Imperial College London
Department of Mathematics

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 $2p$?

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.

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

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 $k^2 \equiv -1 (\operatorname{mod} p)$.

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.

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 $gH = Hg$.

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 $1 \le k \le r$, such that $x^k \in H$.

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

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

$$g_1 H = g_2 H \Leftrightarrow g_1(a) = g_2(a).$$

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

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?