网络安全数学基础(二)

沈佳辰
jcshen@sei.ecnu.edu.cn

- 办公室:理科大楼B1203
- Email: jcshen@sei.ecnu.edu.cn
- 电话：62233147

助教信息

- 姓名：潘宇豪
- Email: 51265902076@stu.ecnu.edu.cn
- 答疑时间：周六9:00~10:30

  地点：理科大楼B1210

主要内容

- 抽象代数

主要内容

- 抽象代数

– 群论
– 环
– 域
– 多项式环
– 椭圆曲线

- 教材：《信息安全数学基础》陈恭亮著

- 参考书目：

《近世代数引论》（第二版），冯克勤、章璞著
《离散数学》，董晓蕾、曹珍富著

- 教材：《信息安全数学基础》陈恭亮著

- 参考书目：

《近世代数引论》（第二版），冯克勤、章璞著

《离散数学》，董晓蕾、曹珍富著

- 考核方式

平时成绩50%，期末考试50%

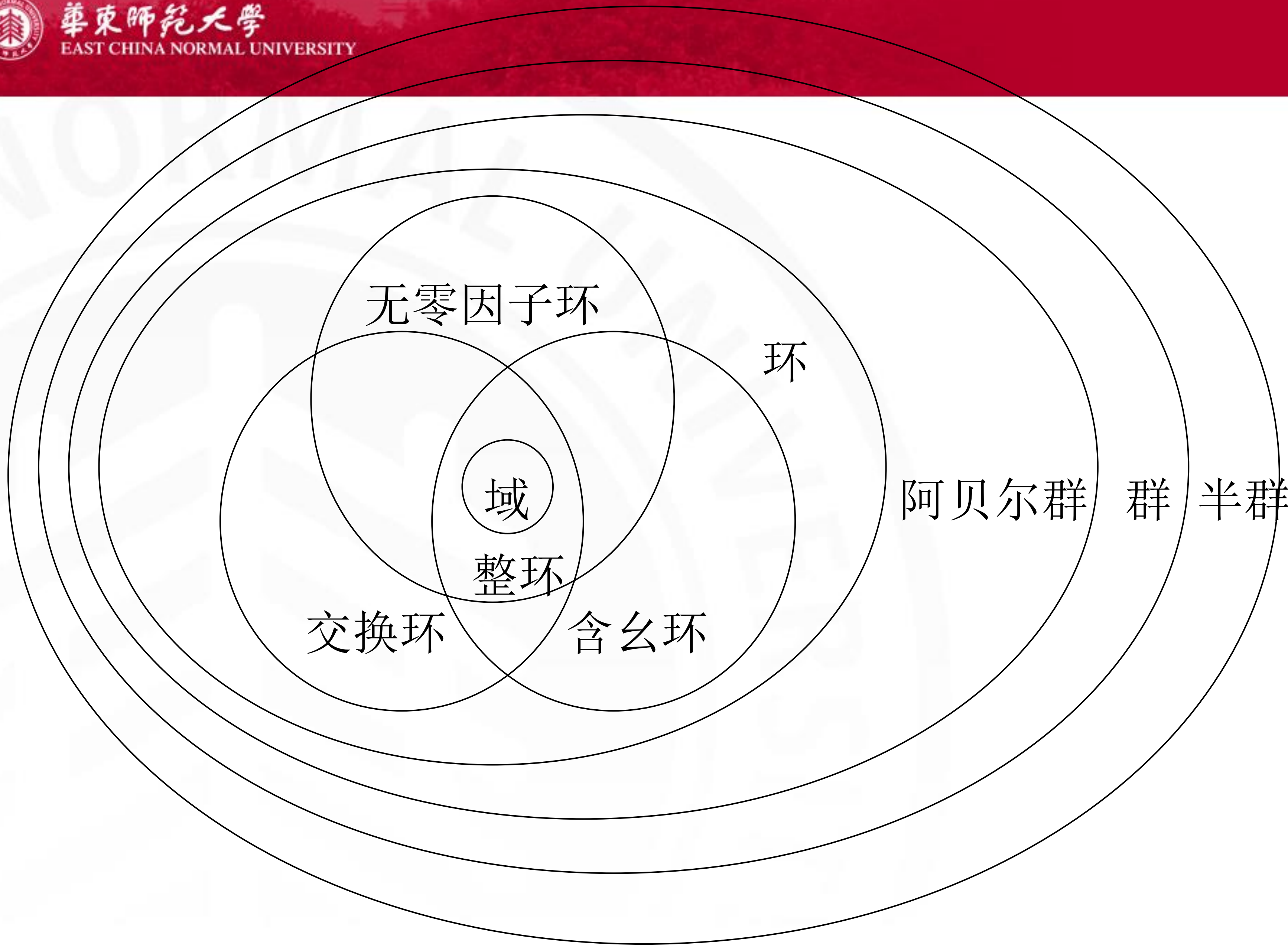
网络安全数学基础

第六章 群

- 整数集合Z是一个带加法、减法、乘法、除法的集合，但它仅对加法、减法和乘法封闭。

- n阶方阵集合$\{A_n\}$是一个带加法和乘法的集合，且对加法和乘法都封闭。

- 近世代数（抽象代数）的研究对象为代数集合，即带运算的非空集合。


无零因子环
环
域
阿贝尔群
群
半群
整环
交换环
含幺环

§6.1 半群

- 定义6.1.1 若干个（有限或无限）事物的全体称为**集合**；这些事物称为这个集合的**元素**。

§6.1 半群

- 定义6.1.1 若干个（有限或无限）事物的全体称为**集合**；这些事物称为这个集合的**元素**。

- 例 $Z=\{0,\pm 1,\pm 2,\dots\}$是全体整数的集合

§6.1 半群

- 定义6.1.1 若干个（有限或无限）事物的全体称为**集合**；这些事物称为这个集合的**元素**。

- 例 $Z = \{0, \pm 1, \pm 2, \ldots\}$是全体整数的集合

- 例 $\phi = \{\}$是一个不包含任何元素的集合，称为空集。

- 定义6.1.2 设A, B是两个非空集合，如果存在一个法则f，对任意$a \in A$，都存在B中唯一元素b与之对应，那么f称为集合A到B的**映射**或**函数**，记作$f: A \to B$，A称为f的定义域，B称为f的值域，b称为a的像，a称为b的原像。

- 定义6.1.2 设A, B是两个非空集合，如果存在一个法则f，对任意$a \in A$，都存在B中唯一元素b与之对应，那么f称为集合A到B的**映射**或**函数**，记作$f: A \to B$，A称为f的定义域，B称为f的值域，b称为a的像，a称为b的原像。

- 例 函数$f(x) = 2x$是一个从整数集Z到实数集R的映射。

- 定义6.1.2 设A, B是两个非空集合，如果存在一个法则f，对任意$a \in A$，都存在B中唯一元素b与之对应，那么f称为集合A到B的**映射**或**函数**，记作$f: A \rightarrow B$，A称为f的定义域，B称为f的值域，b称为a的像，a称为b的原像。

- 例 函数$f(x) = 2x$是一个从整数集Z到实数集R的映射。

- 注意：上例中f同时也是从整数集Z到有理数集Q的映射，也是从整数集Z到偶数集$2Z$的映射。因为值域不一定等于像集$f(A) = \{f(a) | a \in A\}$。

- 定义6.1.3 设f是集合A到B的映射，则f是集合A到B的单射，如果对任意$a_1, a_2 \in A$， $a_1 \neq a_2$，都有$f(a_1) \neq f(a_2)$。

- 定义6.1.3 设f是集合A到B的映射，则f是集合A到B的单射，如果对任意$a_1, a_2 \in A$， $a_1 \neq a_2$，都有$f(a_1) \neq f(a_2)$。
- 定义6.1.4 设f是集合A到B的映射，则f是集合A到B的满射，如果对任意 $b \in B$，都存在$a \in A$，使得$f(a) = b$。

- 定义6.1.3 设f是集合A到B的映射，则f是集合A到B的单射，如果对任意$a_1, a_2 \in A$， $a_1 \neq a_2$，都有$f(a_1) \neq f(a_2)$。

- 定义6.1.4 设f是集合A到B的映射，则f是集合A到B的满射，如果对任意 $b \in B$，都存在$a \in A$，使得$f(a) = b$。

- 定义6.1.5 映射f称为双射，如果它既是单射又是满射。

- 例 上例中f是从Z到R的单射，也是从Z到$2Z$的双射。

- 定义6.1.6 设$A_1, A_2, \dots, A_n$是n个集合，则集合$A = \{(a_1, a_2, \dots, a_n) | a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}$称为$A_1, A_2, \dots, A_n$的笛卡尔积，记作$A_1 \times A_2 \times \cdots \times A_n$。

- 定义6.1.6 设$A_1, A_2, \ldots, A_n$是n个集合，则集合$A = \{(a_1, a_2, \ldots, a_n) | a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}$称为$A_1, A_2, \ldots, A_n$的笛卡尔积，记作$A_1 \times A_2 \times \cdots \times A_n$。

- 例 复数C可以看作R上的二元组，即$R \times R$，因为存在$R \times R$到C的双射$f(a, b) = a + bi$。

- 定义6.1.7 如果S是一个非空集合，那么$S \times S$到S的映射叫做S上的**结合法**或**运算**。一般我们将这个运算称为乘法，记作$a \cdot b$或ab。而$(S,\cdot)$称为一个**带运算的集合**或**代数结构**。

- 定义6.1.7 如果S是一个非空集合，那么$S \times S$到S的映射叫做S上的**结合法**或**运算**。一般我们将这个运算称为乘法，记作$a \cdot b$或ab。而$(S,\cdot)$称为一个**带运算的集合**或**代数结构**。

- 注意：运算$\cdot$在S上是封闭的，即任意$a, b \in S$，都有$a \cdot b \in S$。

- 定义6.1.7 如果S是一个非空集合，那么$S\times S$到S的映射叫做S上的**结合法**或**运算**。一般我们将这个运算称为乘法，记作$a\cdot b$或ab。而$(S,\cdot)$称为一个**带运算的集合**或**代数结构**。
- 注意：运算·在S上是封闭的，即任意$a,b\in S$，都有$a\cdot b\in S$。
- 例 算数加法是整数集Z上的运算，因为它是$S\times S$到S的映射，我们仍然称其为乘法。

- 定义6.1.8 设$(S,\cdot)$是一个代数结构，那么它是一个**半群**，如果运算$\cdot$在S上满足结合律，即任意$a,b,c \in S$，都有$(a \cdot b) \cdot c = a \cdot (b \cdot c)$。

- 定义6.1.8 设$(S,\cdot)$是一个代数结构，那么它是一个**半群**，如果运算$\cdot$在S上满足结合律，即任意$a, b, c \in S$，都有$(a \cdot b) \cdot c = a \cdot (b \cdot c)$。

- 例 设$S = \{a, b, c\}$，S上的运算$\cdot$如下表所示，那么$(S,\cdot)$是一个半群。

$\cdot$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

§6.2 群

- 定义6.2.1 设$(S,\cdot)$是一个代数结构，$e \in S$，那么e是S的**左单位元**，如果对任意$a \in S$，都有$e \cdot a = a$。

§6.2 群

- 定义6.2.1 设$(S,\cdot)$是一个代数结构，$e \in S$，那么e是S的**左单位元**，如果对任意$a \in S$，都有$e \cdot a = a$。

- 定义6.2.2 设$(S,\cdot)$是一个代数结构，$e \in S$，那么e是S的**右单位元**，如果对任意$a \in S$，都有$a \cdot e = a$。

§6.2 群

- 定义6.2.1 设$(S,\cdot)$是一个代数结构，$e \in S$，那么e是S的**左单位元**，如果对任意$a \in S$，都有$e \cdot a = a$。

- 定义6.2.2 设$(S,\cdot)$是一个代数结构，$e \in S$，那么e是S的**右单位元**，如果对任意$a \in S$，都有$a \cdot e = a$。

- 定义6.2.3 设 $(S,\cdot)$ 是一个代数结构，称 $e \in S$ 是它的**单位元**，如果e既是S的左单位元，又是S的右单位元。

- 例 设$S = Z \times Z$，对任意$(a_1, b_1), (a_2, b_2) \in S$，定义$(a_1, b_1) \cdot (a_2, b_2) = (a_1 + a_2, b_2)$，则$(0, b)$都是$(S, \cdot)$的左单位元，其中$b \in Z$。

- 定理6.2.1 设$(S,\cdot)$是一个代数结构，如果它既有左单位元又有右单位元，那么两者相等。

- 定理6.2.1 设$(S,\cdot)$是一个代数结构，如果它既有左单位元又有右单位元，那么两者相等。

证明：设e_1是$(S,\cdot)$的左单位元， e_2是$(S,\cdot)$的右单位元，则$e_1 = e_1 e_2 = e_2$。

- 定理6.2.1 设$(S,\cdot)$是一个代数结构，如果它既有左单位元又有右单位元，那么两者相等。

证明：设e_1是$(S,\cdot)$的左单位元， e_2是$(S,\cdot)$的右单位元，则$e_1 = e_1 e_2 = e_2$。

- 推论 如果代数结构$(S,\cdot)$有单位元，则其唯一。

- 定理6.2.1 设$(S,\cdot)$是一个代数结构，如果它既有左单位元又有右单位元，那么两者相等。

证明：设e_1是$(S,\cdot)$的左单位元， e_2是$(S,\cdot)$的右单位元，则$e_1 = e_1 e_2 = e_2$。

- 推论 如果代数结构$(S,\cdot)$有单位元，则其唯一。

- 上例不可能有右单位元，因为它有多个左单位元。

- 定义6.2.4 设$(S,\cdot)$是一个代数结构，e为其单位元，$a \in S$，那么a'是a的**左逆元**，如果$a' \cdot a = e$。

- 定义6.2.4 设$(S,\cdot)$是一个代数结构，e为其单位元，$a \in S$，那么a'是a的**左逆元**，如果$a' \cdot a = e$。

- 定义6.2.5 设$(S,\cdot)$是一个代数结构，e为其单位元，$a \in S$，那么a'是a的**右逆元**，如果$a \cdot a' = e$。

- 定义6.2.4 设$(S,\cdot)$是一个代数结构，e为其单位元，$a \in S$，那么a'是a的**左逆元**，如果$a' \cdot a = e$。

- 定义6.2.5 设$(S,\cdot)$是一个代数结构，e为其单位元，$a \in S$，那么a'是a的**右逆元**，如果$a \cdot a' = e$。

- 定义6.2.6 设$(S,\cdot)$是一个代数结构，e为其单位元，$a \in S$，那么a'是a的**逆元或逆**（记作a^{-1}），如果a'既是a的左逆元，又是a的右逆元。

- 定理6.2.2 设$(S,\cdot)$是一个半群，e为其单位元，$a \in S$，如果a既有左逆元又有右逆元，那么两者相等。

- 定理6.2.2 设$(S,\cdot)$是一个半群，e为其单位元，$a \in S$，如果a既有左逆元又有右逆元，那么两者相等。

证明：设a'是a的左逆元，a''是a的右逆元，则$a' = a'e = a'aa'' = ea'' = a''$。

- 定理6.2.2 设$(S,\cdot)$是一个半群，e为其单位元，$a \in S$，如果a既有左逆元又有右逆元，那么两者相等。

证明：设a'是a的左逆元，a''是a的右逆元，则$a' = a'e = a'aa'' = ea'' = a''$。

- 推论 如果a有逆，则其唯一。

- 定义6.2.7 称半群$(S,\cdot)$是一个**群**，如果它有单位元，且对任意$a \in A$，都存在它的逆$a^{-1} \in S$。一般用$(G,\cdot)$或G表示一个群，它的元素个数称为它的阶，记为$|G|$。

- 定义6.2.7 称半群$(S,\cdot)$是一个**群**，如果它有单位元，且对任意$a \in A$，都存在它的逆$a^{-1} \in S$。一般用$(G,\cdot)$或G表示一个群，它的元素个数称为它的阶，记为$|G|$。

- 如果$(G,\cdot)$是一个群，那么G关于$\cdot$满足

  (i) 封闭性

  (ii) 结合律

  (iii) 含单位元

  (iv) 所有元素都可逆（可逆性）

- 定义6.2.8 称群$(G,\cdot)$是一个**交换群**或**Abel群**，如果它满足交换律，即对任意$a,b \in G$，都有$a \cdot b = b \cdot a$。

- 定义6.2.8 称群$(G,\cdot)$是一个**交换群**或**Abel群**，如果它满足交换律，即对任意$a, b \in G$，都有$a \cdot b = b \cdot a$。

- 例 设$G = \{e\}$，G上乘法·定义为：$e \cdot e = e$，则$(G,\cdot)$是一个群且是一个交换群。

- 例 整数集Z关于加法，即$(Z,+)$是一个群，也是一个交换群，因为整数集 Z 关于加法满足封闭性、结合律、交换律、含单位元0，且对每个整数a，都存在它的逆$-a \in Z$。

- 例 整数集Z关于加法，即$(Z,+)$是一个群，也是一个交换群，因为整数集 Z 关于加法满足封闭性、结合律、交换律、含单位元0，且对每个整数a，都存在它的逆$-a\in Z$。

- 例 但是整数集Z关于乘法，即$(Z,\times)$不是一个群，它只是一个半群（含幺半群），因为整数集 Z 关于乘法满足封闭性、结合律、含单位元1，但除了 ± 1 之外，所有元素都不可逆。

- 例 令$Z/nZ=\{0,1,2,\dots,n-1\}$，定义Z/nZ上运算$\oplus$：$a\oplus b=a+b\ (mod\ n)$，则$(Z/nZ,\oplus)$构成一个群。

- 例 令$Z/nZ=\{0,1,2,\dots,n-1\}$，定义Z/nZ上运算$\oplus$：$a\oplus b=a+b\ (mod\ n)$，则$(Z/nZ,\oplus)$构成一个群。

- 例 定义$Z/nZ\backslash\{0\}$上运算$\otimes$：$a\otimes b=ab\ (mod\ n)$，其中$n>1$，则当n为素数时，$(Z/nZ\backslash\{0\},\otimes)$构成一个群。

$$(Z/7Z\backslash\{0\},\otimes)$$

$\otimes$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

- 上例中，如果n为合数，则$(Z/nZ\backslash\{0\},\otimes)$构成一个半群（含幺半群），但不构成群。

- 上例中，如果n为合数，则$(Z/nZ\backslash\{0\},\otimes)$构成一个半群（含幺半群），但不构成群。

证明：这里只证明$(Z/nZ\backslash\{0\},\otimes)$不是群。因为$n$是合数，所以存在整数$n_1,n_2, 1<n_1,n_2<n$，使得$n_1 n_2=n$。显然$n_1\in Z/nZ\backslash\{0\}$，且$n_1\otimes n_2=0$，则$n_1$关于$\otimes$不可逆，否则设$a$为它的逆，在证明$(Z/nZ\backslash\{0\},\otimes)$是含幺半群的过程中，我们可知1是$(Z/nZ\backslash\{0\},\otimes)$的单位元，因此$a\otimes n_1=1$，两边同时右乘$n_2$可得$0=a\otimes 0=a\otimes n_1\otimes n_2=1\otimes n_2=n_2$，因此$n_1$关于$\otimes$不可逆，故$(Z/nZ\backslash\{0\},\otimes)$不是群。

- 上例中，如果n为合数，则$(Z/nZ\backslash\{0\},\otimes)$构成一个~~半~~群（含幺半群），但不构成群。

证明：因为n是合数，所以存在整数$n_1,n_2, 1<n_1,n_2<n$，使得$n_1n_2=n$。显然$n_1,n_2\in Z/nZ\backslash\{0\}$，且$n_1\otimes n_2=0$，即$Z/nZ\backslash\{0\}$关于$\otimes$不封闭，因此不是半群（不是代数结构）。

$$(Z/6Z\backslash\{0\},\otimes)$$

$\otimes$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

- 但是，若令Z/nZ^*表示Z/nZ中所有与n互素的数，即$Z/nZ^* = \{x \in Z/nZ \mid (x,n) = 1\}$，则$(Z/nZ^*, \otimes)$构成群。

- 但是，若令Z/nZ^*表示Z/nZ中所有与n互素的数，即$Z/nZ^* = \{x \in Z/nZ \,|(x,n) = 1\}$，则$(Z/nZ^*, \otimes)$构成群。

$$(Z/6Z^*, \otimes)$$

$\otimes$	1	5
1	1	5
5	5	1

证明：(i) 封闭性：对任意$a, b \in Z/nZ^*$，有$(a, n) = (b, n) = 1$，因此$c = a \otimes b = ab \ (mod \ n)$也与$n$互素，否则$(c, n) > 1$，则存在素数$p|(c, n)$，故$p|(ab, n)$，因此$p|ab$，因为$p$为素数，所以有$p|a$或$p|b$，所以$p|(a, n)$或$p|(b, n)$，与假设矛盾。此时有$c \in Z/nZ^*$。

证明：(i) 封闭性：对任意$a, b \in Z/nZ^*$，有$(a,n) = (b,n) = 1$，因此$c = a \otimes b = ab \ (mod\ n)$也与$n$互素，否则$(c,n) > 1$，则存在素数$p|(c,n)$，故$p|(ab,n)$，因此$p|ab$，因为$p$为素数，所以有$p|a$或$p|b$，所以$p|(a,n)$或$p|(b,n)$，与假设矛盾。此时有$c \in Z/nZ^*$。

(ii) 结合律显然成立。

证明：(i) 封闭性：对任意$a, b \in Z/nZ^*$，有$(a, n) = (b, n) = 1$，因此$c = a \otimes b = ab \ (mod\ n)$也与$n$互素，否则$(c, n) > 1$，则存在素数$p|(c, n)$，故$p|(ab, n)$，因此$p|ab$，因为$p$为素数，所以有$p|a$或$p|b$，所以$p|(a, n)$或$p|(b, n)$，与假设矛盾。此时有$c \in Z/nZ^*$。

(ii) 结合律显然成立。

(iii) 单位元：1显然是Z/nZ^*的单位元，且易知$(1, n) = 1$，即$1 \in Z/nZ^*$。

证明：(i) 封闭性：对任意$a, b \in Z/nZ^*$，有$(a, n) = (b, n) = 1$，因此$c = a \otimes b = ab \ (mod\ n)$也与$n$互素，否则$(c, n) > 1$，则存在素数$p|(c, n)$，故$p|(ab, n)$，因此$p|ab$，因为$p$为素数，所以有$p|a$或$p|b$，所以$p|(a, n)$或$p|(b, n)$，与假设矛盾。此时有$c \in Z/nZ^*$。

(ii) 结合律显然成立。

(iii) 单位元：1显然是Z/nZ^*的单位元，且易知$(1, n) = 1$，即$1 \in Z/nZ^*$。

(iv) 可逆性：对任意$a \in Z/nZ^*$，有$(a, n) = 1$，由广义欧几里德除法可知存在$s', t' \in Z$，使得$s'a + t'n = 1$，令$s = s' \ (mod\ n)$，则存在整数k，使得$s = s' + kn$，因此$sa = s'a + kna = 1 - t'n + kna \equiv 1 \ (mod\ n)$，且显然$(s, n) = 1$，即存在$a$的逆$s \in Z/nZ^*$，得证。

- 例 令$GL_n(\boldsymbol{K})$表示域$\boldsymbol{K}$上全体n阶可逆方阵的集合，则$GL_n(\boldsymbol{K})$关于矩阵乘法构成一个群，称为一般线性群。

- 例 令$GL_n(\boldsymbol{K})$表示域$\boldsymbol{K}$上全体n阶可逆方阵的集合，则$GL_n(\boldsymbol{K})$关于矩阵乘法构成一个群，称为一般线性群。

- 例 令$SL_n(\boldsymbol{K})$表示域$\boldsymbol{K}$上全体n阶行列式为1的方阵的集合，则显然$SL_n(\boldsymbol{K}) \subseteq GL_n(\boldsymbol{K})$，且$SL_n(\boldsymbol{K})$关于矩阵乘法也构成一个群，称为特殊线性群。

- 对群$(G,\cdot)$中三个元素a,b,c，因为$(a\cdot b)\cdot c=a\cdot(b\cdot c)$，定义$a\cdot b\cdot c=(a\cdot b)\cdot c=a\cdot(b\cdot c)$

- 对群$(G,\cdot)$中三个元素a,b,c，因为$(a\cdot b)\cdot c=a\cdot(b\cdot c)$，定义$a\cdot b\cdot c=(a\cdot b)\cdot c=a\cdot(b\cdot c)$

- 设$(G,\cdot)$是一个群，$a_1,a_2,\dots,a_n\in G,n\geq 3$，由结合律易证$(a_1\cdot a_2\cdot\cdots\cdot a_{n-1})\cdot a_n=a_1\cdot(a_2\cdot\cdots\cdot a_{n-1}\cdot a_n)$，定义$a_1\cdot a_2\cdot\cdots\cdot a_{n-1}\cdot a_n=(a_1\cdot a_2\cdot\cdots\cdot a_{n-1})\cdot a_n$。

- 定理6.2.3 设$(G,\cdot)$是一个群，对任意$a,b \in G$，都有$(ab)^{-1} = b^{-1}a^{-1}$。

- 定理6.2.3 设$(G,\cdot)$是一个群，对任意$a,b\in G$，都有$(ab)^{-1}=b^{-1}a^{-1}$。

证明：因为$b^{-1}a^{-1}ab=b^{-1}eb=b^{-1}b=e$，且$abb^{-1}a^{-1}=aea^{-1}=aa^{-1}=e$，因此$b^{-1}a^{-1}$是$ab$的逆元，定理得证。

- 定理6.2.3 设$(G,\cdot)$是一个群，对任意$a,b \in G$，都有$(ab)^{-1} = b^{-1}a^{-1}$。

证明：因为$b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e$，且$abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$，因此$b^{-1}a^{-1}$是$ab$的逆元，定理得证。

- 类似的，对任意$a_1, a_2, \dots, a_n \in G$，有$(a_1a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1}a_1^{-1}$。

- 定义6.2.9 设$(G,\cdot)$是一个群，e为其单位元，$a \in G, n \in Z^+$，定义

  $(i)\ a^0 = e$；

  $(ii)\ a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n\text{个}}$；

  $(iii)\ a^{-n} = (a^n)^{-1}$。

- 定理6.2.4 设$(G,\cdot)$是一个群，$a \in G, m, n \in Z$，则有
  $(i)\ a^{-n} = (a^{-1})^n$；
  $(ii)\ a^m a^n = a^{m+n}$；
  $(iii)\ (a^m)^n = a^{mn}$。

- 定义6.2.10 设$(G,\cdot)$是一个群，$H \subseteq G$，如果H关于运算$\cdot$也构成群，那么称$(H,\cdot)$是$(G,\cdot)$的**子群**，或H是G的子群，记作$H \leq G$。

- 定义6.2.10 设$(G,\cdot)$是一个群，$H \subseteq G$，如果H关于运算$\cdot$也构成群，那么称$(H,\cdot)$是$(G,\cdot)$的**子群**，或H是G的子群，记作$H \leq G$。

- 例 我们知道$(Z,+)$是一个群，全体偶数集合$2Z$关于运算$+$也构成群，因此$2Z$是Z的子群。

- 定理 6.2.5 设H是群G的子群，那么G的单位元e必定也是H的单位元。

- 定理 6.2.5 设H是群G的子群，那么G的单位元e必定也是H的单位元。

证明：设e'为H的单位元，$a \in H \subseteq G$，则对任意$b \in G$，有$e'b = e'eb = e'aa^{-1}b = aa^{-1}b = eb = b$以及$be' = bee' = ba^{-1}ae' = ba^{-1}a = be = b$，因此$e'$也是$G$的单位元，由单位元唯一性可知$e' = e$，得证。

- 给定群G，显然$\{e\}$和G都是G的子群，我们称这样的群为**平凡子群**，其它的群称为**真子群**。

- 给定群G，显然$\{e\}$和G都是G的子群，我们称这样的群为**平凡子群**，其它的群称为**真子群**。

- 例 已知全体整数集合Z关于加法构成一个群，那么$\{0\}$和Z是它的平凡子群，而全体偶数集合$2Z$是它的真子群。

- 定理6.2.6 设$(G,\cdot)$是一个群，H是G的非空子集，那么H是G的子群，当且仅当对任意$a,b \in H$，都有$ab^{-1} \in H$。

- 定理6.2.6 设$(G,\cdot)$是一个群，H是G的非空子集，那么H是G的子群，当且仅当对任意$a,b \in H$，都有$ab^{-1} \in H$。

证明：必要性显然，下面证充分性

(i) 结合律显然成立。

- 定理6.2.6 设$(G,\cdot)$是一个群，H是G的非空子集，那么H是G的子群，当且仅当对任意$a, b \in H$，都有$ab^{-1} \in H$。

证明：必要性显然，下面证充分性

(i) 结合律显然成立。

(ii) 单位元：因为H非空，任取$a \in H$，令$b = a$，则有$e = aa^{-1} \in H$，其中e是群G的单位元。

- 定理6.2.6 设$(G,\cdot)$是一个群，H是G的非空子集，那么H是G的子群，当且仅当对任意$a,b\in H$，都有$ab^{-1}\in H$。

证明：必要性显然，下面证充分性

(i) 结合律显然成立。

(ii) 单位元：因为H非空，任取$a\in H$，令$b=a$，则有$e=aa^{-1}\in H$，其中e是群G的单位元。

(iii) 可逆性：对任意$b\in H$，因为$e\in H$，所以$b^{-1}=eb^{-1}\in H$。

- 定理6.2.6 设$(G,\cdot)$是一个群，H是G的非空子集，那么H是G的子群，当且仅当对任意$a,b \in H$，都有$ab^{-1} \in H$。

证明：必要性显然，下面证充分性

(i) 结合律显然成立。

(ii) 单位元：因为H非空，任取$a \in H$，令$b = a$，则有$e = aa^{-1} \in H$，其中e是群G的单位元。

(iii) 可逆性：对任意$b \in H$，因为$e \in H$，所以$b^{-1} = eb^{-1} \in H$。

(iv) 封闭性：对任意$a,b \in H$，则有$b^{-1} \in H$，因此$ab = a(b^{-1})^{-1} \in H$，得证。

- 例 已知全体整数集合Z关于加法构成一个群，全体偶数集合$2Z$是它的真子群。

§6.3 同态和同构

§6.3 同态和同构

- 定义6.3.1 设$(H,\cdot)$和$(G,\otimes)$是两个群，如果映射$f: H \rightarrow G$，满足对任意$a, b \in H$，都有$f(a) \otimes f(b) = f(a \cdot b)$，那么称$f$是$H$到$G$的一个**同态映射**或**同态**；

§6.3 同态和同构

- 定义6.3.1 设$(H,\cdot)$和$(G,\otimes)$是两个群，如果映射$f: H \to G$，满足对任意$a, b \in H$，都有$f(a)\otimes f(b) = f(a \cdot b)$，那么称$f$是$H$到$G$的一个**同态映射**或**同态**；
- 如果f是单射，那么称f是H到G的一个**单同态**；

§6.3 同态和同构

- 定义6.3.1 设$(H,\cdot)$和$(G,\otimes)$是两个群，如果映射$f: H \to G$，满足对任意$a,b \in H$，都有$f(a)\otimes f(b) = f(a \cdot b)$，那么称$f$是$H$到$G$的一个**同态映射**或**同态**；
- 如果f是单射，那么称f是H到G的一个**单同态**；
- 如果f是满射，那么称f是H到G的一个**满同态**；

§6.3 同态和同构

- 定义6.3.1 设$(H,\cdot)$和$(G,\otimes)$是两个群，如果映射$f: H \to G$，满足对任意$a,b \in H$，都有$f(a)\otimes f(b) = f(a \cdot b)$，那么称$f$是$H$到$G$的一个**同态映射**或**同态**；
- 如果f是单射，那么称f是H到G的一个**单同态**；
- 如果f是满射，那么称f是H到G的一个**满同态**；
- 如果f是一一映射，那么称f是H到G的一个**同构**。

§6.3 同态和同构

- 定义6.3.1 设$(H,\cdot)$和$(G,\otimes)$是两个群，如果映射$f\colon H\rightarrow G$，满足对任意$a,b\in H$，都有$f(a)\otimes f(b)=f(a\cdot b)$，那么称$f$是$H$到$G$的一个**同态映射**或**同态**；
- 如果f是单射，那么称f是H到G的一个**单同态**；
- 如果f是满射，那么称f是H到G的一个**满同态**；
- 如果f是一一映射，那么称f是H到G的一个**同构**。
- 如果$H=G$，那么称f是**自同态**或**自同构**。

- 定义6.3.2 设H和G是两个群，则

  称H和G是**同态**的，如果存在H到G的同态映射，记作$H \approx G$；

  称H和G是**同构**的，如果存在H到G的同构映射，记作$H \cong G$。

- 例 给定群 G，则恒等映射是群 G 上的自同态，也是自同构。

- 例 给定群 G ，则恒等映射是群 G 上的自同态，也是自同构。

- 例 设H和G是两个群，e是群G的单位元，定义映射

$$\begin{aligned} f: \quad H &\rightarrow G \\ a &\mapsto e \end{aligned}$$

则对任意$a, b \in H$，都有$f(ab) = e = ee = f(a)f(b)$，因此$f$是一个$H$到$G$的同态映射，$H$和$G$同态。

- 例 设$R[x]$表示所有系数为实数的多项式集合，则$R[x]$关于多项式加法构成一个群。定义映射

$$\begin{array}{cccc} \phi: & R[x] & \rightarrow & R[x] \\ & f & \mapsto & f' \end{array}$$

其中f'为f的导函数，则对任意$f, g \in R[x]$，都有$\phi(f+g) = (f+g)' = f' + g' = \phi(f) + \phi(g)$，因此$\phi$是一个$R[x]$到$R[x]$的同态映射，它是一个自同态，而且任意实系数多项式都可积，因此它是一个满同态，又因为显然f和$f+c$的导函数都是f'，其中$c \in R$，因此它不是单同态。

- 定理6.3.1 设H和G是两个群，f是一个H到G的同态映射，e是群G的单位元，e'是群H的单位元，令$\ker(f) = \{a \in H | f(a) = e\}$称为$f$的核，$\operatorname{im}(f) = f(H) = \{a \in G | \exists b \in H, f(b) = a\}$称为$f$的象集，则

  (i) $e' \in \ker(f)$，即$f(e') = e$；

  (ii) 对任意$a \in H$，都有$f(a)^{-1} = f(a^{-1})$；

  (iii) $\ker(f)$是H的子群，且f是单同态的充要条件是$\ker(f) = \{e'\}$；

  (iv) $f(H)$是G的子群，且f是满同态的充要条件是$f(H) = G$。

证明：(i) 对任意$a \in H$，由同态性质可知$f(a) = f(ae') = f(a)f(e')$以及$f(a) = f(e'a) = f(e')f(a)$，因此$f(e')$是群$G$的单位元，又由单位元唯一性可得$f(e') = e$。

证明：(i) 对任意$a \in H$，由同态性质可知$f(a) = f(ae') = f(a)f(e')$以及$f(a) = f(e'a) = f(e')f(a)$，因此$f(e')$~~是群~~$G$的单位元，又由单位元唯一性可得$f(e') = e$。

证明：(i) 因为H是群，所以$H \neq \emptyset$，因此$f(H) \neq \emptyset$，任取$b \in f(H)$，则存在$b' \in H$，使得$b = f(b')$，此时对任意$a \in G$，有$a = bb^{-1}a$，由同态性质可知$f(e')a = f(e')bb^{-1}a = f(e')f(b')b^{-1}a = f(e'b')b^{-1}a = f(b')b^{-1}a = bb^{-1}a = a$，类似可得$af(e') = a$，因此$f(e')$是群$G$的单位元，又由单位元唯一性可得$f(e') = e$。

(ii) 对任意$a \in H$，由同态性质及(i)可知$e = f(e') = f(aa^{-1}) = f(a)f(a^{-1})$以及$e = f(e') = f(a^{-1}a) = f(a^{-1})f(a)$，再由逆元唯一性可得$f(a)^{-1} = f(a^{-1})$。

(iii) 先证$\ker(f)$是H的子群，由(i)可知$\ker(f)$是H的非空子集，则由定理6.1.6，只需证明对任意$a, b \in \ker(f)$，都有$ab^{-1} \in \ker(f)$。事实上$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = ee^{-1} = e$，因此$ab^{-1} \in \ker(f)$。

華東師範大學
EAST CHINA NORMAL UNIVERSITY

(iii) 先证$\ker(f)$是H的子群，由定义可知$\ker(f)$是H的非空子集，则由定理6.1.6，只需证明对任意$a,b\in\ker(f)$，都有$ab^{-1}\in\ker(f)$。事实上$f(ab^{-1})=f(a)f(b^{-1})=f(a)f(b)^{-1}$
$=ee^{-1}=e$，因此$ab^{-1}\in\ker(f)$。

再证f是单同态的充要条件是$\ker(f)=\{e'\}$。必要性显然，事实上由(i)可知$f(e')=e$，再由f是单射可知仅有e'的象为e，即$\ker(f)=\{e'\}$。再证充分性，假设$a,b\in H$，且$f(a)=f(b)$，则$f(ab^{-1})=f(a)f(b)^{-1}=f(a)f(a)^{-1}=e$，所以$ab^{-1}\in\ker(f)=\{e'\}$，因此$a=b$，即$f$是单射。

(iv) f是满同态的充要条件是$f(H)=G$是显然的。下面证明$f(H)$是G的子群，显然$f(H)$是G的非空子集，由定理6.1.6，只需证明对任意$a,b\in f(H)$，都有$ab^{-1}\in f(H)$，由$a,b\in f(H)$可知存在$a',b'\in H$，使得$f(a')=a,f(b')=b$，则$ab^{-1}=f(a')f(b')^{-1}=f(a')f\left(b'^{-1}\right)=f(a'b'^{-1})\in f(H)$，得证。

- 例 前例中，H和G是两个群，e是群G的单位元，定义映射

$$\begin{aligned} f:\quad H &\to G \\ a &\mapsto e \end{aligned}$$

则f是一个H到G的同态映射，其中$\ker(f) = H \leq H$，$f(H) = \{e\} \leq G$。显然当$|H| \neq 1$时，f不是单同态；当$|G| \neq 1$时，f不是满同态。

- 例 前例中，$R[x]$关于多项式加法构成一个群，定义映射

$$\begin{array}{cccc} \phi: & R[x] & \rightarrow & R[x] \\ & f & \mapsto & f' \end{array}$$

其中f'为f的导函数，则ϕ是一个$R[x]$到$R[x]$的同态映射，它是一个自同态，且是一个满同态，即$\phi(R[x]) = R[x]$，而$\ker(\phi) = \{f(x) \in R[x] | f'(x) = 0\} = \{f(x) = c | c \in R\} = R \leq R[x]$，$\phi$不是单同态。