信息安全数学基础 第八次作业

BY 18340087 李晨曦

(2)

充分性：

$$\begin{aligned}(ab)^2 &= (ab)(ab)\\ &= abab\\ &= aabb\end{aligned}$$

即

$$abab = aabb$$

两边左乘a^{-1}：

$$bab = abb$$

两边右乘b^{-1}：

$$ba = ab$$

这也就是说， 群G是一个交换群。

必要性：

由群G是一个交换群：

$$\begin{aligned}ba &= ab\\ aba &= aab\\ abab &= aabb\\ (ab)^2 &= a^2b^2\end{aligned}$$

(4)

记集合X的生成子群为$\mathrm{gp}(X)$。使$X := \{a\}$， 由于G是一个有限群，G的子群$\mathrm{gp}(\{a\})$也是一个有限群。

这样一来有：

$$a^{|\mathrm{gp}(\{a\})|} = e$$

而由Lagrange定理， 我们有$|\mathrm{gp}(\{a\})|$整除$|G| = n$.

所以：

$$\begin{aligned}a^n &= (a^{|\mathrm{gp}(\{a\})|})^c\\ &= e^c\\ &= e\end{aligned}$$

这就是所要的结论。

(6)

对任意的$a\in G$，$h\in \mathrm{cent}(G)$， 我们有：

$$\begin{aligned} aha^{-1} &= haa^{-1} \\ &= h \end{aligned}$$

所以

$$aha^{-1}\in \mathrm{Cent}(G)$$

这也就是说，$\mathrm{cent}(G)$是G的正规子群。

(7)

令集合$H:=\{h\,|\,h=axa^{-1}\}$.

对于$\forall g\in G$， 令$x=a^{-1}ga$， 那么$g=axa^{-1}\in H$. 也就是说，$G\subset H$.

显然地， 以这种形式给出的映射一定是一个满射。因为值域就是集合H.

所以对于$\forall h\in H$， 一定$\exists g, h=a^{-1}ga$， 由于群的封闭性，$h=a^{-1}ga\in G$， 也就是说，$H\subset G$.

所以，$H=G$.

这样一来， 定义在G上的运算$*$和集合H构成的群$G'=G$.

对于$\forall x,y\in G$， 有：

$$\begin{aligned} \sigma(xy) &= axya^{-1} \\ &= axeya^{-1} \\ &= axa^{-1}aya^{-1} \\ &= \sigma(x)\sigma(y) \end{aligned}$$

这说明σ是一个自同态。

对于$\forall x_1,x_2$，$h_1=ax_1a^{-1},h_2=ax_2a^{-1}$

若$h_1=h_2$， 则有：

$$\begin{aligned} h_1 &= h_2 \\ ax_1a^{-1} &= ax_2a^{-1} \\ x_1 &= x_2 \end{aligned}$$

所以σ是一个单射。结合上面已经说过的σ是一个满射， 可以得到σ是一个双射。

综上所述，σ是一个自同构。

(8)

(i)

自反性：

由群的定义有

$$\begin{aligned} e^{-1}e &= e \\ &\in H \end{aligned}$$

所以eRe成立， 自反性得证。

对称性：

如果$b^{-1}a \in H$,

由群的性质可知：

$$\begin{aligned} (b^{-1}a)^{-1} &\in H \\ a^{-1}b &\in H \end{aligned}$$

对称性得证。

传递性：

如果aRb, bRc， 那么：

$$\begin{aligned} b^{-1}a &\in H \\ c^{-1}b &\in H \end{aligned}$$

由群的封闭性：

$$\begin{aligned} c^{-1}bb^{-1}a &\in H \\ c^{-1}a &\in H \end{aligned}$$

传递性得证。

综上，R是等价关系。

(ii)

充分性：

如果$aH = bH$， 对于$\forall h_1 \in H$， 一定存在$h_2 \in H$， 使得：

$$ah_1 = bh_2$$

所以

$$\begin{aligned} b^{-1}ah_1 &= h_2 \\ b^{-1}a &= h_2h_1^{-1} \end{aligned}$$

由于群的封闭性， 我们有

$$\begin{aligned} h_2h_1^{-1} &\in H \\ b^{-1}a &\in H \end{aligned}$$

必要性：

如果$b^{-1}a \in H$， 那么对于$\forall h_1 \in H$， 有：

$$\begin{aligned} ah_1 &= bb^{-1}ah_1 \\ &= b(b^{-1}ah_1) \end{aligned}$$

由群的封闭性，　有

$$\begin{aligned} b^{-1}ah_1 &\in H \\ b(b^{-1}ah_1) &\in bH \end{aligned}$$

这也就是说，$\forall h_1\in H, ah_1\in bH$，　即$aH\subset bH$.

同理可证$bH\subset aH$，　故$aH=bH$.

(11)

F_{23}实际上是一个数域，　可以看成$(\mathbb{Z}/23\mathbb{Z},+,*)$.

显然地，　如果a是群$(\mathbb{Z}/23\mathbb{Z},+)$的生成元，　它必定是$F_{23}$的生成元。

对于$\forall[a], 1\leqslant a\leqslant 22, \forall[b]\in\mathbb{Z}/23\mathbb{Z}$，　下面的方程

$$ax\equiv b\,(\mathrm{mod}\,23)$$

是有解的，　所以$\{[a], 1\leqslant x\leqslant 22\}$中的每一个元素都是群$(\mathbb{Z}/23\mathbb{Z},+)$的生成元，　自然也是 F_{23}的生成元。