成的集合，则 H 是 G 的子群，称作由 a 生成的子群，记作 $\langle a \rangle$.

令 C 是与 G 中所有的元素都可交换的元素构成的集合，即

$$C = \{a \in G | \forall x \in G, ax = xa\},$$

则 C 是 G 的子群，称作 G 的中心.

子群的交仍是子群，两个子群的并一般不构成子群.

子群的序结构

偏序集 $\langle L(G), \leq \rangle$ 称为群 G 的子群格，其中 $L(G) = \{H | H \leq G\}$.

群的分解

陪集的定义

定义 13.1.8 设 H 是群 G 的子群，$a \in G$. 令

$$Ha = \{ha | h \in H\},$$

称 Ha 是子群 H 在 G 中的右陪集，称 a 为 Ha 的代表元素.

陪集的性质(主教材定理 13.2.4–定理 13.2.6)

设 H 是群 G 的子群.

(1) $He = H$.

(2) $\forall a \in G$ 有 $a \in Ha$.

(3) $a \in Hb \Leftrightarrow ab^{-1} \in H \Leftrightarrow Ha = Hb$.

(4) 在 G 上定义关系 R: $\forall a, b \in G, \langle a, b \rangle \in R \Leftrightarrow ab^{-1} \in H$，则 R 是 G 上的等价关系，且 $[a]_R = Ha$.

(5) $\forall a \in G, H \approx Ha$.

正规子群

定义 13.1.9 设 H 是群 G 的子群，如果对于所有的 $a \in G$ 都有 $aH = Ha$，那么称 H 为 G 的正规子群或不变子群，记作 $H \trianglelefteq G$.

任何群 G 都有正规子群，因为它的两个平凡子群 $\{e\}$ 和 G 都是正规的. 当 G 是交换群时，G 的任意子群都是正规子群.

尽管 H 的右陪集 Ha 和左陪集 aH 可能不一样，但 H 在 G 中的右陪集的个数和左陪集的个数却是相等的，统称为 H 在 G 中的陪集数，也称作 H 在 G 中的指数，记作 $[G:H]$.

定理 13.1.7 (拉格朗日定理) 设 G 是有限群，$H \leq G$，则

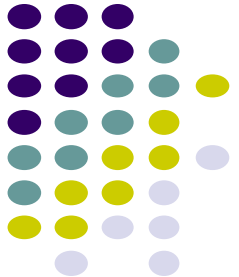
$$|G| = |H| \cdot [G:H].$$

推论 13.1.1

(1) 设 G 是 n 阶群，则 $\forall a \in G, |a|$ 是 n 的因子，且有 $a^n = e$.

(2) 设 G 是素数阶的群，则存在 $a \in G$ 使得 $G = \langle a \rangle$.

循环群



循环群的定义

定义 13.1.10　设 G 是群，若存在 $a \in G$ 使得 $G = \langle a \rangle$，则称 G 为循环群，称 a 为 G 的生成元.

循环群的分类

循环群 $G = \langle a \rangle$ 根据生成元 a 的阶可以分成两类：n 阶循环群和无限循环群.

设 $G = \langle a \rangle$ 是循环群，若 a 是 n 阶元，则

$$G = \{a^0 = e, a^1, a^2, \cdots, a^{n-1}\},$$

那么 $|G| = n$，称 G 为 n 阶循环群.

若 a 是无限阶元，则

$$G = \{a^0 = e, a^{\pm 1}, a^{\pm 2}, \cdots\},$$

这时称 G 为无限循环群.

循环群的生成元

定理 13.1.8　设 $G = \langle a \rangle$ 是循环群.

(1) 若 G 是无限循环群，则 G 只有两个生成元，即 a 和 a^{-1}.

(2) 若 G 是 n 阶循环群，则 G 含有 $\phi(n)$[①]个生成元. 对于任何不大于 n 且与 n 互素的正整数 r，a^r 是 G 的生成元.

循环群的子群

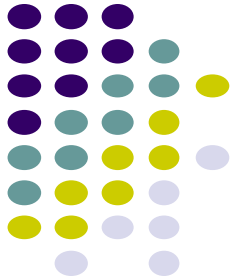
定理 13.1.9

(1) 设 $G = \langle a \rangle$ 是循环群，则 G 的子群仍是循环群.

(2) 若 $G = \langle a \rangle$ 是无限循环群，则 G 的子群除 $\{e\}$ 以外都是无限循环群.

(3) 若 $G = \langle a \rangle$ 是 n 阶循环群，则对 n 的每个正因子 d，G 恰好含有一个 d 阶子群.

置换群



n 元置换

定义 13.1.11 设 $S=\{1,2,\cdots,n\}$，S 上的任何双射函数 $\sigma: S \to S$ 称为 S 上的 *n 元置换*.

三种表示法：置换符号表示、不相交的轮换表示、对换表示.

定义 13.1.12 设 σ,τ 是 n 元置换，σ 和 τ 的复合 $\sigma\circ\tau$ 也是 n 元置换，称作 σ 与 τ 的*乘积*，记作 $\sigma\tau$.

奇置换与偶置换

定义 13.1.13 设 σ 是 $S=\{1,2,\cdots,n\}$ 上的 n 元置换. 若

$$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ \cdots,\ \sigma(i_{k-1})=i_k,\ \sigma(i_k)=i_1,$$

且保持 S 中的其他元素不变，则称 σ 为 S 上的 *k 阶轮换*，记作 $(i_1 i_2 \cdots i_k)$. 若 $k=2$，称 σ 为 S 上的*对换*.

任何 n 元置换都可以表示成不交轮换之积，在不考虑表示式中轮换的次序的情况下，这种表示式是唯一的.

任何轮换又可以进一步表示成对换之积，所以任何 n 元置换都可以表示成对换之积.

需要注意的是，轮换表示式是唯一的，而对换表示式是不唯一的. 尽管如此，可以证明表示式中所含对换个数的奇偶性是不变的.

如果 n 元置换 σ 可以表示成奇数个对换之积，则称 σ 为*奇置换*，否则称 σ 为*偶置换*. 在偶置换和奇置换之间存在一一对应，因此奇置换和偶置换各有 $\frac{n!}{2}$ 个.

n 元置换群

所有的 n 元置换构成的集合 S_n，关于置换的乘法构成一个群，称作 *n 元对称群*. 显然，$|S_n|=n!$.

---

[1] $\phi(n)$ 是欧拉函数，表示 $1,2,\cdots,n$ 中与 n 互素的数的个数.

设 A_n 是所有的 n 元偶置换的集合. 使用子群的判定定理不难证明 $A_n \leq S_n$，称 A_n 为 *n 元交错群*，有 $|A_n|=\frac{n!}{2}$.

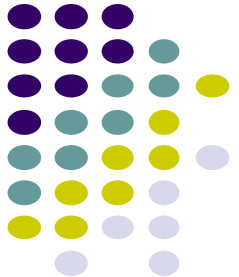
对于 S_n 来说，它的所有子群都称作 *n 元置换群*，而 n 元对称群 S_n 和 n 元交错群 A_n 都是 n 元置换群的特例.

定理 13.1.10 (Polya 定理) 设 $N=\{1,2,\cdots,n\}$ 是被着色物体的集合，$G=\{\sigma_1,\sigma_2,\cdots,\sigma_g\}$ 是 N 上的置换群. 用 m 种颜色对 N 中的元素进行着色，则在 G 的作用下不同的着色方案数是

$$M=\frac{1}{|G|}=\sum_{k=1}^{g} m^{c(\sigma_k)},$$

其中，$c(\sigma_k)$ 是置换 σ_k 的轮换表示式中包含 1 阶轮换在内的轮换个数.

环的定义和性质



环的定义

定义 13.1.14 设 $\langle R,+,\cdot\rangle$ 是代数系统，$+$ 和 $\cdot$ 是二元运算，如果满足以下条件：

(1) $\langle R,+\rangle$ 构成交换群；

(2) $\langle R,\cdot\rangle$ 构成半群；

(3) $\cdot$ 运算关于 $+$ 运算满足分配律，

那么称 $\langle R,+,\cdot\rangle$ 是一个环.

环的实例

整数环、有理数环、实数环、复数环、n 阶实矩阵环、模 n 的整数环.

环的运算性质

定理 13.1.11 设 $\langle R,+,\cdot\rangle$ 是环，则

(1) $\forall a\in R, a0=0a=0$.

(2) $\forall a,b\in R,(-a)b=a(-b)=-ab$.

(3) $\forall a,b,c\in R, a(b-c)=ab-ac,(b-c)a=ba-ca$.

(4) $\forall a_1,a_2,\cdots,a_n,b_1,b_2,\cdots,b_m\in R$，其中 $n,m\geqslant 2$，有

$$\left(\sum_{i=1}^{n}a_i\right)\left(\sum_{j=1}^{m}b_j\right)=\sum_{i=1}^{n}\sum_{j=1}^{m}a_ib_j.$$

几种特殊的环

定义 13.1.15 设 $\langle R,+,\cdot\rangle$ 是环.

(1) 若环中乘法 $\cdot$ 满足交换律，则称 R 为交换环.

(2) 若环中乘法 $\cdot$ 存在单位元，则称 R 为含幺环.

(3) 若 $\forall a,b\in R$，当 $ab=0$ 时，必然有 $a=0$ 或 $b=0$，则称 R 为无零因子环.

(4) 若 R 既是交换环、含幺环，也是无零因子环，则称 R 为整环.

(5) 设 R 是整环，$|R|\geqslant 2$，且 $\forall a\in R^*=R-\{0\}$，都有 $a^{-1}\in R$，则称 R 是域.

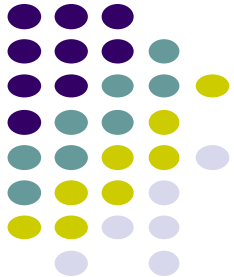
整环和域的实例

通常说的有理数域、实数域和复数域都是域.

整数环是整环，不是域.

对于模 n 的整数环 $\mathbb{Z}_n$，$\mathbb{Z}_n$ 是域当且仅当 n 是素数.

基本要求



- 1. 判断或者证明给定集合和运算是否构成半群、独异点、群、环、域.
- 2. 会运用群的基本性质证明相关的命题.
- 3. 能够证明 G 的子集构成 G 的子群.
- 4. 熟悉陪集的定义和性质.
- 5. 熟悉 Lagrange 定理及其推论.
- 6. 会求循环群的生成元及其子群.
- 7. 熟悉 n 元置换的表示方法、乘法以及 n 元置换群.
- 8. 能够运用 Polya 定理解决简单的计数问题.
- 9. 了解环的运算性质，能够进行环中的运算.
- 10. 能够根据定义判别一些特殊的环

题型一：判别或验证代数结构

1. 判断下列集合关于给定运算能否构成半群、独异点和群. 如果不能，请说明理由.

(1) $\{n\sqrt{2}\mid n\in\mathbb{Z}\}$ 关于普通加法.

(2) $\{m+n\sqrt{2}\mid m,n\in\mathbb{Z}\}$ 关于普通乘法.

(3) 实数集 $\mathbb{R}$ 关于 $\circ$ 运算，其中 $\circ$ 运算定义为 $a\circ b=2(a+b)$.

(4) 设 $\mathbb{R}$ 为实数集，$\mathbb{R}\times\mathbb{R}$ 关于 $\circ$ 运算，其中 $\circ$ 运算定义为 $\langle a,b\rangle\circ\langle c,d\rangle=\langle a+$

2. 在整数环 $\langle\mathbb{Z},+,\cdot\rangle$ 中定义 $*$ 和 $\diamond$ 两个运算，$\forall a,b\in\mathbb{Z}$ 有 $a*b=a+b-1, a\diamond b=a$

环.

解答与分析

1. (1) 构成半群、独异点和群.

(2) 构成半群和独异点，但不构成群，因为 0 没有逆元.

(3) 不构成半群，运算不满足结合律. 例如，

$$(1\circ 1)\circ 0=2(1+1)\circ 0=4\circ 0=2(4+0)=8,$$
$$1\circ(1\circ 0)=1\circ 2(1+0)=1\circ 2=2(1+2)=6.$$

(4) 构成半群、独异点和群.

2. 先验证封闭性：$\forall a,b\in\mathbb{Z}$ 有 $a*b,a\diamond b\in\mathbb{Z}$.

下面验证结合律. 任取 $a,b,c\in\mathbb{Z}$，

$$\begin{aligned}(a*b)*c&=(a+b-1)*c\\&=(a+b-1)+c-1\\&=a+b+c-2,\\a*(b*c)&=a*(b+c-1)\\&=a+(b+c-1)-1\\&=a+b+c-2.\end{aligned}$$

$$\begin{aligned}(a\diamond b)\diamond c&=(a+b-ab)\diamond c\\&=(a+b-ab)+c-(a+b-ab)c\\&=a+b+c-(ab+ac+bc)+abc,\\a\diamond(b\diamond c)&=a\diamond(b+c-bc)\\&=a+(b+c-bc)-a(b+c-bc)\\&=a+b+c-(ab+ac+bc)+abc.\end{aligned}$$

1 为 $*$ 运算的单位元. $2-a$ 为 a 关于 $*$ 运算的逆元. $*$ 运算满足交换律，所以 $\mathbb{Z}$ 关于 $*$ 运算构成交换群，关于 $\diamond$ 运算构成半群.

最后证明 $\diamond$ 关于 $*$ 运算满足分配律.

$$\begin{aligned}a\diamond(b*c)&=a\diamond(b+c-1)\\&=a+(b+c-1)-a(b+c-1)\\&=2a+b+c-ab-ac-1,\\(a\diamond b)*(a\diamond c)&=(a+b-ab)+(a+c-ac)-1\\&=a+b+a+c-ab-ac-1\\&=2a+b+c-ab-ac-1,\end{aligned}$$

即，$a\diamond(b*c)=(a\diamond b)*(a\diamond c)$. 显然，$\diamond$ 运算可交换，故有 $(b*c)\diamond a=(b\diamond a)*(c\diamond a)$.

综上所述，$\langle\mathbb{Z},*,\diamond\rangle$ 构成环.

求解这类问题的主要方法是根据定义进行验证. 对于半群要验证封闭性和结合律；对于独异点要验证封闭性、结合律以及单位元；对于群，除了进行以上验证之外，还必须验证每个元素都有逆元；而对于环则除了要验证两个运算分别构成交换群和半群之外，还要验证乘法对加法的分配律.

题型一：代数系统及运算性质的判别

解答与分析

1. (1) 构成;交换,不结合,无单位元、零元、可逆元.

(2) 构成;交换,不结合,无单位元、零元、可逆元.

(3) 构成;交换,结合,无单位元和可逆元,零元 1.

(4) 构成;交换,不结合,无单位元、零元、可逆元.

(5) 不构成.

(6) 构成;交换、结合,单位元 0,零元 -1,可逆元是 0 和 -2, $0^{-1}=0,(-2)^{-1}=-2$.

在讨论运算性质时注意给定的是什么集合. 例如,如果 (6) 中的运算不是定义在整数集 $\mathbb{Z}$ 上,而是定义在有理数集 $\mathbb{Q}$ 上,那么除了零元 -1 以外,其他有理数 x 都是可逆元素,且 $x^{-1}=-\dfrac{x}{1+x}$.

2. (1) 封闭;交换、结合,单位元是 $\varnothing$,零元是 $\{a,b\}$.

(2) 封闭;可结合,仅当 S 为单元集时可交换,单位元是恒等函数,S 为单元集时单位元也是零元.

(3) 封闭;可结合,仅当 B 为单元集时可交换;单位元为单位矩阵,零元为全 0 矩阵.

(4) 封闭;可交换、可结合;仅当 $n=1$ 时有单位元 1,0 是零元.

(5) 封闭;可交换、可结合;单位元是空集;没有零元.

(6) 当 $|B|<3$ 时,B 上的所有等价关系只有恒等关系和全域关系,运算封闭;此时运算满足交换律和结合律,单位元是恒等关系,零元为全域关系. 当 $|B|\geqslant 3$ 时,两个等价关系的并集不一定具有传递性,运算不封闭.

注意:有的问题中对所给定的集合或者参数没有加以具体说明. 例如 (2) 中的集合 S,(3) 和 (6) 中的集合 B,(4) 中的正整数 n 等,当这些集合或者参数取不同的值时,系统涉及交换律、单位元、零元、可逆元等性质有可能会发生改变,因此要针对不同取值进行分析.

3. $*$ 运算满足交换、结合、幂等律,不满足消去律. 单位元是 b;零元是 a;a,b,c 都是幂等元;可逆元只有 b, $b^{-1}=b$.

$\circ$ 运算满足结合律,幂等律,不满足交换律和消去律. 没有单位元和零元,也没有可逆元素,a,b,c 都是幂等元.

$\cdot$ 运算不满足交换律、结合律、幂等律和消去律;没有单位元、零元、可逆元素;只有 a 是幂等元.

通过运算表可以判别运算性质,也可以求运算的特异元素. 具体方法如下.

如果运算表的元素关于主对角线成对称分布,那么运算是可交换的,如表 12.3.1 中的 $*$ 运算.

如果主对角线元素的排列顺序与表头元素的排列顺序(表 12.3.1 中的 a,b,c)一样,那么运算是幂等的,如表 12.3.1 中的 $*$ 和 $\circ$ 运算.

如果在运算表中的某行或者某列(除了零元所在的行和列之外)有两个相同的元素,那么运算不满足消去律. 例如,上述的 $*$ 运算,由于 a 是零元,不考虑 a 所在的行与列,在 c 所在的行与列中 c 都出现了 2 次,这就意味着 $b*c=c*c$ 或者 $c*b=c*c$,但是显然没有 $b=c$. 因此,破坏了消去律.

如果一个元素所在的行和列的元素排列顺序都与表头元素排列顺序(表 12.3.1 中的 a,b,c)一致,那么这个元素是单位元,如 $*$ 运算表中的 b.

如果一个元素的行和列的元素都是这个元素自身,那么这个元素是零元,如 $*$ 运算表中的 a,其所在的行和列元素全是 a,因此它是零元.

如果元素 x 在主对角线中排列的位置与表头中的位置一致,那么这个元素是幂等元,如 $*$ 运算表中的 a,a 在表头中的位置是第一位,在主对角线也是排在第一位. 类似的,b 和 c 也满足要求.

最后谈谈对结合律的判断. 为判断结合律是否成立,应该对 A 中的所有元素 x,y,z 验证 $(xy)z=x(yz)$ 是否为真. 如果 A 中有 n 个元素,必须验证 n^3 个等式. 注意到以下事实:如果 x,y,z 中存在单位元或者零元,那么等式一定成立. 因此验证只需对 A 中的非单位元和非零元进行. 例如,对于 $*$ 运算只需验证 $(c*c)*c=c*(c*c)$ 是否成立,显然这是成立的,因此满足结合律. 对于 $\circ$ 运算,既没有单位元,也没有零元,这种简化验证的方法就不起作用了. 但是观察到 $\circ$ 运算具有下述特征:每个元素都是左零元,即满足 $x\circ y=x$. 因此,无论是 $(x\circ y)\circ z$ 还是 $x\circ(y\circ z)$ 都等于最左边的元素 x,从而证明了结合律. 对于 $\cdot$ 运算,上述方法都没有用. 观察运算表只有 $a\cdot b=b$,其他都是 a,有可能在涉及 $a\cdot b$ 的运算中破坏结合律. 由于

$$(b\cdot b)\cdot b=a\cdot b=b,$$

$$b\cdot(b\cdot b)=b\cdot a=a,$$

而 $a\neq b$,因此 $\cdot$ 运算不满足结合律.

题型二：群或环中的简单

这些计算包括计算元素的阶、元素的幂、子群的陪集、循环群的生成元和子群、置换群中的乘积和逆、同环中公式的展开式等.

1. 设 $\mathbb{Z}_{18}$ 为模 18 整数加群，求所有元素的阶.
2. 设 G 为群，x,y 属于 G，且 $yxy^{-1}=x^2$，其中 x 不是单位元，y 是 2 阶元. 求 x 的阶.
3. 设 G 为模 12 加群，求 $\langle 3\rangle$ 在 G 中的所有左陪集.
4. 设 G 的运算表如表 13.3.1 所示，问 G 是否为循环群. 如果是，求出它所有的生成元和子群.

表 13.3.1

$\cdot$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

5. 设 $\langle R,+,\cdot\rangle$ 是环，a,b 为环中任意元素，计算 $(a+b)^2(b-a)$.
6. 在域 $\mathbb{Z}_7$ 中解下列方程组：

$$\begin{cases} x-y=5, \\ 2x+y=3. \end{cases}$$

1. 所有元素的阶为

$$\begin{aligned} &|0|=1,\ |1|=|5|=|7|=|11|=|13|=|17|=18, \\ &|2|=|4|=|8|=|10|=|14|=|16|=9, \\ &|3|=|15|=6,\ |6|=|12|=3,\ |9|=2. \end{aligned}$$

2. 因为 y 是 2 阶元，所以 $y=y^{-1}$，且 $y^2=(y^{-1})^2=e$. 由 $yxy^{-1}=x^2$ 得

$$\begin{aligned} x^4=(x^2)^2&=(yxy^{-1})(yxy^{-1})=yx^2y^{-1} \\ &=y(yxy^{-1})y^{-1}=y^2x(y^{-1})^2 \\ &=exe=x. \end{aligned}$$

于是有，$x^3=e$. 因为 $|x|\neq 1$，所以 $|x|=3$.

确定 x 的阶的基本方法就是推导出如下的等式：$x^k=e$. 然后在 k 的正因子中寻找 x 的阶.

3. $\langle 3\rangle=\{0,3,6,9\}$，$\langle 3\rangle$ 的不同左陪集有 3 个，即

$$\begin{aligned} &0+\langle 3\rangle=3+\langle 3\rangle=6+\langle 3\rangle=9+\langle 3\rangle=\langle 3\rangle, \\ &1+\langle 3\rangle=4+\langle 3\rangle=7+\langle 3\rangle=10+\langle 3\rangle=\{1,4,7,10\}, \\ &2+\langle 3\rangle=5+\langle 3\rangle=8+\langle 3\rangle=11+\langle 3\rangle=\{2,5,8,11\}. \end{aligned}$$

对于有限群 G，子群 H 的不同的陪集数（右陪集数或左陪集数）为 $|G|/|H|$. 一般采取枚举的方法计算 H 的所有的陪集，以右陪集为例求解步骤如下.

(1) 第 1 个右陪集就是 H 自身.

(2) 任选元素 $a\in G-H$，求 Ha，作为第 2 个右陪集.

(3) 任选元素 $b\in G-(H\cup Ha)$，求 Hb，作为第 3 个右陪集.

(4) 任选元素 $c\in G-(H\cup Ha\cup Hb)$，求 Hc，作为第 4 个右陪集，……

依次做下去. 由于 G 是有限群，经过有限步就可以得到 G 的全体右陪集.

4. 易见 a 为单位元. 由于生成元的阶与群的阶相等，所以只要是 6 阶元就是生成元. 而 $|b|=6$，所以 b 为生成元，因而 G 是循环群. $|c|=3,|d|=2,|e|=3,c,d,e$ 不是生成元. $|f|=6$，因而 f 也是生成元.

子群有 $\langle a\rangle=\{a\},\langle c\rangle=\{c,e,a\},\langle d\rangle=\{d,a\},G$.

5.

$$\begin{aligned} (a+b)^2(b-a)&=(a^2+ab+ba+b^2)(b-a) \\ &=a^2b+ab^2+bab+b^3-a^3-aba-ba^2-b^2a. \end{aligned}$$

6. 由第一个方程得到 $y=x-5$，代入第二个方程（也可直接将两个方程左右两边分别相加）得到 $3x=1$. 从而得到 $x=5,y=0$.

题型三：子群的证明与子群格结构

1. 设 G 为群，a 是 G 中的 2 阶元，证明 G 中与 a 可交换的元素构成 G 的子群.

2. 设 i 是虚数单位，即 $\mathrm{i}^2=-1$，令

$$G=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\pm\begin{pmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{pmatrix},\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\pm\begin{pmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{pmatrix}\right\},$$

则 G 关于矩阵乘法构成群. 找出 G 的所有子群，并画出它的子群格.

解答与分析

1. 令 $H=\{x\in G\mid xa=ax\}$，下面证明 H 是 G 的子群. 首先 e 属于 H，故 H 是 G 的非空子集. 任取 $x,y\in H$，有 $xa=ax$，$ya=ay$，从而有 $a=x^{-1}ax=yay^{-1}$. 于是得

$$\begin{aligned}(xy^{-1})a&=x(y^{-1}a)=x(y^{-1}yay^{-1})\\&=xay^{-1}=x(x^{-1}ax)y^{-1}\\&=axy^{-1}=a(xy^{-1}).\end{aligned}$$

因此 $xy^{-1}\in H$. 由子群判定定理二命题得证.

证明子群可以用判定定理，特别是判定定理二. 证明的步骤是：首先验证 H 非空，然后对任取的 $x,y\in H$，证明 $xy^{-1}\in H$.

2. 令 A,B,C,D 分别表示 $\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}\mathrm{i}&0\\0&-\mathrm{i}\end{pmatrix},\begin{pmatrix}0&1\\-1&0\end{pmatrix},\begin{pmatrix}0&\mathrm{i}\\\mathrm{i}&0\end{pmatrix}$，$G$ 的运算表如表 13.3.2 所示.

表 13.3.2

·	A	$-A$	B	$-B$	C	$-C$	D	$-D$
A	A	$-A$	B	$-B$	C	$-C$	D	$-D$
$-A$	$-A$	A	$-B$	B	$-C$	C	$-D$	D
B	B	$-B$	$-A$	A	D	$-D$	$-C$	C
$-B$	$-B$	B	A	$-A$	$-D$	D	C	$-C$
C	C	$-C$	$-D$	D	$-A$	A	B	$-B$
$-C$	$-C$	C	D	$-D$	A	$-A$	$-B$	B
D	D	$-D$	C	$-C$	$-B$	B	$-A$	A
$-D$	$-D$	D	$-C$	C	B	$-B$	A	$-A$

G 的子群有 6 个，即

平凡子群：$\langle A\rangle=\{A\},G$.

2 阶子群：$\langle -A\rangle=\{A,-A\}$.

4 阶子群：$\langle B\rangle=\{A,B,-A,-B\},\langle C\rangle=\{A,C,-A,-C\},\langle D\rangle=\{A,D,-A,-D\}$.

G 的子群格如图 13.3.1 所示.

对于较小的有限群 G，可以按照子群格的结构从底层（平凡子群 $\{e\}$）开始，然后逐层向上，从小到大枚举它的子群，直到 G 本身为止，从而得到一个子群格. 目前还没有高效的对每个群都适用的枚举算法. 可以尝试计算每个元素的阶，找到由每个元素生成的子群，然后按照它们之间的包含关系做出一个偏序结构. 接着从下层向上逐步检查子群的并集，看看它们是否构成新的更大的子群. 如果能够构成，就把它加到这个偏序结构中；否则就需要把运算所产生的新元素加到其中，直到它关于运算封闭为止，此时将所产生的新子群加到偏序结构中.

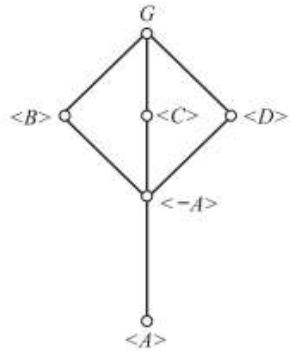


图 13.3.1

4 题型四：证明群中的简单性质

1. 设 G 为群，$a \in G$ 是有限阶元，对于任意 $x \in G$，证明：$|xax^{-1}| = |a|$.
2. 证明：偶数阶群必含 2 阶元(第13.4.1节习题十三第18题).

解答与分析

1. 设 $|a| = n$，由式

$$(xax^{-1})^n = xa^n x^{-1} = e$$

知，xax^{-1} 也是有限阶元. 设 $|xax^{-1}| = m$，则有 $m|n$.

由于 a 可以表示成

$$a = x^{-1}(xax^{-1})(x^{-1})^{-1},$$

所以根据前面的结果，也有 $n \mid m$. 综上所述有 $m = n$.

证明元素 a 和 b 的阶相等的基本方法是：设 $|a| = n$，$|b| = m$，然后证明 $n \mid m$ 和 $m \mid n$. 为此，只要证明 $a^m = e$ 和 $b^n = e$. 在化简 a^m 或 b^n 时，使用的公式主要有群中的结合律以及元素的幂运算规则，即

$$(ab)c = a(bc),$$
$$(a^{-1})^{-1} = a,\ (a_1a_2\cdots a_n)^{-1} = a_n^{-1}\cdots a_2^{-1}a_1^{-1},$$
$$a^n a^m = a^{n+m},\ (a^n)^m = a^{nm}.$$

2. 显然有，$x^2 = e$ 当且仅当 $|x| = 1$ 或 2. 因此，对于 G 中元素 x，如果 $|x| > 2$，那么必有 $x^{-1} \neq x$. 由于 $|x| = |x^{-1}|$，故阶大于 2 的元素成对出现，共有偶数个，所以剩下的 1 阶和 2 阶元总共也应该是偶数个. 1 阶元只有 1 个，就是单位元，从而证明了 G 中必有 2 阶元.

以上证明题都涉及群的简单性质. 这类问题通常要求证明以下命题.

(1) 群中的元素相等，这里的元素通常是若干元素运算的结果.

(2) 群中的子集相等.

(3) 元素的阶相等或者整除.

(4) 其他简单命题，如交换性等.

基本的证明方法可以总结如下.

(1) 证明群中元素相等的基本方法就是用结合律、消去律、单位元及逆元的性质、群的幂运算规则等对等式进行变形和化简.

(2) 证明子集相等的基本方法就是证明两个子集相互包含.

(3) 证明两个元素的阶 r 和 s 相等，r 整除 s、某个元素的阶等于 r 等命题的基本方法是证明整除. 在证明中可以使用结合律、消去律、幂运算规则以及关于元素的阶的性质(定理 13.1.3). 特别地，可能用到 a 为 1 阶或 2 阶元的充分必要条件 $a^{-1} = a$.

题型五：Lagrange 定理的应用

设 H_1, H_2 分别是群 G 的 r, s 阶子群，若 r 和 s 互素，证明：$H_1 \cap H_2 = \{e\}$.（第13.4.1节习题十三第24题）

设 H_1, H_2 分别是群 G 的 r, s 阶子群，若 r 和 s 互素，证明：$H_1 \cap H_2 = \{e\}$.（第13.4.1节习题十三第24题）

解答与分析

易见 $H_1 \cap H_2$ 是 H_1 的子群，也是 H_2 的子群. 由 Lagrange 定理，子群的阶是群的阶的因子，因此 $|H_1 \cap H_2|$ 整除 r，也整除 s. 从而，$|H_1 \cap H_2|$ 整除 r 与 s 的最大公因子. 由已知 r 与 s 的最大公因子 $\gcd(r, s) = 1$，这就得到 $|H_1 \cap H_2| = 1$，故 $H_1 \cap H_2 = \{e\}$.

根据 Lagrange 定理，可以给出一些与有限群相关的计数结果. 设 H 为 G 的子群，a 是 G 中元素，$N(a) = \{x \in G \mid xa = ax\}$ 为 a 的正规化子（可以证明 $N(a) \leq G$ 且 $C \subseteq N(a)$），那么有

(1) $|H| = |xHx^{-1}|$.

(2) $|C|$ 是 $|N(a)|$ 和 $|G|$ 的因子.

(3) $|a| = |\langle a \rangle|$ 是 $|N(a)|$ 和 $|G|$ 的因子.

(4) $|a^n|$ 是 $|a|$ 的因子.

(5) $a^2 = e \Leftrightarrow a = a^{-1} \Leftrightarrow |a| = 1$ 或 2.

题型六：Polya 定理的应用

1. 用 3 种颜色涂色 3×3 的方格棋盘，每个方格一种颜色. 如果允许棋盘任意旋转或翻转，问有多少种不同的涂色方案.
2. 如图 13.3.2，T 是一棵有 7 个结点的树，这里用黑白两色对 T 的结点着色. 如果交换 T 的某个左子树与右子树以后，一种着色方案变成另一种着色方案，那么认为这两种方案是同样的方案. 问不同的着色方案有多少种.

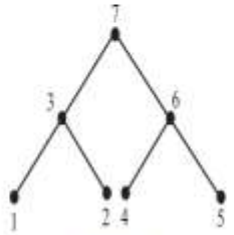


图 13.3.2

解答与分析

1. 群 G 的置换结构为：

恒等置换：(•)(•)(•)(•)(•)(•)(•)(•)(•)	1 个
绕中心旋转 90°、27°：(• • • •)(• • • •)(•)	2 个
绕中心旋转 180°：(• •)(• •)(• •)(• •)(•)	1 个
翻转 180°：(• •)(• •)(• •)(•)(•)(•)	4 个

根据 Polya 定理，不同的着色方案数是

$$M=\frac{1}{8}\times(3^9+2\times3^3+3^5+4\times3^6)=2\,862.$$

2. 置换群 G 含有如下 8 个置换：

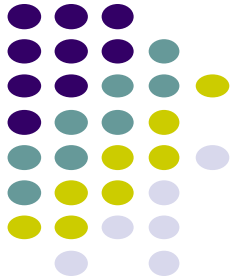
$$(15)(42)(36)(7),$$
$$(12)(3)(4)(5)(6)(7),$$
$$(45)(1)(2)(3)(6)(7),$$
$$(1524)(36)(7),$$
$$(1425)(36)(7),$$
$$(12)(45)(3)(6)(7),$$
$$(14)(25)(36)(7),$$
$$(1)(2)(3)(4)(5)(6)(7).$$

根据 Polya 定理有

$$M=\frac{1}{8}\times(2^7+2\times2^6+2^5+2\times2^4+2\times2^3)=42.$$

图 13.3.2 中有 3 个对称轴，即过顶点 3、顶点 6、顶点 7 的垂直线，所有的置换都可以用围绕这些轴的翻转来表示. 需要注意的是，这些置换必须构成群. 如果两个置换合成以后得到一个新的置换，那么就要把这个新的置换加到群中去，直到所有置换的集合关于合成运算封闭为止. 这里的合成恰好产生 5 个新的置换，因此群中共有 8 个置换.

作业



1. 填空题(6 小题,每小题 5 分,共 30 分).

(1) 设 $G=\langle a\rangle$ 为 12 阶循环群,则 G 的 4 阶子群是_____.

(2) 设 $\mathbb{Z}_n$ 是模 n 整数环,在_____条件下,$\mathbb{Z}_n$ 构成域.

(3) 在 4 元对称群 S_4 中,$\langle(1234)\rangle=$_____.

(4) 设 $G=\langle a\rangle$ 为 24 阶循环群,则 G 的所有生成元为_____.

(5) 设 $\mathbb{R}$ 为实数环,$M_2(\mathbb{R})$ 为 2 阶实数矩阵环,那么在它们的直积 $\langle \mathbb{R}\times M_2(\mathbb{R}),+,\cdot\rangle$ 中,$\langle -1,\begin{pmatrix}1&2\\2&0\end{pmatrix}\rangle\cdot\langle 2,\begin{pmatrix}1&1\\-1&0\end{pmatrix}\rangle=$_____.

(6) $\mathbb{Z}$ 和 $\mathbb{Z}_n$ 分别表示整数环和模 n 整数环,则 $f:\mathbb{Z}\to\mathbb{Z}_n$,$f(x)=$_____是 $\mathbb{Z}$ 到 $\mathbb{Z}_n$ 的满同态映射.

2. 简答题(4 小题,每小题 10 分,共 40 分).

(1) 判断下列集合对于给定运算能否构成群,并简要说明理由.

(1.1) 非零实数集 $\mathbb{R}^*$ 关于 $\circ$ 运算,其中 $a\circ b=2ab$.

(1.2) $G=\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix}\middle|a,b\text{为实数且}a^2+b^2\neq 0\right\}$ 关于矩阵乘法.

(2) 举出满足以下条件的例子.

(2.1) $\langle R_1,+,\cdot\rangle$ 是没有单位元的环,$S\subset R_1$,$\langle S,+,\cdot\rangle$ 也构成环,且含有单位元.

(2.2) $\langle R_2,+,\cdot\rangle$ 是有单位元的环,$S\subset R_2$,$\langle S,+,\cdot\rangle$ 也是有单位元的环,但是这两个单位元不相等.

(3) 设 $\mathbb{Z}_n$ 为模 n 整数加群,$f:\mathbb{Z}_{12}\to\mathbb{Z}_3$,$f(x)=x \bmod 3$. 验证 f 为同态映射,并说明 f 是否为单同态和满同态.

(4) 设 $G=\langle\mathbb{Z}_{24},\oplus\rangle$,求出 G 的全体子群,并画出子群格.

3. 证明题(2 小题,每小题 10 分,共 20 分).

(1) 设 G 为群. 证明:G 为 Abel 群的充分必要条件是对于 G 中的任意元素 a,b 有 $(ab)^2=a^2b^2$.

(2) 设 G 为群,$\sim$ 为 G 上等价关系,且满足 $\forall a,b,c\in G, ab\sim ac\Rightarrow b\sim c$. 证明:等价类 $[e]=\{x\in G\mid e\sim x\}$ 构成 G 的子群.

4. 应用题(10 分).

某一通信编码的码字 $x=(x_1,x_2,\cdots,x_7)$,其中 x_1,x_2,x_3 和 x_4 为数据位,x_5,x_6 和 x_7 为校验位,并且满足:

$$x_5=x_1\oplus x_2\oplus x_3,$$
$$x_6=x_1\oplus x_2\oplus x_4,$$
$$x_7=x_1\oplus x_3\oplus x_4,$$

这里的 $\oplus$ 是模 2 加法. 设 S 为所有这样的码字构成的集合,在 S 上定义二元运算如下:

$$\forall x,y\in S,\ x\circ y=(x_1\oplus y_1,x_2\oplus y_2,\cdots,x_7\oplus y_7).$$

验证 $\langle S,\circ\rangle$ 构成群.