

4 Quotient Groups and Normal Subgroups

We have observed that given any group homomorphism $\phi : G \rightarrow H$, the kernel $K = \ker(\phi)$ is a subgroup of G . So we ask, is every subgroup the kernel of some homomorphism, and if not, how can we characterize those that are.

First notice that the homomorphism ϕ defines a partition of G by $a \sim b \iff \phi(a) = \phi(b)$ (i.e. a and b are in the same “fiber” of ϕ). For $h \in H$, write $\phi^{-1}(h) = \{a \in G \mid \phi(a) = h\}$, the fiber of ϕ over h .

Proposition 4.1 $\forall x \in \phi^{-1}(h), \phi^{-1}(h) = xK = Kx$.

Proof. First show $\forall k \in K, \phi(xk) = \phi(x) = \phi(kx) = h$. This shows $xK \subseteq \phi^{-1}(h)$ and $Kx \subseteq \phi^{-1}(h)$. Then for $g \in \phi^{-1}(h)$, observe $x^{-1}g, gx^{-1} \in K$. This shows the opposite inclusions. (Observe that this is the same partition as considered in §1.7, exercise 18.)

Definition 4.2 *Let N be any subgroup of G . Then $gN := \{gn \mid n \in N\}$ is a left coset of N in G , and $Ng := \{ng \mid n \in N\}$ is a right coset of N in G . g is a coset representative for the coset gN , as is any other $g' \in gN$, for if $g' \in gN$, then $gN = g'N$. (The cosets partition G . (The right cosets are just the orbits in G under the action of N on G by left multiplication; similarly the left cosets are the orbits under the “right” action of right multiplication by elements of N on G .) We write G/N for the set of left cosets of N in G , and $G \backslash N$ for the set of right cosets of N in G .*

Let $[G : N]$ denote the cardinality of the set G/N . This is called the *index of N in G* . It is easy to see that if N is finite, then $|N| = |gN|$ (there is an obvious bijection between the two sets), and since the cosets partition G , we immediately obtain the following.

Theorem 4.3 Lagrange’s Theorem *Let H be a subgroup of G and suppose H is finite. Then every coset of H has $|H|$ elements. If further, either of $|G|$ or $[G : H]$ is finite, then so is the other, and*

$$|G| = [G : H] \cdot |H|.$$

The converse to Lagrange's Theorem is not true. The easiest example where one can see this is A_4 , which we have not yet defined, the *alternating group* on 4 letters. It is a subgroup of index 2 (and hence order 12) in S_4 . It has no subgroup of order 6, even though of course 6 divides 12. Your homework from §3.2 will provide a proof of a partial converse, though:

Theorem 4.4 Cauchy's Theorem *If G is a finite group and p divides the order of G , then G has a subgroup of order p .*

This is taken a step further in Sylow's Theorems, where we will see

Theorem 4.5 *If p^α divides the order of a finite group G , then G has a subgroup of order p^α .*

Corollary 4.6 *If G is a finite group, $x \in G$, then $|x| \mid |G|$, and $x^{|G|} = 1 \quad \forall x \in G$.*

Notice that Proposition 4.1 shows for subgroups which are kernels, left and right cosets are exactly the same. But, looking at S_3 for example, we can see that this is not true in general, so not all subgroups can be kernels. It turns out that for kernels, the set of left cosets in G themselves form a group in the "obvious" way, where the operation is "coset multiplication": $(aN)(bN) = abN$. This does not work if N is not a kernel.

Theorem 4.7 *Let G be a group, $N \leq G$. Then coset multiplication $aN \cdot bN = abN$ is a well-defined binary operation on G/N if and only if $gng^{-1} \in N$ for all $g \in G, n \in N$. In this case, G/N is a group under the operation coset multiplication. Moreover, there exists a group homomorphism $G \rightarrow G/N$, given by $g \mapsto gN$, with kernel N .*

Proof. In order to see that coset multiplication is well defined, we need to see that if $aN = cN, bN = dN$, then $abN = cdN$. The hypothesis says we can write $a = cn_1, b = dn_2$ for some $n_1, n_2 \in N$. Then $ab = cn_1dn_2$. If $gng^{-1} \in N \quad \forall g \in G, n \in N$, then $d^{-1}Nd = N$. Then we can write $cn_1dn_2 = cd(d^{-1}n_1d)n_2 = cdn'_1n_2 \in cdN$, where $n'_1 = d^{-1}n_1d \in N$.

Conversely, assume coset multiplication is well defined. Let $g \in G, n \in N$. Then $1N = nN$, so $g^{-1}N = (1N)(g^{-1}N) = (nN)(g^{-1}N) = ng^{-1}N$, which shows $ng^{-1} \in g^{-1}N$, and $gng^{-1} \in N$.

It then follows immediately from the associativity of the operation in G , as well as existence of identity and inverses in G , that these things hold in G/N , and so G/N is a group. (This is called a *quotient group*.)

Finally, define a map $\pi : G \rightarrow G/N$ by $\pi(g) = gN$. It is immediate to check that this is a group homomorphism, and the kernel is N .

Proposition 4.8 *Let $\phi : G \rightarrow H$ be a group homomorphism, and let $\phi(G)$ be the image of G under ϕ . Then $\phi(G)$ is a subgroup of H . If K is any subgroup of $\phi(G)$, then the complete preimage $\phi^{-1}(K)$ of K in G ($:= \{g \in G \mid \phi(g) \in K\}$) is a subgroup of G containing $\ker(\phi)$.*

Definition 4.9 *gng^{-1} is the conjugate of n by g . The element g normalizes N if $gNg^{-1} = N$. N is normal if $gNg^{-1} = N$ for all $g \in G$. In this case we write $N \trianglelefteq G$.*

(We will see later that $\phi^{-1}(K) \trianglelefteq G \iff K \trianglelefteq \phi(G)$.)

Summarizing, we have for $N \leq G$, the following equivalent statements:

1. $N \trianglelefteq G$, or by definition $gNg^{-1} = N \quad \forall g \in G$.
2. $N_G(N) = G$.
3. $gN = Ng \quad \forall g \in G$.
4. Left coset multiplication is well defined for G/N .
5. N is the kernel of some group homomorphism

More examples and consequences: Every (nontrivial) group G always has at least two normal subgroups, namely $\{1\}$ and G . If these are the only subgroups of G which are normal, G is said to be *simple*. If G is abelian, every subgroup of G is normal in G . Thus the only simple abelian groups are those of prime order. More generally, any subgroup of $Z(G)$ is normal in G . In some sense $G/Z(G)$ measures how far the group G is from being abelian.

Observe that for any group G and any homomorphism ϕ , the image $\phi(G)$ of G is generated by the images $\phi(g)$ of the generators g of G . Thus, in particular, quotients of cyclic groups are cyclic.

Let H be any subgroup of G of index 2. Then H is normal in G . (We will see later that a somewhat more general phenomenon occurs in finite groups:

if p is the least prime dividing the order of G and H is a subgroup of G of index p , then H is normal in G .) For the case of a subgroup of index 2, the proof is basically that there just isn't enough "maneuvering room" for it not to be normal: $gH = \{a \in G \mid a \notin H\} = Hg$ for all $g \notin H$, so left cosets equal right cosets and H is normal.

More on cosets

If H and K are subgroups of a group G , we define $HK := \{hk \mid h \in H, k \in K\}$. This is not in general a subgroup of G . However, if $H \leq N_G(K)$, then it is a subgroup, so in particular, if $K \trianglelefteq G$, then $HK \leq G$ for any $H \leq G$. This is a direct consequence of the next proposition. (But the condition above is not necessary for HK to be a group – see, e.g., example in text pp.95–96.)

Proposition 4.10 *If H, K are subgroups of G , then HK is a subgroup if and only if $HK = KH$.*

Proof. Assume $HK = KH$. We need to see if $a, b \in HK$, then $ab^{-1} \in HK$. Let $a = h_1k_1, b = h_2k_2$. Then $ab^{-1} = h_1k_1k_2^{-1}h_2^{-1}$, but $k_1k_2^{-1}h_2^{-1} = h^3k_3 \exists h_3 \in H, k_3 \in K$, because $KH = HK$. Thus $ab^{-1} = h_2h_3k_3 \in HK$.

Conversely, if $HK \leq G$, since $K \leq HK, H \leq HK$, we must have $KH \subseteq HK$. Now suppose $hk \in HK$. Let $(hk)^{-1} = h_0k_0 \in HK$. Then $hk = k_0^{-1}h_0^{-1} \in KH$, so $HK \subseteq KH$, showing equality.

Whether or not HK is a group, we can say something about the size of the set HK .

Proposition 4.11 Index Theorem *If H, K are finite subgroups of a group G , then*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Also $[G : H \cap K] \leq [G : H][G : K]$, with equality if $[G : H], [G : K]$ both finite and relatively prime.

Proof. $HK = \cup_{h \in H} hK$ is a union of cosets. Each coset has $|K|$ elements, so we need only show that the number of distinct such cosets is $|H|/|H \cap K|$. Now $h_1K = h_2K \iff h_2^{-1}h_1 \in K, \iff h_2^{-1}h_1 \in H \cap K, \iff h_1(H \cap K) = h_2(H \cap K)$. So the number of distinct cosets is the number of cosets of $H \cap K$ in H , which is $|H|/|H \cap K|$.

Now let $\{x_i \mid i \in I\}$ be a set of left coset representatives of $H \cap K$ in G . Then consider pairs of cosets $(x_iH, x_iK), i \in I$. Now $(x_iH, x_iK) =$

$(x_j H, x_j K) \iff x_j^{-1} x_i \in H \cap K, \iff x_i(H \cap K) = x_j(H \cap K)$. Thus the map $x_i(H \cap K) \mapsto (x_i H, x_i K)$ is an injection, so $[G : H \cap K] \leq [G : H][G : K]$. If $[G : H], [G : K]$ finite, each divides $[G : H \cap K]$, and if relatively prime, their product divides it as well.

Notice that if two subgroups H, K have relatively prime orders, then $H \cap K = \{1\}$, so that $|HK| = |H||K|$. This can be surprisingly useful – for example, if we identify D_8 with a subgroup of S_4 , and consider any 3-cycle in S_4 , then the 3-cycle together with the generators of D_8 must generate the entire group – $|D_8| = 8$, and the subgroup generated by the 3-cycle has order 3, so the two subgroups together give a set of order 24, which then must be the whole group. In a similar vein, we see any two distinct transpositions generate all of S_3 , for the subgroup generated by (a, b) and (a, c) must contain the set $\langle (a, b) \rangle \langle (a, c) \rangle$, and since these two subgroups have nontrivial intersection, this set has 4 elements. The smallest subgroup of S_3 containing a 4-element set must be the whole group.