

Lecture 13

MATH 327

Date: Oct. 5, 2026

Instructor: Manish Patnaik

CONTENTS

1. The counting formula for homomorphisms 1
2. Index in a tower of subgroups 2

1. THE COUNTING FORMULA FOR HOMOMORPHISMS

Question 1.1. How many elements does A_n have?

For S_5 , the cycle types, their parity, and the number of permutations of each type are listed below. Here 1 denotes a fixed point.

Cycle type	Example	Parity	Count
1^5	1	Even	1
$2 1^3$	(12)	Odd	10
$2^2 1$	(12)(34)	Even	15
$3 1^2$	(123)	Even	20
$3 2$	(123)(45)	Odd	20
$4 1$	(1234)	Odd	30
5	(12345)	Even	24

Thus S_5 has 60 even and 60 odd permutations, so $|A_5| = 60$.

By the way, how do we know that (123) is even/odd? Remember our homomorphism $\text{sgn} : S_n \rightarrow \{\pm 1\}$. Suppose $\text{sgn}(123) = -1$, i.e. it is odd, then $\text{sgn}((123)^3) = (-1)^3 = -1$, but it must also equal 1 as $(123)^3 = 1$.

Let $\varphi : G \rightarrow H$ be a group homomorphism, and recall

$$K = \ker(\varphi) = \{x \in G : \varphi(x) = e_H\} \leq G,$$

$$\text{im}(\varphi) = \{h \in H : \text{there is } a \in G \text{ with } \varphi(a) = h\} \leq H.$$

Picture G partitioned into the left cosets $K, g_1K, g_2K, \dots$ of the kernel. Since $\varphi(K) = \{e_H\}$, the whole coset gK is sent to the single element $\varphi(g)$:

$$\varphi(gk) = \varphi(g)\varphi(k) = \varphi(g) \quad (k \in K).$$

So φ collapses each coset of K to one point of $\text{im}(\varphi)$.

Proposition 1.1. *The map*

$$G/K \longrightarrow \text{im}(\varphi), \quad gK \longmapsto \varphi(g),$$

is a well-defined bijection.

Proof. Well defined: if $g_1K = g_2K$, then by what we proved earlier $g_1^{-1}g_2 \in K$. Hence $\varphi(g_1^{-1}g_2) = e$, i.e. $\varphi(g_1) = \varphi(g_2)$.

Surjective: every element of $\text{im}(\varphi)$ is $\varphi(g)$ for some $g \in G$, and this is the image of gK .

Injective: could we have $g_1K \neq g_2K$ but $\varphi(g_1) = \varphi(g_2)$? No: if $\varphi(g_1) = \varphi(g_2)$, then

$$\varphi(g_2^{-1}g_1) = \varphi(g_2)^{-1}\varphi(g_1) = e_H,$$

so $g_2^{-1}g_1 \in K$. By the lemma on equality of cosets, this means $g_1K = g_2K$. $\square$

Theorem 1.1 (Counting formula for homomorphisms). *If G is finite and $\varphi : G \rightarrow H$ is a homomorphism, then*

$$|G| = |\ker(\varphi)| \cdot |\operatorname{im}(\varphi)|. \quad (1.1)$$

In particular, $|\operatorname{im}(\varphi)|$ divides both $|G|$ and $|H|$ (the latter when H is finite).

Proof. By Proposition 1.1, $|\operatorname{im}(\varphi)| = |G/\ker(\varphi)|$. The counting formula applied to $\ker(\varphi) \leq G$ gives $|G| = |\ker(\varphi)| \cdot |G/\ker(\varphi)| = |\ker(\varphi)| \cdot |\operatorname{im}(\varphi)|$. Finally, $\operatorname{im}(\varphi) \leq H$, so Lagrange's theorem shows that $|\operatorname{im}(\varphi)|$ divides $|H|$. $\square$

Example 1.1 (The alternating group). For $n \geq 2$, the sign homomorphism $\operatorname{sgn} : S_n \rightarrow \{\pm 1\}$ is surjective (a transposition has sign -1) and its kernel is A_n . Hence

$$n! = |A_n| \cdot 2, \quad |A_n| = \frac{n!}{2}.$$

2. INDEX IN A TOWER OF SUBGROUPS

Recall the counting formula $|G| = [G : H] |H|$, where the index $[G : H] = |G/H|$ is the number of left cosets of H in G . (When we write $[G : H]$ we usually mean that it is finite.)

Theorem 2.1 (Tower law). *Let $K \leq H \leq G$ be a tower of subgroups. Then*

$$[G : K] = [G : H] [H : K]. \quad (2.1)$$

Proof. Assume $[G : H] = m$ and $[H : K] = n$ are finite. Then

$$G = g_1H \sqcup g_2H \sqcup \cdots \sqcup g_mH \quad (g_i \in G), \quad H = h_1K \sqcup \cdots \sqcup h_nK \quad (h_j \in H).$$

Substituting the second decomposition into the first,

$$G = g_1(h_1K \cup \cdots \cup h_nK) \cup \cdots \cup g_m(h_1K \cup \cdots \cup h_nK) = \bigcup_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} g_i h_j K.$$

It remains to show that the mn cosets $g_i h_j K$ are distinct, and hence (being cosets) disjoint. Suppose $g_i h_j K = g_{i'} h_{j'} K$. Since $h_j K \subseteq H$, we have $g_i h_j K \subseteq g_i H$ and similarly $g_{i'} h_{j'} K \subseteq g_{i'} H$. So $g_i H \cap g_{i'} H \neq \emptyset$, which forces $i = i'$. Cancelling g_i then gives $h_j K = h_{j'} K$, so $j = j'$. Therefore G is the disjoint union of exactly mn left cosets of K , and $[G : K] = mn$. $\square$

When G is finite, the tower law also follows directly from the counting formula:

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H] [H : K].$$

The proof above has the advantage that it works for infinite groups, as long as the indices are finite.

Example 2.1. For $8\mathbb{Z} \leq 2\mathbb{Z} \leq \mathbb{Z}$ we have $[\mathbb{Z} : 2\mathbb{Z}] = 2$ and $[2\mathbb{Z} : 8\mathbb{Z}] = 4$ (the cosets are $8\mathbb{Z}, 2 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 6 + 8\mathbb{Z}$), so $[\mathbb{Z} : 8\mathbb{Z}] = 2 \cdot 4 = 8$, matching Lecture 11. In S_3 , the tower $\{1\} \leq \{1, x, x^2\} \leq S_3$ gives $6 = [S_3 : \{1\}] = 2 \cdot 3$.