MATH 30A: CHAPTER 9

9. Normal subgroups and factor groups

This chapter is about normal subgroups $N \triangleleft G$ and the factor group G/N associated to a normal subgroup.

9.1. **Normal subgroup.**

I gave the definition of a normal subgroup and gave some examples.

Definition 9.1. *A subgroup H of G is called* normal *if $aH = Ha$ for all $a \in G$.*

Example 9.2. *Here are some obvious examples:*

1. *If G is abelian then all subgroups H are normal.*
2. *The center $Z(G)$ is normal in G.*
3. *G is a normal subgroup of G.*

Next I pointed out that the equation $aH = Ha$ does not mean that a commutes with the elements of H. In terms of elements it means: For all $h \in H$ there is an $h' \in H$ so that

$$ah = h'a$$

But we know what the element h' has to be. We just multiply both sides of the equation by a^{-1} to get:

$$h' = aha^{-1}$$

The statement is that this element lies in H. This is called a *conjugate* of h.

Theorem 9.3. *A subgroup H of G is normal iff it contains the conjugates of all of its elements. I.e., if*

$$aHa^{-1} = H$$

for all $a \in G$.

The words don't quite match the equation since the words say: $aHa^{-1} \subseteq H$. But this is for all $a \in G$. In particular it is supposed to hold for a^{-1}:

$$(a^{-1})H(a^{-1})^{-1} \subseteq H$$

Conjugating by a this gives $H \subseteq aHa^{-1}$. So, we get $H = aHa^{-1}$.

Date: October 18, 2006.

We looked at the subgroups of the dihedral group D_4 and determined which are normal.

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

The elements r and r^3 are conjugate since

$$r^3 = srs^{-1} = srs$$

r has no other conjugates since these are the only elements of order 4.

The elements s and sr^2 are conjugate. Similarly, sr and sr^3 are conjugate. This means that any normal subgroup containing s will also contain sr^2 and similarly for the other two.

Proposition 9.4. *The normal subgroups of D_4 are the trivial group $\{e\}$, the whole group D_4, the center $\langle r^2 \rangle$ and the three subgroups of order 4:*

$$\langle r \rangle, \quad \left\langle s, r^2 \right\rangle, \quad \left\langle sr, r^2 \right\rangle$$

I pointed out that:

Theorem 9.5. *Any subgroup of index 2 is normal.*

Proof. If $H \le G$ has index 2 then there are only two left cosets. One is H and the other is aH where a is any element of G which is not in H. Since these are disjoint and their union is G, we have

$$aH = G - H$$

The right cosets have the same description:

$$Ha = G - H \quad \text{if } a \in G - H$$

and $Ha = H$ if $a \in H$. So, $H \lhd G$. □

9.2. **Factor groups.** If $N \triangleleft G$ then the set of cosets of N form a group with multiplication defined by

$$(aN)(bN) := abN$$

The additive notation is:

$$(a+N)+(b+N) := (a+b)+N$$

This group, whose elements are the cosets of N with operation defined by one of the two formulas above, is denoted G/N. To check that this is a group the only thing we have to check is that the multiplication is "well-defined" because the other conditions are obvious. (E.g., $eN = N$ is the identity, $(aN)^{-1} = a^{-1}N$.)

Well-defined means *independent of all choices.* But what choices did we make?

As I pointed out before, you get the same left coset in many ways.

$$a_1N = a_2N \iff a_1^{-1}a_2 \in N$$

So, suppose that $a_1N = a_2N$ and $b_1N = b_2N$. Then we have two different formulas for the product and we need to show:

$$a_1b_1N = a_2b_2N$$

In other words, we need to check that $(a_1b_1)^{-1}a_2b_2 \in N$. But:

$$(a_1b_1)^{-1}a_2b_2 = b_1^{-1}a_1^{-1}a_2b_2 = b_1^{-1}(a_1^{-1}a_2)b_1(b_1^{-1}b_2) \in b_1^{-1}Nb_1N = NN = N$$

9.2.1. *$\mathbb{Z}/n$.* Take the additive group $G = \mathbb{Z}$. Since this is abelian, all subgroups are normal. Take the subgroup $4\mathbb{Z}$. Call the cosets

$$\overline{x} := x + 4\mathbb{Z}$$

Then there are 4 cosets: $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ and $\overline{0} = \overline{4} = \overline{8} = \overline{12} = \cdots$ and similarly, the other cosets have many names. Addition is given by:

$$\overline{x} + \overline{y} = \overline{x+y}$$

This is just addition modulo 4. So,

$$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$$

The group $\mathbb{Z}/n\mathbb{Z}$ is often just written $\mathbb{Z}/n$.

9.2.2. *$D_4/Z(D_4)$.* The center of D_4 consists of the identity and rotation by π:

$$Z = Z(D_4) = \langle r^2 \rangle = \{e, r^2\}$$

This is a normal subgroup of D_4 of index 4. So, the factor group D_4/Z has 4 elements:

$$Z = \{e, r^2\}$$

$$A := \{s, sr^2\}$$

$$B := \{sr, sr^3\}$$

$$C := \{r, r^3\}$$

Z is the identity. ($N = eN$ is always the identity.) $A^2 = B^2 = Z$ since A, B contain elements of order 2. $C^2 = r^2 Z = Z$ since $r^2 \in Z$. Thus, D_4/Z is abelian. Finally, $AB = C, BC = A$ and $AC = B$ since, e.g.,

$$AB = (sZ)(srZ) = ssrZ = rZ = C.$$

Question: If $N \triangleleft G$ what is the order of aN? How is the order of aN related to the order of a?

The book points out that:

Theorem 9.6. *For any group G, $G/Z(G) \cong \mathrm{Inn}(G)$.*

Proof. The formula for the isomorphism $\phi : G/Z(G) \cong \mathrm{Inn}(G)$ is $\phi(aZ) = \phi_a$ which is the notation for the inner automorphism

$$\phi_a(x) = axa^{-1}$$

It is easy to see that this mapping is onto (inner automorphisms are given by ϕ_a by definition) and preserves the operation ($\phi_a\phi_b = \phi_{ab}$). What is not obvious is that it is well-defined and 1-1.

To show it is well-defined suppose that $aZ = bZ$. Then $a^{-1}b \in Z$. This is the same as saying that, for all $x \in G$,

$$a^{-1}bx = xa^{-1}b$$

$$a(a^{-1}bx)b^{-1} = a(xa^{-1}b)b^{-1}$$

$$\phi_b(x) = bxb^{-1} = axa^{-1} = \phi_a(x)$$

To show that this mapping is 1-1 suppose that $\phi_a = \phi_b$. Then we have to show that $aZ = bZ$. Just run the above equations from bottom to top. $\square$

9.2.3. *groups of order p^2.* I want to show:

Theorem 9.7. *Groups of order p^2 are abelian.*

This uses a whole bunch of interesting and important theorems. The first deals with the number of conjugates of any element.

Lemma 9.8. *If $g \in G$ then the conjugates aga^{-1} of g are in 1-1 correspondence with the left cosets of the centralizer $C(g)$ of g. In particular the number of conjugates of g is equal to the index $|G : C(g)|$ of the centralizer. This number divides the order of the group.*

Proof. This is easy: $aga^{-1} = bgb^{-1} \iff g = a^{-1}bgb^{-1}a \iff a^{-1}b \in C(g) \iff aC(g) = bC(g)$. □

Lemma 9.9. *If G has p^n elements where $n \geq 1$ then the center of G has at least p elements.*

Proof. Collect the elements of G into conjugacy classes. Use the formula that $g \in G$ has $|G : C(g)|$ conjugacy classes. This number divides the order of the group. So, it is a power of p. So, $|G| = p^n$ is a sum of numbers, all of which are powers of p. But one of them is 1 (the identity is only conjugate to itself). So, at least $p - 1$ of the other powers must also be $p^0 = 1$. These are central elements. □

Lemma 9.10. *If $G/Z(G)$ is cyclic then G is abelian.*

Proof. If G/Z is cyclic, it is generated by one element aZ. Then the cosets are: a^kZ and G is the union of these cosets. This means that every element of G has the form a^kz. So, if we take two elements, they must be: a^jz_1, a^kz_2 which commute:

$$a^jz_1a^kz_2 = a^ja^kz_1z_2 = a^{j+k}z_2z_1 = a^kz_2a^jz_1.$$

So, G is abelian. □

Now we can prove that groups of order p^2 are abelian:

The center Z must have at least p elements. So, G/Z has either p or 1 element. So, it is cyclic. So, G is abelian.