Homework 4

Due: May 25th (Monday), 11:59 pm

- Please submit your work on Blackboard.
- You are required to submit your work as a single pdf.
- Please make sure your handwriting is clear enough to read. Thanks.
- No late work will be accepted.
- There are five randomly picked questions (2 pts for each) that will be graded.
  (1), (2), (6), (8), (9)

---

(1) Find HK in $\mathbf{Z}_{16}^{\times}$, if $H = \langle[3]\rangle$ and $K = \langle[5]\rangle$.

$|\mathbf{Z}_{16}^{\times}| = \varphi(16) = 8$; $H = \langle[3]\rangle = \{[1],[3],[9],[11]\}$ and $K = \langle[5]\rangle = \{[1],[5],[9],[13]\}$

$HK = \mathbf{Z}_{16}^{\times} = \{[1],[3],[5],[7],[9],[11],[13],[15]\}$.

(2) Find the order of the element $([9]_{12},[15]_{18})$ in the group $\mathbf{Z}_{12} \times \mathbf{Z}_{18}$.

$o([9]_{12}) = o([-3]_{12}) = o([3]_{12}) = 4$ in $\mathbf{Z}_{12}$ and $o([15]_{18}) = o([-3]_{18}) = o([3]_{18}) = 6$ in $\mathbf{Z}_{18}$.[1] Thus, $o(([9]_{12},[15]_{18})) = \mathrm{lcm}[4,6] = 12$.

(3) Prove that if G_1 and G_2 are abelian groups, then the direct product $G_1 \times G_2$ is abelian. (Assume that $(G_1,*)$ and $(G_2,\cdot)$ are abelian groups.)

For any two elements $(a_1,a_2),(b_1,b_2) \in G_1 \times G_2$, we have

$$(a_1,a_2)(b_1,b_2) = (a_1 * b_1, a_2 \cdot b_2) = (b_1 * a_1, b_2 \cdot a_2) = (b_1,b_2)(a_1,a_2).$$

(4) Construct an abelian group of order 12 that is not cyclic.

$\mathbf{Z}_2 \times \mathbf{Z}_6$ is abelian by Question (3). Since $(2,6) = 2 \neq 1$, it is not cyclic.[2]

(5) Construct a group of order 12 that is not abelian.

$\mathbf{Z}_2 \times S_3$ is not abelian since S_3 is not abelian. For example, $([0],(123))([0],(12)) = ([0],(13))$, but $([0],(12))([0],(123)) = ([0],(23))$.

(6) Let G_1 and G_2 be groups, with subgroups H_1 and H_2, respectively. Show that

$$\{(x_1,x_2) \mid x_1 \in H_1, x_2 \in H_2\}$$

is a subgroup of the direct product $G_1 \times G_2$.

Let $(G_1,*)$ and $(G_2,\cdot)$ be groups and let $S = \{(x_1,x_2) \mid x_1 \in H_1, x_2 \in H_2\}$.

(i) For $(x_1,x_2),(y_1,y_2) \in S$, we have $(x_1,x_2)(y_1,y_2) = (x_1 * x_2, y_1 \cdot y_2) \in S$ since H_1 and H_2 are the subgroups of G_1 and G_2, respectively.

(ii) The identity element $e = (e_1,e_2) \in S$, where e_i is the identity element of H_i (and also of G_i) for $i = 1,2$.

(iii) Inverses: $(x_1,x_2)^{-1} = (x_1^{-1},x_2^{-1}) \in S$. (Easy to check)

---

[1] Here, we can also apply $\langle[a]_n\rangle = \langle[d]_n\rangle$, where $d = (a,n)$.

[2] Here, we use the fact that $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic if and only if $(n,m) = 1$.

(7) (a) Let $C_1 = \{(a,b) \in \mathbf{Z} \times \mathbf{Z} \mid a = b\}$. Show that C_1 is a subgroup of $\mathbf{Z} \times \mathbf{Z}$.

(i) For $(a,b),(c,d) \in C_1$, we have $(a,b)(c,d) = (a+c, b+d) \in C_1$. It follows from $a = b$ and $c = d$ that $a + c = b + d$.

(ii) The identity element $(0,0) \in C_1$.

(iii) For $(a,b) \in C_1$, its inverse $(a,b)^{-1} = (-a,-b) \in C_1$ since $a = b$.

(b) For each positive integer $n \geq 2$, let $C_n = \{(a,b) \in \mathbf{Z} \times \mathbf{Z} \mid a \equiv b \pmod{n}\}$. Show that C_n is a subgroup of $\mathbf{Z} \times \mathbf{Z}$.

(i) For $(a,b),(c,d) \in C_n$, we have $(a,b)(c,d) = (a+c, b+d) \in C_n$. $a + c \equiv b + d \pmod{n}$ since $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$.

(ii) The identity element $(0,0) \in C_n$ since $0 \equiv 0 \pmod{n}$.

(iii) For $(a,b) \in C_n$, its inverse $(a,b)^{-1} = (-a,-b) \in C_n$. (Easy to see)

(c) Show that every proper subgroup of $\mathbf{Z} \times \mathbf{Z}$ that contains C_1 has the form C_n, for some positive integer n.

Let H be a proper subgroup of $\mathbf{Z} \times \mathbf{Z}$ with $C_1 \subseteq H$.

(i) If $C_1 = H$, then $n = 1$.

(ii) If $C_1 \subsetneq H$, then there exists an element $(a,b) \in H$ but $(a,b) \notin C_1$. Since $(-a,-a) \in C_1 \subsetneq H$, we have $(a,b)(-a,-a) = (0, b-a) \in H$.

$$\text{Let } n := \min\{|b-a| \mid \text{for all } (a,b) \in H \text{ with } a \neq b\}.$$

Claim 1: $n \geq 2$.
If $n = 1$, then $(0,1) \in H$ and so $(1,0) \in H$ since $(1,0) = (-1,0)^{-1} = ((0,1)(-1,-1))^{-1}$. This means $H = \mathbf{Z} \times \mathbf{Z}$ since any element (m,n) in $\mathbf{Z} \times \mathbf{Z}$ can be written as the form $(1,0)^m(0,1)^n$. This contradicts the condition that H is a proper subgroup of $\mathbf{Z} \times \mathbf{Z}$.

Claim 2: $H = C_n$.
(a) $C_n \subseteq H$: For any element $(a,b) \in C_n$, we have $a \equiv b \pmod{n}$. It implies $b - a = nq$ for some $q \in \mathbf{Z}$. So $(a,b) = (a,a)(0, b-a) = (a,a)(0,nq) = (a,a)(0,n)^q \in H$ since H is a subgroup of $\mathbf{Z} \times \mathbf{Z}$.

(b) $H \subseteq C_n$: For any element $(a,b) \in H$, we can write $b - a = nq + r$ with $0 \leq r < n$. So $(0,r) = (a,b)(-a,-a-nq) = (a,b)(-a,-a)(0,-nq) = (a,b)(-a,-a)(0,n)^{-q} \in H$. Thus, $r = 0$ since n is the smallest positive integer such that $(0,n) \in H$. It follows that $b - a = nq$ and so $a \equiv b \pmod{n}$. That is, $(a,b) \in C_n$.

(8) Let G_1 and G_2 be groups, and let G be the direct product $G_1 \times G_2$. Let $H = \{(x_1,x_2) \in G_1 \times G_2 \mid x_2 = e_2\}$ and let $K = \{(x_1,x_2) \in G_1 \times G_2 \mid x_1 = e_1\}$.

(a) Show that H and K are subgroups of G.

We will show H is a subgroup of G and the proof for K should be similar.
(i) $(x_1,e_2),(y_1,e_2) \in H$, we have $(x_1,e_2)(y_1,e_2) = (x_1 * y_1, e_2 \cdot e_2) \in H$.
(ii) The identity element $(e_1,e_2) \in H$.
(iii) For $(x_1,e_2) \in H$, its inverse is $(x_1^{-1}, e_2) \in H$.

(b) Show that $HK = KH = G$.

$HK = KH$: For any element $(x_1, e_2) \in H$ and any element $(e_1, x_2) \in K$, we have

$$\begin{aligned}(x_1, e_2)(e_1, x_2) =&(x_1 * e_1, e_2 \cdot x_2)\\ =&(x_1, x_2)\\ =&(e_1 * x_1, x_2 \cdot e_2)\\ =&(e_1, x_2)(x_1, e_2).\end{aligned}$$

$HK \subseteq G$: HK is a subgroup of G by Proposition 1 since $HK = KH$.

$G \subseteq HK$: For any element $(x_1, x_2) \in G$ for $x_1 \in G_1$ and $x_2 \in G_2$, we can write it as $(x_1, x_2) = (x_1 * e_1, e_2 \cdot x_2) = (x_1, e_2)(e_1, x_2)$, which is in HK.

(c) Show that $H \cap K = \{(e_1, e_2)\}$.

$\{(e_1, e_2)\} \subseteq H \cap K$: By definition, we have $(e_1, e_2) \in H$ and $(e_1, e_2) \in K$.

$H \cap K \subseteq \{(e_1, e_2)\}$: For any element $(x_1, x_2) \in H \cap K$, we have

$$\begin{cases}(x_1, x_2) \in H \Rightarrow x_2 = e_2\\ (x_1, x_2) \in K \Rightarrow x_1 = e_1\end{cases} \implies (x_1, x_2) = (e_1, e_2).$$

(9) Let H, K, L be subgroups of the group G, with $H \subseteq K$. Prove that

$$H(K \cap L) = K \cap HL.$$

Note: This is an equality of sets, since they may not be subgroups.

$H(K \cap L) \subseteq K \cap HL$: For any element $a \in H(K \cap L)$, there exist $h \in H$ and $t \in K \cap L$ such that $a = ht$. Since $h \in H \subseteq K$ and $t \in K \cap L \subseteq K$, so we have $a = ht \in K$ since K is a subgroup of the group G. Again, since $t \in K \cap L \subseteq L$, we have $a = ht \in HL$. Thus, $a = ht \in K \cap HL$.

$K \cap HL \subseteq H(K \cap L)$: For any element $a \in K \cap HL$, there exist $h \in H$ and $l \in L$ such that $a = hl$ and $a = k$ for some $k \in K$. Thus, we have $l = h^{-1}a = h^{-1}k$ since H is a subgroup of G and so h^{-1} always exists. It follows that $l = h^{-1}k \in K$ since $h^{-1} \in H \subseteq K$ and K is a subgroup of G. Therefore, $l \in K \cap L$ and so $a = hl \in H(K \cap L)$.

(10) Let F be a field, and let H be the subset of $\mathrm{GL}_2(F)$ consisting of all invertible upper triangular matrices. Show that H is a subgroup of $\mathrm{GL}_2(F)$.

(i) Let $\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}, \begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} \in H$. In particular, $a_1 d_1 \neq 0, a_2 d_2 \neq 0$. Then

$$\begin{bmatrix} a_1 & b_1 \\ 0 & d_1 \end{bmatrix}\begin{bmatrix} a_2 & b_2 \\ 0 & d_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{bmatrix} \in H.$$

This is because the determinant of the product is $a_1 a_2 d_1 d_2 \neq 0$.

(ii) The identity matrix $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$.

(iii) For any element $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in H$, its inverse is $\begin{bmatrix} 1/a & -b/(ad) \\ 0 & 1/d \end{bmatrix} \in H$.