MA10209 Algebra 1A

Sheet 10 Solutions: GCS

3-xii-18

For materials associated with this course, please see `http://people.bath.ac.uk/masgcs/diary.html`

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 notes at the website 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. However, if $m, n \in \mathbb{N}$, then the index of $\langle n \rangle$ in $\mathbb{Z}$ is n, so groups generated by two different natural numbers are different.

3. 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 $q_1, q_2 \in \mathbb{Q}$.

   (a) Prove that there is $q_3 \in \mathbb{Q}$ such that $\langle \{q_1, q_2\} \rangle \leq \langle q_3 \rangle$, and that in fact there is $q_4 \in \mathbb{Q}$ such that $\langle \{q_1, q_2\} \rangle = \langle q_4 \rangle$.
   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 $q_3 = 1/v_1v_2$, and this value of q_3 does the job. Now we have proved that subgroup of a cyclic group is cyclic (we have proved this at the website), so there is $q_4 \in \mathbb{Q}$ such that $\langle \{q_1, q_2\} \rangle = \langle q_4 \rangle$.

   (b) Deduce that there is no finite subset S of $\mathbb{Q}$ such that $\mathbb{Q} = \langle S \rangle$.
   Solution Use part (a) and a finite induction argument to show that a subgroup of $\mathbb{Q}$ generated by a finite set of elements is cyclic. However, $\mathbb{Q}$ is not cyclic, because for each non-zero rational number q, we have $q/2 \notin \langle q \rangle$.

4. 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.

5. 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 $K \leq G$.

6. Suppose that $H \leq K \leq G$ are groups, and that $|G : K|$ and $|K : H|$ are both finite. Prove that $|G : H|$ is finite.
Solution There is a finite subset T of G such that $G = \cup_{t \in T} tK$ (use a transversal). There is also a finite subset S of K such that $K = \cup_{s \in S} sH$. The set of products ts is called TS and is finite. Now clearly $\cup_{u \in TS} uH \subseteq G$. Also if $g \in G$, there is $t \in T$ such that $g = tk \in tK$ for some $k \in K$. Now $k = sh \in sH$ for some $s \in S$ and $h \in H$. Therefore $g = tsh \in tsH$. Therefore $G \subseteq \cup_{u \in TS} uH \subseteq G$ so these inclusions can be replaced by equality symbols. Therefore $|G : H|$ is finite.

7. Let G be a finite group of order p^n where p is a prime number and n is a positive integer. Let G act on itself by conjugation.

(a) Show that every orbit has size p^m for some non-negative integer m.
Solution If x is in a conjugacy class, then the size of that conjugacy class is $|G : C_G(x)|$ which is a factor of p^n by Lagrange's theorem.

(b) Recall that the orbits of this action (the conjugacy classes) form a partition of G. By counting $|G|$ in two ways, prove that G contains at least one non-identity element which commutes with all elements of G.
Solution The order of G is p^n and the order of G is the sum of the sizes of its conjugacy classes. Therefore the number of conjugacy classes of size 1 must be a multiple of p. The identity element is one such conjugacy class, and so there must be at least $p - 1$ others, one

of which is $\{y\}$ say. Now $C_G(y)$ has index 1 in G so is G. Therefore y commutes with all elements of G.

8. Suppose that the finite group acts on the finite set X. For each $g \in G$, let Fix $g = \{x \mid g \cdot x = x\}$.

   (a) Consider the set $S \subseteq G \times X$ where $S = \{(g, x) \mid g \in G, x \in X, g \cdot x = x\}$. By counting the set in two ways, prove that $\sum_{g \in G} |\text{Fix } g| = \sum_{x \in X} |\text{stab}_G(x)|$.
   Solution You can either look at the number of points in X which are fixed by a particular $g \in G$, and sum over all $g \in G$, or you can note how many elements of G fix a particular $x \in X$, and then sum as x ranges over X.

   (b) Let U be an orbit of G acting on X. Prove that $\sum_{x \in U} |\text{stab}_G(x)| = |G|$.
   Solution Chose a particular $u \in U$. Now $|G : \text{stab}_G(x)| = |G : \text{stab}_G(u)|$ for each $x \in U$ because $|G : \text{stab}_G(x)| = |U|$ for each $x \in U$, so $\sum_{x \in U} |\text{stab}_G(x)| = |U| \cdot |\text{stab}_G(u)| = |G : \text{stab}_G(u)| \cdot |\text{stab}_G(u)| = |G|$ by Lagrange's theorem.

   (c) Deduce that the number of orbits of G acting on X is
   $$\frac{1}{|G|} \sum_{g \in G} |\text{Fix } g|,$$
   i.e. it is the average size of the number of fixed points of an element.
   Solution If there are t orbits, then
   $$\sum_{x \in X} |\text{stab}_G(x)| = t|G|.$$
   Now divide through by $|G|$ to obtain the lemma.

This result is sometimes known as Burnside's counting lemma, though in fact this enumeration principle significantly pre-dates William Burnside.

9. Verify Burnside's lemma (the previous problem) in various specific cases:

   (a) Prove that an element of S_n, chosen uniformly at random, has an average of 1 fixed point.
   Solution S_n has 1 orbit as it acts naturally on $\{1, 2, \ldots, n\}$. Therefore Burnside's counting lemma applies. As a check in a concrete case, try $n = 3$: id has 3 fixes points, each of the three transpositions has 1 fixed point and the two three cyclies have no fixed points. Now $(3 + 1 + 1 + 1)/6 = 1$ as expected.

   (b) Let G be the group of rotational symmetries of a cube, acting on either its vertices, edges, faces or grand diagonals. Show that in each case, an element of G chosen uniformly random, has an average of 1 fixed point.
   Solution The 24 elements of this group comprise: the identity element (fixes 8 vertices, 12 edges, 6 faces and 4 grand diagonals); 8 rotations through $\pm\frac{2\pi}{3}$ about a grand diagonal (each fixes 2 vertices, 0 edges, 0 faces and 1 grand diagonal); 6 rotations through $\pm\frac{\pi}{2}$ about an axis joining the centre of a face to the centre of the opposite face (each fixes 0 vertices, 0 edges, 2 faces and 0 grand diagonals); 3 rotations through π about an axis joining the centre of a face to the centre of the opposite face (each fixes 0 vertices, 0 edges, l faces and 0 grand diagonals); 6 rotations through π about an axis joining the centre of an edge to the centre of the opposite edge (each fixes 0 vertices, 2 edges, 0 faces and 2 grand diagonals). The vertex average is
   $$\frac{1 \times 8 + 8 \times 2}{24} = 1.$$

The edge average is

$$\frac{1 \times 12 + 6 \times 2}{24} = 1.$$

The face average is

$$\frac{1 \times 6 + 6 \times 2 + 3 \times 2}{24} = 1.$$

The grand diagonal average is

$$\frac{1 \times 4 + 8 \times 1 + 6 \times 2}{24} = 1.$$

10. (Challenge!) Consider the paintings of a cube, where the faces are monochromatic, and must each be red, white or blue. Two colourings of the faces of a cube are deemed to be equivalent if one painting of a cube can be rotated into the other. Recall that all 24 orientation-preserving (no reflections) rigid symmetries of a cube are actually rotations (about various axes of symmetry). Let G be this group of symmetries of a cube. Use Burnside's counting lemma to find out how many inequivalent such paintings of a cube there are. *You might want to practise on a painting of the faces using just two colours (say red and white). In this case one orbit consists of all red cubes, another of all white cubes. There is one orbit of 5 red faces and 1 white face, and another orbit of 1 red face and 5 white faces. There are two orbits of 2 red faces and 4 white faces (either the red faces share a common edge, or they are opposite). Similarly there are two orbits 4 red faces and 2 white faces. Finally there are two orbits of 3 red faces and 3 white faces (either there are two opposite red faces, or all three red faces are incident to the same vertex). Thus there are 10 orbits altogether. Now calculate this number again using (not) Burnside's counting lemma.*

Solution The 24 elements of this group comprise: the identity element; 8 rotations through $\pm\frac{2\pi}{3}$ about a grand diagonal; 6 rotations through $\pm\frac{\pi}{2}$ about an axis joining the centre of a face to the centre of the opposite face; 3 rotations through π about an axis joining the centre of a face to the centre of the opposite face; 6 rotations through π about an axis joining the centre of an edge to the centre of the opposite edge.

First do the toy problem, with just two colours. The group acts on the coloured cubes. The identity element fixes all 2^6 colourings. An element of the next type will fix colourings where the faces incident to an axis of symmetry at a particular vertex have the same colour, so there are 2^2 fixed points. Elements of the next type will fix colourings where the four faces through which the axis of symmetry does not pass have the same colour. There are 2^3 such colourings. Elements of the next type will fix colourings where there are four monochromatic regions, two faces, and two pairs of opposite faces. There are 2^4 such colourings. Elements of the last type will fix colourings where there are three monochromatic regions: two pairs of adjacent faces and one pair of opposite faces. There are 2^3 such regions.

By Burnside's lemma, the number of orbits of this group action is

$$\frac{2^6 + 8 \cdot 2^2 + 6 \times 2^3 + 3 \times 2^4 + 6 \times 2^3}{24} = \frac{64 + 32 + 48 + 48 + 48}{24} = \frac{240}{24} = 10$$

as predicted. We modify this for three colours, and obtain that the number of orbits (the number of essentially different colourings) is

$$\frac{3^6 + 8 \cdot 3^2 + 6 \times 3^3 + 3 \times 3^4 + 6 \times 3^3}{24} = \frac{729 + 72 + 162 + 243 + 162}{24} = \frac{1368}{24} = 57.$$