12 Kernels and normal subgroups (10/16)

Definition 12.1 (Kernels)**.** Let $f\colon G \to H$ be a group homomorphism. The kernel of f is the subset $\ker(f) \subseteq G$ consisting of elements $g \in G$ such that $f(g) = e$.

Lemma 12.2 (The kernel is a group)**.** *If $f\colon G \to H$ is a group homomorphism, then $\ker(f) \subseteq G$ is a subgroup.*

Proof. If $a, b \in \ker(f)$, then $f(ab) = f(a)f(b) = ee = e$, so $ab \in \ker(f)$. If $a \in \ker(f)$, then $e = f(e) = f(aa^{-1}) = f(a)f(a^{-1}) = ef(a^{-1}) = f(a^{-1})$, so $a^{-1} \in \ker(f)$. Finally, the kernel is non-empty as $e \in \ker(f)$. □

Example 12.3. Recall the sign homomorphism $\mathrm{sgn}\colon S_n \to \{\pm 1\}$. The kernel, consisting of the subset of *even* elements, is called the alternating group and denoted by A_n.

Definition 12.4 (Normal subgroups)**.** Let G be a group and $N \subseteq G$ be a subgroup. We say that N is a **normal** subgroup of G if for every $g \in G$ and $n \in N$ the conjugate of n by g, namely gng^{-1}, is in N.

Lemma 12.5 (Kernels are normal)**.** *If $f\colon G \to H$ is a group homomorphism, then $\ker(f)$ is a normal subgroup of G.*

Proof. Fix $n \in \ker(f)$, so that $f(n) = e$. Fix $g \in G$. Then, $f(gng^{-1}) = f(g)f(n)f(g^{-1}) = f(g)ef(g)^{-1} = e$, so $gng^{-1} \in \ker(f)$. □

Lemma 12.6 (Subgroups of abelian groups are normal)**.** *If G is an abelian group and $K \subseteq G$ is a subgroup, then K is normal.*

Proof. Indeed, if $n \in K$ and $g \in G$, then $gng^{-1} = gg^{-1}n = n$, which is certainly in K. □

Example 12.7 (Not all subgroups are normal)**.** We must look in a non-abelian group. Our first example is S_3. Consider the subgroup $K = \{e, (1\,2)\}$ in S_3. Then, $(1\,3)(1\,2)(1\,3) = (1\,3)(1\,3\,2) = (2\,3)$, which is not in K. So, letting $n = (1\,2)$ and $g = (1\,3)$ (so that $g^{-1} = (1\,3)$ as well), we see that K is not normal. In particular, this means that K is not the kernel of any group homomorphism $S_3 \to H$, by Lemma 12.5.

Lemma 12.8 (Right is left for cosets of normal subgroups)**.** *Let G be a group. If $N \subseteq G$ is a subgroup, then N is normal in G if and only if every left coset of N in G is a right coset of N in G.*

Proof. Using Exercise 12.2, we see that N is normal if and only if $gNg^{-1} = N$ for all $g \in G$, which is the case if and only if $gN = Ng$ for all $g \in G$. This shows that normality implies that the left and right cosets are the same. Now, suppose that every left coset gN is a right coset, say Nh for some h (depending on G). But, $g \in gN$, so $g \in Nh$, so $Nh = Ng$ by the right coset version of Lemma 11.5. In other words, for every g, we have $gN = Ng$, which yields $gNg^{-1} = N$ by multiplying on the right by g^{-1}. This proves normality of N in G. □

Lemma 12.9 (Products of (right) cosets are cosets)**.** *Fix a normal subgroup N in a group G. Then, the product of two right cosets is again a right coset.*

Proof. Let $g, h \in G$. Then, $(Ng)(Nh) = NN(gh) = N(gh)$, so the product of two right cosets is a right coset. Second, assume that products of right cosets are right cosets. □

Theorem 12.10 (Normal subgroups are kernels)**.** *Let $N \subseteq G$ be a normal subgroup. Then, the set of right cosets G/N is equipped with a group structure via $(Ng)(Nh) = N(gh)$, the map $f\colon G \to G/N$ given by $f(g) = Ng$ is a group homomorphism, and $N = \ker(f)$.*

Proof. The formula $(Ng)(Nh) = N(gh)$ is a well-defined binary operation on right cosets. It has an identity element given by $N = Ne$. The inverse of Ng is $N(g^{-1})$. And, associativity is inherited from the multiplication on G. Thus, G/N is a group under this multiplication of right cosets. Letting $f\colon G \to G/N$ be given by $f(g) = Ng$, we see $f(gh) = N(gh) = (Ng)(Nh) = f(g)f(h)$, so that f is a group homomorphism. Finally, the kernel of f consists of those $g \in G$ such that $f(g) = Ng = Ne = N$. But, this is precisely N. ☐

Definition 12.11 (Quotient groups)**.** If N is a normal subgroup of G, then the set of right cosets G/N with the product defined above is called the **quotient of** G **by** N. Quotient group constructions are ubiquitous and important ways of creating new groups and understanding given ones.

Definition 12.12 (Simple groups)**.** A group G is **simple** if its only normal subgroups are $\{e\}$ and G. Equivalently, G is simple if every group homomorphism $G \to H$ is either injective or sends all of G to $e \in H$. A major achievement of 20th century group theory is the classification of *finite* simple groups.

Example 12.13. Fix an integer $N \geqslant 1$ and let $N\mathbf{Z} \subseteq \mathbf{Z}$ be the subgroup of integers divisible by N. This is a normal subgroup. The quotient group $\mathbf{Z}/N\mathbf{Z}$ is what we have been writing as $\mathbf{Z}/N$. Put another way, there is a group homomorphism $f\colon \mathbf{Z} \to \mathbf{Z}/N$ given by $f(k) \equiv k \mod N$ whose kernel is $N\mathbf{Z}$.

Proposition 12.14 (Lagrange's theorem for normal subgroups)**.** *If N is a normal subgroup of a finite group G, then $|G/N||N| = |G|$.*

Proof. In fact, we already proved this last time under the weaker hypothesis that N is simply a subgroup. That was called Lagrange's theorem. ☐

Remark 12.15. Phrased differently, if $f\colon G \to H$ is a *surjective* group homomorphism where G is a finite group, then $|\ker(f)||H| = |G|$.

Example 12.16. The order of A_n is $\frac{n!}{2} = \binom{n}{2}$.

12.1 Exercises

Exercise 12.1. Fix $n \geqslant 3$ and let s denote the composition of the inclusion $D_{2n} \to S_n$ and the sign homomorphism $\mathrm{sgn}\colon S_n \to \{\pm 1\}$. Determine $\ker(s) \subseteq D_{2n}$.

Exercise 12.2. Prove that a subgroup $N \subseteq G$ is normal if and only if for every $g \in G$, the subset $gNg^{-1} = \{gng^{-1} : n \in N\}$ is equal to N.

Exercise 12.3. Prove that if $f\colon G \to H$ is a surjective group homomorphism with kernel $N = \ker(f)$, then $H \cong G/N$.

Exercise 12.4. Prove that if $N \geqslant 2$, then $\mathbf{Z}/N$ is simple if and only if N is prime.

Exercise 12.5. Prove that if A is a non-trivial abelian group (meaning that it is not isomorphic to the group $\{e\}$), then A is simple if and only if $A \cong \mathbf{Z}/p$ for some prime number p.