群

1. 在整数集$\mathbb{Z}$中定义二元运算"*"如下:

(1) $n*m=-m-n,\ m,n\in\mathbb{Z}$. 证明这个二元运算是交换的, 但不是结合的.

(2) $n*m=n+m-2,\ m,n\in\mathbb{Z}$. 证明$(\mathbb{Z},*)$是群.

证明 (1) 略.

(2) 封闭性、结合律显然, 单位元为2, 对于任意n, 其逆元为$4-n$.

2. 证明: 若G为有限集且对运算"$\cdot$"封闭, 满足结合律和消去律, 则$(G,\cdot)$构成一个群.

证明 引理: 若半群G满足$\forall a,b\in G$, 方程$xa=b,ax=b$均有解, 则G 为群.

引理的证明: $\because xa=a$有解, 解为e_a, $\therefore e_a a=a$. 对于$\forall c\in G$, $ax=c$有解, 解为d, 则$ad=c$, 从而有$e_a c=e_a(ad)=e_a ad=ad=c$. $\therefore G$存在幺元, 幺元为e_a. 对于$\forall f\in G, xf=e_a, fx=e_a$有解, $\therefore x$为f的逆元. 综上, G是群.

$\forall a\in G$, $\because$满足消去律且$|G|$有限, $\therefore aG=G$, 从而$\forall a,b\in G, ax=b, xa=b$有解.

3. 已知群$(G_1,+_1)$, $(G_2,+_2)$, 构造集合$G=G_1\times G_2=\{(x,y)|x\in G_1,y\in G_2\}$ 以及运算+满足

$$(x_1,y_1)+(x_2,y_2)=(x_1+_1 x_2,y_1+_2 y_2)$$

证明$(G,+)$是群.

证明: 封闭、结合律、幺元为(e_1,e_2)、存在逆元

4. 设群中每个非幺元的阶为2, 证明该群是Abel群.

证明: $\forall a,b\in G,a^2=b^2=(ab)(ab)=e$. 对$(ab)(ab)=a^2$两边左乘$a$, 有$bab=a,\therefore b(bab)=ba$. 由$b^2=e$知$ab=ba,\therefore G$为Abel群.

5. 对于集合S，定义2^S为S的幂集. 证明:

(1) $(2^S,\cup)$与$(2^S,\cap)$均为半群;

(2) 若在S的子集上定义运算$A\Delta B=(A\setminus B)\cup(B\setminus A)$, 则$(2^S,\Delta)$是群.

证明: 略.

6*. 设M是幺半群, e是其幺元. 对于M中的元素a, 若存在元素$a^{-1}\in M$满足

$$a^{-1}a=aa^{-1}=e$$

则称a是可逆的. 试证明下列命题:

(1) 若$a\in M$, 且存在$b,c\in M$使得$ab=ca=e$, 则a可逆且$a^{-1}=b=c$;

(2) 若$a \in M$可逆, 则$b = a^{-1}$当且仅当$aba = a, ab^2a = e$;

(3) M中的非空子集G为群的充要条件是G中每个元素可逆, 且$\forall g_1, g_2 \in G$有$g_1^{-1}g_2 \in G$;

(4) M中所有可逆元素构成一群.

证明:

(1) 只需证明$b = c$. 易知$b = (ca)b = c(ab) = c$, 故a可逆且$a^{-1} = b = c$.

(2) "$\Rightarrow$": 显然.

"$\Leftarrow$": 要证明$b = a^{-1}$, 需证$ab = ba = e$. $ab = abaa^{-1} = aa^{-1} = e, ba = a^{-1}aba = a^{-1}a = e, \therefore ab = ba = e$.

(3) "$\Rightarrow$": 显然.

"$\Leftarrow$": 封闭性、结合律、逆元存在是显然的. $\forall g \in G, g^{-1}g \in G$, 即$e \in G$.

(4) 若g_1, g_2可逆, 则$(g_2^{-1}g_1^{-1})(g_1g_2) = (g_1g_2)(g_2^{-1}g_1^{-1}) = e$, 故$g_1g_2$可逆, 满足封闭性. 结合律、幺元、逆元存在是显然的.

7. 设G是一个群, H是G的一个非空有限子集, 证明H是G的子群的充要条件是: 对任意$a, b \in H$有$a \cdot b \in H$.

证明:

"$\Rightarrow$": 显然.

"$\Leftarrow$": 群满足消去律. 有限半群满足消去律是群.

注：请注意, 本题条件与教材中定理6.2.2不同.

8. 设H是$\mathbb{Z}$的子群, 证明必存在整数m使得$H = m\mathbb{Z}$.

证明: 构造法.

令$m = \min\{|n| \mid n \in H, n \neq 0\}$. $\because H$是$\mathbb{Z}$的子群, $\therefore H$中的元素都是整数. $\forall a \in H$, 由带余除法可知$a = mq + r, 0 \leq r < m$. $\because mq \in H$(q个m相加), $\therefore r \in H$. 由m的定义知$r = 0$, 从而$H = m\mathbb{Z}$.

9. 证明群G不能写成两个真子群的并.

证明: 设H_1和H_2是G的真子群且$H_1 \cup H_2 = G$. 取$a \in H_1, b \in H_2$且$a \notin H_2, b \notin H_1$, 则$ab \notin H_1, ab \notin H_2$, 从而$ab \notin G$, 矛盾.

10. 证明群中元素与其逆元具有相同的阶.

证明: $(a^n)^{-1} = (a^{-1})^n$, 从而有$a^k = 1$当且仅当$(a^{-1})^k = 1$, 故a与a^{-1}同阶.

11. 证明有限群G中的任何元素的阶都可整除$|G|$.

证明: 教材(机械工业出版社)定理6.3.4, $\mathrm{ord}(a) = |\langle a \rangle|$, 定理6.5.4(拉格朗日定理), $|\langle a \rangle| \mid |G|$.

12. 证明$(\mathbb{Z}_p, +)$有$p-1$个生成元, 其中p为素数.

证明: 教材(机械工业出版社)定理6.3.2的推论.

13. 设G是群, $a \in G$, $\langle a \rangle$是G中唯一的二阶子群. 证明对于$\forall x \in G$, 有$ax = xa$.

证明: $\langle a \rangle = \{e, a\}$, $a \neq e$, $a^2 = e$, 且a是G中唯一的二阶元. $\forall x \in G$, $(x^{-1}ax)(x^{-1}ax) = e, \therefore x^{-1}ax = e$或$a$. 若$x^{-1}ax = e$, 则$ax = x$, $a = e$, 矛盾. 于是, $x^{-1}ax = a$, 从而有$ax = xa$.

14. 证明只有有限个子群的群为有限群.

证明: 假设G为无限群, 若$\exists g \in G$, g的阶为∞, 则$\langle g \rangle \cong \mathbb{Z}$, $\mathbb{Z}$有无限多个子群, 矛盾. $\therefore$ G中每个元素的阶有限, 从而取$a \in G$, $\exists b \in G$但$b \notin \langle a \rangle$, $\exists c \in G, c \notin \langle a \rangle, c \notin \langle b \rangle, \ldots$, 依次类推, G有无限个子群, 矛盾. $\therefore$ G必为有限群.

15. 设G是Abel群, H, K是其循环子群, 阶分别为r, s, 证明:

(1) 若$(r, s) = 1$, 则G有阶为rs的循环子群;

(2) G包含一个阶为$[r, s]$的循环子群.

证明: 设$H = \langle a \rangle, K = \langle b \rangle$, ab的阶为k, 那么有$(ab)^k = a^k b^k = e, \therefore r \mid k, s \mid k, \therefore [r, s] \mid k$. 另一方面, $(ab)^{[r,s]} = a^{[r,s]} b^{[r,s]} = e, \therefore k \mid [r, s]$. 故可以得到$k = [r, s]$, 于是$\langle ab \rangle$是$G$ 中的$[r, s]$阶循环子群. 由(2)可直接推出(1).

16. 证明质数阶群只有平凡子群.

证明: 拉格朗日定理.

17*. 已知群G_1, G_2是G的有限子群, 证明:

$$|G_1G_2| = [G_1 : 1][G_2 : 1]/[G_1 \cap G_2 : 1].$$

证明: 即证明$|G_1G_2| = |G_1||G_2|/|G_1 \cap G_2|$. 考虑左陪集$aG_2, a \in G_1$, 则$\{aG_2\}$是对$G_1G_2$的一个划分, 于是问题变成找到陪集$aG_2$把$G_1G_2$分成了多少份. 下面考虑$aG_2, bG_2$在什么情况下是同一个陪集. $aG_2 = bG_2, a, b \in G_1 \Leftrightarrow b^{-1}a \in G_2 \Leftrightarrow b^{-1}a \in G_1 \cap G_2 \Leftrightarrow a(G_1 \cap G_2) = b(G_1 \cap G_2)$. 此推导过程表明$aG_2 = bG_2 \Leftrightarrow a(G_1 \cap G_2) = b(G_1 \cap G_2), a, b \in G_1$, 于是陪集$aG_2$把$G_1G_2$分成的份数等同于$a(G_1 \cap G_2)$把$G_1$分成的份数. 得证.

18. 已知群G_1, G_2是G的有限子群且$G_1 \subset G_2$, 证明

$$[G : G_1] = [G : G_2][G_2 : G_1].$$

证明: $[G : G_1] = \frac{|G|}{|G_1|}, [G : G_2] = \frac{|G|}{|G_2|}, [G_2 : G_1] = \frac{|G_2|}{|G_1|}$.

19. 设H是群G的正规子群, 证明商群G/H是Abel群的充要条件是

$$gkg^{-1}k^{-1} \in H, \ \forall g, k \in G.$$

证明: G/H是Abel群$\Leftrightarrow gHkH = kHgH \Leftrightarrow gkH = kgH \Leftrightarrow gk(kg)^{-1} = gkg^{-1}k^{-1} \in H$

20. 设H, K是群G的两个正规子群且$H \cap K = \{1\}$, 证明:

$$hk = kh, \ \forall h \in H, k \in K.$$

证明: 对于$\forall h \in H, k \in K$, $(kh)^{-1}hk = h^{-1}k^{-1}hk$. $\because H$是正规子群, $\therefore k^{-1}hk \in H, \therefore h^{-1}k^{-1}hk \in H$; 同理可得$h^{-1}k^{-1}h \in K, \therefore h^{-1}k^{-1}hk \in K$, 故$h^{-1}k^{-1}hk \in H \cap K$. $\because H \cap K = \{1\}, \therefore h^{-1}k^{-1}hk = 1, \therefore hk = kh$.

21. 设G为交换群, 幺元为e. 定义G中的**扭元**为满足$g^n = e (n \in \mathbb{Z}^+)$的元素$g$, 扭元集合为$G_{tor} = \{g \in G | \exists n \in \mathbb{Z}^+, g^n = e\}$. 证明$G_{tor}$是$G$的正规子群.

证明: $\forall g_1, g_2 \in G_{tor}, (g_1 g_2^{-1})^n = g_1^n (g_2^n)^{-1} = e, \therefore g_1 g_2^{-1} \in G_{tor}$.

$\forall g \in G, g_0 \in G_{tor}$, 设$n \in \mathbb{Z}^+$使$g_0^n = e$, 那么$(g g_0 g^{-1})^n = g^n g_0^n (g^{-1})^n = e, \therefore g g_0 g^{-1} \in G_{tor}$.

22*. 设H是群G的子群且$[G : H] = 2$, 证明$H \lhd G$.

证明: $\because [G : H] = 2, \therefore \exists a \in G$且$a \notin H$, 使得$G = eH \cup aH$且$eH \neq aH$. 要证明$H \lhd G$, 即要证$\forall g \in G, h \in H, ghg^{-1} \in H$. 下面分两种情况讨论:

1) 当$g \in eH = H$时, 显然有$ghg^{-1} \in H$;

2) 当$g \in aH$时, $\exists h_1 \in H$, 使得$g = ah_1$, 那么$ghg^{-1} = ah_1 h (ah_1)^{-1}$. $\because ghg^{-1} \in G$, 若$ghg^{-1} \notin H$, 则必有$ghg^{-1} \in aH$, 从而$\exists h_2 \in H$, 使得$ghg^{-1} = ah_2$, 即$ah_1 h h_1^{-1} a^{-1} = ah_2$, 从而有$h_1 h h_1^{-1} a^{-1} = h_2 \Rightarrow a = h_2^{-1} h_1 h h_1^{-1} \Rightarrow a \in H$, 矛盾. $\therefore ghg^{-1} \in H$.

综上, 对于$\forall g \in G, h \in H, ghg^{-1} \in H$成立. $\therefore H \lhd G$.

23. 设H,K是两个群. 在$H\times K=\{(h,k)|h\in H,k\in K\}$中定义乘法

$$(h_1,k_1)(h_2,k_2)=(h_1h_2,k_1k_2).$$

证明:

(1) $H\times K$是一个群;

(2) $H_1=\{(h,1_K)|h\in H\}$和$K_1=\{(1_H,k)|k\in K\}$是$H\times K$的正规子群，其中$1_H,1_K$分别是H,K的幺元;

(3) $H_1\cap K_1=\{(1_H,1_K)\}$;

(4) $H\times K=H_1K_1$.

证明:

(1) 略.

(2) $\forall(h_1,1_K)\in H_1,(h,k)\in H\times K,(h,k)(h_1,1_K)(h,k)^{-1}=(hh_1h^{-1},kk^{-1})=(hh_1h^{-1},1_K)\in H_1,\therefore H_1$是$H\times K$的正规子群. 同理可证$K_1$是$H\times K$的正规子群.

(3) 设$(h,k)\in H_1$且$(h,k)\in K_1$, 则$k=1_K,h=1_H,\therefore H_1\cap K_1=\{(1_H,1_K)\}$.

(4) $(h,k)=(h,1_K)(1_H,k)$. $H\times K\subseteq H_1K_1,H_1K_1\subseteq H\times K$.

24. 设f为群G到群H的映射, 分别判断如下的f是否为同态, 如果是则给出$\mathrm{ker}f$:

(1) 加法群$G=\mathbb{R},\ H=\mathbb{Z},\ f(x)=[x]$, 其中$[x]$为取整函数, 即不大于$x$的最大整数;

(2) 乘法群$G=\mathbb{R}^*,\ H=\mathbb{R}^+,\ f(x)=|x|$;

(3) $G=\mathbb{Z}_5,\ H=\mathbb{Z}_2,\ f(x)=x \bmod 2$.

解:

(1) 不是.

(2) 是. $\mathrm{ker}f=\{1,-1\}$.

(3) 不是.

25. 设G是群, 证明其自同构集合Aut$G$是一个群.

证明: 集合Aut$G=\{f|f:G\to G\}$, 运算为映射的复合. 封闭、结合律显然. 幺元为id, 逆元为逆映射.

26. 设G是群, 证明:

(1) $g\mapsto g^{-1}$是G的自同构映射当且仅当G是Abel群;

(2) 若G是Abel群，对任意整数k，$g\mapsto g^k$是G的自同态映射.

证明: (1) “$\Leftarrow$”: $\forall g\in G, f(g)=g^{-1}, \because g^{-1}\in G, \therefore f$是$G\to G$的映射; 显然$f$是满射; $f(a)=f(b)\Rightarrow a^{-1}=b^{-1}\Rightarrow a=b, \therefore f$是单射; $\forall a,b\in G, f(ab)=(ab)^{-1}=b^{-1}a^{-1}$, 由于$G$是Abel群, 可知$f(ab)=b^{-1}a^{-1}=a^{-1}b^{-1}=f(a)f(b)$. 综上, f是自同构.

“$\Rightarrow$”: $\forall a,b\in G, f(ab)=(ab)^{-1}=b^{-1}a^{-1}$, 又$\because f$是同态, $\therefore f(ab)=f(a)f(b)=a^{-1}b^{-1}, \therefore a^{-1}b^{-1}=b^{-1}a^{-1}$.

27**. 证明例6.1.7中的Klein四元群K的自同构群与S_3同构.

证明: 令$\varphi:\mathrm{Aut}K\to S_3, f\mapsto f|_X$, 其中$f$为$K$的自同构映射, $X=\{a,b,c\}$, $f|_X$表示将映射f限制到集合X上. 注意到Klein四元群中a,b,c都是二阶元, 自同构映射将二阶元映射为二阶元, $\therefore f|_X\in S_3, f(e)=e$, 则$\varphi$是满射. 若$f|_X=g|_X$, 又$f(e)=g(e)=e$, 有$f=g$, $\therefore \varphi$是单射. $\forall f,g\in$

Aut$K, \varphi(fg) = fg|_X = f|_X g|_X = \varphi(f)\varphi(g), \therefore \varphi$是同构映射. 综上, φ是同构映射, 即Aut$K \cong S_3$.

28. 将置换$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 8 & 1 & 4 & 7 & 3 \end{pmatrix}$分解成不相交的轮换.

解: $(1\quad 2\quad 5)(3\quad 6\quad 4\quad 8)$

29. 将置换之积$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 8 & 1 & 4 & 7 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 6 & 4 & 1 & 8 & 7 & 3 \end{pmatrix}$分解成不相交的轮换.

解: $(1\quad 5\quad 2)(3\quad 4\quad 8\quad 6)$

30. 求出S_5中的元素$\sigma\tau$, $\sigma^{-1}\tau\sigma$, σ^2, σ^3, 其中$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$.

解:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}, \quad \sigma^{-1}\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}, \quad \sigma^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$