NOTES ON GROUPS, MATH 369.101

Group homomorphisms

Suppose that we consider a finite group G (say that $|G| = n$), and suppose that G is cyclic. Then there is some $a \in G$ so that $\langle a \rangle = G$. So

$$G = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Notice that if $i + j \geq n$, then $a^{i+j} = a^i a^j$ is equal to a power of a that is smaller than $i + j$. For example, $a^1 a^{n-1} = a^n = e = a^0$ and $a^3 a^{n-1} = a^2$. The formal way to say it is:

$$i + j \equiv k (\text{mod } n) \qquad \text{if and only if} \qquad a^{i+j} = a^k.$$

So in some sense our cyclic group G works just like the cyclic group $\mathbb{Z}_n$, though the elements and operations are different.

Definition 1. Say $(G_1, *)$ and $(G_2, \cdot)$ are groups with their associated operations. A function $\varphi : G_1 \to G_2$ is a group homomorphism if it preserves the operation. That is:

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b) \qquad \text{for any } a, b \in G_1.$$

If $\varphi : G_1 \to G_2$ is a homomorphism that is bijective, then φ is called an isomorphism.

Proposition 1. *Given a homomorphism $\varphi : G_1 \to G_2$, let e_i be the identity of G_i. Then $\varphi(e_1) = e_2$ and φ is one-to-one if and only if* $\ker \varphi = \{e_1\}$.

Proof. For any $x \in G_1$, $\varphi(x)\varphi(e_1) = \varphi(xe_1) = \varphi(x)$. Multiplying on the left by $\varphi(x)^{-1}$ we get that $\varphi(e_1) = \varphi(x)^{-1}\varphi(x) = e_2$.

(Note, as a consequence, that $\varphi(x^{-1}) = \varphi(x)^{-1}$ since $\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e_1) = e_2$.)

If φ is one-to-one and $x \in \ker \varphi$, then $\varphi(x) = e_2 = \varphi(e_1)$ implies $x = e_1$ and so e_1 is the only element of the kernel. If $\ker \varphi = \{e_1\}$, then if there is $\varphi(x) = \varphi(y)$ then (using that φ is a homomorphism, and that $\varphi(y^{-1}) = \varphi(y)^{-1}$, $\varphi(xy^{-1}) = e_2$ and so $xy^{-1} = e_1$, which implies $x = y$. $\square$

Proposition 2. *The composition of two homomorphisms (isomorphisms) is another homomorphism (isomorphism).*

The inverse of an isomorphism is an isomorphism.

Proposition 3. *Given a homomorphism $\varphi : G_1 \to G_2$, the image $\varphi(G_1)$ is a subgroup of G_2.*

Date: Nov. 16, Nov. 21.

Example 1: We've considered the group $(\mathbb{Z}_9)^\times$ before, which has elements $\{1, 2, 4, 5, 7, 8\}$ and multiplication modulo 9 as an operation.

Notice that $\langle 2 \rangle = (\mathbb{Z}_9)^\times$ (since $2^2 = 4$, $2^3 = 8$, $2^4 \equiv 7$, $2^5 \equiv 5$, and $2^6 \equiv 1$). With the observations about a cyclic group in mind, we define a homomorphism

$$\varphi : (\mathbb{Z}_9^\times, \cdot) \to (\mathbb{Z}_6, +)$$

by saying: if $a \in (\mathbb{Z}_9)^\times$ is equal to $a = 2^k$, then define $\varphi(a) = [k]$, the congruence class mod 6 of k. (We included the notation of the operations just to clarify what the group operation was on each side.

Claim: φ is well-defined and an isomorphism.

We need to be careful, since there are more than one way to write a given element a as 2^k in $\mathbb{Z}_9^\times$. To this end, suppose that $2^j \equiv 2^k$ in $\mathbb{Z}_9^\times$. Then by a Proposition from a previous class, j is congruent to k mod $o(2)$. Since the order of 2 is 6, $j \equiv k \pmod 6$ and so $\varphi(2^j)$ and $\varphi(2^k)$ agree in $\mathbb{Z}_6$.

φ is a homomorphism: if $a = 2^k$ and $b = 2^l$ then

$$\varphi(a \cdot b) = \varphi(2^{k+l}) = [k + l] = [k] + [l] = \varphi(a) + \varphi(b).$$

We note also that $\ker \varphi = \{a \in \mathbb{Z}_9^\times \mid a = 2^0\} = \{1\}$. So the kernel is just the identity and so φ is one-to-one. And finally, since $2^k \in \mathbb{Z}_9^\times$ for all $k = 0, 1, \ldots, 5$, φ is onto.

So $\mathbb{Z}_9^\times$, with multiplication is isomorphic to the integers mod 6 (under addition)!

Proposition 4. *Let $G = \langle a \rangle$ be any cyclic group and consider the group of integers $\mathbb{Z}$ with addition. Then $\varphi : \mathbb{Z} \to G$ defined by $\varphi(n) = a^n$ is an onto homomorphism.*

Proof. Try to prove this. □

Proposition 5. *If $\varphi : G_1 \to G_2$ is a group homomorphism and $a \in G_1$ has order n, then the order of $\varphi(a)$ in G_2 is a divisor of n.*

Proposition 6. *Let $\varphi : G_1 \to G_2$ be an isomorphism of groups. Then*

(a) *If $a \in G_1$ has order n then $\varphi(a) \in G_2$ has order n.*
(b) *If G_1 is abelian then so is G_2.*
(c) *If G_1 is cyclic then so is G_2.*

Example 2: The symmetric group S_3 is isomorphic to the symmetry group of an equilateral triangle.

Define an isomorphism φ as follows. First associate vertex a with 1, vertex b with 2 and vertex c with 3. Then, given a symmetry of the triangle send it to the permutation that acts on $\{1, 2, 3\}$ in the same way that the symmetry acts on the vertices of the triangle.

So for r_a (the reflection that fixes vertex a and interchanges b and c) define $\varphi(r_a) = (2, 3)$, the permutation that fixes 1 and interchanges 2 and 3. Set $\varphi(r_b) = (1, 3)$ (r_b fixes b and the transposition $(1, 3)$ fixes 2), and set

$\varphi(r_c) = (1,2)$. Finally, for t_1, which takes $a \mapsto b \mapsto c \mapsto a$ define $\varphi(t_1) = (1,2,3)$ and define $\varphi(t_2) = (1,3,2)$. We claim this defines an isomorphism.

It is clearly one-to-one and onto. The reason that φ preserves the group operation is because it was composition of functions on both sides and we were careful to match up how a symmetry acted on vertices to how the permutation in the image acted on $\{1,2,3\}$.

For example: Recall that $r_c \circ r_a = t_1$ and

$$\varphi(r_c)\varphi(r_a) = (1,2)(2,3) = (1,2,3) = \varphi(t_1) = \varphi(r_c \circ r_a).$$

Example 3: In your homework you looked at the group of symmetries on a square, D_4. This group had 8 elements and they could all be written as products of one reflection r which had order 2 ($r^2 = e$) and one rotation t which had order 4 ($t^4 = e$).

Since the symmetric group S_4 has $4 \cdot 3 \cdot 2 \cdot 1 = 24$ elements, D_4 and S_4 cannot be isomorphic. But, try to construct a one-to-one, but not onto, homomorphism from D_4 into S_4 (this will mean that D_4 is isomorphic to a subgroup of S_4).