Math 371 Lecture #32
§7.6 (Ed.2), 8.2 (Ed.2): Normal Subgroups, Part II

Recall that definition of a normal subgroup: a subgroup $N$ of $G$ is normal if $Na = aN$ for all $a \in G$.

Recall that to make the set of right cosets of a subgroup $N$ of a group $G$ into a group requires the normality of $N$, i.e., to ensure that the “product”

$$(Na)(Nc) = N(ac)$$

is well-defined.

We formalize this now.

**Theorem 8.1.** Suppose $N$ is a normal subgroup of a group $G$. If $a \equiv b \pmod N$ and $c \equiv d \pmod N$, then $ac \equiv bd \pmod N$.

**Proof.** Suppose that $a \equiv b \pmod N$ and $c \equiv d \pmod N$.

Then there are elements $m, n \in N$ such that $ab^{-1} = m$ and $cd^{-1} = n$.

Since we are after $ac \equiv bd \pmod N$, we want to show that $(ac)(bd)^{-1} \in N$.

This product is

$$(ac)(bd)^{-1} = a(cd)^{-1}b^{-1} = anb^{-1}.$$  

By the normality of $N$ as a subgroup, we have $aN = Na$, so there exists $n_2 \in N$ such $an = n_2a$.

Hence

$$anb^{-1} = n_2ab^{-1} = n_2m.$$  

Since $n_2, m \in N$, then $n_2m \in N$.

Therefore $(ac)(bd)^{-1} = n_2m \in N$, so that $ac \equiv bd \pmod N$.  

We will discuss in depth the group of right cosets of a normal subgroup next lecture.

For now we develop some tests to determine whether a subgroup of a group is normal or not.

We will need some notation for these tests.

**Notation.** For a subgroup $N$ of a group $G$ and an element $a \in G$, we set

$$a^{-1}Na = \{a^{-1}na : n \in N\} \text{ and } aNa^{-1} = \{ana^{-1} : n \in N\}.$$  

What kind of subsets are these in $G$?

**Theorem.** For a subgroup $N$ of a group $G$, and for each $a \in G$, the subsets $aNa^{-1}$ and $a^{-1}Na$ are subgroups of $G$ isomorphic to $N$.

**Proof.** WLOG, we consider for each $a \in G$, the mapping $f_a : G \to G$ defined by $f_a(g) = a^{-1}ga$, which is an inner automorphism of $G$.

We show that that subset $a^{-1}Na$ of $G$ is a subgroup of $G$. 

Theorem 8.11. The following conditions on a subgroup $N$ of a group $G$ are equivalent.

1. $N$ is a normal subgroup of $G$.
2. $a^{-1}Na \subseteq N$ for all $a \in G$.
3. $aN a^{-1} \subseteq N$ for all $a \in G$.
4. $a^{-1}Na = N$ for all $a \in G$.
5. $aN a^{-1} = N$ for all $a \in G$.

Proof. (1) $\Rightarrow$ (2). Suppose $N$ is normal, and for any $a \in G$ consider $a^{-1}na \in a^{-1}Na$.
The goal is to show that $a^{-1}na \in N$.

Now the product $na$ belongs to $Na$, and since $N$ is normal, we have $Na = aN$, so that $na \in aN$.
Thus there is $n_1 \in N$ such that $na = an_1$.

This means that $a^{-1}na = a^{-1}an_1 = n_1 \in N$, and hence that $a^{-1}Na \subseteq N$.

(2) $\iff$ (3). If $a^{-1}Na \subseteq N$ for all $a \in G$, then it holds for all $a^{-1} \in G$, namely that

$$aNa^{-1} = (a^{-1})^{-1}Na^{-1} \subseteq N.$$  

On the other hand, if $aN a^{-1} \subseteq N$ for all $a \in G$, then it holds for all $a^{-1} \in G$, namely that

$$a^{-1}Na = a^{-1}N(a^{-1})^{-1} \subseteq N.$$  

(3) $\Rightarrow$ (4). Suppose that $aN a^{-1} \subseteq N$ for all $a \in G$.

Then as (3) $\Rightarrow$ (2), we have that $a^{-1}Na \subseteq N$ for all $a \in G$.

It remains to show the opposite inclusion, $N \subseteq a^{-1}Na$ for all $a \in G$.

Let $n \in N$.

Then we have for any $a \in G$ that $n = a^{-1}(ana^{-1})a$.

Since $ana^{-1} \in aNa^{-1}$ and $aN a^{-1} \subseteq N$ by (3), there is $n_2 \in N$ such that $ana^{-1} = n_2$.

Thus $n = a^{-1}(ana^{-1})a = a^{-1}n_2a \in a^{-1}Na$, so that $a^{-1}Na = N$ for all $a \in G$.

(4) $\iff$ (5). If $a^{-1}Na = N$ holds for all $a \in G$, then it holds with $a^{-1}$ in place of $a$ to give $aN a^{-1} = N$ for all $a \in G$.

On the other hand, if $aN a^{-1} = N$ holds for all $a \in G$, then it holds with $a^{-1}$ in place of $a$ to give $a^{-1}Na = N$ for all $a \in G$.

(5) $\Rightarrow$ (1). Suppose that $aN a^{-1} = N$ for all $a \in G$. 

The goal is to show that $N$ is normal, that $Na = aN$ for all $a \in G$, which we do by showing the two containments $Na \subseteq aN$ and $aN \subseteq Na$.

Let $an \in aN$.

Then $ana^{-1} \in aNa^{-1} = N$, so that there is $n_3 \in N$ such that $ana^{-1} = n_3$.

Multiplying $ana^{-1}$ on the right by $a$ gives $an = n_3a$, showing that $an \in Na$.

This shows that $aN \subseteq Na$ for all $a \in G$.

Conversely, let $na \in Na$.

Then $a^{-1}na \in a^{-1}Na$, and since (5) implies (4), that $a^{-1}na \in a^{-1}Na = N$.

Hence there is $n_4 \in N$ such that $a^{-1}na = n_4$.

Multiplying on the left by $a$ gives $na = an_4$.

This says that $na \in aN$, and so $Na \subseteq aN$ for all $a \in G$. $\square$

Examples. (a) Recall that we showed that the subgroup $N = \{(1), (123), (132)\}$ of $S_3$ is normal by showing $Na = aN$ for all $a \in S_3$.

With Theorem 8.11 (Ed.3) and knowledge about the order of subgroups of $S_3$, we have a simpler argument for the normality of $N$.

The subgroup $N$ is the only subgroup of order 3 of $S_3$ while every other proper subgroup of $S_3$ has order 2 by Lagrange’s Theorem.

We know for each $a \in S_3$ that $a^{-1}Na$ is a subgroup of $S_3$ because the map $n \mapsto a^{-1}na$ is an inner automorphism of $S_3$ for each $a \in S_3$.

Since an automorphism is a bijection, we have $|a^{-1}Na| = 3$.

Since $a^{-1}Na$ is a subgroup of $S_3$ of order 3, there is only one subgroup of $S_3$ that can contain it, namely $N$, so that $a^{-1}Na \subseteq N$.

By Theorem 8.11 (Ed.3), we conclude that $N$ is a normal subgroup of $S_3$.

(b) For any integer $n \geq 2$, is the subgroup $SL(n, \mathbb{R})$ of the group $GL(n, \mathbb{R})$ a normal subgroup?

The condition for $B \in SL(n, \mathbb{R})$ is that $\det(B) = 1$.

Because $\det(A^{-1}BA) = \det(A^{-1})\det(B)\det(A) = \det(B) = 1$, we have that $A^{-1}BA \in SL(n, \mathbb{R})$, and so $SL(n, \mathbb{R})$ is normal.

Normal subgroups also appear in groups homomorphisms.

Theorem. For groups $G$ and $H$, if $f : G \to H$ is a homomorphism, then $\ker f$ is a normal subgroup of $G$, and $\text{Im } f$ is normal subgroup of $H$.

You will prove the two conclusions of this theorem as homework problems.

Example. For an integer $n \geq 2$, the map $f : GL(n, \mathbb{R}) \to \mathbb{R}^*$ given by $f(A) = \det(A)$ is a homomorphism because

$$f(AB) = \det(AB) = \det(A)\det(B) = f(A)f(B)$$

for all $A, B \in GL(n, \mathbb{R})$.

What is the kernel of this homomorphism?

It is precisely $SL(n, \mathbb{R})$, and hence it is a normal subgroup of $GL(n, \mathbb{R})$. 