Imperial College London
Department of Mathematics

Solutions to Question Sheet 8

MATH40003 Linear Algebra and Groups — Term 2, 2019/20

This is the final problem sheet for this module (released on Wednesday of week 10). Questions 2 and 5 are suitable for tutorials. Material for questions 7, 8, 9 will be covered on Wednesday and Friday of week 11. Solutions will be released on Friday of week 11.

Question 1 Suppose that $(G, .)$ is a group and H is a subgroup of G of index 2.

(a) Prove that the two left cosets of H in G are H and $G \setminus H$.

(b) Show that for every $g \in G$ we have $gH = Hg$.

Solution: (a) Certainly H is one of the two left cosets of H in G. The other one, C, satisfies $H \cup C = G$ and $H \cap G = \emptyset$, as the left H-cosets partition G. So $C = G \setminus H$ and $C = gH$ for any $g \in G \setminus H$.

(b) There are two right cosets of H in G. One way to see this is that, for *any* subgroup H the map $gH \mapsto Hg^{-1}$ gives a well-defined bijection between the set of left cosets of H in G and the set of right H-cosets of H in G.

So by a similar argument to (a), we have that the two right cosets are H and $G \setminus H$. Thus if $g \in H$ we have $gH = H = Hg$ and if $g \in G \setminus H$, then $gH = G \setminus H = Hg$.

Question 2 Suppose $(G, .)$ is a group. Invent a test which allows you to check whether a subset $X \subseteq G$ is a left coset (of some subgroup of G). Prove that your test works.

Solution: Note that, by definition, X is a left coset iff there exists a subgroup $H \leq G$ and $g \in G$ with $gH = X$. Note that in this case, $g^{-1}X = H$, for any $g \in X$. So X is a left coset iff $X \neq \emptyset$ and for every (or equivalently, for some) $g \in X$ we have that $g^{-1}X$ is a subgroup of G. Of course, we can use the usual test from the notes to check whether this is a subgroup.

You could finish the answer here, or go on to write down what this means in terms of X.

We have to check that if $x_1, x_2 \in X$ then:
(i) $g^{-1}x_1g^{-1}x_2 \in g^{-1}X$, that is, $x_1g^{-1}x_2 \in X$;
(ii) $(g^{-1}x_1)^{-1} = x_1^{-1}g \in g^{-1}X$, that is $gx_1^{-1}g \in X$.

Question 3 Let X be any non-empty set and $G \leq \mathrm{Sym}(X)$. Let $a \in X$ and $H = \{g \in G : ga = a\}$ and $Y = \{g(a) : g \in G\}$.

(a) Prove that $H \leq G$ and for $g_1, g_2 \in G$ we have

$$g_1H = g_2H \Leftrightarrow g_1(a) = g_2(a).$$

Deduce that there is a bijection between the set of left cosets of H in G and the set Y. In particular, if G is finite, then $|G|/|H| = |Y|$.

(b) Use (a) to justify why the order of the group G of rotations of a cube (as in Question sheet 7) is 24.
[Hint: let X be the set of 6 faces of the cube, or the set of 8 vertices of the cube.]

Solution: (a) From the notes, or below, we know that $g_1H = g_2H \Leftrightarrow g_1^{-1}g_2 \in H$. But $g_1^{-1}g_2 \in H \Leftrightarrow g_1^{-1}g_2(a) = a \Leftrightarrow g_2(a) = g_1(a)$, as required.

The map $gH \mapsto g(a)$ gives the required bijection.

[This result is a version of the *Orbit - Stabiliser Theorem.*]

(b) Let X be the set of 6 faces, labelled $1, \ldots, 6$. In the notation of (a), let a be the face 1. Note that any face can be moved to any other face by a suitable rotation, so $Y = \{1, \ldots, 6\}$. Let $H = G_1$, the subgroup of rotations fixing face 1. Clearly this has order 4. By (a), there are 6 left cosets of H in G, so it follows that $|G| = 6.4 = 24$.

Question 4 Let G be a finite group of order n, and H a subgroup of G of order m.

(a) For $x, y \in G$, show that $xH = yH \Longleftrightarrow x^{-1}y \in H$.

(b) Suppose that $r = n/m$. Let $x \in G$. Show that there is an integer k in the range $1 \le k \le r$, such that $x^k \in H$.

Solution:

(a) Suppose $xH = yH$. Then $x \in yH$, and so $x = yh$ for some $h \in H$. But now $x^{-1}y = h^{-1}y^{-1}y = h^{-1}$, and so $x^{-1}y \in H$. Conversely, suppose that $x^{-1}y \in H$. Then $x^{-1}y = h$ for some $h \in H$, and now $y = xh$. So $y \in xH \cap yH$, and so $xH = yH$ (since distinct cosets contain no common elements).

(b) There are r distinct cosets of H in G, and so the cosets $H, xH, x^2H, \ldots, x^rH$ cannot be distinct (or there would be $r + 1$ of them). So we must have $x^iH = x^jH$ for some $0 \le j < i \le r$. But now we have $x^{i-j} \in H$ by (a). So set $k = i - j$; then clearly $1 \le k \le r$ as required.

Question 5 Prove that the following are homomorphisms:

(i) G is any group, $h \in G$ and $\phi : G \to G$ is given by $\phi(g) = hgh^{-1}$.

(ii) $G = \mathrm{GL}_n(\mathbb{R})$ and $\phi : G \to G$ is given by $\phi(g) = (g^{-1})^T$.

(Here $\mathrm{GL}_n(\mathbb{R})$ is the group of invertible $n \times n$-matrices over $\mathbb{R}$ and the ^{T} denotes transpose.)

(iii) G is any abelian group and $\phi : G \to G$ is given by $\phi(g) = g^{-1}$.

(iv) $\phi : (\mathbb{R}, +) \to (\mathbb{C}^\times, \cdot)$ given by $\phi(x) = \cos(x) + \mathrm{i}\sin(x)$.

In each case say what is the kernel and the image of ϕ. In which cases is ϕ an isomorphism?

Solution: (i) $\phi(g_1)\phi(g_2) = hg_1h^{-1}hg_2h^{-1} = hg_1g_2h^{-1} = \phi(g_1g_2)$, so ϕ is a homomorphism. As $\phi(g) = e \Leftrightarrow hgh^{-1} = e \Leftrightarrow g = e$, the kernel of ϕ is the trivial subgroup $\{e\}$. As $\phi(h^{-1}gh) = g$, ϕ is surjective. (Thus ϕ is an isomorphism.)

(ii) $\phi(g_1g_2) = ((g_1g_2)^{-1})^T = (g_2^{-1}g_1^{-1})^T = (g_1^{-1})^T(g_2^{-1})^T = \phi(g_1)\phi(g_2)$ (which properties of matrices are being used here?). Note that $\phi(g) = h$ iff $g = (h^{-1})^T$ so ϕ is a bijection: the kernel is $\{e\}$, and ϕ is surjective.

(iii) As G is abelian, $\phi(g_1g_2) = g_2^{-1}g_1^{-1} = g_1^{-1}g_2^{-1} = \phi(g_1)\phi(g_2)$. Again, ϕ is an isomorphism.

(iv) To see that ϕ is a homomorphism, note that $\phi(x) = \exp(ix)$ and use the fact that $\exp(i(x+y)) = \exp(ix)\exp(iy)$ (or write it out in full and use trig formulae). The kernel is $\{2\pi n : n \in \mathbb{Z}\}$ and ϕ is surjective.

Question 6 (a) Use the inclusion - exclusion principle to give a formula for the number of permutations in S_n which have no fixed points. Prove that the proportion of such permutations in S_n tends to $1/e$ as $n \to \infty$.

(b) Give a formula for the number of permutation in S_n which have one fixed point.

(c) A standard deck of 52 cards is shuffled at random. What (approximately) is the probability that at least one card is still in the same place after the shuffle?

Solution: (a) Perhaps you did the inclusion - exclusion principle in the Introductory or Probability and Statsistics module. If not, you should have looked on the internet (eg. at the Wikipedia article), or looked in a book. Suppose $A_1, \ldots, A_n$ are subsets of a set S. If $I \subseteq \{1, \ldots, n\}$ is non-empty let $A_I = \bigcap_{i \in I} A_i$. Then

$$|\bigcup_{i=1}^{n} A_i| = -\sum_{I} (-1)^{|I|} |A_I|,$$

where the sum is over all non-empty subsets I of $\{1, \ldots, n\}$.

Let $S = S_n$ and for $i = 1, \ldots, n$ let A_i be the set of permutations in S_n fixing i. Note that $\bigcup_{i=1}^{n} A_i$ is the set of permutations fixing at least one point, which is the complement in S_n of the set we are interested in. Moreover, A_I is the set of permutations fixing all points in I: so this has size $(n - |I|)!$ It follows that the set of permutations in S_n which fix no point has size

$$d(n) = \left(n! + \sum_{k=1}^{n} (-1)^k \binom{n}{k} (n-k)! \right) = n! \left(1 + \sum_{k=1}^{n} (-1)^k \frac{1}{k!} \right)$$

The familiar Taylor series for e^x then shows that $d(n)/n! \to e^{-1}$ as $n \to \infty$.

(b) A permutation in S_n fixes exactly the point i if and only if it fixes i and gives a fixed point-free permutation of the remaining $n-1$ points. So there are $d(n-1)$ such permutations and therefore exactly $nd(n-1)$ permutations in S_n fixing exactly one point.

(c) The probability that no card is in the same place is $d(52)/52!$ which is approximately $1/e$. So the probability that at least one card is still in the same place is approximately $1 - 1/e$.

Question 7 (a) Write down all of the cycle shapes of the elements of S_5. For each cycle shape, calculate how many elements there are with that shape. (Check that your answers add up to $|S_5| = 120$.)

(b) How many elements of S_5 have order 2?

(c) How many subgroups of size 3 are there in the group S_5?

Solution:

(a)

	Shape	Example	Formula	Number
1	(1^5)	id		1
2	$(2^1 1^3)$	$(1\,2)$	$\binom{5}{2}$	10
3	$(3^1 1^2)$	$(1\,2\,3)$	$2\binom{5}{3}$	20
4	$(2^2 1^1)$	$(1\,2)(3\,4)$	$\frac{1}{2}\binom{5}{2}\binom{3}{2}$	15
5	$(4^1 1^1)$	$(1\,2\,3\,4)$	$3!\binom{5}{4}$	30
6	$(3^1 2^1)$	$(1\,2)(3\,4\,5)$	$2\binom{5}{3}$	20
7	(5^1)	$(1\,2\,3\,4\,5)$	$4!$	24

(b) Cycle shapes 2 and 4 in the table give elements of order 2, so there are $10+15 = 25$ of them.

(c) A subgroup of H order 3 must be cyclic, since if $g \in H \setminus \{e\}$ then $H = \{e, g, g^2\}$. The elements of order 3 are those with cycle shape 3 in the table. There are 20 of these, and each cyclic subgroup of order 3 contains two of them. Moreover, two distinct subgroups of order 3 intersect only in the trivial group. So there are 10 subgroups of order 3.

Question 8 What is the largest order of an element of S_8?

Solution: Consider the possible cycle shapes of an element of S_8. The one giving the largest order is the shape $5^1 3^1$. An element of this cycle shape has order 15.

Question 9 Let G be a group, and let S be a subset of G. Recall that we say that S *generates* G if every element in G can be written as a product of elements of S and their inverses.

(i) Let $2 \leq k \leq n$. Show that a k-cycle $(a_1 \, \ldots, \, a_k)$ in S_n can be written as a product of $k-1$ distinct cycles of length 2. Deduce that the set of 2-cycles in S_n generates S_n.

(ii) (Harder) Let α be the n-cycle $(1234\ldots n)$ and β the 2-cycle (12). Prove that $\langle \alpha, \beta \rangle = S_n$.

[Hint: $\alpha\beta\alpha^{-1} = (23)$. Use tricks like this.]

Solution: (i) We have

$$(a_1 \, a_2 \, \cdots \, a_k) = (a_1 \, a_2)(a_2 \, a_3) \cdots (a_{k-1} \, a_k).$$

So any cycle is a product of 2-cycles. Since every element of S_n is a product of cycles, we see that every element is a product of 2-cycles. So the set of 2-cycles generates S_n.

(ii) By (i), it suffices to show that every 2-cycle is in $\langle \alpha, \beta \rangle$. We may assume $n \geq 3$. Note that $\alpha\beta\alpha^{-1} = (23)$ and similarly $\alpha(23)\alpha^{-1} = (34)$, etc. So using this repeatedly, we obtain $(12), (23), \ldots, (n-1, n), (n1) \in \langle \alpha, \beta \rangle$. But then note that $(13) = (23)(12)(23)$, $(14) = (34)(13)(34)$, etc . Repeating this we obtain $(1k) \in \langle \alpha, \beta \rangle$ for all $2 \leq k \leq n$. But then for $j \neq k$ we have $(1j)(1k)(1j) = (jk) \in \langle \alpha, \beta \rangle$.