Abstract Algebra
Lecture 4
Monday, 9/13/2010

1 Group Homomorphisms

Defn: Let $(G, *)$, and $(G', \star)$ be groups. A map of sets $\phi : G \to G'$ is a **homomorphism** if

$$\phi(a * b) = \phi(a) \star \phi(b)$$

for all $a, b \in G$.

Ex: Let V, W be vector spaces, and let $L : V \to W$ be a linear transformation. For any $v_1, v_2 \in V$, we have $L(v_1 + v_2) = L(v_1) + L(v_2)$. So, for the groups $(V, +)$ and $(W, +)$, L is a homomorphism.

Ex: Let G be a group. Define $I = I_G$ by $I(a) = a$ for all $a \in G$. This is known as the Identity map.

Ex: Let $\phi : \mathbb{Z} \to \mathbb{Z}_n$ be given by $\phi(r) = r \mod n$. Then ϕ is a group homomorphism. Note that, for $a, b \in \mathbb{Z}$, we have $(a + b) \mod n = (a \mod n + b \mod n) \mod n$. We are allowed the additional "wrapper" $\mod n$ because the addition operation is modular addition.

Theorem: Fact:

$$\forall n \in \mathbb{N}, \exists a, b, c, d \in \mathbb{Z} \text{ such that } n = a^2 + b^2 + c^2 + d^2$$

Question: can this be done with 3 squares?
Proposition: No. There are infinitely many positive integers which are not the sum of three squares. In fact, this is true for all n such that $n = 7 \mod 8$.

Proof: Choose n such that $n = 7 \mod 8$. If $n = a^2 + b^2 + c^2$, then $n \mod 8 = (a^2 \mod 8 + b^2 \mod 8 + c^2 \mod 8) \mod 8$. If a is even, then $a^2 \mod 8 = 0, 4$. If a is odd, then $a^2 \mod 8 = 1$. The same holds for b and c. So our set of possible numbers is $\{0, 1, 4\}$. There is no combination of these three numbers that can add to $7 \mod 8$. Our original supposition must have been false, so 3 numbers is insufficient. ∎

Ex: Let $\psi : S_n \to \mathbb{Z}_2$ be given by

$$\psi(\sigma) = \begin{cases} 0, & \sigma \text{ even} \\ 1, & \sigma \text{ odd} \end{cases}$$

Where σ even means that σ can be written as a composition of an even number of 2-cycles (recall from last week).

$$\psi(\sigma \cdot \tau) = \psi(\sigma)\psi(\tau)$$

Note that we must be doing addition modulo 2 in $\mathbb{Z}_2$, because if we were doing multiplication, we would have two identity elements, which just should not happen.

Defn: Let $\phi : G \to G'$ be a homomorphism. Then G is the domain of ϕ, and G' is the codomain of ϕ.

Theorem: Let $\phi : G \to G'$ be a homomorphism. For all $a \in G$, $n \in \mathbb{Z}$, the following are true:

1. $\phi(1_G) = 1_{G'}$, i.e. $\phi(1) = 1$
2. $\phi(a)^{-1} = \phi(a^{-1})$
3. $\forall a_1, \ldots, a_n \in G, \phi(a_1 \cdots a_n) = \phi(a_1) \cdots \phi(a_n)$
4. $\phi(a)^m = \phi(a^m)$

Proof:

1. $\phi(1) \cdot \phi(1) = \phi(1 \cdot 1) = \phi(1)$. Now, $\exists \phi(1)^{-1} \in G'$, so $\phi(1) = 1$ (Be very careful of the domain / codomain distinction here.)
2. $\phi(a)\phi(a^{-1} = \phi(aa^{-1}) = \phi(1) = 1$. Because inverses are unique, it must be that $(\phi(a))^{-1} = \phi(a^{-1})$.
3. etc.
4. etc. some more

■

Theorem: Let $\phi : G \to G'$, $\psi : G' \to G''$ be homomorphisms. Then $\psi \circ \phi : G \to G''$ is a homomorphism.

Proof: Let $a, b \in G$. Then $(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b)$. ■

Defn: An **isomorphism** is a bijective homomorphism. We say that $G \cong G'$ if G is isomorphic to G'.

Theorem: Let $\phi : G \to G'$ be a homomorphism. Then the following are equivalent:

- ϕ is an isomorphism
- $\exists \psi : G' \to G$ such that $\psi \circ \phi = I_G$ and $\phi \circ \psi = I_{G'}$.

If ψ is one such map of sets, then is ψ a group homomorphism?

Ex:

- $G \cong G$
- exp: $(\mathbb{R}, +) \xrightarrow{\sim} (\mathbb{R}^+, \times)$. The two homomorphisms are $e^{a+b} = e^a \cdot e^b$, and the inverse is $\ln(a \cdot b) = \ln(a) + \ln(b)$.
- $D_n \cong \mathcal{D}_{2n}$ (Recall that the book uses D_{2n} to notate what Dagan calls $\mathcal{D}_{2n}$.)
- $S_3 \cong D_3$.

Defn: An **endomorphism** of G is a homomorphism from G to itself. An **automorphism** of G is an isomorphism from G to itself.

Theorem: The automorphisms of a group for a group themselves, under composition. We denote this group $\text{Aut}(G)$

Note: If G is not Abelian, then $\text{Aut}(G)$ is not trivial.

Theorem: Let G be a group. For all $a \in G$, the map $\alpha_a : G \to G$ given by $\alpha_a(x) = axa^{-1}$ for all $x \in G$ is an automorphism of G. Also, the map $\alpha : G \to \text{Aut}(G)$ given by $\alpha(a) \to \alpha_a$ is a group homomorphism.

Proof: We want to show that α_a is a homomorphism. Let $x, y \in G$. Inspect $\alpha_a(xy) = axya^{-1} = ax(1)ya^{-1} = axa^{-1}aya^{-1} = alpha_a(x)\alpha_a(y)$. Consider $\alpha_{a^{-1}}$. We want to show $\alpha_a\alpha_{a^{-1}} = I = \alpha_{a^{-1}}\alpha_a$. We compute $\alpha_a\alpha_{a^{-1}}(x) = \alpha_a(a^{-1}xa) = a(a^{-1}xa)a^{-1} = x$. Therefore α_a is an endomorphism with an inverse, so it is an automorphism.
Now, let $a, b \in G$. Then $\alpha(ab) = \alpha_{ab}$. Let $x \in G$. Then $\alpha_{ab}(x) = abx(ab)^{-1} = abxb^{-1}a^{-1} = \alpha_a(\alpha_b(x)) = \alpha_a \circ \alpha_b(x)$, as desired. ∎