Cosets, Lagrange's theorem and normal subgroups

1 Cosets

Our goal will be to generalize the construction of the group $\mathbb{Z}/n\mathbb{Z}$. The idea there was to start with the group $\mathbb{Z}$ and the subgroup $n\mathbb{Z} = \langle n \rangle$, where $n \in \mathbb{N}$, and to construct a set $\mathbb{Z}/n\mathbb{Z}$ which then turned out to be a group (under addition) as well. (There are two binary operations $+$ and $\cdot$ on $\mathbb{Z}$, but $\mathbb{Z}$ is just a group under addition. Thus, the fact that we can also define multiplication on $\mathbb{Z}/n\mathbb{Z}$ will not play a role here, but its natural generalization is very important in Modern Algebra II.) We would like to generalize the above constructions, beginning with congruence mod n, to the case of a general group G (written multiplicatively) together with a subgroup H of G. However, we will have to be very careful if G is not abelian.

Definition 1.1. Let G be a group and let $H \leq G$. We define a relation $\equiv_\ell \pmod{H}$ on G as follows: if $g_1, g_2 \in G$, then $g_1 \equiv_\ell g_2 \pmod{H}$ if $g_1^{-1}g_2 \in H$, or equivalently if there exists an $h \in H$ such that $g_1^{-1}g_2 = h$, i.e. if $g_2 = g_1 h$ for some $h \in H$.

Proposition 1.2. *The relation* $\equiv_\ell \pmod{H}$ *is an equivalence relation. The equivalence class containing* g *is the set*

$$gH = \{gh : h \in H\}.$$

Proof. For all $g \in G$, $g^{-1}g = 1 \in H$. Hence $g \equiv_\ell g \pmod{H}$ and $\equiv_\ell \pmod{H}$ is reflexive. If $g_1 \equiv_\ell g_2 \pmod{H}$, then $g_1^{-1}g_2 \in H$. But since the inverse of an element of H is also in H, $(g_1^{-1}g_2)^{-1} = g_2^{-1}(g_1^{-1})^{-1} = g_2^{-1}g_1 \in H$. Thus $g_2 \equiv_\ell g_1 \pmod{H}$ and hence $\equiv_\ell \pmod{H}$ is symmetric. Finally, if $g_1 \equiv_\ell g_2 \pmod{H}$ and $g_2 \equiv_\ell g_3 \pmod{H}$, then $g_1^{-1}g_2 \in H$ and $g_2^{-1}g_3 \in H$. Since H is closed under taking products, $g_1^{-1}g_2g_2^{-1}g_3 = g_1^{-1}g_3 \in H$. Hence $g_1 \equiv_\ell g_3 \pmod{H}$ so that $\equiv_\ell \pmod{H}$ is transitive. Thus $\equiv_\ell \pmod{H}$ is an equivalence relation. (Notice how we exactly used the defining properties of a subgroup.) Clearly, the equivalence class containing g is the set gH defined above. $\square$

Definition 1.3. The set gH defined above is the *left coset* of H containing g. By general properties of equivalence classes, $g \in gH$ and two left cosets g_1H and g_2H are either disjoint or equal. Note that the subgroup H is itself a coset, since $H = 1 \cdot H = hH$ for every $h \in H$. It is called the *identity coset*. The set of all left cosets, i.e. the set of all equivalence classes for the equivalence relation $\equiv_\ell \pmod{H}$, is denoted G/H.

Right cosets $Hg = \{hg : h \in H\}$ are similarly defined. They are equivalence relations for the equivalence relation $\equiv_r \pmod{H}$ defined by: $g_1 \equiv_r g_2 \pmod{H}$ if $g_2g_1^{-1} \in H$, or equivalently if there exists an $h \in H$ such that $g_2g_1^{-1} = h$, i.e. if $g_2 = hg_1$ for some $h \in H$. The set of all equivalence classes for the equivalence relation $\equiv_r \pmod{H}$, is denoted $H\backslash G$. However, we will sometimes just use "coset" to mean "left coset" and use "right coset" for emphasis. Of course, if G is abelian, there is no difference between left cosets and right cosets. (There is also a somewhat non-obvious bijection from the set G/H to the set $H\backslash G$; this is a homework problem. However, as we shall see below, in general the sets G/H and $H\backslash G$ are different.)

Example 1.4.

1. For $G = \mathbb{Z}$ (under addition) and $H = \langle n\rangle = n\mathbb{Z}$, where $n \in \mathbb{N}$, we recover $\mathbb{Z}/n\mathbb{Z}$. Here the cosets are the subsets of $\mathbb{Z}$ of the form $0 + \langle n\rangle = [0]_n, \dots, (n-1) + \langle n\rangle = [n-1]_n$.

2. For any G, with $H = G$, for all $g_1, g_2 \in G$, $g_1 \equiv_\ell g_2 \pmod{G}$, there is just one left coset $gG = G$ for all $g \in G$, and G/G is the single element set $\{G\}$. Similarly there is just one right coset $G = Gg$ for every $g \in G$; in particular, the set of right cosets is the same as the set of left cosets. For the trivial subgroup $\{1\}$, $g_1 \equiv_\ell g_2 \pmod{\{1\}} \iff g_1 = g_2$, and the left cosets of $\{1\}$ are of the form $g\{1\} = \{g\}$. Thus $G/\{1\} = \{\{g\} : g \in G\}$, the set of 1-element subsets of G, and hence there is an obvious bijection from $G/\{1\}$ to G. As $\{1\}g = \{g\}$, every right coset is again a left coset and vice-versa.

3. In the group S_3, with notation as in the handout on group tables, taking for H the subgroup $A_3 = \langle \rho_1\rangle = \{1, \rho_1, \rho_2\}$, there are two left cosets: $A_3 = \{1, \rho_1, \rho_2\}$ and $\tau_1A_3 = \{\tau_1, \tau_2, \tau_3\}$. It is easy to see that these two sets are also the right cosets for A_3.

4. Again with $G = S_3$, if instead of A_3 we take for H the 2-element subgroup $\langle \tau_1\rangle = \{1, \tau_1\}$, then there are three left cosets: $\{1, \tau_1\}$, $\{\rho_1, \tau_3\}$, and $\{\rho_2, \tau_2\}$, each with two elements. Thus S_3 is divided up into three disjoint subsets. We can also consider the right cosets for $\{1, \tau_1\}$. There are three right cosets: $\{1, \tau_1\}$, $\{\rho_1, \tau_2\}$, and $\{\rho_2, \tau_3\}$. In partic-

ular, we see that the right cosets are not in general equal to the left cosets.

5. To generalize the first part of (3) above, consider $G = S_n$ and $H = A_n$. Our discussion on A_n showed that, if τ is any odd permutation, then the coset τA_n is the subset of odd permutations of S_n. Hence there are exactly two left cosets of A_n in S_n, the identity coset A_n which is the subset of even permutations and the set τA_n, where τ is any odd permutation, which is the same as the set of odd permutations and hence equals $S_n - A_n$. It is easy to see that $S_n - A_n = A_n\tau$ for every odd permutation τ, and hence the right cosets are the same as the left cosets in this case.

In general, we would like to count how many elements there are in a left coset as well as how many left cosets there are.

Proposition 1.5. *Let G be a group, H a subgroup, and $g \in G$. The function $f(h) = gh$ defines a bijection from H to gH. Hence, if g_1H and g_2H are two cosets, there is a bijection from g_1H to g_2H. Finally, if H is finite, then every left coset gH is finite, and $\#(gH) = \#(H)$.*

Proof. Defining f as in the statement, clearly f is surjective by definition, and f is injective by cancellation, since $gh_1 = gh_2 \implies h_1 = h_2$. Thus f is a bijection. The remaining statements are clear. $\square$

Definition 1.6. Let G be a group and let H be a subgroup of G. If the set G/H is finite, then we say H *is of finite index in* G and call the number of elements $\#(G/H)$ the *index* of G in H. We denote $\#(G/H)$ by $(G : H)$. If G/H is infinite, then we say H *is of infinite index in* G.

Thus, for $n \in \mathbb{N}$, the index $(\mathbb{Z} : n\mathbb{Z})$ is n, even though both $\mathbb{Z}$ and $n\mathbb{Z}$ are infinite. On the other hand, $\{0\}$ is of infinite index in $\mathbb{Z}$. Clearly, if G is finite, then every subgroup H has finite index. Every element of G is in exactly one left coset gH. There are $(G : H)$ left cosets gH, and each one has exactly $\#(H)$ elements. Adding up all of the elements in all of the left cosets must give the number of elements of G. Hence:

Proposition 1.7. *Let G be a finite group and let H be a subgroup of G. Then $\#(G) = (G : H)\#(H)$. In other words, the index $(G : H)$ satisfies:*

$$(G : H) = \#(G)/\#(H). \quad \square$$

This very simple counting argument has a large number of significant corollaries:

Corollary 1.8 (Lagrange's Theorem). *Let G be a finite group and let H be a subgroup of G. Then $\#(H)$ divides $\#(G)$.* $\square$

Remark 1.9. We have already seen that Lagrange's Theorem holds for a cyclic group G, and in fact, if G is cyclic of order n, then for each divisor d of n there exists a subgroup H of G of order n, in fact exactly one such. The "converse to Lagrange's Theorem" is however **false** for a general finite group, in the sense that there exist finite groups G and divisors d of $\#(G)$ such that there is no subgroup H of G of order d. The smallest example is the group A_4, of order 12. One can show that there is no subgroup of A_4 of order 6 (although it does have subgroups of orders $1, 2, 3, 4, 12$). Also, a group that is noncyclic can have more than one subgroup of a given order. For example, the Klein 4-group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ has three subgroups of order 2, as doers S_3.

Corollary 1.10. *Let G be a finite group and let $g \in G$. Then the order of g divides $\#(G)$.*

Proof. This follows from Lagrange's Theorem applied to the subgroup $\langle g \rangle$, noting that the order of g is equal to $\#(\langle g \rangle)$. $\square$

Corollary 1.11. *Let G be a finite group of order N and let $g \in G$. Then $g^N = 1$.*

Proof. Clear from the above corollary, since the order of g divides N. $\square$

Corollary 1.12. *Let G be a finite group of order p, where p is a prime number. Then G is cyclic, and hence $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Proof. Since $p > 1$, there exists a $g \in G$ such that $g \neq 1$. Hence the order of $\langle g \rangle$ is greater than 1 and, by Lagrange's theorem, $\#(\langle g \rangle)$ divides $\#(G) = p$. Thus $\#(\langle g \rangle) = p = \#(G)$, and hence $\langle g \rangle = G$ and G is cyclic. $\square$

Corollary 1.13 (Fermat's Little Theorem). *Let p be a prime number and let $a \in \mathbb{Z}$. Then $a^p \equiv a \pmod{p}$.*

Proof. First suppose that p does not divide a. Then a defines an element in $(\mathbb{Z}/p\mathbb{Z})^*$, also denoted by a. Since the order of $(\mathbb{Z}/p\mathbb{Z})^*$ is $p - 1$, it follows that $a^{p-1} = 1$ in $(\mathbb{Z}/p\mathbb{Z})^*$. Viewing a instead as an integer, this says that $a^{p-1} \equiv 1 \pmod{p}$, and multiplying both sides by a gives $a^p \equiv a \pmod{p}$. The remaining case is when p divides a, but then both a^p and a are $\equiv 0 \pmod{p}$, so the equality holds in this case as well. $\square$

Corollary 1.14 (Euler's Generalization of Fermat's Little Theorem)**.** *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$, $\gcd(a, n) = 1$. Then, if ϕ is the Euler ϕ-function, $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Proof. The proof is similar to the previous proof, viewing a as an element of $(\mathbb{Z}/n\mathbb{Z})^*$, and using the fact that the order of $(\mathbb{Z}/n\mathbb{Z})^*$ is $\phi(n)$. $\square$

We record one useful numerical property of the index:

Lemma 1.15. *Let G be a finite group and let H, K be two subgroups of G with $K \leq H$. Then the index is multiplicative in the sense that*

$$(G : K) = (G : H)(H : K).$$

Proof. This follows from Proposition 1.7:

$$(G : H)(H : K) = \left(\frac{\#(G)}{\#(H)}\right)\left(\frac{\#(H)}{\#(K)}\right) = \frac{\#(G)}{\#(K)} = (G : K).$$

$\square$

The lemma is still true in case G is infinite, with the meaning that if any two of the terms in the formula are finite, then so is the third and the equality holds. The proof is somewhat more involved.

2 Normal subgroups

We would now like to find a binary operation on the set of left cosets G/H, by analogy with the way that we were able to add cosets in $\mathbb{Z}/n\mathbb{Z}$. Of course, for a multiplicative group G, we will want to **multiply** cosets, not add them. However, as we shall see, if G is not abelian, this will not always be possible. In general, given two cosets aH and bH, there is really only one reasonable way to define the product $(aH)(bH)$: it should be the coset $(ab)H$. In other words, we choose the representatives $a \in aH$ and $b \in bH$ and multiply the cosets aH and bH by multiplying the representatives a and b and taking the unique coset $(ab)H$ which contains the product ab. As is usual with working with equivalence classes, we must check that this procedure is **well-defined**, in other words that changing the choice of representatives does not change the final coset. As we shall see, this imposes a condition on the subgroup H.

To analyze this condition, suppose that we pick **different** representatives from the cosets aH and bH, necessarily of the form ah_1 and bh_2. The condition that the product $(ah_1)(bh_2)$ is in the same left coset as ab is just the statement that there exists an $h_3 \in H$ such that $(ah_1)(bh_2) = abh_3$. So this is the condition that coset multiplication is well-defined: for all $a, b \in G$ and for all $h_1, h_2 \in H$, there exists an $h_3 \in H$ such that

$$ah_1bh_2 = abh_3.$$

Of course, we can cancel the a's in front, and move the h_2 to the right hand side by multiplying by h_2^{-1}, giving $h_1b = bh_3h_2^{-1}$. Since we just require that h_3 is some element of H and hence that $h_3h_2^{-1}$ is some element of H, we see that coset multiplication is well-defined $\iff$ for all $b \in G$ and for all $h_1 \in H$, there exists an $h' \in H$ such that $h_1b = bh'$. The choice of names $b \in G$ and $h_1 \in H$ is not really optimal, since they are meant to be arbitrary, so we write this as follows:

Proposition 2.1. *Coset multiplication is well-defined on the set G/H of left cosets $\iff$ for all $g \in G$ and all $h \in H$, there exists an $h' \in H$ such that $hg = gh'$.* $\square$

There are many more suggestive ways to rewrite this condition. Clearly, the set $\{hg : h \in H\}$ is just the **right** coset Hg. So the proposition can be more simply rewritten as:

Proposition 2.2. *Coset multiplication is well-defined on the set G/H of left cosets $\iff$ for all $g \in G$, the right coset Hg is contained in the left coset gH.* $\square$

The above rewording still looks somewhat asymmetrical as far as left and right are concerned. The trick here is to note that, if an inclusion $Hg \subseteq gH$ holds for **all** $g \in G$, then it also holds for g^{-1}. But the inclusion $Hg^{-1} \subseteq g^{-1}H$ says that, for all $h \in H$, there exists an $h' \in H$ such that $hg^{-1} = g^{-1}h'$, and hence that $gh = h'g$. This says that the **left** coset gH is contained in the right coset Hg. Thus, if $Hg \subseteq gH$ holds for **all** $g \in G$, then $gH \subseteq Hg$ for all $g \in G$ as well, and hence $Hg = gH$. Of course, a symmetrical argument shows that, if the left coset gH is contained in the right coset Hg for all $g \in G$, then again $Hg = gH$. We see that we have proved:

Proposition 2.3. *Let G be a group and let H be a subgroup. Then the following are equivalent:*

(i) *Coset multiplication is well-defined on the set G/H of left cosets.*

(ii) *For all $g \in G$, the right coset Hg is contained in the left coset gH.*

(iii) *For all $g \in G$, the left coset gH is contained in the right coset Hg.*

(iv) *For all $g \in G$, $gH = Hg$, i.e. every left coset gH is also a right coset, necessarily equal to Hg since $g \in gH$.* □

It is often useful to rework these conditions yet again. Clearly, the condition that for all $g \in G$ and for all $h \in H$, there exists an $h' \in H$ such that $hg = gh'$ is the same as the condition that, for all $g \in G$ and for all $h \in H$, $g^{-1}hg = h'$ is some element of H. Write $g^{-1}Hg$ for the set $\{g^{-1}hg : h \in H\}$. Then we have the following:

Proposition 2.4. *Let G be a group and let H be a subgroup of G. Then the following are equivalent:*

(i) *Coset multiplication is well-defined on the set G/H of left cosets.*

(ii) *For all $g \in G$, $g^{-1}Hg \subseteq H$.*

(iii) *For all $g \in G$, $g^{-1}Hg = H$.*

Proof. We have seen that (i) and (ii) are equivalent, and clearly (iii) $\implies$ (ii). To see that (ii) $\implies$ (iii), we use the previous trick of replacing g by g^{-1}: If $(g^{-1})^{-1}Hg^{-1} = gHg^{-1} \subseteq H$, then for all $h \in H$, there exists an h' such that $ghg^{-1} = h'$, so that $h = g^{-1}h'g$. This says that $H \subseteq g^{-1}Hg$, hence $H = g^{-1}Hg$. Thus (ii) $\implies$ (iii) and so (ii) and (iii) are equivalent. □

Remark 2.5. Replacing g by g^{-1}, we will usually replace (ii) above by the condition that, all $g \in G$, $gHg^{-1} \subseteq H$, and (iii) by the condition that, all $g \in G$, $gHg^{-1} = H$.

Remark 2.6. Define a function $i_g : G \to G$ by $i_g(x) = gxg^{-1}$. As we have seen in the homework, i_g is an automorphism of G (i.e. an isomorphism from G to itself), and hence $i_g(H) = gHg^{-1}$ is a subgroup of G. Then the condition (iii) of the previous proposition is that, for all $g \in G$, $i_g(H) = H$.

Definition 2.7. Let G be a group and let H be a subgroup of G. Then H is a *normal subgroup* of G, written $H \lhd G$, if H satisfies any (and hence all) of the equivalent conditions of the previous two propositions.

Remark 2.8. (i) In practice, one usually checks that H is a normal subgroup of G by showing that, for all $g \in G$, $gHg^{-1} \subseteq H$.

(ii) By negating the definition, H is **not** a normal subgroup of G if there exists a $g \in G$ and an $h \in H$ such that $ghg^{-1} \notin H$.

Example 2.9. Here are some examples of normal subgroups.

1. For every group G, the subgroup G and the trivial subgroup $\{1\}$ are normal subgroups.

2. If G is **abelian** then every subgroup of G is abelian. For example, there is no difference in this case between left and right cosets; alternatively, $gHg^{-1} = H$ for all $g \in G$.

3. A_n is a normal subgroup of S_n, since if $\sigma \in A_n$ and $\rho \in S_n$, then
$$\varepsilon(\rho\sigma\rho^{-1}) = \varepsilon(\rho)\varepsilon(\sigma)\varepsilon(\rho^{-1}) = \varepsilon(\rho)\varepsilon(\rho^{-1}) = 1.$$
We will have other ways of seeing this later.

4. $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$, since, if $B \in SL_n(\mathbb{R})$ and $A \in GL_n(\mathbb{R})$, then
$$\det(ABA^{-1}) = (\det A)(\det B)(\det A^{-1}) = (\det A)(\det A)^{-1} = 1.$$
Again, we will see that this is part of a general picture later.

5. Let G_1 and G_2 be two groups and consider the Cartesian product $G_1 \times G_2$. As we have seen, there are two special subgroups of $G_1 \times G_2$: $H_1 = G_1 \times \{1\}$ and $H_2 = \{1\} \times G_2$. It is easy to check from the definitions that H_1 and H_2 are normal subgroups of $G_1 \times G_2$.

6. Recall that, for any group G, the *center* $Z(G)$ is the subgroup given by
$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\ \}.$$
Clearly, if $H \leq Z(G)$, then $H \lhd G$, since for all $g \in G$ and all $h \in H$, $ghg^{-1} = h$. In particular, $Z(G) \lhd G$.

Example 2.10. Here are some examples of subgroups which are **not** normal subgroups.

1. Consider the subgroup $\langle\tau_1\rangle$ of S_3, whose left cosets were worked out above: they are $\{1, \tau_1\}$, $\{\rho_1, \tau_3\}$, and $\{\rho_2, \tau_2\}$. We claim that coset multiplication is not well-defined, and hence $\langle\tau_1\rangle$ is not a normal subgroup of S_3. Consider the "product" of the identity coset $\{1, \tau_1\}$ and $\{\rho_1, \tau_3\}$. Choosing the representatives $1 \in \{1, \tau_1\}$ and $\rho_1 \in \{\rho_1, \tau_3\}$ would give the product as $\rho_1\langle\tau_1\rangle = \{\rho_1, \tau_3\}$. Choosing instead the representatives τ_1 and ρ_1, and noting that $\tau_1\rho_1 = \tau_2$, we would get instead the coset $\tau_2\langle\tau_1\rangle = \{\rho_2, \tau_2\} \neq \{\rho_1, \tau_3\}$. Hence coset multiplication is not well-defined.

2. D_4 is not a normal subgroup of S_4. As we have seen, the only transpositions contained in D_4 are $(1,3)$ and $(2,4)$, corresponding to reflections about the diagonals of a square. But $(2,3)(1,3)(2,3)^{-1} = (1,2) \notin D_4$, so that there exist $g = (2,3) \in S_4$ and $h = (1,3) \in D_4$ such that $ghg^{-1} \notin D_4$. Hence D_4 is not normal.

3. Most of the linear algebra subgroups we have written down are not normal. For example, O_n is not a normal subgroup of $GL_n(\mathbb{R})$ and SO_n is not a normal subgroup of $SL_n(\mathbb{R})$. In fact, for many groups G (despite the example of abelian groups), it is rather rare to find normal subgroups other than the obvious subgroups G and $\{1\}$.

Let us return to the example of $A_n \leq S_n$ given above and generalize it:

Proposition 2.11. *Let G be a group, not necessarily finite, and let H be a subgroup of G such that the index $(G : H) = 2$. Then H is a normal subgroup of G.*

Proof. If there are only two left cosets, then H is one of them, and the other must be of the form gH for any $g \notin H$, with $H \cup (gH) = G$ and $H \cap gH = \emptyset$. Thus (as with $A_n \leq S_n$) $gH = G - H$. Now suppose that Hg is a right coset. If $g \in H$, then $Hg = H$ is a left coset. If $g \neq H$, then $Hg \cap H = \emptyset$, hence $Hg \subseteq G - H = gH$. Thus every right coset Hg is contained in a left coset and hence H is normal. □

Now let us return to our original motivation of turning G/H into a group.

Proposition 2.12. *Let G be a group and let H be a normal subgroup of G. Then G/H is a group under coset multiplication, called the quotient group. Moreover, if $\pi\colon G \to G/H$ is the function defined by $\pi(g) = gH$, then π is a surjective homomorphism, called the quotient homomorphism, and $\operatorname{Ker}\pi = H$.*

Proof. The main point is that, as we have seen, coset multiplication is well-defined. Once this is so, all the the basic properties we need to check to show that G/H is a group are "inherited" from the corresponding properties in the group G. We run through them:

1. Associativity: we must show that, for all $g_1, g_2, g_3 \in G$,

$$(g_1H)[(g_2H)(g_3H)] = [(g_1H)(g_2H)](g_3H).$$

But by definition

$$(g_1H)[(g_2H)(g_3H)] = (g_1H)(g_2g_3H) = (g_1(g_2g_3))H$$
$$= ((g_1g_2)g_3)H = [(g_1H)(g_2H)](g_3H),$$

where we have used the fact that multiplication in G is associative. Hence coset multiplication is associative.

2. Identity: For all $g \in G$, $H \cdot gH = (1H) \cdot gH = (1g)H = gH$, and similarly $(gH) \cdot H = gH$.

3. Inverses: we shall show that $(gH)^{-1} = g^{-1}H$. In fact,

$$gHg^{-1}H = (gg^{-1})H = 1H = H,$$

and similarly $g^{-1}HgH = H$.

Thus G/H is a group under multiplication. Next we check that the function π is a homomorphism: for all $g_1, g_2 \in G$,

$$\pi(g_1g_2) = (g_1g_2)H = (g_1H)(g_2H) = \pi(g_2)\pi(g_2).$$

Hence by definition π is a homomorphism. It is clearly surjective since every element of G/H is of the form gH and hence is in the image of π. Finally, $g \in \operatorname{Ker}\pi \iff \pi(g) = gH = H$, the identity coset. Since $g \in gH$, if $gH = H$ then $g \in H$; conversely, if $g \in H$, then clearly $gH \subseteq H$ and hence $gH = H$. We see that $\operatorname{Ker}\pi$, which by definition is the inverse image of the identity coset, i.e. is the set of $g \in G$ such that $gH = H$, is exactly H. $\square$

Remark 2.13. (i) Some people call the group G/H a *factor group*.

(ii) Arguing as in the proof that G/H is associative, it is easy to see that, if G is abelian, then G/H is abelian. However, it is possible for G not to be abelian but for G/H to be abelian. For example, in case H has index two in G, for example in the case $G = S_n$ and $H = A_n$, then G/H has order two and hence is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. But S_n is not abelian if $n \geq 3$.

(iii) It is easy to see that, if G is cyclic, then G/H is cyclic. For example, let $G = \mathbb{Z}/n\mathbb{Z}$. Then for each $d|n$ we have the subgroup $H = \langle d \rangle$, or order n/d. Since G is abelian, H is automatically a normal subgroup of G. Hence $(\mathbb{Z}/n\mathbb{Z})/\langle d \rangle$ is a cyclic group of order equal to the index of $\langle d \rangle$ in $\mathbb{Z}/n\mathbb{Z}$, namely $n/(n/d) = d$. Thus $(\mathbb{Z}/n\mathbb{Z})/\langle d \rangle \cong \mathbb{Z}/d\mathbb{Z}$.

For future reference, we collect some facts about normal subgroups. The proofs are straightforward.

Proposition 2.14. *Let G be a group and let H and K be subgroup of G. Then:*

(i) *If $H \lhd G$ and $K \lhd G$, then $H \cap K \lhd G$.*

(ii) *If $H \lhd G$ and $K \leq G$, then $H \cap K \lhd K$.*

(iii) *If $H \leq K \leq G$ and $H \lhd G$, then $H \lhd K$.*

(iv) *If $H \lhd G$ and $K \leq G$, then the subset*

$$HK = \{hk : h \in H \text{ and } k \in K\}$$

is a subgroup of G.

Remark 2.15. (i) **Warning:** It is possible that, in the above notation, we could have $H \lhd K$ and $K \lhd G$ but that H is not a normal subgroup of G. In other words, the property of being a normal subgroup is **not transitive** in general. Examples will be given in the homework.

(ii) If H and K are two arbitrary subgroups of G, neither one of which is normal, then the set HK defined in (4) above need not be a subgroup. For example, taking $G = S_3$, $H = \langle \tau_1 \rangle = \{1, \tau_1\}$ and $K = \langle \tau_2 \rangle = \{1, \tau_2\}$, it is easy to see that

$$HK = \{1, \tau_1, \tau_2, \tau_1\tau_2 = \rho_1\}.$$

In particular, $\#(HK) = 4$ and so HK cannot be a subgroup, since otherwise we would get a contradiction to Lagrange's theorem.

3 Homomorphisms and normal subgroups

We begin with a discussion of the relationship between quotient groups and homomorphisms. If G is a group and $H \lhd G$, then we have the quotient group G/H and the quotient homomorphism $\pi \colon G \to G/H$, with $\operatorname{Ker} \pi = H$. Conversely, suppose that $f \colon G_1 \to G_2$ is a homomorphism from a group G_1 to another group G_2. We want to analyze f in terms of quotient groups. A first step is the following:

Lemma 3.1. *If $f \colon G_1 \to G_2$ is a homomorphism, then* $\operatorname{Ker} f$ *is a normal subgroup of G_1.*

Proof. We must show that, for all $h \in \operatorname{Ker} f$ and for all $g \in G$, $ghg^{-1} \in \operatorname{Ker} f$, or equivalently that $f(ghg^{-1}) = 1$. But, since $h \in \operatorname{Ker} f$, $f(h) = 1$ by definition, hence

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g) \cdot 1 \cdot f(g)^{-1} = 1.$$

Thus $\operatorname{Ker} f \triangleleft G_2$. $\square$

The *First Isomorphism Theorem*, also called the *Fundamental Theorem of Homomorphisms*, which states among other things that every homomorphism between two groups is built up out of three basic types of homomorphisms: quotient homomorphisms, isomorphisms, and inclusions.

Theorem 3.2. *Let G_1 and G_2 be groups, let $f\colon G_1 \to G_2$ be a homomorphism, and set $K = \operatorname{Ker} f \triangleleft G_1$ and $H = \operatorname{Im} f \leq G_2$. Then $G_1/K \cong H$. More precisely, if $\pi\colon G_1 \to G_1/K$ is the quotient homomorphism and if $i\colon H \to G_2$ is the inclusion homomorphisn, then there is a unique isomorphism $\tilde{f}\colon G_1/K \to H$ such that $f = i \circ \tilde{f} \circ \pi$. The situation is summarized by the following diagram:*

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ {\scriptstyle\pi}\big\downarrow & & \big\uparrow{\scriptstyle i} \\ G_1/K & \xrightarrow{\tilde{f}} & H. \end{array}$$

Proof. We begin by trying to define the function $\tilde{f}\colon G_1/K \to H$. Clearly, the only natural way to define $\tilde{f}$ on a coset gK is to set $\tilde{f}(gK) = f(g)$. We must check that this is well-defined, i.e. independent of the choice of representative $g \in gK$. If instead we choose a different representative of gK, necessarily of the form gk, then $f(gk) = f(g)f(k) = f(g) \cdot 1 = f(g)$, hence $\tilde{f}$ is well-defined, and its values $\tilde{f}(gK) = f(g)$ lie in $H = \operatorname{Im} f$. So we can view $\tilde{f}$ as a function $G_1/K \to H$, and it is clearly surjective. Moreover, $\tilde{f}$ is a homomorphism since

$$\tilde{f}(g_1Kg_2K) = \tilde{f}(g_1g_2K) = f(g_1g_2) = f(g_1)f(g_2) = \tilde{f}(g_1K)\tilde{f}(g_2K).$$

To see that it is an isomorphism, since we know that it is surjective, it suffices to show that it is injective. Equivalently we must show that $\operatorname{Ker} \tilde{f} = \{K\}$, the single element set consisting of the identity in G_1/K, namely the identity coset. Suppose that $\tilde{f}(gK) = 1$. By definition $f(g) = \tilde{f}(gK) = 1$, hence $g \in K$ and therefore $gK = K$. Thus $\operatorname{Ker} \tilde{f} = \{K\}$ and hence $\tilde{f}$ is injective, thus an isomorphism. (Compare also Remark 2.5 in the handout on homomorphisms.)

Finally we establish that $f = i \circ \tilde{f} \circ \pi$. To see that these two functions are equal, it is enough to check that they take the same value for every $g \in G$. But

$$i \circ \tilde{f} \circ \pi(g) = i \circ \tilde{f}(gK) = i(f(g)) = f(g),$$

where when we write $i(f(g))$ we view the term $f(g)$ as an element of $H = \operatorname{Im} f$ and in the final step of the equality we view $f(g)$ as an element of G_2. Thus $i \circ \tilde{f} \circ \pi(g) = f(g)$ for all $g \in G_1$, so that $f = i \circ \tilde{f} \circ \pi$. $\square$

Corollary 3.3. *Let G be a group and H a subgroup of G. If there exists a group G' and a surjective homomorphism $f\colon G \to G'$ such that* $\operatorname{Ker} f = H$*, then H is a normal subgroup of G and $G/H \cong G'$.*

We can sometimes use the corollary to identify quotient groups G/H as more familiar groups. The idea is to find a homomorphism f such that $H = \operatorname{Ker} f$. Here are some examples:

Example 3.4.

1. Let G be a group and let $g \in G$. We have seen that there is a unique homomorphism $f\colon \mathbb{Z} \to G$ such that $f(a) = g^a$ for all $a \in \mathbb{Z}$. Hence $\operatorname{Im} f = \langle g \rangle$. If g has infinite order, then f is injective. If g has finite order n, then $\operatorname{Ker} f = \langle n \rangle = n\mathbb{Z}$. Hence there is a unique induced isomorphism $\tilde{f}\colon \mathbb{Z}/n\mathbb{Z} \to G$ such that $\tilde{f}([a]_n) = g^a$ for all $a \in \mathbb{Z}$.

2. Let G_1 and G_2 be two groups, with normal subgroups $H_1 \triangleleft G_1$ and $H_2 \triangleleft G_2$, and let $\pi_1\colon G_1 \to G_1/H_1$ and $\pi_2\colon G_2 \to G_2/H_2$ be the quotient homomorphisms. Then there is a homomorphism
$$\pi = (\pi_1, \pi_2)\colon G_1 \times G_2 \to (G_1/H_1) \times (G_2/H_2),$$
defined by $\pi(g_1, g_2) = (\pi_1(g_1), \pi_2(g_2)) = (g_1H_1, g_2H_2)$. Clearly π is surjective and $\operatorname{Ker} \pi = H_1 \times H_2$. Thus
$$(G_1 \times G_2)/(H_1 \times H_2) \cong (G_1/H_1) \times (G_2/H_2).$$
In particular, taking $H_1 = \{1\}$ and $H_2 = G_2$ shows that
$$(G_1 \times G_2)/(\{1\} \times G_2) \cong G_1.$$
For example, taking $G_1 = G_2 = \mathbb{Z}$, we see that $(\mathbb{Z} \times \mathbb{Z})/(\{0\} \times \mathbb{Z}) \cong \mathbb{Z}$, where $\{0\} \times \mathbb{Z} = \langle (0,1) \rangle$. Similarly, if W is a vector subspace of the finite dimensional vector space V, say $\dim V = n$ and $\dim W = d$, then there is a basis $e_1, \dots, e_n$ of V such that $W = \operatorname{span}\{e_1, \dots, e_d\}$. This identifies V with $\mathbb{R}^n$ and W with the vector subspace $\mathbb{R}^d$ consisting of all vectors whose last $n - d$ coordinates are zero. Hence $V \cong \mathbb{R}^n \cong \mathbb{R}^d \times \mathbb{R}^{n-d}$, in such a way that the subspace W is identified with the first factor $\mathbb{R}^d$, so that the quotient $V/W \cong \mathbb{R}^{n-d}$. Here, V/W is more than just a group, since W is more than just a subgroup of V (it is in addition closed under scalar multiplication), and in fact V/W is a vector space in its own right.

3. The homomorphism $f\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ defined by $f(n,m) = n-m$ is surjective, and $\operatorname{Ker} f = \{(n,n) : n \in \mathbb{Z}\} = \langle (1,1)\rangle$. Hence $(\mathbb{Z}\times\mathbb{Z})/\langle(1,1)\rangle \cong \mathbb{Z}$. As we shall see in the homework, a similar argument works to show that $(\mathbb{Z}\times\mathbb{Z})/\langle(a,b)\rangle \cong \mathbb{Z}$ provided that $\gcd(a,b) = 1$.

4. If (as in the homework) $\mathcal{B} = \left\{\begin{pmatrix} a & b \\ 0 & d\end{pmatrix} : a,b,d \in \mathbb{R}, a,d \neq 0\right\}$ and $\mathcal{U} = \left\{\begin{pmatrix} 1 & b \\ 0 & 1\end{pmatrix} : b \in \mathbb{R}\right\}$, then there exists a homomorphism $f\colon \mathcal{B} \to \mathbb{R}^*\times\mathbb{R}^*$, namely $f\left(\begin{pmatrix} a & b \\ 0 & d\end{pmatrix}\right) = (a,d)$, such that f is surjective and $\operatorname{Ker} f = \mathcal{U}$. Hence $\mathcal{U} \lhd \mathcal{B}$ and $\mathcal{B}/\mathcal{U} \cong \mathbb{R}^*\times\mathbb{R}^*$.

5. Again by the homework, we have seen that $f(t) = e^{2\pi i t}$ defines a surjective homomorphism from $\mathbb{R}$ (under addition) to $U(1)$ whose kernel is $\mathbb{Z}$. Hence $\mathbb{R}/\mathbb{Z} \cong U(1)$ (a fact which also has topological significance). Looking instead at the subgroup $\mathbb{Q}/\mathbb{Z} \leq \mathbb{R}/\mathbb{Z}$, it is easy to see that the image of $\mathbb{Q}/\mathbb{Z}$ in $U(1)$ under g is the subgroup of all torsion elements of $U(1)$, i.e. the subgroup which we denoted in the homework μ_∞ (the union of all of the n^{th} roots of unity for every n).

One reason to call G/H a quotient group is that the notation G/H has many properties that look like the analogous ones for fractions. For example, $G/G \cong \{1\}$ and $G/\{1\} \cong G$. We have also seen that, for $H_1 \lhd G_1$ and $H_2 \lhd G_2$, $(G_1\times G_2)/(H_1\times H_2) \cong (G_1/H_1)\times(G_2/H_2)$. Another property is the following: We called Theorem 3.2 the First Isomorphism Theorem, so we naturally expect there to be other isomorphism theorems as well. We shall describe the second isomorphism theorem in a separate handout and just state and prove the *Third Isomorphism Theorem*:

Theorem 3.5. *Let G be a group and let H and K be* ***normal*** *subgroups of G with $H \leq K$. Let $\pi\colon G \to G/H$ be the quotient homomorphism. Then $K/H = \pi(K)$ is a normal subgroup of G/H, and*

$$(G/H)\Big/(K/H) \cong G/K.$$

(The way to remember this is that, if we think the expressions G/H, K/H as fractions, then the denominators above cancel each other.)

Proof. We will prove the theorem by applying the First Isomorphism Theorem. Begin by defining $f\colon G/H \to G/K$ by: $f(gH) = gK$. Here f is a function defined on the set of cosets G/H by choosing a representative, so we must check that f is well-defined. If $g' \in gH$ is another representative, then $g' = gh$ for some $h \in H$ and so $g'K = ghK = gK$, since gh and g differ by an element of H and hence of K since $H \subseteq K$. Clearly f is surjective. Also,

$$f((g_1H)(g_2H)) = f(g_1g_2H) = g_1g_2K = (g_1K)(g_2K) = f(g_1H)f(g_2H).$$

Hence f is a homomorphism. Finally,

$$\operatorname{Ker} f = \{gH : gK = K\} = \{gH : g \in K\} = K/H.$$

Hence $K/H \triangleleft G/H$ and $(G/H)\Big/(K/H) \cong G/K$ by the First Isomorphism Theorem. $\square$

Example 3.6. Suppose that $n, d \in \mathbb{N}$ and that $d|n$. Then $\langle n\rangle \leq \langle d\rangle \leq \mathbb{Z}$, and all subgroups of $\mathbb{Z}$ are normal since $\mathbb{Z}$ is abelian. The image of $\langle d\rangle$ in $\mathbb{Z}/\langle n\rangle = \mathbb{Z}/n\mathbb{Z}$ is the cyclic subgroup generated by d viewed as an element of $\mathbb{Z}/n\mathbb{Z}$. Applying the Third Isomorphism Theorem, we see that $\mathbb{Z}/n\mathbb{Z}/\langle d\rangle \cong \mathbb{Z}/d\mathbb{Z}$, which we have also argued by a direct inspection of the cosets and the group operation.

Remark 3.7. Quite generally, let G be a group and let H be a normal subgroup of G. Then there is a bijection from the set X_1 defined by

$$\begin{aligned} X_1 &= \{\text{all subgroups of } G \text{ containing } H\} \\ &= \{K \leq G : H \leq K\} \end{aligned}$$

to the set X_2 defined by

$$X_2 = \{\text{all subgroups of } G/H\}.$$

To find this bijection, we define functions $F_1 \colon X_1 \to X_2$ and $F_2 \colon X_2 \to X_1$ as follows: given K a subgroup of G with $H \leq K$ (so $K \in X_1$), define $F_1(K) = \pi(K) = K/H$, which is a subgroup of G/H and hence an element of X_2. Conversely, given a subgroup $J \leq G/H$ (so $J \in X_2$), define $F_2(J) = \pi^{-1}(J)$; this is a subgroup of G containing H (why?) and so an element of X_1. It is easy to see that $\pi(\pi^{-1}(J)) = J$ (since π is surjective), and that, if $H \leq K$, then $\pi^{-1}(\pi(K)) = K$ (since an element of $\pi^{-1}(\pi(K))$ is of the form kh with $k \in K$ and $h \in H$, and since $H \leq K$, $kh \in K$), so that F_1 and F_2 are inverse functions.

In this correspondence, a subgroup $K = \pi^{-1}(J)$ of G containing H is a normal subgroup of G $\iff$ the image subgroup $J = \pi(K)$ of G/H is a normal subgroup of G/H, and the Third Isomorphism Theorem says that $G/\pi^{-1}(J) \cong (G/H)/J$.