Imperial College London
Department of Mathematics

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 $\mathbb{Q}$.

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 $2p$?

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.

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 $2m$.

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 $\left[\frac{p+1}{5}\right]$.

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

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

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 $p \equiv 1 (\mathrm{mod}\, 4)$, then there is $k \in \mathbb{N}$ with $k^2 \equiv -1 (\mathrm{mod}\, 4)$.

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.