第七讲陪集、拉格朗日定理

陈建文

October 9, 2022

定义1. 设G为一个群，G的任意子集称为群子集。在2^G中借助于G的乘法引入一个代数运算，称为群子集的乘法：$\forall A, B \in 2^G$，

$$AB = \{ab | a \in A且b \in B\}$$

$\forall g \in G, A \in 2^G, \{g\}A$简写为$gA$，即$gA = \{ga | a \in A\}$。

定义2. 设H为群G的一个子群，$a \in G$，则集合aH称为子群H的一个左陪集，Ha称为H的一个右陪集。

定理1. 设H为群G的一个子群，则$\forall a \in G$，$aH = H$的充分必要条件是$a \in H$。

定理2. 设H为群G的一个子群，则$\forall a, b \in G$，$aH = bH$的充分必要条件是$a^{-1}b \in H$。

定理3. 设H为群G的一个子群，则$\forall a, b \in G$，$aH = bH$或者$aH \cap bH = \phi$。

定理4. 设H为群G的一个子群，则$\forall a, b \in G$，$|aH| = |bH|$。

定理5. 设H为群G的一个子群，则H的所有左陪集构成的集合为G的一个划分。

定义3. 设H为群G的一个子群，如果H的所有不同的左陪集的个数为有限数j，则称j为H在G中的指数，记为$j = [G : H]$，否则称H在G中的指数为无穷大。

定理6. 设G为一个有限群，H为G的一个子群，则$|G| = |H| \cdot [G : H]$。

推论1. 有限群中每个元素的阶都能整除该有限群的阶。

推论2. 如果群G的阶为素数，则G为一个循环群。

推论3. 设G为一个群，则$\forall a \in G$，$a^{|G|} = e$。

例. 阶小于等于5的群为交换群。

定理7. 设H为群G的一个子群，S_l为H的所有左陪集构成的集合，S_r为H的所有右陪集构成的集合，则$|S_l| = |S_r|$。

定义4. 设$a, b, n \in Z$，$n > 0$，如果$n | (a - b)$，则称a与b模n同余，记为$a \equiv b (\mod n)$。

定理8. $\forall a, b \in Z, a \equiv b(\mod n)$等价于$a \mod n = b \mod n$。

定理9. *1.* $\forall a \in Z, a \equiv a(\mod n)$;

2. $\forall a, b \in Z$，如果$a \equiv b(\mod n)$，则$b \equiv a(\mod n)$;

3. $\forall a, b, c \in Z$，如果$a \equiv b(\mod n)$并且$b \equiv c(\mod n)$，则$a \equiv c(\mod n)$;

4. $\forall a, b, k \in Z$，如果$a \equiv b(\mod n)$，则$a + k \equiv b + k(\mod n)$;

5. $\forall a, b, c, d \in Z$，如果$a \equiv b(\mod n)$并且$c \equiv d(\mod n)$，则$a + c \equiv b + d(\mod n)$;

6. $\forall a, b, k \in Z$，如果$a \equiv b(\mod n)$，则$ak \equiv bk(\mod n)$;

7. $\forall a, b, c, d \in Z$，如果$a \equiv b(\mod n)$并且$c \equiv d(\mod n)$，则$ac \equiv bd(\mod n)$

8. $\forall a, b \in Z$，$ab(\mod n) = (a \mod n)(b \mod n)(\mod n)$。

RSA算法:

（1）随机选择两个大的素数p和q;

（2）计算$n = pq$;

（3）选择数e，使得e与$(p-1)(q-1)$互素;

（4）计算数d，使得对于某个整数k，$ed = 1 + k(p-1)(q-1)$;

（5）将(e, n)作为公钥发布，保留私钥(d, n)。

设待加密的明文为M，$M < n$。

加密过程：$C = M^e \mod n$;

解密过程：$M = C^d \mod n$。

定理10. 在以上描述的RSA算法中，$(M^e \mod n)^d \mod n = M$。

证明. 由于$(M^e \mod n)^d \mod n = (M^e)^d \mod n = m^{ed} \mod n$，因此只需证$M^e d \mod n = M$。当$M$与$p$互素时，

$$
\begin{aligned}
& M^{ed} \mod p \\
=& M^{1+k(p-1)(q-1)} \mod p \\
=& M(M^{p-1})^{k(q-1)} \mod p \\
=& M(1)^{k(q-1)} \mod p \\
=& M \mod p
\end{aligned}
$$

于是$(M^{ed}) \equiv M(\mod p)$。当$p|M$时，该式显然也成立。

同理可证$(M^{ed}) \equiv M(\mod q)$，进一步可得$M^{ed} \equiv M(\mod pq)$，即$M^{ed} \equiv M(\mod n)$，从而$M^{ed} \mod n = M \mod n = M$。 □

课后作业题:

练习1. 证明：六阶群里必有一个三阶子群。

练习2. 设p为一个素数，证明：在阶为p^m的群里一定含有一个p阶子群，其中$m \geq 1$。

练习3. 在三次对称群S_3中，找一个子群H，使得H的左陪集不等于H的右陪集。

练习4. 设H为群G的一个子群，如果左陪集aH等于右陪集Ha，即$aH = Ha$，则$\forall h \in H, ah = ha$一定成立吗？