MTH 236, Spring 2024 - Homework 4

Due on Friday, February 16 at 11:59pm on gradescope

Question 1. Recall that $\mathrm{GL}_2(\mathbb{R})$ is the group of all invertible 2×2 real matrices (under multiplication).

(a) Let $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Find all elements of the cyclic group $\langle A \rangle$ in $\mathrm{GL}_2(\mathbb{R})$.

(b) Let $z = \frac{1}{2} + \frac{\sqrt{3}}{2}i$. Find all elements of the cyclic group $\langle z \rangle$ in $\mathbb{C}^* = \langle \mathbb{C}^*, \cdot \rangle$.

Question 2. Let $k \in \mathbb{Z}_+$ and let $\theta = \frac{2\pi}{k}$, so that the complex number $z = e^{i\theta} = \cos\theta + i \sin\theta$ is a generator of the cyclic group U_k. Let $f : U_k \to M_{2,2}(\mathbb{R})$ be defined for all $n \geq 0$ by

$$f(z^n) = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix}.$$

Observe that f is defined on all of U_k, because every element of U_k is a power of z.

(a) Prove that f is well-defined, that is, if $z^n = z^m$, then $f(z^n) = f(z^m)$. (If this were not true, then f would not actually be a function!)

(b) Prove that the image (or the range) H of f is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. (In order to do this, first you have to show that H is a subset of $\mathrm{GL}_2(\mathbb{R})$. In showing that H is a subgroup, some elementary trig identities will be useful.)

(c) Prove that f is an isomorphism from U_k to H.

Question 3. Let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \in \mathrm{GL}_2(\mathbb{R})$. Show that $\langle A \rangle$ is isomorphic to $\mathbb{Z} = \langle \mathbb{Z}, + \rangle$.

Question 4. Let G be a group and let H be a subset of G. Consider the relation $\sim$ defined on G by $a \sim b$ if $a^{-1}b \in H$. In HW 3, you showed that if H is a subgroup of G, then $\sim$ is an equivalence relation. Now show instead that if $\sim$ is an equivalence relation, then H must be a subgroup of G.

Question 5. In HW 1 we introduced the "modulo n" equivalence relation on $\mathbb{Z}$ for the integer $n \geq 2$, defined by $x \sim y$ if $x - y = nq$ for some $q \in \mathbb{Z}$. Recall that $\overline{x} = \{y \in \mathbb{Z} : y \sim x\}$.

(1) Use the division algorithm to show that there are exactly n equivalence classes under $\sim$, which are $\overline{0}, \overline{1}, \ldots, \overline{n-1}$.

(2) Let S be the set of equivalence classes of $\sim$. Define a binary operation $+$ on S in the following way: to add the classes C_1 and C_2, pick any $x_1 \in C_1$ and $x_2 \in C_2$, and define

$$C_1 + C_2 = \overline{x_1 + x_2}.$$

Show that $C_1 + C_2$ always gives the same equivalence class as output no matter which $x_1 \in C_1$ and $x_2 \in C_2$ are chosen. (In other words, $+$ is a well-defined operation on S.)

(3) Prove that $\langle S, + \rangle$ is a cyclic group of order n. (First, show it is a group!)

Question 6. True or false? Justify your answers, with examples where necessary.

(a) Every cyclic group has a unique generator.

(b) Any element of a cyclic group is a generator of the group.

(c) The quadratic equation $x^2 = e$ has at most two solutions in any group.

(d) The quadratic equation $x^2 = e$ has at most two solutions in any cyclic group.

(e) There exists an abelian group of order n for all $n > 0$.

(f) If $G \neq \{e\}$ is a cyclic group with only 1 generator, then $|G| = 2$.

Question 7. Recall that $\mathbb{Z}_8$ is the group $\{0, 1, 2, \ldots, 7\}$ under addition mod 8.

(a) Write down all the elements of the cyclic subgroups $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, $\langle 5 \rangle$, $\langle 6 \rangle$ and $\langle 7 \rangle$.

(b) Which elements of $\mathbb{Z}_8$ are generators of the entire group?

Question 8. Draw subgroup diagrams of $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{12}$.

Question 9. Let $G \neq \{e\}$ be a group whose only subgroups are $\{e\}$ and G. Prove that G must be cyclic, then prove that its order is prime.

Question 10. Find 3 cyclic groups of 3 different finite orders such that each one has precisely 4 generators.