Imperial College London
Department of Mathematics

Solutions to Question Sheet 7 - Probl. Class week 10

MATH40003 Linear Algebra and Groups — Term 2, 2022/23

Problem sheet released on Monday of week 9. All questions can be attempted before the problem class on Monday in Week 10. Solutions will be released on week 10 after the problem classes.

Question 1 Let $\mathbb{F}_p$ denote the field of integers modulo p, for p a prime number. Find an element of order p in $\mathrm{GL}_2(\mathbb{F}_p)$. Can you also find an element of order $2p$?

Solution: A matrix with order p is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. If $p > 2$ then a matrix with order $2p$ is $\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$. If $p = 2$ then

$$\mathrm{GL}_2(F_2) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\}$$

and it is easy to check that none of these has order 4. (Or use Lagrange's Theorem.)

Question 2 Suppose that G is a finite group which contains elements of each of the orders $1, 2, \ldots, 10$. What is the smallest possible value of $|G|$? Find a group of this size which does have elements of each of these orders.

Solution: By a corollary to Lagrange's theorem, $|G|$ must be divisible by each of $1, \ldots, 10$. So the smallest possible value for $|G|$ is $\mathrm{lcm}(1, \ldots, 10)$, which is $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$. The cyclic group of order 2520 has elements of each of these orders, since if g is a generator, and if d is any divisor of 2520, then $g^{2520/d}$ has order d.

Question 3 Suppose $n \in \mathbb{N}$ and recall from the Introductory module that $\mathbb{Z}_n$ is the notation for the set $\{[r]_n : r \in \mathbb{Z}\}$ of residue classes modulo n. If n is clear from the context, we write $[r]$ instead of $[r]_n$. We denote by $\mathbb{Z}_n^\times$ the subset consisting of elements with a multiplicative inverse.

(i) Show that $(\mathbb{Z}_n, +)$ is a cyclic group of order n.

(ii) Show that $(\mathbb{Z}_n^\times, .)$ is an abelian group of order $\phi(n)$, where ϕ is the Euler totient function. Find the smallest value of n for which this group is not cyclic.

(iii) Show that if p is an odd prime, then $\mathbb{Z}_p^\times$ has exactly one element of order 2.

(iv) Show that if p is a prime number with $p \equiv 4 \bmod 5$, then the inverse of $[5]$ in $\mathbb{Z}_p^\times$ is $\left[\frac{p+1}{5}\right]$.

Solution: (i) Checking the group axioms was essentially done in the Intro module. Note that $[1]_n$ is a generator of the group.

(ii) The main thing to check about the group axioms is that multiplication gives a binary operation. This is the usual proof that (for associative operations) a product of invertible things has an inverse. For the order of the group, observe that $[k]_n$ has a multiplicative inverse iff $gcd(k, n) = 1$ (find this in the Intro module) and then the result follows. The smallest value of n where this group is not cyclic is $n = 8$ (if n is a prime the group will be cyclic as then $\mathbb{Z}_n$ is a field and we can apply a result below; $n = 2, 6$ give groups of order 1 and 2 respectively). Here the group has order 4 and all non-identity elements have order 2 (do the calculations!).

(iii) If $[x]^2 = [1]$ then p divides $x^2 - 1 = (x + 1)(x - 1)$. So either p divides $x - 1$ or p divides $x + 1$. In the first case, $[x] = [1]$ which has order 1. So $[x]$ has order 2 only in the second case, when $[x] = [-1]$.

(iv) Just check that $[5] \cdot \left[\frac{p+1}{5}\right] = [p + 1] = [1]$.

Question 4 (i) Suppose $(G, .)$ is a finite abelian group and for every $k \in \mathbb{N}$ we have

$$|\{g \in G : g^k = e\}| \leq k.$$

By using Euler's totient function, or otherwise, prove that G is cyclic.
(ii) Suppose F is a field and G is a finite subgroup of the multiplicative group $(F^\times, .)$. Using (i), prove that G is cyclic.
(iii) Prove that if p is a prime number and $p \equiv 1 (\operatorname{mod} 4)$, then there is $k \in \mathbb{N}$ with $k^2 \equiv -1 (\operatorname{mod} p)$.

Solution: (i) Let $n = |G|$. We show that G has an element of order n. Note that if $g \in G$ then its order d divides n. Moreover $H = \langle g \rangle$ has d elements and for every $h = g^m \in H$, we have $h^d = g^{md} = e$. So by our assumption, H contains all elements of order d. As H is a cyclic group of order d, it follows that the number of elements of order d in H (and therefore in G) is $\phi(d)$. Thus, if $d|n$, then the number of elements of G of order d is 0 or $\phi(d)$. By Cor 1.23, we have $\sum_{d|n} \phi(d) = n$. Thus if $d|n$, then number of elements of G of order d is $\phi(d)$ (not 0). In particular, there are $\phi(n)$ elements of G of order n. As $\phi(n) \neq 0$, G is therefore cyclic.

(ii) If F is a field then there are at most k solutions $x \in F$ to the equation $x^k = 1$ (see 5.2.6 in the Linear Algebra notes). So G satisfies the conditions in (i).

(iii) Consider the field $\mathbb{F}_p$ and the group $G = \mathbb{F}_p^\times$. By (ii), G is cyclic, of order $p - 1$. Let y be a generator and $z = y^{(p-1)/4}$. Then $z^2 \neq [1]$ and $(z^2)^2 = z^4 = [1]$. So $z^2 = [-1]$ and this gives the result.

Question 5 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 6 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 7 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 $xH = yH \iff x^{-1}y \in H$.

(b) Suppose that $r = n/m$. Let $x \in G$. Show that there is an integer k in the range $1 \leq k \leq r$, 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 $0 \leq j < i \leq r$. But now we have $x^{i-j} \in H$ by (a). So set $k = i - j$; then clearly $1 \leq k \leq r$ as required.

Question 8 Let X be any non-empty set and $G \leq \mathrm{Sym}(X)$. Let $a \in X$ and $H = \{g \in G : g(a) = a\}$ and $Y = \{g(a) : g \in G\}$.

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

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

(b) 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 $|G|/|H| = |Y|$.

Solution: (a) From the notes, or the previous question, 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.

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

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

Question 9 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 not surjective as its image is the unit circle.