Dillan Marroquin
MATH 331.1001
Midterm Review

Definitions

Definition. A **group** $(G, *, e)$ is a set G equipped with a binary operator $*$ and an identity element $e \in G$ such that the following hold:

1. Associativity: $(ab)c = a(bc) \forall a, b, c \in G$
2. Existence of Identity: $\exists e \in G$ such that $ae = ea = a \forall a \in G$
3. Existence of Inverses: Given $a \in G, , \exists b \in G$ such that $ab = ba = e$.

Definition. Let $(G, *)$ be a group. A **subgroup** of G is a subset $H \subset G$ such that

1. $e \in H$
2. $x, y \in H \Rightarrow x * y \in H$
3. $x \in H \Rightarrow x^{-1} \in H$.

Definition. Let G be a group and $a \in G$. The subset $\langle a \rangle := \{a^k | k \in \mathbb{Z}\}$ is a subgroup of G called the **cyclic subgroup** generated by a. A group is **cyclic** iff $a \in G$ such that $G = \langle a \rangle$.

Definition. Let $(G, *, e_G)$ and $(H, \circ, e_H)$ be groups. A **group homomorphism** between G and H is a function $\varphi : G \to H$ such that $\forall a, b, \in G$, $\varphi(a * b) = \varphi(a) \circ \varphi(b)$.

Definition. A function $\varphi : G \to H$ is a **group isomorphism** iff φ is bijective and a homomorphism. $G \cong H$ iff G and H are isomorphic.

Definition. For $x \in G$, the **left coset** containing x is $xH := \{xh | h \in H\} \subset G$. (Note that $y \in xH$ implies $yH = xH$).

Definition. Let G be a group, $H \leq G$ a subgroup. Denote G/H as the **SET of left cosets** of H in G. The size of this set is the **index** of H in G, denoted $[G : H] = |G/H|$.

Definition. Let $\varphi : G \to H$ be a group homomorphism. The **kernel** of φ is the subset of G $\ker \varphi = \{x \in G | \varphi(x) = e_H\}$.

Examples

Example. $\mathbb{Z}/n := \{[0], [1], \ldots, [n-1]\}$ set of equivalence classes of $\equiv \pmod{n}$ on $\mathbb{Z}$.

Example. $GL_n(\mathbb{R}) := \{n \times n \text{ matrix } A | \det(A) \neq 0\}$. $(GL_n(\mathbb{R}), \cdot, I_n)$ is an abelian group.

Theorems

Proposition (8.3 ($\Leftarrow$ Direction))**.** Let G be a group, and $H \subseteq G$ a subset. Then H is a subgroup iff $H \neq \emptyset$ and $\forall a, b \in H$, $ab^{-1} \in H$.

Proof. ($\Leftarrow$) Assume $H \neq \emptyset$ and $\forall a, b \in H$, $ab^{-1} \in H$. Observe that $H \neq \emptyset$ implies $\exists x \in H$. Let $a = b = x$. Then $xx^{-1} = e \in H$. Now verify Axiom 3: Let $x \in H$. We want to show $x^{-1} \in H$. Let $a = e$ and $b = x$. Then $ab^{-1} = ex^{-1} \in H$ by assumption. This implies $x^{-1} \in H$. For Axiom 2, let $x, y \in H$. Set $a = x$. We know $y^{-1} \in H$ by proof of Axiom 3. Therefore $x((y^{-1})^{-1} = xy \in H$. ■

Theorem (13.1)**.** If $|G| = p$ for p prime, then G is cyclic. In particular, $\forall a \in G - \{e\}$, $G = \langle a \rangle$.

Proof. Let $a \in G \setminus \{e\}$. Corollary 12.6 (if G is a finite group, then $\forall a \in G$, $|a|\big||G|$) implies $|a|\big|p$ since $p = |G|$. Therefore $|a| = 1$ or $|a| = p$. Since $a \neq e$, then $|a| = p$. Proposition 12.5 (if $|a| = n$ for $a \in G$, then $|\langle a \rangle| = |a|$) implies $|\langle a \rangle| = p = |G|$. Therefore $G = \langle a \rangle$. ∎

Theorem (15.3)**.** If $G = \langle a \rangle$ is cyclic order n, then $G \cong \mathbb{Z}/n$.

Proof. Suffices to construct a group isomorphism $\varphi : \mathbb{Z}/n \to G$. Let $\varphi([k]) = a^k$. First we check if φ is well-defined. Suppose $l \in [k]$. WTS $\varphi([k]) = \varphi([l])$, i.e. that $a^k = a^l$. We have $l \in [k]$ which implies $l \equiv k \pmod{n}$. Therefore $\exists m \in \mathbb{Z}$ such that $l - k = nm$ which implies $a^{l-k} = a^{nm} = (a^n)^m = e^m = e$. Therefore $a^{l-k} = e$ which implies $a^l = a^k$.
Now we show φ is a group homomorphism: $\varphi([k] + [l]) = \varphi([k + l]) = a^{k+l} = a^k a^l = \varphi([k]) + \varphi([l])$.
Next we show φ is surjective. Note that the image of $\varphi(\mathbb{Z}/n) = \{\varphi([k]) | [k] \in \mathbb{Z}/n\} = \{a^k | [k] \in \mathbb{Z}/n\} = G$. Thus φ is surjective.
Finally, we show φ is injective: Suppose $\varphi([k]) = \varphi([l])$. Then $a^k = a^l$ which implies $a^{k-l} = e$ and by Lemma 14.3 (), we have $n | k - l$. So $k \equiv l \pmod{n}$ and thus $[k] = [l]$. ∎

Problem Sets