Math 3140 - Assignment 5

Due February 21, 2024

These problems are review for Midterm 1 on February 21. Do them before the exam!

(1) Compute the multiplicative inverses of the following if they exist:
  (a) $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ in $\mathrm{GL}(2, \mathbb{R})$
  (b) $b = (2\ 3\ 4)(1\ 2\ 3)$ in S_4 (give a decomposition in disjoint cycles)
  (c) $c = [9]$ in $\mathbb{Z}_{25}$

Solution
  (a) Recall from Linear Algebra:
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = \frac{1}{1 \cdot 4 - 2 \cdot 3} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix}$$
  (b) First compute $b = (1\ 3)(2\ 4)$. Then $b^{-1} = b$.
  (c) Use the extended Euclidean algorithm to solve $x9 + y25 = 1$ for $x \in \mathbb{Z}$. Then $c^{-1} = [x] = [14]$.

(2) Prove or disprove:
$\mathbb{Z}$ with the operation $x \oplus y := x + y + 3$ for $x, y \in \mathbb{Z}$ is a group.

Solution This is a group since
  (a) $\oplus$ maps integers to integers,
  (b) $\oplus$ inherits associativity from $(\mathbb{Z}, +)$,
  (c) -3 is the identity for $\oplus$ because $x \oplus (-3) = x = (-3) \oplus x$ for all $x \in \mathbb{Z}$,
  (d) every $x \in \mathbb{Z}$ has an inverse $x^{-1} \in \mathbb{Z}$ such that $x \oplus x^{-1} = -3$, namely $x^{-1} = x - 6$.

(3) For G a permutation group on X and $x \in X$, the **stabilizer** of x in G is
$$\mathrm{stab}_G(x) := \{g \in G \ : \ g(x) = x\}.$$
Show that $\mathrm{stab}_G(x)$ is a subgroup of G.

Solution $\mathrm{stab}_G(x)$ is a subgroup since it's non-empty, closed under multiplication and inverses:
  (a) $() \in \mathrm{stab}_G(x) \neq \emptyset$,
  (b) for $f, g \in \mathrm{stab}_G(x)$ we see $f(g(x)) = x$ and $f \circ g \in \mathrm{stab}_G(x)$,

(c) for $f \in \mathrm{stab}_G(x)$ we see $f^{-1}(x) = x$ and $f^{-1} \in \mathrm{stab}_G(x)$.

(4) The **exponent** of a group G is the smallest $n > 0$ such that $g^n = 1$ for all $g \in G$ if it exists; else the exponent of G is infinite.
Show that every group G of exponent 2 is abelian.

Solution Let G have exponent 2, let $a, b \in G$. Then

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

and G is abelian.

(5) Let $(G, \cdot)$ be a group and $g \in G$. Show that

$$a_g \colon G \to G,\ x \mapsto gx,$$

is a permutation on G. Is a_g a homomorphism on G?

Solution a_g is bijective (hence a permutation) since it has an inverse $a_g^{-1} = a_{g^{-1}}$.
For $x, y \in G$,

$$a_g(xy) = gxy \quad \text{and} \quad a_g(x)a_g(y) = gxgy$$

are equal only if $g = 1$. Hence a_g is a homomorphism iff $g = 1$.

(6) Let $(G, \cdot)$ be a group and $S \subseteq G$. Show that the subgroup generated by S consists of all finite products of integer powers of elements in S, i.e.

$$\langle S \rangle = \{a_1^{k_1} \cdots a_n^{k_n} \ :\ n \geq 0, k_1, \ldots, k_n \in \mathbb{Z}, a_1, \ldots, a_n \in S\}$$

Hint: Show that if a subgroup H contains S, then it also contains all products of powers of elements in S.
Conversely, show that the set of products of powers of elements in S is a subgroup of G.

Solution Let $H := \{a_1^{k_1} \cdots a_n^{k_n} \ :\ n \geq 0, k_1, \ldots, k_n \in \mathbb{Z}, a_1, \ldots, a_n \in S\}$.
$\supseteq$: Since $\langle S \rangle$ is closed under multiplication and inverses, we have

- $a \in S \ \Rightarrow\ a^k \in \langle S \rangle$ for all $k \in \mathbb{Z}$ and further
- $a_1, \ldots, a_k \in S \ \Rightarrow\ a_1^{k_1} \cdots a_n^{k_n} \in \langle S \rangle$ for all $k_1, \ldots, k_n \in \mathbb{Z}$.

Hence $\langle S \rangle \supseteq H$.
$\subseteq$: Since $\langle S \rangle$ is the smallest subgroup containing S, it suffices to show that H is a subgroup that contains S:

- $S \subseteq H$ is clear.
- For $a_1^{k_1} \cdots a_n^{k_n}, b_1^{\ell_1} \cdots b_m^{\ell_m} \in H$ we see that $a_1^{k_1} \cdots a_n^{k_n} b_1^{\ell_1} \cdots b_m^{\ell_m} \in H$.

- For $a_1^{k_1} \cdots a_n^{k_n} \in H$ we see that $(a_1^{k_1} \cdots a_n^{k_n})^{-1} = a_n^{-k_n} \ldots a_1^{-k_1}$ is also in H.

Hence H is a subgroup and contains $\langle S \rangle$.

(7) Assume that a group G contains elements of all orders between 1 and 10. What is the smallest possible order of G?

Solution By Lagrange's Theorem, $|G|$ is a multiple of all integers between 1 and 10. Hence the smallest possible order of G is the least common multiple of $1, \ldots, 10$, that is, $\text{lcm}(1, 2, \ldots, 10) = 8 \cdot 9 \cdot 5 \cdot 7$.

(8) Let G be a nontrivial group that has no proper, nontrivial subgroups (i.e. 1 and G are the only subgroups of G). Show that $|G|$ is prime.

Hint: Do not assume at the outset that G is finite.

Solution: Let $a \in G, a \neq 1$. Then $\langle a \rangle$ is a nontrivial subgroup of G. Hence $\langle a \rangle = G$ is cyclic.

Now G cannot be infinite because otherwise $\langle a^2 \rangle$ is a proper nontrivial subgroup.

So G is finite, say of order n. For $d|n$, the subgroup $\langle a^d \rangle$ must either be 1 or G. In the former case $d = n$, in the latter $d = 1$. Anyways, n is only divisible by 1 and by n. Thus n is prime. $\square$