现代密码学

第三十六讲 群的概念

信息与软件工程学院

群的定义和简单性质

定义 1 设 G 是一个具有代数运算 $\circ$ 非空集合，并且满足：

（1）结合律： $\forall a, b, c \in G$ ，有

$$(a \circ b) \circ c = a \circ (b \circ c)\ ;$$

（2）有单位元。即 G 中存在一个元素 e ： $\forall a \in G$ ，有

$$e \circ a = a \circ e = a$$

（3）有逆元。即对于任意 $a \in G$，存在一个元素 $a^{-1} \in G$，使得

$$a \circ a^{-1} = a^{-1} \circ a = e$$

称非空集合 G 关于代数运算 $\circ$ 构成一个群。

群的定义和简单性质

例

（1）全体整数Z 对于通常的加法成一个群，这个群称为整数加群，在整数加群中，单位元是0，a 的逆元是$-a$ ；同样全体有理数集合 Q ，全体实数集合R ，全体复数集合C 对加法也构成群。

（2）全体非零实数 R^* 对于通常的乘法构成一个群，全体正实数 R^+ 对于通常的乘法也构成一个群。

（3）模正整数n 的最小非负完全剩余系 Z_n ，对于模n 的加法构成一个群，这个群称为整数模n 加群，其单位元为0，a 的逆元是 $n-a$ 。

群的定义和简单性质

交换群

如果群 G 上的乘法运算还满足交换律，即对于群 G 中的任意元素 $a, b \in G$ 都有

$$ab = ba$$

则称群 G 为交换群或阿贝尔群。

群的定义和简单性质

有限群和无限群

定义 2 若群 G 中只含有有限个元素，则称群 G 为有限群；若群 G 中含有无限多个元素，则称群 G 为无限群。一个有限群 G 中的元素个数称为群的阶，记为 $|G|$ 。

例 中的（1）（2）都是无限群，而整数模 n 加群 Z_n 为有限群，且 $|Z_n| = n$ 。

群的定义和简单性质

有限群的判定

定理 1　一个有乘法的有限集合 G，若其乘法在 G 中封闭，且满足结合律和消去律，则 G 是群。

证明思路：（定理 1）对于 G 中的任意元素 $a,b\in G$，方程

$$ax=b \quad \text{和} \quad xa=b$$

在 G 中有解，则 G 是群。

证明： 假定 G 中有 n 个元素，不妨设这 n 个元素为 $a_1,a_2,\cdots,a_n$ 用 a 左乘所有的 a_i，可做成集合 $G'=\{aa_1,aa_2,\cdots,aa_n\}$

群的定义和简单性质

有限群的判定

定理.1 的证明（续）：

由于乘法在 G 上封闭，所以 $G' \subseteq G$ 。

但当 $i \neq j$ 的时候,$aa_i \neq aa_j$ 。不然的话，由消去律可知，$a_i = a_j$

与假定不合。因此 G' 有 n 个不同的元素，所以有 $G' = G$ 。这样，对于方程中的 b，必然存在某个 k ，使得 $b = aa_k$ ，也就是说方程 $ax = b$ 在 G 中有解。

同理可证，方程 $xa = b$ 在 G 中也有解。

根据定理，G 是群。

群的定义和简单性质

例 取模 m 的最小非负简化剩余系，记为 Z_m^* ，其中元素个数为 $\varphi(m)$ 个，定义其上的乘法为模 m 的乘法。显然其乘法在 Z_m^* 上封闭，且满足结合律。由扩展欧几里德算法可知，Z_m^* 中的元素均存在模 m 的乘法逆元。对于任意 $a,b,c\in Z_m^*$ ，若

$$ab\equiv ac(\mathrm{mod} m)$$

则有

$$a^{-1}ab\equiv a^{-1}ac(\mathrm{mod} m)$$

即 $b\equiv c(\mathrm{mod} m)$ 。因此，模 m 的乘法在 Z_m^* 上满足消去律。根据定理 1，Z_m^* 是群。

感 谢 聆 听!

xionghu.uestc@gmail.com