

CONTENTS

1. Review: normal subgroups.....	1
2. More examples: determinant and sign	2
3. Simple groups	4

1. REVIEW: NORMAL SUBGROUPS

Last time we introduced the notion of normal subgroups.

Definition 1.1. A subgroup $N \leq G$ is said to be *normal* if

$$gNg^{-1} \subseteq N \quad \text{for every } g \in G.$$

As we saw last time, this is equivalent to requiring

$$gNg^{-1} = N \text{ for all } g \in G.$$

We write $N \trianglelefteq G$ to mean that N is a normal subgroup.

We gave some concrete examples of normal subgroups, but here is a general fact: normal subgroups arise naturally as kernels of group homomorphisms.

Proposition 1.1. If $\varphi : G \rightarrow H$ is a homomorphism, then $\ker(\varphi) \trianglelefteq G$.

Proof. We already know that $\ker(\varphi)$ is a subgroup. If $a \in \ker(\varphi)$ and $g \in G$, then

$$\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(g)e_H\varphi(g)^{-1} = e_H.$$

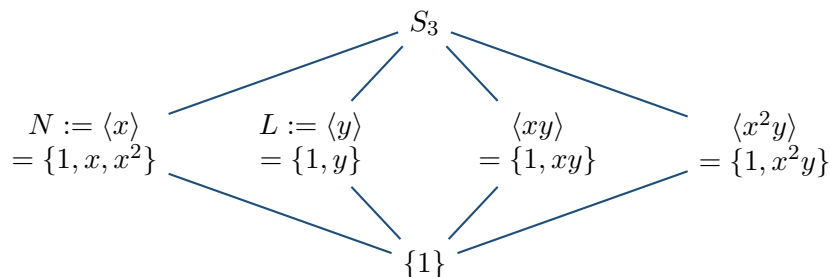
Thus $gag^{-1} \in \ker(\varphi)$, as required. $\square$

We will see later in the course that the converse also holds: every normal subgroup of G is the kernel of some homomorphism with domain G .

Example 1.1. Recall our example from last time about the group

$$S_3 = \{1, x, x^2, y, xy, x^2y\}, \quad x^3 = 1, \quad y^2 = 1, \quad yx = x^2y.$$

Its subgroups and their inclusions are depicted as follows:



We argued last time that $N \trianglelefteq S_3$ (there we called it H) but that L is not normal. The same kind of computation shows that $\langle xy \rangle$ and $\langle x^2y \rangle$ are not normal either (exercise). Thus, by Proposition 1.1, none of the three subgroups of order two can be the kernel of a homomorphism. But is N a kernel? We will see shortly that it is: N is the kernel of the sign homomorphism.

2. MORE EXAMPLES: DETERMINANT AND SIGN

Example 2.1 (The determinant homomorphism). Multiplicativity of the determinant says that

$$\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^*, \quad A \longmapsto \det(A), \quad (2.1)$$

is a homomorphism, where $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ is a group under multiplication. Its kernel is

$$\ker(\det) = \mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) : \det(A) = 1\}.$$

Since kernels are normal, $\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$.

Next we construct the sign homomorphism on S_n . We give two constructions: Approach A is combinatorial and builds on Lecture 5, while Approach B uses linear algebra and the determinant. Throughout, $\{\pm 1\}$ denotes the group with two elements under usual multiplication, with identity 1. Up to isomorphism, it is the unique group with two elements.

Approach A: parity of permutations. Recall from Lecture 5 that $\sigma \in S_n$ is *even* if it can be written as a product of an even number of simple transpositions, and *odd* otherwise. We proved there that this is well defined: no permutation can be written both as a product of an even number and as a product of an odd number of simple transpositions. Since $\sigma = s_{i_1} \cdots s_{i_k}$ with $k = \ell(\sigma)$, the permutation σ is even exactly when $\ell(\sigma)$ is even.

Definition 2.1 (Sign). The *sign* of $\sigma \in S_n$ is

$$\mathrm{sgn}(\sigma) = (-1)^{\ell(\sigma)} = \begin{cases} +1, & \text{if } \sigma \text{ is even,} \\ -1, & \text{if } \sigma \text{ is odd.} \end{cases} \quad (2.2)$$

Proposition 2.1. *The map $\mathrm{sgn} : S_n \rightarrow \{\pm 1\}$ is a homomorphism.*

Proof. Let $\sigma, \tau \in S_n$, and write σ as a product of a simple transpositions and τ as a product of b simple transpositions. Concatenating the two expressions writes $\sigma\tau$ as a product of $a + b$ simple transpositions. Since parity is well defined, $(-1)^a = \mathrm{sgn}(\sigma)$ and $(-1)^b = \mathrm{sgn}(\tau)$. Therefore,

$$\mathrm{sgn}(\sigma\tau) = (-1)^{a+b} = (-1)^a(-1)^b = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).$$

□

In other words, the multiplication rule in $\{\pm 1\}$ has exactly the parity table of permutations:

	even	odd
even	even	odd
odd	odd	even

Approach B: permutation matrices. We next construct the sign homomorphism geometrically. For $\sigma \in S_n$, let $e_1, \dots, e_n$ be the standard basis of $\mathbb{R}^n$ and define the permutation matrix $[\sigma]$ by

$$[\sigma]e_i = e_{\sigma(i)}. \quad (2.3)$$

Equivalently, the i th column of $[\sigma]$ is $e_{\sigma(i)}$. If E_{ij} denotes the matrix with a 1 in row i , column j , and zeros elsewhere, then

$$[\sigma] = \sum_{i=1}^n E_{\sigma(i), i}. \quad (2.4)$$

Example 2.2. For $\sigma = (1 \ 2 \ 3) \in S_3$,

$$[\sigma] = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad [\sigma] \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}.$$

Warning

The entry in output position j is $x_{\sigma^{-1}(j)}$. Indeed, the i th basis vector is sent to $e_{\sigma(i)}$, so the entry originally in position i appears in position $\sigma(i)$. In column-vector notation,

$$[\sigma] \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\sigma^{-1}(1)} \\ x_{\sigma^{-1}(2)} \\ \vdots \\ x_{\sigma^{-1}(n)} \end{pmatrix}.$$

Proposition 2.2. *The assignment $\sigma \mapsto [\sigma]$ is a homomorphism $S_n \rightarrow \text{GL}_n(\mathbb{R})$.*

Proof. Using right-to-left composition, for every standard basis vector e_i we have

$$[\sigma][\tau]e_i = [\sigma]e_{\tau(i)} = e_{\sigma(\tau(i))} = [\sigma\tau]e_i.$$

Since the matrices agree on every basis vector, $[\sigma][\tau] = [\sigma\tau]$. Also, $[\text{id}] = I_n$, so

$$[\sigma][\sigma^{-1}] = I_n = [\sigma^{-1}][\sigma].$$

Thus $[\sigma]^{-1} = [\sigma^{-1}]$, which shows that $[\sigma]$ belongs to $\text{GL}_n(\mathbb{R})$ and completes the proof. $\square$

Both $[\sigma]$ and $[\sigma^{-1}]$ have integer entries, so their determinants are integers. Since they are inverse matrices,

$$\det([\sigma]) \det([\sigma^{-1}]) = 1.$$

Hence $\det([\sigma]) \in \{+1, -1\}$.

The map $\sigma \mapsto \det([\sigma])$ is the composition of the two homomorphisms $[\cdot] : S_n \rightarrow \text{GL}_n(\mathbb{R})$ and $\det : \text{GL}_n(\mathbb{R}) \rightarrow \mathbb{R}^*$. It is therefore a homomorphism, since

$$\det([\sigma\tau]) = \det([\sigma][\tau]) = \det([\sigma]) \det([\tau]).$$

This calculation is an instance of the following general fact, which is left as an exercise.

Lemma 2.1 (Composition of homomorphisms). *Let G_1, G_2, G_3 be groups, and let $\varphi : G_1 \rightarrow G_2$ and $\psi : G_2 \rightarrow G_3$ be homomorphisms. Then $\psi \circ \varphi : G_1 \rightarrow G_3$ is a homomorphism.*

Proposition 2.3. *For every $\sigma \in S_n$, we have $\text{sgn}(\sigma) = \det([\sigma])$.*

Proof. The matrix of a simple transposition exchanges two columns of I_n , so it has determinant -1 . If $\sigma = s_{i_1} \cdots s_{i_k}$ is any expression as a product of simple transpositions, multiplicativity gives

$$\det([\sigma]) = \prod_{j=1}^k \det([s_{i_j}]) = (-1)^k.$$

Taking a shortest expression, $k = \ell(\sigma)$, gives $\det([\sigma]) = (-1)^{\ell(\sigma)} = \text{sgn}(\sigma)$. $\square$

Remark. Approach B gives a second proof of Proposition 2.1, and in fact more. Since the argument above works for *every* expression of σ , the number $(-1)^k = \det([\sigma])$ depends only on σ . So Approach B independently proves the result of Lecture 5 that parity is well defined, without counting inversions.

The kernel of sign. Recall from Lecture 5 the alternating group

$$A_n = \{\sigma \in S_n : \sigma \text{ is even}\}.$$

We can now see it in a new light: $A_n = \ker(\text{sgn})$. Therefore, by Proposition 1.1, $A_n \trianglelefteq S_n$.

Example 2.3 (Sign on S_3). With $x = (1\ 2\ 3)$ and $y = (1\ 3)$, the values of sgn on the elements of S_3 are:

element	cycle decomposition	parity	sgn
1	(1)	even	+1
x	(1 2 3)	even	+1
x^2	(1 3 2)	even	+1
y	(1 3)	odd	-1
xy	(2 3)	odd	-1
x^2y	(1 2)	odd	-1

Hence

$$\ker(\text{sgn}) = A_3 = \{1, x, x^2\} = N,$$

which answers the question from Section 1: N is a kernel. This supplies another proof that $N \trianglelefteq S_3$.

3. SIMPLE GROUPS

There is a very important idea in group theory: start with certain “simple” groups and build more complicated groups out of them.

Definition 3.1 (Simple group). Recall from last time that a nontrivial group G is *simple* if its only normal subgroups are $\{e_G\}$ and G .

As a product of a vast collaborative effort spanning much of the twentieth century, mathematicians were able to classify all finite simple groups completely—every finite simple group is isomorphic to one of the following:

- (1) **Cyclic groups** of prime order, $\mathbb{Z}/p\mathbb{Z}$. These are the only abelian ones.
- (2) **Alternating groups** A_n for $n \geq 5$.
- (3) **Groups of Lie type**, which come in 16 infinite families.
- (4) **The 26 sporadic groups**, which fit into no infinite family; the largest of them is called the Monster.

Later in this course we will show that cyclic groups of prime order and the alternating groups A_n for $n \geq 5$ are simple. How are more complicated groups built from simple ones? The key tool is the *quotient group* G/N of a group by a normal subgroup. To construct it, we first need the notion of a coset.