MATH 111A HOMEWORK 6 SOLUTIONS

---

7) Let $H \leq G$ and define a relation $\sim$ on G by $a \sim b$ if and only if $b^{-1}a \in H$. Prove that $\sim$ is an equivalence relation and describe the equivalence classes for each $a \in G$. Use this to prove Proposition 4.

Solution. First we show that $\sim$ is an equivalence relation, i.e. it is reflexive, symmetric, and transitive.

(i) Reflexivity: For any $a \in G$, we have $a^{-1}a = 1 \in H$ because H is a subgroup of G, whence $a \sim a$.

(ii) Symmetry: If $a \sim b$ then $b^{-1}a \in H$. Since H is closed under inverses, we have

$$a^{-1}b = (b^{-1}a)^{-1} \in H \quad \text{whence} \quad b \sim a \text{ also.}$$

(iii) Transitivity: If $a \sim b$ and $b \sim c$ then $b^{-1}a \in H$ and $c^{-1}b \in H$. Since H is closed under multiplication,

$$c^{-1}a = (c^{-1}b)(b^{-1}a) \in H \quad \text{whence} \quad a \sim c \text{ also.}$$

Next we show that the equivalence class $[a]$ of any $a \in G$ is the left coset aH. Indeed, we have

$$\begin{aligned}
b \in [a] &\iff b \sim a \\
&\iff b^{-1}a \in H \\
&\iff b^{-1}a = h \quad \text{for some } h \in H \\
&\iff b = ah^{-1} \quad \text{for some } h \in H \\
&\iff b = ah \quad \text{for some } h \in H \quad \text{(because } H \text{ is closed under inverses)} \\
&\iff b \in aH.
\end{aligned}$$

Finally, we use this to prove Proposition 4. Recall that:

Proposition 4. *Let N be any subgroup of the group G. The set of left cosets N in G form a partition of G. Furthermore, for all $u, v \in G$ we have $uN = vN$ if and only if $v^{-1}u \in N$ and in particular, $uN = vN$ if and only if u and v are representatives of the same coset.*

Let $\sim$ be the relation on G given by $u \sim v$ if and only if $v^{-1}u \in N$. Then $[u] = uN$ by the above. There are two claims to prove (the claim after "in particular" follows from claim (ii)).

(i) The set of left cosets N in G form a partition of G: It is a fact (from Math 8 for example) that the equivalence classes of an equivalence relation on G form a partition of G. Since the left cosets N are the equivalence classes of $\sim$ the claim follows.

(ii) $uN = vN$ if and only if $v^{-1}u \in N$ for all $u, v \in G$: By definition of equivalence classes, we have

$$[u] = [v] \iff u \sim v, \text{ that is, } uN = vN \iff v^{-1}u \in N.$$

---

11) Let $H \leq K \leq G$. Prove that $[G : H] = [G : K][K : H]$ (do not assume G is finite).

Solution. Let S be a set of (left) coset representatives of K in G. Define a map

$$f : S \times K/H \to G/H$$

by setting $f(g, kH) = gkH$ for $g \in S$ and $k \in K$. Since

$$[G : H] = |G/H|,\ [G : K] = |G/K| = |S|,\ \text{and}\ [K : H] = |K/H|$$

by definition, it suffices to show that f is well-defined and bijective.

(i) Well-defined: If $k_1H = k_2H$ then $gk_1H = gk_2H$ and so $f(g, k_1H) = f(g, k_2H)$.

(ii) Injectivity: If $f(g_1, k_1H) = f(g_2, k_2H)$ then $g_1k_1H = g_2k_2H$. We deduce that

$$\begin{aligned} g_1k_1 \in g_2k_2H &\implies g_1k_1 \in g_2k_2K \quad (\text{since } H \leq K) \\ &\implies g_1 \in g_2K \quad (\text{since } k_1, k_2 \in K) \\ &\implies g_1 \text{ and } g_2 \text{ represents the same left coset of } K \text{ in } G \\ &\implies g_1 = g_2 \quad (\text{since } g_1, g_2 \in S). \end{aligned}$$

Consequently, $g_1k_1H = g_2k_2H \implies k_1H = k_2H$, and so $(g_1, k_1H) = (g_2, k_2H)$, proving injectivity.

(iii) Surjectivity: Let $gH \in G/H$ and consider the coset gK. We have $gK = \tilde{g}K$ for some $\tilde{g} \in S$ by definition of S. So we can write $g = \tilde{g}k$ for some $k \in K$. Then, $(\tilde{g}, kH) \in S \times K/H$ and

$$f(\tilde{g}, kH) = \tilde{g}kH = gH,$$

which proves that f is surjective.

This proves that f is bijective and completes the proof.

---

22) Use Lagrange's Theorem in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ to prove *Euler's Theoreme*: $a^{\varphi(n)} \equiv 1 \pmod{n}$ for every integer a relatively prime to n, where φ denotes the Euler's φ-function.

Solution. Recall that $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \mid (a, n) = 1\}$ (see Proposition 4 on p.10 for example). So, if $a \in \mathbb{Z}$ and $(a, n) = 1$, then $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $\langle\overline{a}\rangle \leq (\mathbb{Z}/n\mathbb{Z})^\times$. By Lagrange's Theorem, we have

$$|\langle\overline{a}\rangle| \text{ divides } |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

Since $|\langle\overline{a}\rangle| = |\overline{a}|$ (proved previously in class) and $|(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ by definition, we deduce that

$$|\overline{a}| \text{ divides } \varphi(n) \implies \overline{a}^{\varphi(n)} = \overline{1} \implies a^{\varphi(n)} \equiv 1 \pmod{n},$$

as desired.

---

4) Let $G = \langle x\rangle$ be a finite cyclic group of order m, i.e. $G = \{x^n \mid n \in \mathbb{Z}\}$ with $|x| = m < \infty$.

a) Prove that $G \simeq \mathbb{Z}/m\mathbb{Z}$.

Proof. Let $\varphi : \mathbb{Z} \to G$ be defined by $\varphi(n) = x^n$. It is a homomorphism because

$$\varphi(n + m) = x^{n+m} = x^nx^m = \varphi(n)\varphi(m)$$

and is clearly surjective because $G = \{x^n \mid n \in \mathbb{Z}\}$. The kernel of φ is the subgroup

$$\begin{aligned} \ker(\varphi) &= \{n \in \mathbb{Z} \mid x^n = 1\} \\ &= \{n \in \mathbb{Z} \mid m \text{ divides } n\} \quad (\text{because } |x| = m) \\ &= m\mathbb{Z}. \end{aligned}$$

Hence, by the first isomorphism theorem, we have $\mathbb{Z}/m\mathbb{Z} \simeq G$.

b) For every positive divisor k of m there exists a subgroup H of G with $|G/H| = k$.

Proof. Let $k \in \mathbb{N}$ be a divisor of m and write $k = nm$ for $n \in \mathbb{N}$. Then $|x^k| = n$ (see Proposition 5 on p. 57; you may also cite that it was proved in class) and so $|\langle x^k \rangle| = |x^k| = n$. Taking $H = \langle x^k \rangle$, we have

$$|G/H| = |G|/|H| = m/n = k$$

by Lagrange's Theorem, as desired.
