Imperial College London
Department of Mathematics

Solutions to Question Sheet 7

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

Problem sheet released on Wednesday of week 9. All questions can be attempted before the problem class on Monday Week 10. Questions 1 and 3 are suitable for tutorials. Solutions will be released on Wednesday of week 10.

Question 1 Prove that if $\{q_1, \ldots, q_k\}$ is any finite subset of $\mathbb{Q}$, then the subgroup $\langle q_1, \ldots, q_k \rangle$ is cyclic. Deduce that this is not equal to $\mathbb{Q}$.

Solution: Let $\{q_1, \ldots, q_k\}$ be a finite subset of $\mathbb{Q}$. Let $d_1, \ldots, d_k$ be the denominators, when $q_1, \ldots, q_k$ are expressed in lowest terms. Then each of $q_1, \ldots, q_k$ is in the cyclic subgroup generated by $1/\ell$, where ℓ is $\mathrm{lcm}(d_1, \ldots, d_k)$. So $\langle q_1, \ldots, q_k \rangle$ is a subgroup of a cyclic group and is therefore cyclic. But $\langle 1/\ell \rangle$ is not $\mathbb{Q}$, since it contains only rational numbers whose denominators divide ℓ. So $\{q_1, \ldots, q_k\}$ does not generate $\mathbb{Q}$.

Question 2 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 3 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 4 Suppose G is a group and $a, b \in G$ are of order 2. Let $c = ab$ and suppose that c has finite order $m \geq 3$.

(a) Prove that $aca = c^{-1}$ and deduce that for all $n \in \mathbb{N}$ we have $ac^n a = c^{-n}$.

(b) Show that $H = \{a^s c^t : s = 0, 1 \text{ and } 0 \leq t < m\}$ is a subgroup of G of order $2m$.

Solution: (a) Note that $a^{-1} = a$ and $b^{-1} = b$. Then

$$aca^{-1} = aca = aaba = ba = (ab)^{-1} = c^{-1}.$$

It follows that $c^{-n} = (aca^{-1})^n = ac^n a$, as required.

(b) To show that it is a subgroup note that $(a^s c^t)(a^\sigma c^\tau)$ is equal to $a^s c^{t+\tau}$ if $\sigma = 0$ and (by (b)) $a^{s+\sigma} c^{t-\tau}$ if $\sigma = 1$. This is in H. We can similarly show that H is closed under taking inverses.

Clearly H has at most $2m$ elements. We need to show that there are exaclty $2m$. If $(a^s c^t) = (a^\sigma c^\tau)$ for $\sigma, s = 0, 1$ and $0 \leq \tau, t < m$, then we show $s = \sigma$ and $t = \tau$. If $s \neq \sigma$ then a is a power of c and so commutes with c. It follows from (a) that $m = 2$ - a contradiction. So $s = \sigma$ and as c has order m, it then follows that $t = \tau$.

[Remark: It now follows that H is isomorphic to the dihedral group D_{2m}.]

Question 5 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 2). 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 6 (a) Find the remainder when 5^{110} is divided by 13.

(b) Find the inverses of $[2]$ and of $[120]$ in $\mathbb{Z}_{9871}^\times$. (The number 9871 is prime.)

(c) Use Fermat's Little Theorem to show that $n^{17} \equiv n \bmod 255$ for all $n \in \mathbb{Z}$.

(d) Prove that if p and q are distinct prime numbers then

$$p^{q-1} + q^{p-1} \equiv 1 \bmod pq.$$

Solution:

(a) Observe that $5^2 = 25 \equiv -1 \bmod 13$. So $5^4 \equiv 1 \bmod 13$, and so the order of $[5]$ in $\mathbb{Z}_{13}^*$ is 4. Now we have

$$5^{110} = 5^{4\cdot 27+2} \equiv 1^{27} \times 5^2 \equiv 12 \bmod 13.$$

So the remainder is 12.

(b) Observe that $9871 + 1 = 9872 = 2 \times 4936$. So $2^{-1} = 4936$. Use the Euclidean algorithm to calculate $120^{-1} = 7321$.

(c) Note that $255 = 3 \cdot 5 \cdot 17$. By FLT we have $n^p \equiv n \bmod p$ for all $n \in \mathbb{Z}$. So

$$n^{17} = n^{15} \cdot n^2 \equiv n^5 \cdot n^2 \equiv n^6 \cdot n \equiv n^2 \cdot n \equiv n^3 \equiv n \bmod 3,$$

$$n^{17} = n^{15} \cdot n^2 \equiv n^3 \cdot n^2 \equiv n^5 \equiv n \bmod 5.$$

So $n^{17} - n$ is divisible by each of 3, 5 and 17, and so it is divisible by their lowest common multiple, which is 255.

(d) We have $p^{q-1} \equiv 1 \bmod q$. Since $q^{p-1} \equiv 0 \bmod q$, we have $p^{q-1} + q^{p-1} \equiv 1 \bmod q$, and so q divides $p^{q-1} + q^{p-1} - 1$. But we also have that p divides $p^{q-1} + q^{p-1} - 1$, by an exactly similar argument. So pq divides $p^{q-1} + q^{p-1} - 1$, and so $p^{q-1} + q^{p-1} \equiv 1 \bmod pq$.

Question 7 (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) Prove that if p is a prime number and $p \equiv 1 (\bmod\, 4)$, then there is $k \in \mathbb{N}$ with $k^2 \equiv -1 (\bmod\, 4)$.

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) Consider the field $\mathbb{F}_p$ and the group $G = \mathbb{F}_p^\times$. As the polynomial $x^k = 1$ has at most k distinct roots in any field, G satisfies the condition in (i) and so 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 8 Describe the group G of rotational symmetries of a cube, saying what the possible axes of rotation are and what the possible angles of rotation are. Hence show that there are 24 such rotational symmetries. Consider one of the three pairs of opposite faces of the cube. Show that the set of rotational symmetries of the cube which send this pair of faces to itself forms a subgroup of G of order 8.

Solution: You should draw some pictures for this.

The possibilities are:

(i) Axis of rotation through centres of a pair of opposite faces; angle of rotation π. There are 3 symmetries of this type.

(ii) Axis of rotation through centres of a pair of opposite faces; angle of rotation $\pm\pi/2$. There are 6 symmetries of this type.

(iii) Axis of rotation through mid-points of a pair of (diametrically) opposite edges; angle of rotation π. There are 12 edges, so 6 such pairs of edges, and therefore 6 symmetries of this type.

(iv) Axis of rotation through mid-points of (diametrically) opposite vertices; angle of rotation $\pm 2\pi/3$. There are 4 such axes, so 8 symmetries of this type.

Adding in the identity element, we get $1 + 3 + 6 + 6 + 8 = 24$ rotational symmetries.

For the final part, note that, by inspection, the rotations which send the pair of faces to itself are the rotations about an axis through the centres of the faces (4 of these, type (i), (ii) above); rotations through π about axis through centres of pairs of opposite edges between the faces (2 of these, type (iii)); rotation through π about an axis through one of the other pairs of opposite faces (2 of these, type (i) above). This gives 8 symmetries in total.