1.2 Mappings and Morality

If there is one central idea which is common to all aspects of modern algebra it is the notion of homomorphism.

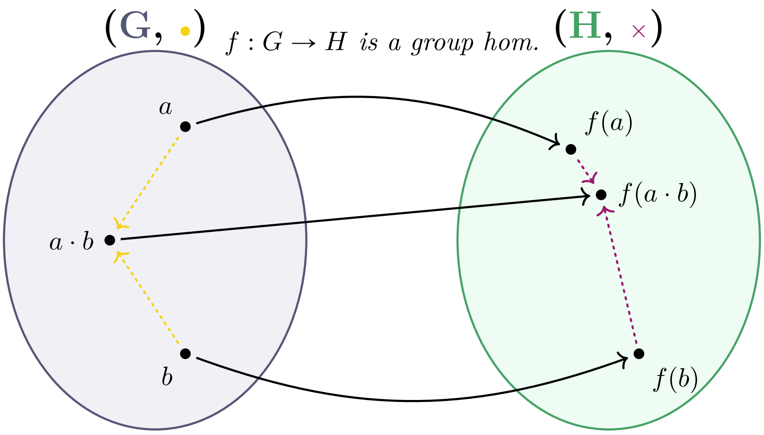
∼ I. N. Herstein

We have now seen enough of the fundamentals of Group Theory to utilize them in introducing what is by far the most important concept in all of Abstract Algebra. Homomorphisms will remain the centerpoint and moral grounding to our survey of the algebraic landscape from this point onward. We begin this saga by defining them.

Definition 1.19 (Homomorphisms of Groups)**.** Let $(G, \cdot)$ and $(H, \times)$ be groups. A homomorphism f of these groups is a map of sets $f : G \to H$ that takes one operation into the other opertaion, i.e.

$$f(a \cdot b) = f(a) \times f(b)$$

for all pairs $a, b \in G$.



Observe that $f(a \cdot b) = f(a) \times f(b)$ holds.

Fig. 1.7: Illustration of a homomorphism f of groups G, H.

Note that it does not matter "when" the mapping f occurs, i.e. you are free to send elements a, b into $f(a), f(b) \in H$ and combine them there via × or combine them and get $a \cdot b$ in G first and then send that single element to $f(a \cdot b) = f(a) \times f(b) \in H$. We should think of this as a way to build analogies between the group structures G and H.

Our homomorphism f sends an element a in G to some analogy element $f(a)$ in H. And this analogy is strictly compatible with the operations native to the groups. In G, we combine a, b to yield $a \cdot b$. The analogy of their $\cdot$ combine in G is the combine × of their analogies in H under f.

Part of this is wrapped up in the idea that if our homomorphism f is capturing the moral truth of a link between the two group multiplications, it shouldn't matter "when" it occurs. We should be able to do the multiplication in G first then have f tell us where that belongs in H, or f should be smart enough to send our a and b to locations in H where the multiplication there will do the same thing.

Not all functions that only take G and H as sets will do this. The ones that do, the group homomorphisms, are indispensable to the modern algebraist. Let us look at a few examples.

Example 1.20. Let G, H be any groups. There is always a *trivial* homomorphism $f : G \to H$ such that $f(g) = 1_H$ for every $g \in G$. As such, we do not have a word like “homomorphic” do describe when a pair of groups has a homomorphism between them. Every pair of groups has a trivial homomorphism either ways.

Example 1.21. There is a homomorphism from the additive group of integers $(\mathbb{Z}, +)$ to any finite cyclic group. Let $G = \langle g \rangle$ cyclic of order $|g|$. Define

$$\begin{aligned} f : \mathbb{Z} &\to G \\ n &\mapsto g^{n \pmod{|g|}}. \end{aligned}$$

Suppose $|g| = 4$, $n = 8 = 3|g|$, $m = 5 = |g| + 1$, $\ell = 3$. Then, $f(n) = 1_G$, the identity in G (as opposed to the $1 \in \mathbb{Z}$), $f(m) = g$, and $f(\ell) = g^3$. Observe that $f(m+\ell) = f(n) = 1_G$, and $f(m) \cdot f(\ell) = g \cdot g^3 = g^4 = 1_G$. So, this is a homomorphism.

Remark. This particular homomorphism has much to do with the division in the integers. As such, we will let it inspire a particular choice of notation $\mathbb{Z}/n\mathbb{Z}$ for a generic cyclic group for which an unnamed generator has order n. We write the elements as $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-2, n-1\}$. We will very soon see all this quotient notation has to offer.

Example 1.22. Let $(\mathbb{C}[x], +)$ denote the additive group of polynomials with complex coefficients. The derivative mapping is a homomorphism $(\mathbb{C}[x], +) \to (\mathbb{C}[x], +)$, by linearity.

Example 1.23. Consider the additive and multiplicative groups of the real numbers $(\mathbb{R}, +)$, $\mathbb{R}^\times = (\mathbb{R} - \{0\}, \times)$. There is a homomorphism $\exp : \mathbb{R} \to \mathbb{R}^\times$ given by $\exp(x) = e^x$. See why: $e^{x+y} = e^x e^y$ is a usual property of exponents.

We will now state and prove some important properties of homomorphisms of groups.

Theorem 1.6 (Properties of Group Homomorphisms I)**.** *Let $f : G \to H$ be a homomorphism of groups, and $K < G$. Then:*

- $f(1_G) = 1_H$.
- $f(g^{-1}) = f(g)^{-1}$.
- $f(g^n) = f(g)^n$ *for all natural numbers* n.
- $|g|$ *is a divisor of* $|f(g)|$.

Proof. We prove them in order of appearance. For any $g \in G$, we have $f(g) = f(g \cdot 1_G) = f(g)f(1_G)$. Therefore, $1_H = f(1_G)$ follows from left cancellation.

For any $g \in G$, we have $1_H = f(1_G) = f(g \cdot g^{-1}) = f(g)f(g^{-1})$, and thusly $f(g^{-1})$ is the unique inverse in H of $f(g)$.

Next, we will make an inductive argument. For $n = 1$, we get $f(g) = f(g)$ holds. Assume this holds for $n = k - 1$. Write $g^k = \underbrace{g \cdot g \cdot \ldots \cdot g}_{k \text{ times}}$. Then,

$$\begin{aligned} f(g^k) &= f(g)f(g^{k-1}) \\ &= f(g)\left(f(g)^{k-1}\right) \\ &= f(g)^k. \end{aligned}$$

Observe that $f(g^{|f(g)|}) = f(g)^{|f(g)|} = 1_H = f(g^{|g|})$. So, $|f(g)|$ must be an integer multiple of $|g|$. ♣

Every homomorphism gives immediate rise to two special subgroups, one in the domain and one in the domain. I will introduce you to them.

Definition 1.24 (Kernel, Image of Group Hom.)**.** Let $f : G \to H$ be a homomorphism of groups. Then, there is a subgroup of G called the *kernel* of f, denoted $\ker f$, given by

$$\ker f \overset{\text{def}}{=\!=} \{g \in G : f(g) = 1_H\}.$$

There is also a subgroup of H called the *image* of f, denoted $\mathrm{Im} f$ and given by

$$\mathrm{Im} f \overset{\text{def}}{=\!=} \{h \in H : \exists g \in G \text{ such that } f(g) = h\}.$$

Exercise 1.25. Verify that these are subgroups as claimed.

Example 1.26. Consider the permutation group S_n. There is a homomorphism $\mathrm{sgn} : S_n \to \{\pm 1\}$ called the *sign* map, sending even permutations to 1 and odd permutations to -1. The kernel of this homomorphism is the even permutations, which as a subgroup of S_n is called the *alternating group on n letters*, denoted $A_n \overset{\text{def}}{=\!=} \ker \mathrm{sgn}$.

These subgroups can help us say more about the homomorphism $f : G \to H$. For example, see why f is a surjective group homomorphism if and only if $\mathrm{Im} f = H$. Our next lemma uses the kernel to characterize injectivity.

Lemma 1.7 (Injectivity iff Trivial Kernel)**.** *Let $f : G \to H$ be a group homomorphism. Then, f is injective if and only if $\ker f = \{1_G\}$, in which case we say that the kernel of f is "trivial."*

Proof. We have seen that $1_G \in \ker f$, and if f is injective then this must be unique as a preimage of 1_H. Conversely, we assume the kernel of f is trivial and suppose $f(g) = f(g') = h$. Then, $f(g^{-1}) = h^{-1}$, and so $f(g^{-1}g') = h^{-1}h = 1_H$. Hence, $g^{-1}g' \in \ker f$ which implies $g^{-1}g' = 1_G$. By left cancellation, we get $g' = g$. ♣

What we want next is some way to characterize subgroups and the additional structural insights they provide. We begin with the notion of the *isomorphism*. The word itself comes from ancient Greek. *Iso-* means "same" and *-morph* means "shape" or "form". Morally speaking, an isomorphism is our way of using homomorphisms to conclude that two structures are morally the same. Let us define them formally.

Definition 1.27 (Isomorphism of Groups)**.** Let $f : G \to H$ be a homomorphism of groups. If f is bijective, we say it is an isomorphism. Furthermore, we say that G and H are *isomorphic* as groups, and we write $G \cong H$.

Basically, we are using this bijection pair every element in G with a unique element in H. And, our pairing is a homomorphism, so that the operation in H is must be an exact replica of the structure of G, just on a different set. Literally as set theoretic objects these groups may be quite different, but Group Theory cannot tell them apart. Their group structures are of the same form, and there are no group theory conclusion about one that is inaccessible as a statement about the other. The isomorphism acts as our translation guide, in such case.

The clearest picture we can have of an isomorphism in the case of manageably-sized groups is given by the *Cayley Table*, which is a vocabulary word in honor of British mathematician Arthur Cayley (1821-1895) that simply means a multiplication table for the group. I will draw the Cayley tables for two isomorphic groups in our next example.

Example 1.28. Consider the group of positive and negative one under multiplication $\{\pm 1, \times\}$. Consider also the group of permutations of 🟪🟩, taking the default arrangement to be 🟪🟩 such that flipping them yields 🟩🟪. Flipping them twice gets us back where we started. The Cayley tables are as follows.

○	🟪🟩	🟩🟪
🟪🟩	🟪🟩	🟩🟪
🟩🟪	🟩🟪	🟪🟩

({🟪🟩, 🟩🟪}, ○)

$\times$	1	-1
1	1	-1
-1	-1	1

$(\{\pm 1\}, \times)$

Fig. 1.8: Cayley tables for isomorphic 2-element groups.

The choice of isomorphism is somewhat obvious on inspection, especially when we consider the properties of homomorphisms. In fact, the only nonzero homomorphism between these two is an isomorphism (see why!). We define f : {🟪🟩, 🟩🟪} $\to \{\pm 1\}$ by $f($🟪🟩$) = 1$ and $f($🟩🟪$) = -1$. You can check this. Replace the color pair labels in the first table by what numbers they map to in the second.

As objects, these are clearly different. One is about numbers. The other is about ways of arranging patches of color. But as groups, there is an isomorphism. They're the same table. So they're the same group in turn.

Exercise 1.29. Consider the equilateral triangle in the plane and its symmetry group of rotations and reflections, what we will eventually call D_3, for "the dihedral group of order $6 = 2 \times 3$." Consider also the set of bijective functions from $\{\star, \heartsuit, \female\}$ to itself (spoiler: there are indeed six of them), and define a group of these functions whose operation is composition. This is the group of permutations of $\{\star, \heartsuit, \female\}$, and is denotes $\mathrm{Aut}\{\star, \heartsuit, \female\}$. Draw the Cayley Tables, and use them to see an isomorphism $D_3 \to \mathrm{Aut}\{\star, \heartsuit, \female\}$.

Example 1.30. It should be clear that $G \cong G$ for all G. The identity map $g \mapsto g$, for all $g \in G$ is an isomorphism of G into itself, which we call an *automorphism*. This is but one example of a whole family of automorphisms. Take $g \in G$ a group. Define a map $c_g : G \to G$ by $c_g(h) = ghg^{-1}$. We call this the *conjugation* of h by g. This c_g is bijective because it is invertible. Explicitly, $c_g^{-1} = c_{g^{-1}}$:

$$c_{g^{-1}}(c_g(h)) = g^{-1}(ghg^{-1})g = h \text{ and } c_g(c_{g^{-1}}(h)) = g(g^{-1}hg)g^{-1} = h.$$

And, conjugation by fixed element gives a homomorphism:

$$c_g(h)c_g(h') = (ghg^{-1})(gh'g^{-1}) = ghh'g^{-1} = c_g(hh').$$

Denote by $\mathrm{Aut}(G)$ the group of all automorphisms of G, with multiplication $(x \circ y)(g) = x(y(g))$ for automorphisms x, y of G. There is a very natural homomorphism

$$\begin{aligned} \varphi : G &\to \mathrm{Aut}(G) \\ g &\mapsto c_g \end{aligned}$$

whose image is called the *inner automorphism group of* G, often written $\mathrm{Inn}(G)$. The kernel of this map is particularly exciting. By definition, it is the set of elements $g \in G$ for which $ghg^{-1} = h$ for all $h \in G$, such that the conjugation we get is the identity map on G. But this is true if and only if $gh = hg$ for all other elements h, i.e. g commutes with everything in G. We call the set of elements in a group that commute with everything else the *center* of a group, and denote it $Z(G)$. For an Abelian group A, $Z(A) = A$.

Example 1.31. Let $G = \langle g \rangle$ and $H = \langle h \rangle$ be such that $\#G = \#H$. Then, $G \cong H$. The particular isomorphism is simply the homomorphism $f : g \mapsto h$, in which case $f(g^n) = h^n$ for all n. For any $h^j \in H$, we have $j < |h| = |g|$ and so $g^j \in G$ such that we have $f(g^j) = h^j$. This is surjectivity. Toward injectivity, observe that $h^j \neq 1_H$ for all $1 \leqslant j \leqslant |h| - 1$. Thus, $f(g^j) \neq 1_H$ for all such indices j. Therefore, the only remaining possibility is $f(g^0) = 1_H$, which we appreciate is our having a trivial kernel.

Next, we invoke a gadget called the coset to turn ideas about isomorphisms into something truly fundamental and deep.

Definition 1.32 ((left) Coset)**.** Let $H < G$. For any $g \in G$, one obtains its *left coset of H in G* which is the set of elements $gH \overset{\text{def}}{=\!=} \{gh : h \in H\}$. We call g or any other $g' \in gH$ a *representative* of this coset. We denote by G/H (pronounced, "G mod H") the set of left cosets of H in G, $G/H \overset{\text{def}}{=\!=} \{gH : g \in G\}$.

Remark. There are also such things as right cosets constructed similarly: $Ha \overset{\text{def}}{=\!=} \{ha : h \in H\}$. We will discuss these more later.

Observation. *Since H is a subgroup, $1 \in H$, and so any coset representative g of gH actually lands in the coset. That is to say, taking $1 \in H$, we have $g \cdot 1 \in gH$. Consequently, H is always a coset.*

Before we visualize left cosets, we need to obtain fact about them to be handled symbolically until it can help us build a clear picture of the left cosets of a subgroup.

Proposition 1.8 (Cosets Partition G)**.** *Let $H < G$. Then, G/H partitions G.*

Proof. We will show that two cosets aH, bH are either equal as sets or disjoint. Suppose they are not disjoint, such that their intersection contains an element g. Then, there exists h_1, h_2 such that

$$\begin{aligned} & g = ah_1 = bh_2 \\ \Longleftrightarrow\ & gh_1^{-1} = a = bh_2h_1^{-1}, \end{aligned}$$

the key takeaway being $a = bh_2h_1^{-1}$. So, for any $ah \in aH$, we may write $ah = bh_2h_1^{-1}h$, expressing $ah \in bH$ since $h_2h_1^{-1}h \in H$. This proves $aH \subset bH$, and the other inclusion is essentially the same, where in the last line we might use these notations to conclude $bh = ah_1h_2^{-1}h \in aH$. Thus, $aH = bH$ whenever $aH \cap bH$ is nonempty. So, these cosets are disjoint. To complete the proof, we refer to our prior observation that every element belongs to the coset it represents, so in particular every element belongs to a coset. Left cosets are disjoint subsets which exhaust the group. ♣

Exercise 1.33. Let $H < G$ and fix $g \in G$. Does $g^2H = gH$? Find a necessary and sufficient condition for this to be true. Extend this to the question of when $g^jH = gH$.

Now we have realized these left cosets of the subgroup are a partition of the whole group, we may justify drawing them as such:

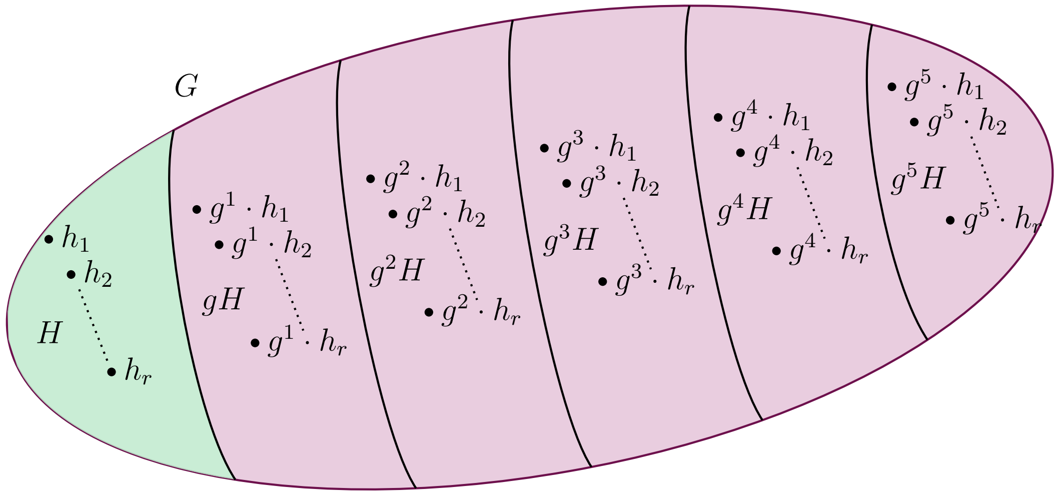


Fig. 1.9: Left cosets of $H = 1 \cdot H$ as a partition of G, with powers of some $g \notin H$ as representatives.

Example 1.34. Consider $A_3 < S_3$. The coset represented by identity is the subgroup A_3 itself. In the cyle notation, we write $A_3 = \{\mathbb{I}, (123), (132)\}$. We then take a representative odd permutation, (12), and get $(12)A_3 = \{(12)\mathbb{I}, (12)(123), (12)(132)\} = \{(12), (23), (13)\}$, the remaining three elements of S_3. Observe we got two cosets of equal size, and may write $S_3 = A_3 \sqcup \{(12), (23), (13)\}$.

Example 1.35. Consider the cyclic group $\mathbb{Z}/6\mathbb{Z}$ and the order two subgroup $\{0, 3\}$. We compute the left cosets:

$$\begin{aligned}
0 + \{0,3\} &= \{0,3\} \\
1 + \{0,3\} &= \{1,4\} \\
2 + \{0,3\} &= \{2,5\} \\
3 + \{0,3\} &= \{3,0\} = \{0,3\} \\
4 + \{0,3\} &= \{4,1\} = \{1,4\} \\
5 + \{0,3\} &= \{5,2\} = \{2,5\}
\end{aligned}$$

We have diced our original group into fragments whose size is given by the size of subgroup H.

So far, a pattern has emerged. We seem to only get cosets having the same size as the subgroup Every coset Our next lemma is here to assure us this is no mere coincidence, and that it is appropriate to think of left cosets as a set of *translates* of H in G under the left multiplication by elements of G as they become coset representatives.

Lemma 1.9 (Cosets Give an Equipartition of G)**.** *Let $H < G$, and take left cosets aH, bH. Then, $\#aH = \#bH = \#H$.*

Proof. This is not abundantly surprising if one recalls the cancellation laws. Suppose we have elements h, h' in the subgroup H. Then $ah = ah'$ if and only if $h = h'$. Cancellation laws prevent two elements of H taking a single representative to two elements in its coset. Hence, there is a natural bijection $H \to aH$ such that $h \mapsto ah$, whose inverse is guaranteed by left cancellation. $\clubsuit$

This lemma leads us immediately to a theorem of Joseph-Louis Lagrange. Among other notable gains, this theorem tells us exactly the value of r in the figure no. We will need a new piece of notation before we are ready to state it.

Definition 1.36 (Index of Subgroup)**.** Let $H < G$. We define the *index of H in G* to be the number of left cosets of H in G, and we denote it $[G : H]$. Symbolically, $[G : H] \overset{\text{def}}{=\!=} \#G/H$.

Theorem 1.10 (Lagrange)**.** *Let G be a finite group and $H < G$. Then, $\#H | \#G$. In particular, $[G : H]\#H = \#G$*

Proof. We have seen in the above lemma that cosets give an equipartition of G. And, we know how many pieces there are. By definition, there are $[G : H]$ pieces, each of size $\#H$ elements of G by lemma. ♣

Remark. This is one of the cleanest proofs we will see in our entire exploration of Algebra. Where possible, the goal will be to develop the subject in such a way that, when it comes time to state a powerful result, we have built up enough ammunition as to make it seem truly deserving of being our next step as was possible here.

Corollary 1.10.1 (Order of Element Divides Order of Finite Group)**.** *Let G be a finite group and $g \in G$. Then, $|g|$ givides $\#G$.*

Proof. We have a cyclic subgroup $\langle g \rangle$ of order $\#\langle g \rangle = |g|$. ♣

Corollary 1.10.2 (Groups of Prime order are Cyclic)**.** *Let G be a group of $\#G = p$ for p a prime number. Then, G is cyclic of order p.*

Proof. The order of G is finite, so any $g \in G$ has a divisor of p as its order. The only possibilities are 1, such that we get $g = 1_G$, or p itself, in which case g generates the whole group $G = \langle g \rangle$. ♣

Observation. *Every nonidentity element in a cyclic group of prime order is a generator. Contrapositively, you should closely check that if a nonidentity element fails to generate the whole cyclic group, then the group has composite order.*

Cosets have given us some way of fragmenting a group into pieces whose size is determined by a particular subgroup. Namely, the subgroup equal to the coset represented by identity. A natural extension of this discussion is how to do Algebra with cosets. Explicitly, we seek a structure on the left cosets of H in G which is analogous to the group G itself. And we have already introduced a notation similar to this.

Consider $\mathbb{Z}$ and its subgroup $n\mathbb{Z}$. The left cosets are the set $\mathbb{Z}/n\mathbb{Z} = \{j + n\mathbb{Z} : j \in \mathbb{Z}\}$. But notice that, if i, j are such that $i = j + mn$ for some $m \in \mathbb{Z}$, then $i + n\mathbb{Z} = j + mn + n\mathbb{Z}$, with $mn \in \mathbb{Z}$. Therefore, the moral equivalent of a coordinate change over the "h" in our subgroup $H = n\mathbb{Z}$ we traverse in the definition of left coset reveals $i + n\mathbb{Z} = j + n\mathbb{Z}$.

This insight in hand, we see that there are as many cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ as there are differences $i - j \pmod n$. We pick these remainders modulo n to be a set of coset representatives, and we find $\mathbb{Z}/n\mathbb{Z} = \{0+n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots, (n-2)+n\mathbb{Z}, (n-1)+n\mathbb{Z}\}$. If we ignore the left coset notation, these are precisely the elements of the cyclic group we called $\mathbb{Z}/n\mathbb{Z}$ before. Naturally, then, the analogy of the group structure of $\mathbb{Z}$ we seek is the cyclic group $\mathbb{Z}/n\mathbb{Z}$ for cosets of $n\mathbb{Z}$ in $\mathbb{Z}$.

Such a structure exists if a certain condition on the subgroup is met. The most immediate choice we might make to define a multiplication on G/H is $(aH)(bH) = (ab)H$. In the case of cyclic groups as quotients of $\mathbb{Z}$, this is clearly the "right" choice. But we need to ensure it is well-defined, and does not say something ambiguous about the product coset you should obtain.

For example, returning to $\mathbb{Z}/6\mathbb{Z}$, we have cosets $\{1+6\mathbb{Z}, 4+6\mathbb{Z}\}$ and $\{2+6\mathbb{Z}, 5+6\mathbb{Z}\}$. Take $a = 1, b = 2$ and find that $\{1+6\mathbb{Z}, 4+6\mathbb{Z}\} + \{2+6\mathbb{Z}, 5+6\mathbb{Z}\} = 3 + \{0+6\mathbb{Z}, 3+6\mathbb{Z}\} = \{0+6\mathbb{Z}, 3+6\mathbb{Z}\}$. But we could have chosen coset representatives $a = 4$ or $b = 5$. In this one example, this does not change the fact that these cosets sum to $\{6\mathbb{Z}, 3+6\mathbb{Z}\}$. How are we sure this does not change what we get in general? The answer involves the idea of H being a so-called *normal* subgroup.

Definition 1.37 (Normal Subgroup)**.** Let $H < G$. We call H a normal subgroup of G, and write $H \lhd G$, if and only if $gH = Hg$ for all $g \in G$. That is, if and only if the left cosets are the right cosets. When H is a proper normal subgroup, we may write $H \mathrel{\underset{\neq}{\lhd}} G$

Observation. *This is true if and only if H is closed under conjugation by elements of G. See why: $gHg^{-1} = H \iff gH = Hg$. I warn this is not invariance, but mere closure. It is possible for the left and right cosets to be equal with $gh = h'g$ with $h \neq h'$ elements of H. This is the case in non-Abelian groups with their normal subgroups.*

Observation. *Let $H < G$ for G Abelian. Then, for every $g \in G, h \in H < G$, we have $gh = hg$. And so $H \lhd G$. In general, every subgroup of an Abelian group is normal.*

Fig. 1.10: Illustration of a closed under conjugation cyclic subgroup

Example 1.38 (Product of Subgroups). Given $H, N < G$, we can construct a subset called their product, given by $HN \overset{\text{def}}{=\!=} \{hn : h \in H, n \in N\}$. When at least one of them is normal, this gives a subgroup. To see this, suppose $N \lhd G$. Then, $gN = Ng$ for any $g \in G$, in which case $hN = Nh$ for any $h \in H < G$. So,

$$(hn)(h'n')^{-1} = hnn'^{-1}h'^{-1} = h(nn'^{-1}h'^{-1}) = hh'^{-1}n^* \in HN,$$

where we took $nn'^{-1}, n^* \in N$ and by normality we know n^* exists. There is a similar proof for the case of NH as a subgroup.

Exercise 1.39. Prove $HN \lhd G$ if both $H, N \lhd G$. If this is true and $H \cap N = \{1\}$, we call G the *internal direct product* of H and N. Prove further $N \lhd HN$ and $H \cap N \lhd H$.

Our next lemma showcases the most famous normal subgroup of all.

Lemma 1.11 ($\ker f$ is Normal)**.** *Let $f : G \to \bar{G}$ be a homomorphism of groups. Then, $\ker f \lhd G$. Suppose $k \in \ker f$. Then, for any $g \in G$, we have $f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)1_{\bar{G}}f(g)^{-1} = 1_{\bar{G}}$. Therefore, $gkg^{-1} \in \ker f$, and so the kernel is closed under conjugation.*

Before we use this lemma to obtain the theorem we seek in terms of a well defined group law on left cosets, I divert our attention on a salient voyage to say more about the normality of the kernel of a group homomorphism.

Proposition 1.12 (On Equality of Cosets)**.** *Let $H < G$ and obtain cosets aH, bH. Then, $aH = bH$ if and only if $b^{-1}a \in H$.*

Proof. If $b^{-1}a = h \in H$, then $a = bh \in bH$. We also have $a^{-1}b = (b^{-1}a)^{-1} = h^{-1} \in H$, and so $b = ah \in aH$. Conversely, if $aH = bH$, then $\exists h, h' \in H$ such that $ah = bh'$, which implies $a = bh'h^{-1} \iff b^{-1}a = h'h^{-1} \in H$. ♣

Observation. *Since $a^{-1}a = 1_G \in H$, an element and its inverse always represent the same coset.*

Proposition 1.13 (Homomorphisms are Functions of Cosets of the Kernel)**.** *Let $f : G \to \bar{G}$ be a homomorphism of groups. Then, $f(a) = f(b)$ if and only if $a \ker f = b \ker f$.*

Proof. Suppose $f(a) = f(b)$. Then $f(b)^{-1}f(a) = 1_{\bar{G}}$, and so $b^{-1}a \in \ker f$ by the prior proposition. If instead we assume $a \ker f = b \ker f$, then we may take $k, k' \in \ker f$ such that $ak = bk'$. We let f take these into $\bar{G}$, and we find $f(ak) = f(a)f(k) = f(a)$ and $f(bk') = f(b)f(k') = f(b)$, where these are then equal because ak, bk' are. ♣

Remark. This gives us another way to think about the property that a homomorphism is injective if and only if it has trivial kernel. If the kernel is singleton, containing only 1_G, then we have seen why every coset will be singleton as translates of this trivial kernel. Then, this proposition tells us that $f(a) = f(b) \iff a \ker f = b \ker f$ in a set of left cosets where by assumption $g \ker f = \{g\}$ for all $g \in G$.

Now that we have completed that side quest for our own entertainment and edification, we state and prove our next major theorem.

Theorem 1.14 (Coset Multiplication Independent of Representative)**.** *Let $H < G$. Then, $(ab)H = (a'b')H$ for all $aH = a'H$, $bH = b'H$ if and only if $H \lhd G$.*

Proof. Suppose $(ab)H = (a'b')H$ for all pairs of cosets $aH = a'H$, $bH = b'H$. Fix choices of a, a', b, b' according to this groundwork. Then $b^{-1}a^{-1}a'b' \in H$. Moreover, $a^{-1}a' \in H$ by a proposition seen on representatives of the same coset. Thus, $b^{-1}Hb' = H \iff b^{-1}H = Hb'^{-1}$, equivalent to $bH = Hb' \iff b'H = Hb'$. Since we assumed nothing of which particular cosets aH, bH we are referring to, we conclude $b'H = Hb'$ for all $b' \in G$, which proves $H \lhd G$.

Toward the other direction, suppose we have normality $gH = Hg$ for all $g \in G$. Then let us attempt to formally obtain a well-defined multiplication on cosets that is independent of representative. For $aH, bH \in G/H$, we take the map $(aH, bH) \mapsto aHbH$ via the multiplication in G, thusly well defined straight away. Then, by normality and associativity,

$$aHbH = a(Hb)H = a(bH)H = abHH = (ab)(HH) = (ab)H,$$

and we get the multiplication originally said we wanted. ♣

This theorem empowers us to confidently define what for two arduous pages we have sought after. In doing so, we will be able to speak more broadly about a homomorphism we have seen some time ago, with more sophisticated and general language.

Definition 1.40 (Quotient Group, Quotient Map)**.** Let $H \lhd G$. We define a group structure for the quotient group on cosets G/H by $(aH)(bH) = (ab)H$. There is an extremely natural homomorphism

$$\begin{aligned} \pi : G &\to G/H \\ g &\mapsto gH, \end{aligned}$$

which is clearly surjective, and is injective if and only if $H = \{1\}$, in which case $G \cong G/H$.

Exercise 1.41. Verify the quotient map π is a homomorphism.

Remark. Though there is no way to introduce the concept in this way without circular argument, this proves the converse of a statement we showed earlier. By way of conjugation, we showed that the kernel of a group homomorphism is normal in the domain. Conversely, every normal subgroup is the kernel of a homomorphism. There it is! Namely, the quotient map. And this gets at something said earlier. I called the kernel of a group homomorphism the most famous example of a normal subgroup. While this is still true, it should now be less interesting. It's the most famous example because it is the only example.

Example 1.42. The cyclic group $\mathbb{Z}/n\mathbb{Z}$ is a quotient group of $\mathbb{Z}$ by its normal subgroup $n\mathbb{Z}$. Since $\mathbb{Z}$ is Abelian, every subgroup is automatically normal. One of our very early examples was the quotient map. In slightly different language, we defined $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ by $\pi(j) = j \pmod n$. In our first attempt at such a map, we took $j \pmod n$ to be a power of a generator g of the cyclic group. But since then we have previously shown all cyclic groups of equal order are isomorphic as groups, so can safely treat them as quotients of integers.

Example 1.43. We will draw a clock and use it in abstract construction of a cyclic group of order three.

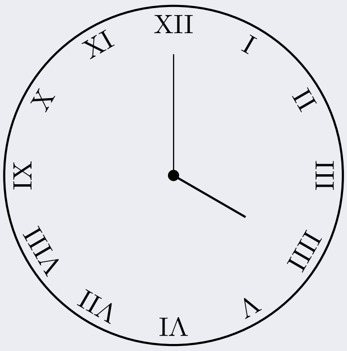


Fig. 1.11: An analog clock, labeled with Roman numerals. It looks about time for some afternoon tea.

There are too many hours on this clock compared to the pictures we saw of all three rotational positions of the equilateral triangle in our prior example. One way around this would be to only consider the multiples of four. After all, there are three of them, and they fit neatly under the vertices of an equilateral triangle in this example. But I would like to propose an example might seem counterintuitive for now, but uses cosets. This basic construction is one of the most versatile tools in all of group theory, which is why it should be seen so plainly in action like this.

Let us split the hours into three sets of four, given by the least residue classes modulo three. That is, multiples of three: $\mathit{0} \overset{\text{def}}{=\!=} \{\text{III, VI, IX, XII}\}$; those which are one more than a multiple of three: $\mathit{1} \overset{\text{def}}{=\!=} \{\text{IIII, VII, X, I}\}$; and those which are two more (equivalently, one less) than a multiple of three: $\mathit{2} \overset{\text{def}}{=\!=} \{\text{V, VIII, XI, II}\}$. Observe that the difference of any two hours in any of these sets is in $\mathit{0}$. This is important for what we aim to do.

Now, let us define our addition. We will define the addition of these subsets in terms of where

Theorem 1.15 (First Isomorphism). *Let $f : G \to H$ be a homomorphism of groups. Then, f induces an isomorphism of groups $\tilde{f} : G/\ker f \to \operatorname{Im} f$.*

Proof. We attempt to define the induced isomorphism. With so little hypothesis, the only reasonable choice is $\tilde{f}(g \ker f) = f(g)$. We have a prior proposition that this is well defined. Injectivity comes from the fact that $f(g) = 1_H \iff g \in \ker f \iff g \ker f = \ker f$. Surjectivity comes from the fact that every $g \in G$ belongs to a coset and so every $f(g) \in \operatorname{Im} f$ is attained. All that remains is to verify this is a group homomorphism, which is essentially inherited from the fact f is. Consider $\tilde{f}$ on a product of cosets $a \ker f, b \ker f$. We have

$$\tilde{f}((a \ker f)(b \ker f)) = \tilde{f}((ab) \ker f) = f(ab) = f(a)f(b).$$

♣

Remark. In such a situation, we often say that $f : G \to H$ "factors through" the quotient group $G/\ker f$. Here, factoring is in the sense that composition of maps gives a group multiplication. In particular, what we are saying is that there are homomorphisms $\pi, \tilde{f}$ such that $f = \tilde{f} \circ \pi$, and as a whole what we get looks like

$$G \xrightarrow{\pi} G/\ker f \xrightarrow{\tilde{f}} \mathrm{Im} f < H.$$

This theorem is often expressed in terms of a *commutative diagram*, and also forms the first example you will see of a *short exact sequence* of groups. As a commutative diagram, this theorem looks like:

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, two heads, "\pi"'] & \mathrm{Im} f < H \\
G/\ker f \arrow[ur, "\sim", "\tilde{f}"'] &
\end{tikzcd}$$

As a short exact sequence, for now think of this as the fact that we can "build" a group as a kernel group and an image group on either side. There is a short exact sequence of these groups $1 \to \ker f \to G \to G/\ker f \to 1$. We will discuss exact sequences more in our Third Study. The whole diagram, linking the short exact sequence with the theorem, looks like:

$$\begin{tikzcd}
& & 1 \arrow[dr] & & 1 \\
& & & G/\ker f \arrow[ur] \arrow[dr, hook, two heads, "\tilde{f}"] & \\
& & G \arrow[ur, two heads, "\pi"] \arrow[rr, two heads, "f"] & & \mathrm{Im} f < H \\
& \ker f \arrow[ur, hook, "\iota"] & & & \\
1 \arrow[ur] & & & &
\end{tikzcd}$$

We state and prove our next two isomorphism theorems, the proofs of which are well lubricated by our First Isomorphism Theorem.

Corollary 1.15.1 (Second Isomorphism Theorem)**.** *Let G be a group with $H < G$ and $N \lhd G$. Then, $H/(H \cap N) \cong HN/N$.*

Proof. Let $\pi : G \to G/N$ be the quotient map. Then, $\ker \pi|_H = H \cap N$. Therefore, $H/(H \cap N) \cong \mathrm{Im}\pi|_H$, by the First Isomorphism Theorem. To justify why $\mathrm{Im}\pi|_H = HN/N$, note that if $h \notin N$, then $hn^*N = hN \neq N$ for any $n^* \in N$. ♣

Corollary 1.15.2 (Third Isomorphism Theorem)**.** *Let G be a group with $H \lhd G$ and $N \lhd G$. Further suppose $N \subset H$. Then, $G/H \cong (G/N)/(H/N)$.*

Proof. We define $f : G/N \to G/H$ by $(gN) = gH$. This map is well defined, as $gN = g'N \iff g'^{-1}g \in N \subset H$, and for the same reason this gives us a homomorphism. This is clearly surjective, as any aH is such that $a \in G$ and so $aN \in G/N$. And, $\ker f = H/N$, as we get $f(aN) = H \iff a \in H$. ♣

Exercise 1.44. Think through the statements of the above two isomorphism theorems carefully. Why are they “obvious” even without invoking the First Isomorphism Theorem. Think about what information an explicitly constructed isomorphism would send from domain to codomain, and see why this would be well defined.