Graduate Algebra, Fall 2014
Lecture 5

Andrei Jorza

2014-09-05

1 Group Theory

1.9 Normal subgroups

Example 1. Specific examples.

1. The alternating group $A_n = \ker \varepsilon$ is a normal subgroup of S_n as ε is a homomorphism.

2. For $R = \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$, $\mathrm{SL}(n, R) \lhd \mathrm{GL}(n, R)$.

3. Recall that for any group G, $Z(G) \lhd G$ and $G/Z(G)$ is a group, which we'll identify later as the group of inner automorphisms. If $R = \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$ then $R^\times I_n = Z(\mathrm{GL}(n, R))$ and denote the quotient

$$\mathrm{PGL}(n, R) = \mathrm{GL}(n, R)/R^\times$$

   The case of $\mathrm{SL}(n, R)$ is more subtle as the center is the set of n-th roots of unity in R, which depends on what R is. For example $Z(\mathrm{SL}(2, \mathbb{R})) = \pm I_2$ but $Z(\mathrm{SL}(3, \mathbb{R})) = I_3$ while $Z(\mathrm{GL}(3, \mathbb{C})) = \{I_3, \zeta_3 I_3, \zeta_3^2 I_3\}$.

4. But $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\}$ is not normal in $\mathrm{GL}(2, R)$. Indeed, if $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ then $w \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} w = \begin{pmatrix} c & 0 \\ b & a \end{pmatrix}$.

5. But $\{\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\}$ is a normal subgroup of $\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\}$.

Remark 1. If $H, K \subset G$ are subgroups such that K is normal in G then HK is a subgroup of G. Indeed, $KH = HK$.

Interlude on the big picture in the theory of finite groups

We have seen that if G is a finite group and N is a normal subgroup then G/N is also a group. The idea is to try to use the smaller groups G/N and N to understand G.

1. If G/N can be "realized" as a subgroup of G then G can be described explicitly as a semidirect product, which we'll study next time.

2. More generally there is a Jordan-Holder composition series theorem, to be thought of as a generalization of the Jordan canonical form describing conjugacy classes of matrices.

A crucial component of these theorems is that various groups can be combined into bigger groups after understanding their automorphism groups.

Definition 2. A finite group is **simple** if it has no proper normal subgroups.

The preceding description of the classification of finite groups suggests that simple groups are the basic building blocks.

The following huge theorem take decades and tens of thousands of pages to complete.

Theorem 3. *All finite simple groups fit in one of the following four families:*

1. $\mathbb{Z}/p\mathbb{Z}$ *for* p *prime.*

2. A_n *for* $n \neq 4$.

3. *finite groups of "Lie type" which are certain matrix groups with entries in* $\mathbb{Z}/p\mathbb{Z}$.

4. *26 complicated exceptional groups about which I'll say nothing more.*

This should explain why most examples in class and homeworks are either finite abelian groups (for which the building blocks are $\mathbb{Z}/p\mathbb{Z}$), symmetric groups or matrix groups; they really do form the basic building blocks of the whole theory.

Three important questions in the theory of finite groups:

1. CLassify all simple groups.

2. Given a specific group, describe it "well" (perhaps in terms of simple groups).

3. Represent groups on a computer.

The main technical tool that allows us to tackle the first and second questions is the notion of groups acting on sets. This is a very general notion that includes groups representations, but our initial main use will be via the Sylow theorems.

For the third question, there are two avenues of study: representing groups as permutation groups, for which we'll study S_n and A_n; and representing groups as quotients of free groups by relations, which turns out to be very important in representation theory as well.

1.10 The isomorphism theorems

Theorem 4. *Suppose* $f : G \to H$ *is a homomorphism.*

1. *Suppose* $N \lhd G$ *contained in* $\ker f$. *Then* $\overline{f} : G/N \to H$ *sending* $gN \to f(g)$ *is a well-defined homomorphism.*

2. *Then* $G/\ker f \cong \operatorname{Im} f$.

Proof. Need to check that if $gN = hN$ then $f(g) = f(h)$, which follows from $gh^{-1} \in N \subset \ker f$. Taking $N = \ker f$ gives the second part as now the map $\overline{f}$ becomes injective. □

Theorem 5. *Suppose* $H, N \subset G$ *are subgroups with* N *normal in* G. *Recall that* HN *is a subgroup of* G. *Then* $HN/N \cong H/H \cap N$.

Proof. The map $H \to HN/N$ taking h to hN is surjective and has kernel $H \cap N$. □

Theorem 6. *If* $H, N \lhd G$ *and* $N \subset H$ *then* $G/H \cong (G/N)/(H/N)$.

Proof. Take $f : G/N \to G/H$ taking gN to gH. This has kernel H/N and is clearly surjective. The rest follows from the first isomorphism theorem. □

Example 7. 1. $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$.

1.11 Automorphisms

Definition 8. $\mathrm{End}(G)$ is the set of homomorphisms $f : G \to G$ and $\mathrm{Aut}(G)$ is the set of isomorphisms $f : G \to G$.

Proposition 9. *If G is a group then $\mathrm{End}(G)$ is a monoid and $\mathrm{Aut}(G)$ is a group wrt composition.*

Lemma 10. *If $f : G \to H$ is an injective homomorphism then $\mathrm{ord}(f(g)) = \mathrm{ord}(g)$.*

Proposition 11. *Let G be a group.*

1. *$f(x) = x^{-1}$ is a homomorphism iff G is abelian, in which case it is an automorphism.*
2. *If $g \in G$ then $f_g(x) = gxg^{-1}$ is an automorphism, called an inner automorphism. The set of inner automorphisms forms a subgroup $\mathrm{Inn}(G) \subset \mathrm{Aut}(G)$.*
3. *$\mathrm{Inn}(G) \cong G/Z(G)$.*

Proof. The first part is clear. The second follows from the fact that $f_g \circ f_h = f_{gh}$. For the third part note that $f_g = f_h$ iff $f_{gh^{-1}} = \mathrm{id}$ iff $gh^{-1} \in Z(G)$ by definition of $Z(G)$. Thus the map $G \to \mathrm{Aut}(G)$ sending g to f_g is a homomorphism with kernel $Z(G)$. □