Algebraic Structures (MST20010)

Problem sheet 9

1. (a) Recall that $(\mathbb{Z},+)$ is cyclic if there is $a \in \mathbb{Z}$ such that $\mathbb{Z} = \langle a \rangle$, and that $\langle a \rangle$ is the set of everything you can obtain out of a and $-a$ (recall that $-a$ is the inverse of a in the group $(\mathbb{Z},+)$) and using the group operation as many times as you want (with a and $-a$ appearing as many times as you want and in any order). We clearly see that in this case
$$\langle a \rangle = \{na \mid n \in \mathbb{Z}\} = a\mathbb{Z}.$$
In particular $\langle 1 \rangle = \mathbb{Z}$, so $(\mathbb{Z},+)$ is cyclic.

Let a be a generator of $(\mathbb{Z},+)$, i.e., $\langle a \rangle = \mathbb{Z}$, i.e., $a\mathbb{Z} = \mathbb{Z}$. If this holds, then $1 \in a\mathbb{Z}$, so a divides 1, so $a = 1$ or $a = -1$. We already saw that 1 is a generator of $\mathbb{Z}$, and clearly $(-1)\mathbb{Z} = \mathbb{Z}$, so -1 is also a generator of $\mathbb{Z}$.

(b) Assume that $(\mathbb{R} \setminus \{0\}, \cdot)$ is cyclic. So $\mathbb{R} = \langle a \rangle$ for some $a > 0$ (the case $a < 0$ is very similar, just a bit longer to write). Since the operation is the product, we have $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. This set does not contain all the elements of $\mathbb{R}$. There are several ways to see this, I give two:

(1) If $a > 1$, then all the elements of $\langle a \rangle$ that are greater than 1 are $\{a, a^2, a^3, \ldots\}$ and $a < a^2 < a^3 \cdots$. Therefore the elements of the interval $(1, a)$ are not in $\langle a \rangle$. Similarly, if $a < 1$, then the elements of $\langle a \rangle$ that are greater than 1 are $a^{-1}, (a^{-1})^2, \ldots$ with $a^{-1} < (a^{-1})^2 < \cdots$, so the elements of the interval $(1, a^{-1})$ are not in $\langle a \rangle$.

(2) The element $a^{1/2}$ is not in H: If it were in H we would have $a^{1/2} = a^n$ for some $n \in \mathbb{Z}$, Taking the logarithm, we get $(1/2)\ln(a) = n\ln(a)$ so $1/2 = n$, impossible.

(c) Every element of $\mathbb{Z}/n\mathbb{Z}$ is of the form k for some $k \in \{0, \ldots, n-1\}$, so $k = 1+1+\cdots+1$ (k times). It shows that $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$ (again: the operation is the sum).

(d) (1) $(\mathbb{Z}/3\mathbb{Z},+)$: We simply looks at the subgroup generated by all possible 3 elements.
$\langle 0 \rangle = \{0\}$, so 0 is not a generator.
$\langle 1 \rangle = \{1, 2, 0\} = \mathbb{Z}/3\mathbb{Z}$, so 1 is a generator.
$\langle 2 \rangle = \{2, 4 = 1, 0\}$, so 2 is a generator.

(2) $(\mathbb{Z}/6\mathbb{Z},+)$: We simply looks at the subgroup generated by all possible 6 elements.
$\langle 0 \rangle = \{0\}$, so 0 is not a generator.
$\langle 1 \rangle = \{1, 2, 3, 4, 5, 6 = 0\} = \mathbb{Z}/6\mathbb{Z}$, so 1 is a generator.
$\langle 2 \rangle = \{2, 4, 0\}$, so 2 is not a generator.
$\langle 3 \rangle = \{3, 6 = 0\}$, so 3 is not a generator.
$\langle 4 \rangle = \{4, 8 = 2, 0\}$, so 4 is not a generator.
$\langle 5 \rangle = \{5, 10 = 4, 9 = 3, 8 = 2, 7 = 1, 6 = 0\}$, so 5 is a generator.

2. We apply the criterion seen in class:
(1) $C_G(a)$ is a subset of G by definition, and is non-empty since it contains e.
(2) We show that $C_G(a)$ is closed under products: Let $x, y \in C_G(a)$, i.e. $xa = ax$ and

$ya = ay$. Then $xya = xay = axy$, so $xy \in C_G(a)$.
(3) We show that $C_G(a)$ is closed under taking inverses: Let $x \in C_G(a)$, i.e. $xa = ax$. Then $a = x^{-1}ax$ and $ax^{-1} = x^{-1}a$, so $x^{-1} \in C_G(a)$.

3. Take for instance $\sigma = (1\ 3)$. Then $H\sigma = \{(1\ 3), (1\ 2)(1\ 3)\}$ and $\sigma H = \{(1\ 3), (1\ 3)(1\ 2)\}$. They are different since $(1\ 2)(1\ 3) \neq (1\ 3)(1\ 2)$.

4. Option 1: Directly from the definition of aH:

   "$\Rightarrow$" We show $aH \subseteq H$ and $H \subseteq aH$ (so that they are equal):
   Since $a \in H$ and H is a subgroup, we have $ax \in H$ for every $x \in H$, and thus $aH \subseteq H$.

   Let $h \in H$. We want to show that $h = ax$ for some $x \in H$. Solving for x we get $x = a^{-1}h$, and $x \in H$ since both a and h are in H.

   "$\Leftarrow$" Assume $aH = H$. Since $e \in H$, we have $a = ae \in aH = H$, so $a \in H$.

   Option 2: Using the equivalence relation $\sim_H$. Recall that bH is the equivalence class of b for this relation. Then

   $$aH = H \Leftrightarrow aH = eH \Leftrightarrow [a] = [e] \Leftrightarrow a \sim_H e \Leftrightarrow e^{-1}a \in H \Leftrightarrow a \in H.$$

5. (a) Since $a \in H$ and H is a subgroup, we have $-a \in H$, and then all possible sums of a and $-a$ are in H, so $a\mathbb{Z} \subseteq H$.

   (b) We have $r = n - aq$. We know that $n \in H$ and $-aq \in H$. Therefore $n + (-aq) = r \in H$.

   (c) If $r \neq 0$, then r is a positive element of H that is smaller that a. It contradicts the choice of a. Therefore $r = 0$, so $n = aq \in a\mathbb{Z}$.

   (d) The previous questions prove both $a\mathbb{Z} \subseteq H$ and $H \subseteq a\mathbb{Z}$.