信息安全数学基础

第三章 群

陈大江

信息与软件工程学院

第三章 群

3.3 子群、陪集

定义3.3.1 如果群G的非空子集合H对于G中的运算也构成一个群，那么H称为G的子群，记为$H \leq G$。

在群G中，仅有单位元素 构成的子集合$\{e\}$和G本身显然都是G的子群。这两个子群称为G的平凡子群，其余的子群称为非平凡子群。

例3.3.1 设n是一个正整数，在整数加群Z中所有n的倍数对于加法显然构成一个群，因而是Z的子群。这个子群记为nZ。

3.3 子群、陪集

定理 3.3.1　一个群G和它的一个子群H有：

1）G 的单位元和H 的单位元是同一的；

2）如果 $a \in H$, a^{-1} 是a在G中的逆元，则$a^{-1} \in H$.

证明　对于任意$a \in H$，有$a \in G$.

1）设G 的单位元为$\boldsymbol{e}$，H 的单位元为$\boldsymbol{e}'$.

则　$\boldsymbol{ee}' = \boldsymbol{e}' = \boldsymbol{e}'\boldsymbol{e}'$. 故由消去律知：$\boldsymbol{e} = \boldsymbol{e}'$.

2）反证法．对于任意 $a \in H$ ，假设$a^{-1} \notin H$ ，则 a 在H 中存在另一逆元a'，由于 $a' \in G$ ，则a在G中存在两个逆元，得到矛盾$a^{-1} \in H$.

由于群中的运算满足结合律，因此对于$a_1, a_2, \cdots, a_n \in G$

$$a_1 a_2 \cdots a_n$$

是有意义的。

据此，可在群中定义元素的方幂。对于任意正整数n，定义

$$a^n = \overbrace{aa\cdots a}^{n\text{ 个}}$$

即n个a连乘。再约定

$$a^0 = e$$

$$a^{-n} = (a^{-1})^n$$

.

3.3 子群、陪集

容易验证

$$a^n a^m = a^{m+n}$$

$$(a^n)^m = a^{mn}$$

例3.3.2 设G是群，对于任意$a \in G$，定义

$$\langle a \rangle = \{a^i | i \in Z\}$$

则$\langle a \rangle$是G的子群。

证明思路：根据群的定义逐条验证即可。

证明：对于任意 $i, j \in Z$，有 $a^i a^j = a^{i+j}$，所以 $\langle a \rangle$ 对于 G 中的乘法封闭。

乘法结合律在 $\langle a \rangle$ 显然成立。

设 e 是群 G 中的单位元。由于 $a^0 = e$，且对于任意 $i \in Z$，有 $a^i a^0 = a^0 a^i = a^i$，所以 $\langle a \rangle$ 中存在单位元 $e = a^0$。

又任意 $a^i \in \langle a \rangle$，存在 $a^{-i} \in \langle a \rangle$,使得 $a^i a^{-i} = a^{-i} a^i = a^0$，所以 $\langle a \rangle$ 任意元素又有逆元。

根据群的定义,$\langle a \rangle$ 是 G 的子群。 □

实际上，证明 $H \subseteq G$ 是 G 的子群，并不需要逐条验证 H 满足群的定义。

子群的判定定理

定理3.3.2 群G的非空集合H是一子群的充要条件是：对于任意$a,b\in H$，有

$$ab^{-1}\in H$$

证明： 必要性显然。

充分性：H非空，则H中至少存在一个元素，设为a，因而有

$$aa^{-1}=e\in H \quad \text{单位元}$$

$$e,a\in H\Rightarrow a^{-1}=ea^{-1}\in H \quad \text{逆元}$$

$$e,b\in H\Rightarrow b^{-1}\in H\Rightarrow ab=a(b^{-1})^{-1}\in H \quad \text{封闭性}$$

3.3 子群、陪集

子群的例子

例3.3.3 找出 Z_6 关于模6加法所构成群的子群。

例3.3.4 找出 Z_7^* 关于模7乘法所构成群的子群。

3.3 子群、陪集

等价关系

定义3.3.3 设集合A上的一个二元关系~，满足下列条件：

若$a \in A$，则$a \sim a$；（自反性）

若$a, b \in A$, $a \sim b$，则$b \sim a$；（对称性）

若$a, b, c \in A$, $a \sim b$, $b \sim c$，则$a \sim c$；（传递性）

那么称~是集合A上的一个等价关系。

若~是A上的一个等价关系，$a \in A$，则与a等价的所有元素组成的一个子集合称为A中由a确定的等价类，记为$[a]$。

陪集

设G是群，H是群G的一个子群，在群G上定义关系$a\sim b$当且仅当$b^{-1}a\in H$。

对于任意$a\in G$,$a^{-1}a=e\in H$，故$a\sim a$；

若$a\sim b$，则$b^{-1}a\in H$，从而$a^{-1}b=(b^{-1}a)^{-1}\in H$，故$b\sim a$；

若$a\sim b, b\sim c$，则$b^{-1}a\in H, c^{-1}b\in H$，从而$c^{-1}a\in H$，故$a\sim c$。

因此$\sim$是G上的一个等价关系，记为R_H。

陪集（续）

定义3.3.4 设H是群G的一个子群。对于G中的任意元素a，称集合

$$\{ah \mid h \in H\}$$

为H的一个左陪集，简记为aH。因为H中有单位元素，所以$a \in aH$。同样可以定义右陪集为

$$Ha = \{ha \mid h \in H\}$$

对于任意元素$a \in G$，aH与H中有相同的元素个数。因为对于任意$h_1, h_2 \in H$，由$ah_1 = ah_2$可推导出$h_1 = h_2$。

3.3 子群、陪集

定理3.3.3 设 G 是一个群.

1）对于任意 $a \in G$，集合

$$aG = \{ah | h \in G\} = G.$$

2）$GG = \{ah | h \in G, a \in G\} = G.$

3.3 子群、陪集

证明　1）a, h 都是的G 元素，由G 的封闭性，我们有

$$ah \in G$$

则对于任意$b \in aG$，总有$b \in G$，于是$aG \subseteq G$ 。

对于任意$b \in G$，我们有

$$b = eb = (aa^{-1})b = a(a^{-1}b)$$

由于$a^{-1}b \in G$，

所以

$$b = a(a^{-1}b) \in aG$$

于是

$$G \subseteq aG$$

故$G = aG$ 。

2）

$$GG = \bigcup_{a \in G} aG = \bigcup G = G$$

陪集（续）

定理3.3.4 设H是G的子群，$a \in G$，则在等价关系R_H下，a的等价类$[a] = aH$。

证明：

$$\begin{aligned} [a] &= \{b \mid b \sim a\} \\ &= \{b \mid a^{-1}b \in H\} \\ &= \{b \mid b \in aH\} \\ &= aH \end{aligned}$$

3.3 子群、陪集

定理3.3.5 设H是群G的一个子群。H 的任意两个陪集或者相等或者无公共元素。群G可以表示成H的若干个不相交的陪集之并。

证明思路 假设H的两个陪集有公共元素从而推导出这两个陪集相等。

证明：设aH, bH是两个左陪集。假如它们由公共元素，即有$h_1, h_2 \in H$，使得

$$ah_1 = bh_2$$

于是有 $a = bh_2h_1^{-1}$，其中$h_2h_1^{-1} \in H$。

定理3.3.5的证明（续）

由 $$ah = bh_2h_1^{-1}h \in bH$$

可知$aH \subseteq bH$。同理可证，$bH \subseteq aH$，即有$aH = bH$

这就证明了第一个结论。

因为$a \in aH$，所以 $G = \bigcup_{a \in G} aH$

把其中重复出现的左陪集去掉，即可得 $G = \bigcup_{\alpha} a_\alpha H$

其中当$\alpha \neq \beta$时，有 $a_\alpha H \cap a_\beta H = \emptyset$ 。

这就证明了第二点。

3.3 子群、陪集

指数

定义3.3.5 群G关于子群H的左陪集的个数称为H在G中的**指数**，记为$[G:H]$。

推论3.3.1（**拉格朗日定理**）设群G是一个有限群，H是群G的一个子群，则H的阶$|H|$是群G的阶$|G|$的因子，而且

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

证明 设$|G| = n, |H| = m$，$[G:H] = t$。由定理3.3.3可知，G可以表示成H的不相交的左陪集之并，即

$$G = a_1 H \cup \cdots \cup a_t H$$

又因为$|a_i H| = |H| = m$，所以有$n = mt$，

即：

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

元素的阶

群G中的任意一个元素a的全体方幂构成的集合，对于群G中的乘法构成子群，这个子群称为由a生成的子群，记为

$$\langle a \rangle = \{a^i \mid i \in Z\}$$

定义3.3.6 对于群G当中的任一元素a，若存在正整数k，使得

$$a^k = e$$

那么，称满足上式的最小正整数k为元素a的阶，记为$o(a)$。等价地，a生成的子群的阶也为$o(a)$。若不存在上述的正整数k，则称a是无限阶元，记

$$o(a) = \infty$$

推论3.3.2 设G是一个有限群，则G中每一个元素的阶一定是$|G|$的因子。设$|G|=n$，对于G中的每一个元素a，有

$$a^n = e$$

推论3.3.3 （欧拉定理）设m是正整数，$\varphi(m)$为m的欧拉函数 ,$r \in Z_m$，若$\gcd(r,m)=1$，则

$$r^{\varphi(m)} \equiv 1 \pmod m$$

证明 根据例3.2.2, $r \in Z_m^*$, $|Z_m^*| = \varphi(m)$。根据推论3.3.2, 有

$$r^{\varphi(m)} \equiv 1 \pmod m$$