Problem Set #5

Exercise 1 :
If $S \neq \emptyset$ subset of G then $W_S = \{a_1 \dots a_r : r < \infty, a_r \in S \cup S^{-1}\}$ is a subgroup and is equal $< S >$.
Solution :
If $s \in S$ then $e = s \cdot s^{-1} \in W_S$, (taking $r = 2$). If $x = a_1 \dots a_r \in W_S$ then $y = a_r^{-1} \dots a_1^{-1}$ is $= x^{-1} and is in W_S$. Finally, if $x = a_1 \dots a_r$, $y = b_1 \dots b_s \in W_S$, we have $xy = a_1 \dots a_r b_1 \dots b_s$ (a word of length $r+s$ in the symbols $s \in S \cup S^{-1}$). W_S is a subgroup. But if H is any group containing S the element in S^{-1} are in H, so that $S \cup S^{-1} \subseteq H$ and then every word in W_S lies in H. Therefore W_S is the smallest subgroup containing S and $W_S =< S >$.
Exercise 2 :
In $(\mathbb{Z}/12\mathbb{Z}, +)$, determine the subgroup H generated by :

1. $[2]$.
2. $[3]$.
3. $[2]$ and $[3]$.

Solution :

1. $[2]$. Then $H =< [2] >$ is $\{m \cdot [2] : m \in \mathbb{Z}\} = \{[0], [2], [4], \dots, [10]\}$ (cyclic group of 6 elements) $\simeq (\mathbb{Z}/6\mathbb{Z}, +)$.
2. $[3]$. Now $H = \{[0], [3], [6], [9]\}$ cyclic group $\simeq (\mathbb{Z}/4\mathbb{Z}, +)$.
3. $[2]$ and $[3]$. H contains all elements $r[2] + s[3]$ for $r, s \in \mathbb{Z}$. $\mathbb{Z}[2] + \mathbb{Z}[3] = \{[k] : k \in \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot 3 \ in \ \mathbb{Z}\} \subseteq H$. Since $gcd(2, 3) = 1$, $\Gamma = \mathbb{Z} \cdot 2 + \mathbb{Z} \cdot 3$ is all $\mathbb{Z}$ and H is all of $\mathbb{Z}/12\mathbb{Z}$.

Exercise 3 :
Prove that if H is a subgroup of $(\mathbb{Z}, +)$, $\exists m \geqslant 0$ in $\mathbb{Z}$ such that $H = m\mathbb{Z}$.
Solution : For the trivial subgroup $H = \{0\}$ take $m = 0$. If $H \neq 0$ then $H = -H$. So $H \cap \mathbb{N} \neq \emptyset$. By the Minimum principle, there is a smallest element $a > 0$ in H $a = min\{H \cap \mathbb{N}\}$. Obviously, $\mathbb{Z} \cdot a \subseteq H$. To see $H \subseteq \mathbb{Z} \cdot a$: if $x \in H$ then by the Euclidean division, $\exists$ smallest element $a > 0$ in H, $a = min\{H \cap \mathbb{N}\}$. Obviously, $\mathbb{Z} \cdot a \subseteq H$. To see $H \subseteq \mathbb{Z} \cdot a$, if $x \in H$ then by Euclidean division ; $\exists q, m \in \mathbb{Z}$ such that $x = qa + r$ with $0 \leqslant r < a$. That implies $r = x - qa \in H - H = H$. But $0 \leqslant r < a$ violates minimality of a in $\mathbb{N} \cap H$ unless $r = 0$. Therefore $r = 0$, $x = qa \in \mathbb{Z}x$. $H \subseteq \mathbb{Z}a$. Thus $H = \mathbb{Z}a$.

Exercise 4 :
In $(\mathbb{Z}/12\mathbb{Z}, +)$, find all $[k]$ that are cyclic generators with respect to $(+)$. We are looking

for $a = [k]$ with additive order $o(a) = |\mathbb{Z}/12\mathbb{Z}| = 12$.
Solution :
Compute $< a >$ for each $a = [0], [1], \dots, [11]$;

a	$H =< a >$	$o(a) = \|H\|$
0	0	1
1	$\{0, 1, 2, \dots, 11\} = \mathbb{Z}/12\mathbb{Z}$	12
2	$\{0, 2, 4, 6, 8, 10\}$	6
3	$\{0, 3, 6, 9\}$	4
4	$\{0, 4, 8\}$	3
5	$\{0, 5, 10, 15 \equiv 3, 8, 13 \equiv 1, 6, 11, 16 \equiv 4, 9, 14 \equiv 2, 7\} = \mathbb{Z}/12\mathbb{Z}$	12
6	$\{0, 6\}$	2
$-5 = 7$	$\mathbb{Z}/12\mathbb{Z}$	12
$-4 = 8$	*same as* 4	3
$-3 = 9$	*same as* 3	4
$-2 = 10$	*same as* 2	6
$-1 = 11$	*same as* $1 = \mathbb{Z}/12\mathbb{Z}$	12

Exercise 5 :
Suppose a group element $x \in (G, \cdot)$ has the property $x^m = e$ for some integer $m \neq 0$. Then x has finite order $o(x)$, but the exponent m might not be the order $o(x)$ of the element x. Prove that any such exponent m must be a multiple of $o(x)$. (Hint : Letting $s = o(x)$, write $m = qs + r$ with $0 \leqslant r < s$).
Solution :
Given $|G = n < \infty$, we seek $N \in \mathbb{N}$ such that $x^N = e$, $\forall x \in G$. If we label the group elements $x_1 = e, x_3, \dots x_n$ let $m_k = 0(x_k)$ for $1 \leqslant k \leqslant n$. Then $(x_k)^{m_k} = e$. Take $N = \prod_{k=1}^{n} m_k$. Then $x_i^N = (x_i^{m_i})^{N'}$ where $N' = \prod_{j \neq i} m_j$ (by the exponent laws) $= e^{N'} = e$, for every i. Done.

Exercise 6 :
Prove that $(U_8, \cdot)$ is not cyclic. Prove that $(U_7, \cdot)$ is cyclic.
Solution :

$$U_8 = \{[k] \neq [0] in\ \mathbb{Z}/8\mathbb{Z} : gcd(k, 8) = 1\} = \{[1], [3], [5], [7]\}$$

But all elements in this group have multiplicative order $o(x) = 2$ (expect for $[1]$) :

$$[1], [3], [3]^2 = [9] = [1],\ o([3]) = 2$$

$$[1], [5], [5]^2 = [25] = [1],\ o([5]) = 2$$

$$[1], [7], [7]^2 = [49] = [1],\ o([7]) = 2\ (and\ o([1]) = 1)$$

There are no elements of order $|U_8| = 4$; so $(U_8, \cdot)$ cannot be cyclic. Compute orders of all elements in $U_7 = \{1, 2, \dots, 6\}$ (we omit the brackets, looking for an element of order

$o(x) = 6$).

x	$o(x)$	$H =< x >$
1	1	1
2	3	$1, 2, 4, 8 \equiv 1$
3	$1, 3, 9 \equiv 2, 18 \equiv 4, 12 \equiv 5, 15 \equiv 1$	
4	3	$1, 4, 16 \equiv 2, 8 \equiv 1$
5	6	$1, 5, 25 \equiv 4, 20 \equiv 6, 30 \equiv 2, 10 \equiv 3, 15 \equiv 1$
$-1 \equiv 6$	2	$1, -1$

Exercise 7 :
If a group G is generated by a subset S, prove that any homomorphism $\phi : G \to G'$ *is determined by what it does to the generators*, in the following sense :

> *If $\phi_1, \phi_2 : G \to G'$ are homomorphisms such that $\phi_1(s) = \phi_2(s)$ for all $s \in S$, then $\phi_1 = \phi_2$ everywhere on G.*

This can be quite useful in constructing homomorphisms of G, especially when the group has a single generator.

Solution :
$\phi_1(s^{-1}) = \phi_1(s)^{-1} = \phi_2(s)^{-1} = \phi_2(s^{-1})$, $\forall s \in S$, so $\phi_1 = \phi_2$ on $S_1 \cup S_2$. But $< S >=$ all words $a_1 \ldots a_r$ such that $r < \infty$, $a_i \in S \cup S^{-1}$. Then

$$g = a_1 \ldots a_r \Rightarrow \phi_1(g) = \phi_1(a_1) \ldots \phi_1(a_r) = \phi_2(a_1) \ldots \phi_2(a_r) = \phi_2(a_1 \ldots a_r) = \phi_2(g)$$