群的概念

- 定义 设G是一个非空集合，“*”是G是上的一个代数运算，即

  对所有的a，b∈G，有a*b∈G.

  如果G的运算还满足：

  (G1)结合律:即对所有的a，b，c∈G，有

  $$(a*b)*c=a*(b*c)$$

  (G2) G中存在元素e，使得对每个a∈G，有

  $$e*a=a*e=a$$

  (G3) 对G中每个元素a，存在元素b∈G，使得

  $$a*b=b*a=e.$$

则称G关于运算“*”构成一个群(group)，记为(G，*).

- 注1：(G2)中的元素e 称为群G的单位元(unit element)或恒等元(identity). 群G的单位元是唯一的.

- 注2：(G3)中的元素b称为元素a的逆元(inverse). 元素a的逆元是唯一的,记为a^{-1}. 即有$a*a^{-1}=a^{-1}*a=e$

有限群

- 交换群

  如果群G的运算还满足:

  (G4)交换律:即对所有的a, b∈G, 有a*b=b*a.

  则称G是一个交换群(commutative group),或阿贝尔群(abelian group).

- G中元素的个数称为群G的阶(order), 记为|G|. 如果|G|是有限数,则称G是有限群(finite group), 否则称G是无限群(infinite group).
- 例: 整数加群(Z, +); 有理数加群(Q, +); 实数加群(R, +); 数加群(C, +).
- 令$Q^*=Q-\{0\}$, $(Q^*, \times)$是群; $Q_+=\{q\in Q \mid q>0\}$, $(Q_+, \times)$是群.

- 群的概念

例1 设G={1, −1, i, −i}, 则(G, ×) 是一个有
换
群

元素a	1	-1	i	−i
逆元a^{-1}	1	-1	−i	i

- 例2 设$m \in Z_+$， $Z_m=\{0, 1, \cdots, m-1\}$，则$(Z_m，\oplus)$
  一个有限交换群．称为模m剩余类加群.

✓ 单位元是e=0； $a \in Z_m$ 的逆元$a^{-1}= m-a$.

✓ 特别地：取m=5，有$Z_5=\{0, 1, 2, 3, 4\}$，

元素a	0	1	2	3	4
逆元a^{-1}	0	4	3	2	1

- 有时把交换群(G, ∗)记为(G, +), 称为“
  群”.

✓ 把运算“∗”称为“加” 法, 运算结果记
  :
  a∗b= a+b,称为a与b的“和”;

✓ 单位元称为“零元”, 记为
  “0”;

✓ a∈G的逆元称为G的负元, 记为: “− a”, 有a+(−a)= 0.

- 例1

  G={1, −1, i, −i}, (G, *)是一个有限交换
  可记为:(G, *)= (G, +), 运算式为:

1+(−1)=−1, 1+i=i, 1+(−i)=−i, (−1)+i=−i
(−1)+(−
i)=i, i+(−i)=1, 1+1=1

请问零元是? 利用, a+e=e+a=a

试求 (-i)+(-i), i+i, (-1)+(-1).

- 例2 加群：$(Z_5, \oplus) = (Z_5, +)$，其中$Z_5 = \{0, 1, 2, 3, 4\}$.

零元0=0, 负元为:

元素x	0	1	2	3	4
负元-x	0	4	3	2	1

- 群的概念

✓ 有时把群(G, *)记为(G, ·), 称为“ 乘群”.

✓ 把运算“*”称为“乘” 法, 运算结果记为: a*b= a·b, 称为a与b的“积”;

✓ 运算符号通常省略, 简记为: a*b=a·b=ab.

单位元记为: e=1.

- 例3 设$m\in Z_+$, $Z_m=\{0,1,\ldots, m-1\}$, 则$(Z_m, \otimes)$不是一个群.元素0无逆元!
  $0\times ?=1$ 找不到这样的元素!
- 例4 设$m\in Z_+$是素数, $Z_m^* = \{1,2,\ldots,m-1\}$, 则$(Z_m^*, \otimes)$是一个有限交换群.
  单位元: $e=1$; $a\in Z_m$的逆元a^{-1}: $a\times a^{-1}=1 \pmod m$.

特别地: 取m=5, 有Z_5*={1,2,3,4},

- $1\times1=1 \bmod 5$ 所以1的逆元素是1
- 求出其他元素的逆元素

元素a的逆元

元素a	1	2	3	4
逆元a-1	1	3	2	4

- 群的 幂

设(G, ·)是一个群，$n \in Z^{+}$, $a \in G$的n次幂为:

$a^n = a \cdot a \cdot \ldots \cdot a$ (n个a)

$a^0 = e$, $a^{-n} = (a^{-1})^n$

指数法则: 设$a,b \in G$, $n, m \in Z$, 则有

(1) $a^n \cdot a^m = a^{n+m}$;

(2) $(a^n)^m = a^{nm}$;

(3) 如果G是一个交换群，则$(a \cdot b)^n = a^n \cdot b^n$.

加群的倍数

设(G, +)是一个加群，$n\in$,Z $a\in G$的n倍为：

+

$na= a+a+\cdots+a$ (n个a)

$0a=0$，$(-n)a=n(-a)$.

倍数法则：设$a,b\in G$，n，$m\in Z$，则有

(1) $na+ma=(n+m)a$;

(2) $m(na)=(nm)a$;

(3) $n(a+b)=na+nb$.

群元素的 阶

- 设G是一个群， e是G的单位元， $a\in G$， 如果存在正整数r， 使得$a^r=e$, 则称a是有限阶的, 否则称a是无限阶的.
- 如果a是有限阶的， 则把满足$a^r=e$的最小正整数r称为a的阶(order), 记为ord a=r.
- 如果a是无限阶的， 则记ord a =∞.

计算群(Z_5^*, $\otimes$)每个元素的阶，$Z_5^*=\{1, 2, 3, 4\}$.

解：对于a=2，有

$2^1=2$，$2^2=2\otimes2=4$，$2^3=2\otimes2\otimes2=8=3$，$2^4=2\otimes2\otimes2\otimes2=16=1$.

∴ ord 2=4.

下面，**请**求出各元素的**阶**

元素a的阶如下

a	1	2	3	4
a的阶	1	4	4	2

例7 计算群(Z_6， $\oplus$)每个元素的阶，$Z_6=\{0, 1, 2, 3, 4, 5\}$

解:对于a=2，有

$1\times 2=2$， $2\times 2=2\oplus 2=4$， $3\times 2=2\oplus 2\oplus 2=6=0$.

$\therefore$ ord 2=3.

a	0	1	2	3	4	5
Ord a	1	6	3	2	3	6

- 设G是一个群，如果存在a∈G，使得

$G=\{a^1, a^2, \cdots\}=\langle a\rangle$,

则称G是一个循环群(cyclic group)，并称a是G的一个生成元(generator).

- 如果G是一个n阶循环群，则

$G=\{a^1, a^2, \cdots, a^n\}=\langle a\rangle$.

提示:**计**算**时请**从a^1开始

- 如果G是一个n阶循环群，且元素$a\in G$的阶= 群G的阶，则a是G的一个生成元.
- 例8 设$m\in Z^+$，$Z_m=\{0, 1, \cdots, m-1\}$，则$(Z_m, \oplus)$是m阶循环群. 1是一个生成元.

- 特别地：取m=6，$Z_6=\{0, 1, 2, 3, 4, 5\}$的生成元有：5.

$1\times 5=5$， $2\times 5=10=4$， $3\times 5=15=3$， $4\times 5=20=2$， $5\times 5=25=1$， $6\times 5=30=0$.

$\therefore$ $Z_6=\{0, 1, 2, 3, 4, 5\}=\{6\times 5$， 5×5， 4×5， 3×5， $1\times 5\}$.

- 注意：循环群的生成元不是唯一的！

- 循环群

定理　设p是素数，则$(Z_p^*, \otimes)$是p-1阶循环群.

- Z_p^*的生成元a称为Z的一个模p元根 (primitive root).

- 群(Z_5*, ⊗)是4阶循环群, Z_5*={1, 2, 3, 4}. 成元有：2, 3.

解 对于a=2，有

$2^1=2$， $2^2=2\otimes 2=4$， $2^3=2\otimes 2\otimes 2=8=3$，

$2^4=2\otimes 2\otimes 2\otimes 2=16=1$.

∴ Z_5*={1, 2, 3, 4}={2^4, 2^1, 2^2, 2^3}.

请验证生成元3的情形