

Proposition 5. Let G be a group and let N be a subgroup of G .

(1) The operation on the set of left cosets of N in G described by

$$uN \cdot vN = (uv)N$$

is well defined if and only if $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$.

(2) If the above operation is well defined, then it makes the set of left cosets of N in G into a group. In particular the identity of this group is the coset $1N$ and the inverse of gN is the coset $g^{-1}N$ i.e., $(gN)^{-1} = g^{-1}N$.

Proof: (1) Assume first that this operation is well defined, that is, for all $u, v \in G$,

$$\text{if } u, u_1 \in uN \text{ and } v, v_1 \in vN \quad \text{then} \quad uvN = u_1v_1N.$$

Let g be an arbitrary element of G and let n be an arbitrary element of N . Letting $u = 1, u_1 = n$ and $v = v_1 = g^{-1}$ and applying the assumption above we deduce that

$$1g^{-1}N = ng^{-1}N \quad \text{i.e.,} \quad g^{-1}N = ng^{-1}N.$$

Since $1 \in N, ng^{-1} \cdot 1 \in ng^{-1}N$. Thus $ng^{-1} \in g^{-1}N$, hence $ng^{-1} = g^{-1}n_1$, for some $n_1 \in N$. Multiplying both sides on the left by g gives $gng^{-1} = n_1 \in N$, as claimed.

Conversely, assume $gng^{-1} \in N$ for all $g \in G$ and all $n \in N$. To prove the operation stated above is well defined let $u, u_1 \in uN$ and $v, v_1 \in vN$. We may write

$$u_1 = un \text{ and } v_1 = vm, \quad \text{for some } n, m \in N.$$

We must prove that $u_1v_1 \in uvN$:

$$\begin{aligned} u_1v_1 &= (un)(vm) = u(vv^{-1})nvm \\ &= (uv)(v^{-1}nv)m = (uv)(n_1m), \end{aligned}$$

where $n_1 = v^{-1}nv = (v^{-1})n(v^{-1})^{-1}$ is an element of N by assumption. Now N is closed under products, so $n_1m \in N$. Thus

$$u_1v_1 = (uv)n_2, \quad \text{for some } n_2 \in N.$$

Thus the left cosets uvN and u_1v_1N contain the common element u_1v_1 . By the preceding proposition they are equal. This proves that the operation is well defined.

(2) If the operation on cosets is well defined the group axioms are easy to check and are induced by their validity in G . For example, the associative law holds because for all $u, v, w \in G$,

$$\begin{aligned} (uN)(vNwN) &= uN(vwN) \\ &= u(vw)N \\ &= (uv)wN = (uNvN)(wN), \end{aligned}$$

since $u(vw) = (uv)w$ in G . The identity in G/N is the coset $1N$ and the inverse of gN is $g^{-1}N$ as is immediate from the definition of the multiplication.

As indicated before, the subgroups N satisfying the condition in Proposition 5 for which there is a natural group structure on the quotient G/N are given a name:

Definition. The element gng^{-1} is called the *conjugate* of $n \in N$ by g . The set $gNg^{-1} = \{gng^{-1} \mid n \in N\}$ is called the *conjugate* of N by g . The element g is said to *normalize* N if $gNg^{-1} = N$. A subgroup N of a group G is called *normal* if every element of G normalizes N , i.e., if $gNg^{-1} = N$ for all $g \in G$. If N is a normal subgroup of G we shall write $N \trianglelefteq G$.

Note that the structure of G is reflected in the structure of the quotient G/N when N is a normal subgroup (for example, the associativity of the multiplication in G/N is induced from the associativity in G and inverses in G/N are induced from inverses in G). We shall see more of the relationship of G to its quotient G/N when we consider the Isomorphism Theorems later in Section 3.

We summarize our results above as Theorem 6.

Theorem 6. Let N be a subgroup of the group G . The following are equivalent:

- (1) $N \trianglelefteq G$
- (2) $N_G(N) = G$ (recall $N_G(N)$ is the normalizer in G of N)
- (3) $gN = Ng$ for all $g \in G$
- (4) the operation on left cosets of N in G described in Proposition 5 makes the set of left cosets into a group
- (5) $gNg^{-1} \subseteq N$ for all $g \in G$.

Proof: We have already done the hard equivalences; the others are left as exercises.

As a practical matter, one tries to minimize the computations necessary to determine whether a given subgroup N is normal in a group G . In particular, one tries to avoid as much as possible the computation of all the conjugates gng^{-1} for $n \in N$ and $g \in G$. For example, the elements of N itself normalize N since N is a subgroup. Also, if one has a set of *generators* for N , it suffices to check that all conjugates of these generators lie in N to prove that N is a normal subgroup (this is because the conjugate of a product is the product of the conjugates and the conjugate of the inverse is the inverse of the conjugate) — this is Exercise 26 later. Similarly, if generators for G are also known, then it suffices to check that these generators for G normalize N . In particular, if generators for *both* N and G are known, this reduces the calculations to a small number of conjugations to check. If N is a *finite* group then it suffices to check that the conjugates of a set of generators for N by a set of generators for G are again elements of N (Exercise 29). Finally, it is often possible to prove directly that $N_G(N) = G$ without excessive computations (some examples appear in the next section), again proving that N is a normal subgroup of G without mindlessly computing all possible conjugates gng^{-1} .

We now prove that the normal subgroups are precisely the same as the kernels of homomorphisms considered earlier.

Proposition 7. A subgroup N of the group G is normal if and only if it is the kernel of some homomorphism.

Proof: If N is the kernel of the homomorphism φ , then Proposition 2 shows that the left cosets of N are the same as the right cosets of N (and both are the fibers of the

map φ). By (3) of Theorem 6, N is then a normal subgroup. (Another direct proof of this from the definition of normality for N is given in the exercises).

Conversely, if $N \trianglelefteq G$, let $H = G/N$ and define $\pi : G \rightarrow G/N$ by

$$\pi(g) = gN \quad \text{for all } g \in G.$$

By definition of the operation in G/N ,

$$\pi(g_1 g_2) = (g_1 g_2)N = g_1 N g_2 N = \pi(g_1) \pi(g_2).$$

This proves π is a homomorphism. Now

$$\begin{aligned} \ker \pi &= \{g \in G \mid \pi(g) = 1N\} \\ &= \{g \in G \mid gN = 1N\} \\ &= \{g \in G \mid g \in N\} = N. \end{aligned}$$

Thus N is the kernel of the homomorphism π .

The homomorphism π constructed above demonstrating the normal subgroup N as the kernel of a homomorphism is given a name:

Definition. Let $N \trianglelefteq G$. The homomorphism $\pi : G \rightarrow G/N$ defined by $\pi(g) = gN$ is called the *natural projection (homomorphism)*¹ of G onto G/N . If $\overline{H} \leq G/N$ is a subgroup of G/N , the *complete preimage* Of \overline{H} in G is the preimage of \overline{H} under the natural projection homomorphism.

The complete preimage of a subgroup of G/N is a subgroup of G (cf. Exercise 1) which contains the subgroup N since these are the elements which map to the identity $\bar{1} \in \overline{H}$. We shall see in the Isomorphism Theorems in Section 3 that there is a natural correspondence between the subgroups of G that contain N and the subgroups of the quotient G/N .

We now have an “internal” criterion which determines precisely when a subgroup N of a given group G is the kernel of some homomorphism, namely,

$$N_G(N) = G.$$

We may thus think of the normalizer of a subgroup N of G as being a measure of “how close” N is to being a normal subgroup (this explains the choice of name for this subgroup). Keep in mind that the property of being normal is an *embedding* property, that is, it depends on the relation of N to G , not on the internal structure of N itself (the same group N may be a normal subgroup of G but not be normal in a larger group containing G).

We began the discussion of quotient groups with the existence of a homomorphism φ of G to H and showed the kernel of this homomorphism is a normal subgroup N of G and the quotient G/N (defined in terms of fibers originally) is naturally isomorphic

¹The word “natural” has a precise mathematical meaning in the theory of categories; for our purposes we use the term to indicate that the definition of this homomorphism is a “coordinate free” projection i.e., is described only in terms of the elements themselves, not in terms of generators for G or N (cf. Appendix II).

to the image of G under φ in H . Conversely, if $N \trianglelefteq G$, we can find a group H (namely, G/N) and a homomorphism $\pi : G \rightarrow H$ such that $\ker \pi = N$ (namely, the natural projection). The study of homomorphic images of G (i.e., the images of homomorphisms from G into other groups) is thus equivalent to the study of quotient groups of G and we shall use homomorphisms to produce normal subgroups and vice versa.

We developed the theory of quotient groups by way of homomorphisms rather than simply defining the notion of a normal subgroup and its associated quotient group to emphasize the fact that the *elements* of the quotient are *subsets* (the fibers or cosets of the kernel N) of the original group G . The visualization in Figure 1 also emphasizes that N (and its cosets) are projected (or collapsed) onto single elements in the quotient G/N . Computations in the quotient group G/N are performed by taking *representatives* from the various cosets involved.

Some examples of normal subgroups and their associated quotients follow.

Examples

Let G be a group.

- (1) The subgroups 1 and G are always normal in G ; $G/1 \cong G$ and $G/G \cong 1$.
- (2) If G is an *abelian* group, any subgroup N of G is normal because for all $g \in G$ and all $n \in N$,

$$gng^{-1} = gg^{-1}n = n \in N.$$

Note that it is important that G be abelian, not just that N be abelian. The structure of G/N may vary as we take different subgroups N of G . For instance, if $G = \mathbb{Z}$, then every subgroup N of G is cyclic:

$$N = \langle n \rangle = \langle -n \rangle = n\mathbb{Z}, \quad \text{for some } n \in \mathbb{Z}$$

and $G/N = \mathbb{Z}/n\mathbb{Z}$ is a cyclic group with generator $\bar{1} = 1 + n\mathbb{Z}$ (note that 1 is a generator for G).

Suppose now that $G = Z_k$ is the cyclic group of order k . Let x be a generator of G and let $N \leq G$. By Proposition 2.6 $N = \langle x^d \rangle$, where d is the smallest power of x which lies in N . Now

$$G/N = \{gN \mid g \in G\} = \{x^\alpha N \mid \alpha \in \mathbb{Z}\}$$

and since $x^\alpha N = (xN)^\alpha$ (see Exercise 4 below), it follows that

$$G/N = \langle xN \rangle \quad \text{i.e., } G/N \text{ is cyclic with } xN \text{ as a generator.}$$

By Exercise 5 below, the order of xN in G/N equals d . By Proposition 2.5, $d = \frac{|G|}{|N|}$.

In summary,

quotient groups of a cyclic group are cyclic

and the image of a generator g for G is a generator \bar{g} for the quotient. If in addition G is a *finite* cyclic group and $N \leq G$, then $|G/N| = \frac{|G|}{|N|}$ gives a formula for the order of the quotient group.

- (3) If $N \leq Z(G)$, then $N \trianglelefteq G$ because for all $g \in G$ and all $n \in N$, $gng^{-1} = n \in N$, generalizing the previous example (where the center $Z(G)$ is all of G). Thus, in particular, $Z(G) \trianglelefteq G$. The subgroup $\langle -1 \rangle$ of Q_8 was previously seen to be the kernel of a homomorphism but since $\langle -1 \rangle = Z(Q_8)$ we obtain normality of this subgroup