Math 562/662 **Exam 2**
Spring 2022 **Fri Apr 1**

No electronic devices are allowed. There are 4 pages and each page is worth 6 points, for a total of 24 points.

Problem 1. Consider a group homomorphism $\varphi : (G, *, \varepsilon) \to (G', \bullet, \delta)$.

(a) Prove that $\varphi(\varepsilon) = \delta$.

Proof. We apply φ to the identity $\varphi * \varphi = \varphi$:

$$\begin{aligned} \varepsilon * \varepsilon &= \varepsilon && \text{group property} \\ \varphi(\varepsilon * \varepsilon) &= \varphi(\varepsilon) && \\ \varphi(\varepsilon) \bullet \varphi(\varepsilon) &= \varphi(\varepsilon) && \text{homomorphism property} \\ \varphi(\varepsilon)^{-1} \bullet \varphi(\varepsilon) \bullet \varphi(\varepsilon) &= \varphi(\varepsilon)^{-1} \bullet \varphi(\varepsilon) && \text{group property} \\ \varphi(\varepsilon) &= \delta. && \end{aligned}$$

□

(b) Prove that $\varphi(a^{-1}) = \varphi(a)^{-1}$.

Proof. We apply φ to the identity $a * a^{-1} = \varepsilon$:

$$\begin{aligned} a * a^{-1} &= \varepsilon && \text{group property} \\ \varphi(a * a^{-1}) &= \varphi(\varepsilon) && \\ \varphi(a) \bullet \varphi(a^{-1}) &= \varphi(\varepsilon) && \text{homomorphism property} \\ \varphi(a) \bullet \varphi(a^{-1}) &= \delta && \text{part (a)} \\ \varphi(a)^{-1} \bullet \varphi(a) \bullet \varphi(a^{-1}) &= \varphi(a)^{-1} \bullet \delta && \text{group property} \\ \varphi(a^{-1}) &= \varphi(a)^{-1}. && \end{aligned}$$

□

(c) Assuming that the inverse function $\varphi^{-1} : G' \to G$ exists, prove that φ^{-1} is also a group homomorphism.

Proof. Given $a', b' \in G'$, let $a = \varphi^{-1}(a')$ and $b = \varphi^{-1}(b')$, so that $\varphi(a) = a'$ and $\varphi(b) = b'$. Then we have

$$\begin{aligned} \varphi^{-1}(a' \bullet b') &= \varphi^{-1}(\varphi(a) \bullet \varphi(b)) && \\ &= \varphi^{-1}(\varphi(a * b)) && \varphi \text{ is a homomorphism} \\ &= a * b && \\ &= \varphi^{-1}(a') * \varphi^{-1}(b'). && \end{aligned}$$

□

Problem 2. Let $\omega = e^{2\pi i/6}$ and let $(\Omega_6, \times, 1)$ be the group of 6th roots of unity. Write down the elements of every subgroup of Ω_6, expressed in terms of ω.

Note that $\Omega_6 = \langle \omega \rangle = \{\omega^0, \omega^1, \omega^2, \omega^3, \omega^4, \omega^5\} = \{\omega^1, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$. The Fundamental Theorem of Cyclic Groups tells us that every subgroup has the form $\Omega_d = \langle \omega^{6/d} \rangle$ for some divisor $d|6$. Hence the subgroups are

$$\begin{aligned} \Omega_6 &= \{\omega^1, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}, \\ \Omega_3 &= \{\omega^2, \omega^4, \omega^6\}, \\ \Omega_2 &= \{\omega^3, \omega^6\}, \\ \Omega_1 &= \{\omega^6\}. \end{aligned}$$

Problem 3. Let $H \subseteq G$ be a normal subgroup.

(a) Prove that the following operation on cosets is well-defined: $(aH)(bH) := (ab)H$.

Proof. Suppose that $a_1H = a_2H$ and $b_1H = b_2H$, so that $a_1^{-1}a_2 \in H$ and $b_1^{-1}b_2 \in H$. Our goal is to show that $(a_1b_1)^{-1}(a_2b_2) \in H$, and hence $(a_1b_1)H = (a_2b_2)H$.

Let's write $a_1^{-1}a_2 = h_1 \in H$ and $b_1^{-1}b_2 = h_2 \in H$. Since $H \subseteq G$ is normal, we also have $h_1b_2 = b_2h_3$ for some $h_3 \in H$. Therefore

$$\begin{aligned} (a_1b_1)^{-1}(a_2b_2) &= b_1^{-1}a_1^{-1}a_2b_2 \\ &= b_1^{-1}h_1b_2 \\ &= b_1^{-1}b_2h_3 \\ &= h_2h_3 \in H. \end{aligned}$$

□

(b) The operation from part (a) makes the set of cosets G/H into a group. Use this to prove that H is the kernel of some group homomorphism $\varphi : G \to G'$.

Proof. Consider the function $\varphi : G \to G/H$ defined by $\varphi(a) := aH$. This function is a group homomorphism by definition of the group product on G/H:

$$\varphi(ab) = (ab)H = (aH)(bH) = \varphi(a)\varphi(b).$$

Since $H \in G/H$ is the identity element of the quotient group, we have

$$\begin{aligned} \ker \varphi &= \{a \in G : \varphi(a) = H\} \\ &= \{a \in G : aH = H\} \\ &= \{a \in G : a \in H\} \\ &= H. \end{aligned}$$

Problem 4. Consider a group $(G, *, \varepsilon)$. For any element $a \in G$ and integer $k \in \mathbb{Z}$ we can define an element $a^k \in G$ in such a way that $\varphi(k) = a^k$ is a group homomorphism from $(\mathbb{Z}, +, 0)$ to $(G, *, \varepsilon)$. Denote the image by $\langle a \rangle = \operatorname{im} \varphi \subseteq G$.

(a) Use the First Isomorphism Theorem to prove that $\langle a \rangle$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some integer $n \geq 0$.

Proof. Consider the group homomorphism $\varphi : \mathbb{Z} \to G$ defined by $\varphi(k) = a^k$. The kernel is a (normal) subgroup of $\mathbb{Z}$, hence it has the form $\ker \varphi = n\mathbb{Z}$ for some unique integer $n \geq 0$. Then the First Isomorphism Theorem gives

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\ker \varphi \cong \operatorname{im} \varphi = \langle a \rangle \subseteq G.$$

□

(b) Let $p \geq 2$ be prime. Prove that any group G of size p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. [Hint: Choose some non-identity element $a \in G$. Apply Lagrange's Theorem to the subgroup $\langle a \rangle \subseteq G$.]

Proof. Let $p \geq 2$ be prime and let G be a group of size p. Since $\#G \geq 2$ there exists some non-identity element $a \in G$. Consider the non-trivial subgroup $\{\varepsilon\} \neq \langle a \rangle \subseteq G$. From Lagrange's Theorem we know that $\#\langle a \rangle | \#G = p$. Since p is prime and $\#\langle a \rangle \neq 1$, this implies that $\#\langle a \rangle = p$, and hence $\langle a \rangle = G$.

From part (a) we know that $\langle a \rangle \cong \mathbb{Z}/n\mathbb{Z}$ for some $n \geq 0$. Finally, since $p = \#\langle a \rangle = \#(\mathbb{Z}/n\mathbb{Z}) = n$ we must have $G = \langle a \rangle \cong \mathbb{Z}/p\mathbb{Z}$. □