MA10209 Algebra 1A

Sheet 10 Problems and Solutions v0: GCS

4-xii-11

The course website is http://people.bath.ac.uk/masgcs/diary.html

Hand in work to your tutor by 13:00, Monday December 12^{th}.

1. Let G be a group. Consider the map $s : G \longrightarrow G$ defined by $s(g) = g^2$. Prove that s is a homomorphism of groups if, and only if, G is abelian.
   Solution If s is a homomorphism, then for all $x, y \in G$ we have $s(xy) = s(x)s(y)$ and so $xyxy = x^2y^2$. Premultiply by x^{-1} and postmultiply by y^{-1}, and we discover that for all $x, y \in G$ we have $yx = xy$, and so G is abelian.

   Next assume instead that G is abelian. Then for all $x, y \in G$ we have $s(xy) = (xy)(xy) = x(yx)y = x(xy)y$, the final equality because G is abelian. Now for all $x, y \in G$ we have $s(xy) = (x^2)(y^2) = s(x)s(y)$ and so s is a homomorphism.

2. View the integers $\mathbb{Z}$ as a group under addition. Classify the subgroups of $\mathbb{Z}$ (i.e. describe them all in an organized way).
   Solution The integers are a cyclic group, all elements being "powers" (iterated additions and subtractions) of 1. We proved in lectures that a subgroup of a cyclic group must be cyclic. Notice that the cyclic group generated by 0 is a trivial group. If $n \in \mathbb{N}$, then the cyclic group generated by n is $\{kn \mid k \in \mathbb{Z}\}$, which is also the cyclic group generated by $-n$. The only issue that remains is whether the cyclic groups generated by two different natural numbers can be the same. This does not happen, because if $m, n \in \mathbb{N}$ and $m < n$, then m is not a multiple of n, but m is a multiple of m.

3. Let G be a group and suppose that X is a subset of G. Let $\langle X \rangle$ denote the intersection of all subgroups of G which contain the subset X. If $H = \langle X \rangle$, then we say that X *generates* H.

   (a) Prove that $\langle X \rangle$ is a subgroup of G.
   Solution We have already proved that the intersection of two subgroups of G is a subgroup. However, the difficulty (if you can call it that) here is that there may be arbitrarily many (possibly uncountably many) subgroups of G which contain X, so we cannot just use induction. Suppose that the set of subgroups of G which contain X is $\mathfrak{C}$. We must show that $Y = \cap_{H \in \mathfrak{C}} H \leq G$. First, observe that $G \in \mathfrak{C}$ so we cannot be in the awkward situation that $\mathfrak{C} = \emptyset$. Now $1 \in H$ for each $H \in \mathfrak{C}$ so $Y \neq \emptyset$. Next suppose that $y, z \in Y$. Then for all $H \in \mathfrak{C}$ we have $y, z \in H$ and so $yz^{-1} \in H$. Therefore $yz^{-1} \in Y$. The two (necessary and sufficient) conditions have been checked, and so Y is a subgroup of G.

(b) Prove that G is a cyclic group if, and only if, there is a singleton set $T = \{t\}$ such that $G = \langle T \rangle$.
Solution Suppose that G is cyclic, and consists of the powers of g. Let $T = \{g\}$. Now G is the unique subgroup of G which contains T, so $G = \langle T \rangle$.

On the other hand, suppose that $G = \langle T \rangle$ where $T = \{t\}$. Let H be the set of powers of t, so $\langle T \rangle \leq H \leq G$ so $H = G$ as required.

(c) Suppose that $H \leq G$. Prove that there is $Y \subseteq G$ such that $H = \langle Y \rangle$.
Solution Let $Y = H$. Since H is a group, $H \leq \langle H \rangle \leq H$ and so $H = \langle H \rangle$.

4. Consider the set $\mathbb{Q}$ of rational numbers viewed as an additive group. We use the notation $+$ for the group operation, and 0 for the identity element. Suppose that $q_1, q_2 \in \mathbb{Q}$. Borrowing the notation of Problem 3, prove that there is $q_3 \in \mathbb{Q}$ such that $\langle \{q_1, q_2\} \rangle \subseteq \langle \{q_3\} \rangle$.
Solution Suppose that $q_i = u_i/v_i$ where for $i = 1, 2$ we have $u_i, v_i \in \mathbb{Z}$ and $v_i \neq 0$. Let $q_3 = 1/v_1 v_2$, and this value of q_3 does the job.

5. Let n be a natural number, and write $\Omega_n = \{1, 2, \ldots, n\}$. Let S_n denote the collection of all bijections $f : \Omega_n \longrightarrow \Omega_n$. Now S_n is a group where the operation is composition of maps.

(a) Let H be the subset of S_5 consisting of all elements h of S_5 such that $h(1) = 1$. Is H a subgroup of S_5? Justify your answer.
Solution id $\in H$ so $H \neq \emptyset$. Now suppose that $h, k \in H$. Now $k(1) = 1$ so applying the map k^{-1} we have $1 = k^{-1}(1)$. Now $hk^{-1}(1) = h(k^{-1}(1)) = h(1) = 1$ so $hk^{-1} \in H$. The two necessary and sufficient conditions are satisfied, so $H \leq S_5$.

(b) Let K be the subset of S_6 consisting of all elements k of S_6 such that $k(1) = 2$. Is K a subgroup of S_6? Justify your answer.
Solution id $\notin K$ so K is not a subgroup of S_6.

(c) Let L be the subset of S_7 consisting of all elements l of S_7 such that $l(i) - i$ is even for every $i \in \Omega_7$. Is L a subgroup of S_7? Justify your answer.
Solution id $\in L$ so $L \neq \emptyset$. Suppose that $k, l \in L$. Choose any $i \in \Omega_7$. There is $j \in \Omega_7$ such that $l(j) = i$, and therefore $i - j$ is even. Now $kl^{-1}(i) = k(j)$ and $k(j) - j$ is even. Therefore $kl^{-1}(i) - i = k(j) - i = (k(j) - j) - (i - j)$ which is even because it is the difference of two even integers. Therefore $kl^{-1} \in L$ and so $L \leq G$.

(d) Let M be the subset of S_8 consisting of all elements m of S_8 such that $|\{i \mid i \in \Omega_8, m(i) = i\}|$ is even. Is M a subgroup of S_8? Justify your answer.
Solution In cycle notation, $(1, 2, 3, 4)$ and $(2, 3, 4, 5)$ are in M because they each fix four elements of Ω_8. However $(2, 3, 4, 5)(1, 2, 3, 4) = (1, 3, 5, 2, 4)$ which fixes three elements of M. Therefore M is not closed under composition, and so is not a subgroup.

6. Suppose that G, H are groups and that f_1, f_2 are homomorphisms from G to H Let $K = \{g \mid g \in G, f_1(g) = f_2(g)\}$. Prove that $K \leq G$.
Solution Observe that $f_1(1) = 1 = f_2(1)$ so $1 \in K \neq \emptyset$. Suppose that $k, l \in K$, then $f_1(kl^{-1}) = f_1(k) f_1(l)^{-1}$ since f_1 is a homomorphism. However $f_1(k) = f_2(k)$ and $f_1(l) = f_2(l)$ so $f_1(k) f_1(l)^{-1} = f_2(k) f_2(l)^{-1} = f_2(kl^{-1})$, the final equality because f_2 is a homomorphism. Therefore $kl^{-1} \in K$. Both conditions are satisfied, and so $K \leq G$.

7. Let G be a group and suppose that K a subgroup of G, and H is a subgroup of K. The sets X, Y and Z are subsets of G.

   (a) Suppose that $K = \cup_{y\in Y} Hy$ and $G = \cup_{z\in Z} Kz$. Define $YZ = \{yz \mid y \in Y, z \in Z\}$. Prove that $G = \cup_{t\in YZ} Ht$.
   Solution
   $$G = \cup_{z\in Z} Kz = \cup_{z\in Z} \left(\cup_{y\in Y} Hy\right) z$$
   $$= \cup_{z\in Z} \cup_{y\in Y} Hyz = \cup_{t\in YZ} Ht$$

   (b) Suppose that $G = \cup_{x\in X} Hx$. Show that $K = \cup_{x\in X\cap K} Hx$.
   Solution Clearly $\cup_{x\in X\cap K} Hx \subseteq K$. Of the other hand, if $k \in K$ then $k \in Hx$ for some $x \in X$. Therefore $k = hx$ for some $x \in X$ and so $x = h^{-1}k \in K$. We conclude that $K \subseteq \cup_{x\in X\cap K} Hx$. Therefore $K = \cup_{x\in X\cap K} Hx$.

   (c) Suppose that $G = \cup_{z\in Z} Kz$. Prove that $G = \cup_{z\in Z} z^{-1}K$.
   Solution Suppose that $g \in G$, so there is $z \in Z$ such that $g^{-1} = kz \in Kz$ for some $k \in K$. Now $g = z^{-1}k^{-1} \in z^{-1}K$ and we are done.

8. Suppose that A and B are subgroups of a group G. Let $AB = \{ab \mid a \in A, b \in B\}$. Define a map $\theta : A \times B \longrightarrow G$ by $\theta((a, b)) = ab$ for all $(a, b) \in A \times B$.

   (a) Suppose that $ab = a'b'$ for $a, a' \in A$ and $b, b' \in B$. Prove that $a^{-1}a' \in A \cap B$ so there is $c \in A \cap B$ such that $ac = a'$ and $c^{-1}b = b'$.
   Solution Since $ab = a'b'$, we have $a^{-1}a' = bb'^{-1} = c$. Now $a^{-1}a' \in A$ and $bb'^{-1} \in B$ so $c \in A \cap B$. Notice that $c^{-1} = b'b^{-1}$ so $b' = c^{-1}b$.

   (b) Suppose that $a \in A$ and $b \in B$ and $c \in A \cap B$. Prove that $ac \in A$, $c^{-1}b \in B$.
   Solution There is very little to say. This follows because c is an element both of A and of B, and each of A and B is a subgroup of G.

   (c) Suppose that G is finite. Deduce that all non-empty fibres of θ have the same size, and go on to conclude that
   $$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$
   Solution Parts (a) and (b) show that the fibre of $\theta((a, b))$ is $\{(ac, c^{-1}b) \mid c \in A \cap B\}$. Now if $c_1, c_2 \in A \cap B$ and $ac_1 = ac_2$, then $c_1 = c_2$ by the cancellation law (or by premultiplying by a^{-1}). Therefore each non-empty fibre of θ has size $A \cap B$, so
   $$|\text{Im } \theta| = \frac{|A \times B|}{|A \cap B|}$$
   and this is what is required.

   (d) Suppose that U and V are subgroups of the finite group G, and $|U|, |V| > \sqrt{|G|}$. Prove that $U \cap V$ is not a trivial group.
   Solution By part (c), we have
   $$|U \cap V| = \frac{|U| \cdot |V|}{|UV|} > \frac{\sqrt{|G|} \cdot \sqrt{|G|}}{|G|} = 1.$$
   Therefore $U \cap V$ has more than one element.

9. (Harder but not too hard) Let G be a group, and suppose that X is a subset of G. Let W denote the set of elements of G which have the form

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m}$$

where $m \in \mathbb{N}$, $x_i \in X$ for each $i = 1, 2, \ldots, m$ and $\varepsilon_i \in \{1, -1\}$ for each $i = 1, 2, \ldots, m$. Borrowing the notation of Problem 3, prove that $W \cup \{1\} = \langle X \rangle$.

Solution The set $W \cup \{1\}$ is visibly a subgroup of G (the $\{1\}$ is there just in case $X = \emptyset$, otherwise it is not necessary). Also if H is any subgroup of G which contains X, then it must contain $W \cup \{1\}$ because H is closed under taking inverses and the forming of products. Therefore $W \cup \{1\} \leq \langle X \rangle$. On the other hand, $X \subseteq W \cup \{1\} \leq G$ so $\langle X \rangle \leq W \cup \{1\}$. Therefore $\langle X \rangle = W \cup \{1\}$.

10. (Harder but not too hard) A group G is *finitely generated* if there is a finite subset X of G such that $G = \langle X \rangle$. Is the additive group of rational numbers a finitely generated group?

Solution Suppose that $\mathbb{Q}$ were finitely generated, say by $q_1, q_2, \ldots, q_n$, where for each i, $q_i = u_i/v_i$ for integers u_i, v_i where $v_i \neq 0$. Let $v = \prod_{i=1}^n v_i$. From Problem 9, we know that the group H generated by this set of rational numbers is the set

$$\left\{ \sum_{i=1}^{n} \lambda_i q_i \mid \lambda_i \in \mathbb{Z} \text{ for } i = 1, 2, \ldots, n \right\}.$$

We have converted the multiplicative "words" into additive notation, and then used the fact that group is abelian. Thus H is a subgroup of the cyclic group generated by $1/v$, so $1/2v \notin H$ and therefore $H \neq \mathbb{Q}$.