NOTES ON GROUPS, MATH 369.101

Factor groups

We begin with our motivation for the term *normal* subgroup.

Theorem 1. *Suppose that H is a normal subgroup of G. Then the set of (right) cosets $\{Ha \mid a \in G\}$ forms a group under the operation $Ha * Hb = H(ab)$. This* **factor group** *is written G/H.*

Proof. As we saw before, we need to know that the operation $*$ is well-defined. That is, if $Ha = Hb$ then for any $c \in G$ we need to know both that $Ha * Hc = Hb * Hc$, and that $Hc * Ha = Hc * Hb$.

To see the former: by definition, $Ha * Hc = H(ac)$ and $Hb * Hc = H(bc)$. So it is enough to check that $H(ac) = H(bc)$. Since $Ha = Hb$ we know that $a \in Hb$, so $a = h_1 b$ for some $h_1 \in H$. Then $ac = h_1 bc \in H(bc)$. Using the same proposition again (but this time with the cosets $H(ac)$ and $H(bc)$), this implies that $H(ac) = H(bc)$.

For the latter, we want that $Hc * Ha = Hc * Hb$. By the definition of $*$ we need $H(ca) = H(cb)$ and, just as in the previous paragraph, we know that $a = h_1 b$ for some $h_1 \in H$. Unlike in the previous paragraph, this does not immediately tell us that $ca \in H(cb)$, it only says that $ca = ch_1 b$.

Here we use the fact that H is normal. Recall, this means that for any $x \in G$, and any $h \in H$ we have $xhx^{-1} \in H$. In particular, there exists some $h_2 \in H$ so that $ch_1 c^{-1} = h_2$, which means that $ch_1 = h_2 c$.

From this we have that $ca = ch_1 b = h_2(cb)$ which is an element of $H(cb)$. So $ca \in H(cb)$ and by that same proposition $H(ca) = H(cb)$.

The above has shown that $*$ is a well-defined operation.

To see that we have a group:

(1) (Associativity): for $a, b, c \in G$, since the operation of G is associative,

$$(Ha*Hb)*Hc = H(ab)*Hc = H((ab)c) = H(a(bc)) = Ha*H(bc) = Ha*(Hb*Hc).$$

(2) (Identity): let e be the identity in G. Since H is a subgroup, $e \in H$, so $H = He$, and so for any $a \in G$,

$$Ha * H = H(ae) = Ha, \quad \text{and} \quad H * Ha = H(ea) = Ha.$$

(3) (Inverses): for any $a \in G$,

$$Ha * H(a^{-1}) = H(aa^{-1}) = He = H,$$

which is the identity of the operation. Similarly, $H(a^{-1}) * Ha = H$.

□

Date: Nov. 16, Nov. 21.

The idea of the factor group G/H is that you are collapsing the subgroup H to one element (the new identity), and each other coset to one element of the new group, like we do with congruence classes where there are infinitely many elements all representing one thing.

Note that if $|G|$ is finite then the number of elements in G/H is the index of H in G, equaling $|G|/|H|$. One can have G/H be a finite group even if G is infinite, e.g. $\mathbb{Z}/n\mathbb{Z}$.

Example 1: Recall our example from last class: $K = \{e, (1,2,3), (1,3,2)\} \subset S_3$ is a normal subgroup. Let's understand S_3/K.

The only elements of S_3 not in K are $(1,2), (1,3)$ and $(2,3)$. As these are transpositions, they are their own inverses.

Now, $(1,2)(1,3)$, $(1,2)(2,3)$, $(1,3)(1,2)$, $(1,3)(2,3)$, $(2,3)(1,2)$ and $(2,3)(1,3)$ are each either $(1,2,3)$ or $(1,3,2)$ (Do you know why, without computing?) This means that each of these products are in K, and so $K(1,2) = K(1,3) = K(2,3)$, and there are exactly 2 cosets in S_3/K (we could also see this by noting $|S_3| = 6$ and $|K| = 3$).

For the group structure, $K(1,2) * K(1,2) = K$, which is the identity. So the order of the coset $K(1,2)$ is 2.

Exercise 1: Let $G = (\mathbb{Z}_{16})^\times$ and let $\langle 9 \rangle$ be the cyclic subgroup generated by 9 (this subgroup has only 2 elements in it). Write out the cosets in $G/\langle 9 \rangle$ (there are four), then figure out their orders in $G/\langle 9 \rangle$. Note the order of an element will be the lowest power to which you raise it before getting into the normal subgroup, $\langle 9 \rangle$. Is $G/\langle 9 \rangle$ cyclic?

Now do the same for $G/\langle 7 \rangle$.

Proposition 1. *If $\varphi : G_1 \to G_2$ is a group homomorphism, then* $\ker \varphi$ *is a normal subgroup of G_1.*

Proof. We already know it is a subgroup. Given any $x \in G_1$ and $h \in \ker \varphi$, we need to see that $\varphi(xhx^{-1}) = e_2$, the identity in G_2.

Since $\varphi(h) = e_2$ we have $\varphi(xhx^{-1}) = \varphi(x)\varphi(h)\varphi(x)^{-1} = \varphi(x)\varphi(x)^{-1} = e_2$. So $xhx^{-1} \in \ker \varphi$, and the kernel is normal. □

Let's try to get a non-trivial homomorphism $\varphi : S_3 \to \mathbb{Z}_2$ (where $\mathbb{Z}_2$ has $+$ as operation).

If we had such a φ, then the order of $\varphi((1,2,3))$ divides the order of $(1,2,3)$ (which is 3: $(1,2,3)^3 = e$) by previous a proposition (see the 4th set of notes on groups). But the only orders of elements in $\mathbb{Z}_2$ are 1 or 2, so $\varphi((1,2,3))$ must be 0 (the identity). Similarly, it must be $\varphi((1,3,2)) = 0$.

Since the identity of S_3 must be sent to 0 also, we cannot have anything else in the kernel (it must be a subgroup, so $|\ker \varphi|$ divides $|S_3| = 6$ which means $|\ker \varphi| \leq 3$, since φ is not trivial, and we already have $e, (1,2,3), (1,3,2) \in \ker \varphi$. So we must set $\varphi((1,2)) = \varphi((1,3)) = \varphi((2,3)) = 1$. We've defined $\varphi(\sigma)$ for each $\sigma \in S_3$.

This defines a homomorphism $\varphi : S_3 \to \mathbb{Z}_2$, though a straightforward check that our definition preserves the group operation would require several calculations.

Instead of doing that, note that φ sends even permutations to 0 and odd permutations to 1. A product of two even permutations is even, and a product of two odd permutations is even, and on the $\mathbb{Z}_2$ side $0 + 0 = 0$ and $1 + 1 = 0$. This shows that φ preserves operations when the parity of permutations is the same. If one permuation is even and one is odd, then their product is odd. Likewise, $0 + 1 = 1$ and $1 + 0 = 1$ in $\mathbb{Z}_2$. This proves that φ is a homomorphism.

Observe! In fact, the last paragraph did more. In one fell swoop that paragraph (along with the well-definedness of even & odd in S_n) proves that the function $\varphi : S_n \to \mathbb{Z}_2$ that sends an even σ to 0 and an odd σ to 1 is a group homomorphism.

By Proposition 1, $K = \ker\varphi$ (the set of even permutations) is a normal subgroup. (If you count how many even permutations there are, you see it is half of $|S_n|$, so you could also use your homework problem for this). So S_n/K (permutations mod even permutations) is a group. If σ_1, σ_2 are odd permutations, then $K(\sigma_1^2) = K = K(\sigma_1\sigma_2^{-1})$ since σ_1^2 and $\sigma_1\sigma_2^{-1}$ are even. This means that S_n/K has only two elements (cosets), and the non-identity one has order 2.

Remember that for $\varphi : G_1 \to G_2$, the image $\varphi(G_1) \subset G_2$ is a subgroup.

Theorem 2. *(Fundamental Homomorphism Theorem) Let $\varphi : G_1 \to G_2$ be a homomorphism of groups and set $K = \ker\varphi$. Then G_1/K is isomorphic to $\varphi(G_2)$. In particular, if φ is onto then $G_1/K \cong G_2$.*

So, for example, taking $\varphi : S_n \to \mathbb{Z}_2$ to be the even/odd homomorphism above, we get that $S_n/K \cong \mathbb{Z}_2$.

Proof. The proof of this theorem is essentially the same as it was for the Fund. Homomorphism Th'm for Rings. You define a function $\psi : G_1/K \to \phi(G_2)$ by setting $\psi(Ka) = \phi(a)$. Then you check that this is a bijective homomorphism (so an isomorphism). □

Exercise 2: Using the notation from the example in the last set of notes, show that the factor group $\mathfrak{M}/\mathfrak{N}(1)$ is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ (with addition in each component). For this, you may want to remember that $\{1, -1\}$, with the operation of multiplication, is isomorphic to $(\mathbb{Z}_2, +)$.