Section 11: Normal Subgroups

It has probably occurred to you that we have made a group, $\mathbb{Z}_5$, of the cosets of $5\mathbb{Z}$ in $\mathbb{Z}$; so why don't we try to make a group out of the cosets of any subgroup of any group? The answer is that sometimes we can, but we can't do it in general because the obvious way to define an operation on subgroups, $(Ha)(Hb) = H(ab)$, may not be well-defined. What might go wrong? Well, suppose $Ha = Hc$ and $Hb = Hd$; i.e., $ac^{-1}, bd^{-1} \in H$. For the product to be well-defined, we need $H(ab) = H(cd)$, i.e., $ab(cd)^{-1} \in H$, i.e., $abd^{-1}c^{-1} \in H$. With the benefit of hindsight, we throw $a^{-1}a$ into the middle of this product: For the product to be well-defined, we need

$$(a(bd^{-1})a^{-1})(ac^{-1}) \in H \ .$$

Now we know that $ac^{-1} \in H$ and $bd^{-1} \in H$, so we need $a(bd^{-1})a^{-1} \in H$; but bd^{-1} could be any element of H, and a could be any element of G. So what we need to make this operation on cosets well-defined is that every conjugate of every element of H, by an element of G, is again an element of H.

Prop and Def: Let H be a subgroup of a group G. Then we call H a *normal* subgroup of G, and write $H \lhd G$, if and only if any of the following equivalent conditions hold:

(a) $(Ha)(Hb) = H(ab)$ gives a well-defined operation on the family of right cosets of H in G. (In this case, the family of right cosets is a group, denoted G/H and called the *factor group* or *quotient group* of G by H, or sometimes just "G mod H".)

(b) H contains all the conjugates of all of its elements; i.e., $gHg^{-1} \subseteq H$ for all g in G.

(c) $gHg^{-1} = H$ for all g in G.

(d) For all g in G, $Hg = gH$; i.e., each right coset of H in G is a left coset and vice versa.

Pf: (a)–(d) are equivalent: The paragraph before the statement is the proof that (b) implies (a). To see that (a) implies (b), let h, g be any element of H, G respectively; then clearly $Hg = Hg$ and $Hh = H$. By (a), i.e., well-definedness of the operation, we get $Hgh = Hg$, or equivalently $(gh)g^{-1} \in H$; but this is (b). It is clear that (c) implies (b). To see that (b) implies (c), note that for each g in G, we have $gHg^{-1} \subseteq H$, but we also have $g^{-1} \in G$, so assuming (b), $g^{-1}H(g^{-1})^{-1} \subseteq H$, and hence $H \subseteq gHg^{-1}$ also; i.e., $gHg^{-1} = H$. The equivalence of $gHg^{-1} = H$ and $gH = Hg$ is clear, so (d) is equivalent to (c).

To see that the family of cosets of a normal subgroup forms a group under the operation in (a), we only need to check that the operation is associative (which is very easy because the operation on G is associative:

$$(HaHb)Hc = (H(ab))Hc = H(ab)c = Ha(bc) = HaH(bc) = Ha(HbHc)\ ),$$

that $He = H$ acts as an identity, and that Ha^{-1} acts as an inverse of the coset Ha for each a in G, both of which are also easy.//

When $H \lhd G$, I think of G/H as G with all of the H collapsed to the identity, and the other cosets collapsed to other single elements. Of course, if $H \lhd G$, then $|G/H| = [G : H]$ (both sides are the number of cosets of H in G), and if G is abelian, then so is G/H. (But I hasten to add that G/H may be abelian even if G isn't; we'll see examples below.)

Sufficient conditions for normality: Let H be a subgroup of a group G. If any of the following conditions are satisfied, then $H \lhd G$. (But for each one, there are normal subgroups for which the condition is not satisfied.)

(a) $H \subseteq Z(G)$ (so every subgroup of an abelian group is normal).

(b) $[G : H] = 2$.

(c) H is the only subgroup of G of its order (cardinality).

Pf: (a) Suppose $H \subseteq Z(G)$. Then for all h in H and g in G, because h commutes with every element of G, $ghg^{-1} = hgg^{-1} = h \in H$, so $gHg^{-1} \subseteq H$. (Counterexample to the converse: Any group is normal in itself, but a nonabelian group is not contained in its center.)

(b) If $[G : H] = 2$, then there are only two right cosets of H in G, one being H itself, and the other the complement of H in G; but the same is true of the left cosets, so the right and left cosets of H in G are equal. (Counterexample to the converse: The trivial subgroup $\{0\}$ is normal in the abelian group $\mathbb{Z}_3$, but its index is 3, not 2.)

(c) It is not hard to show that conjugation by an element g of G is a homomorphism $G \to G$ (that is, a function that respects the operation), and it is very easy (and probably was an exercise) to see that it is one-to-one and onto G. Later we will see that the image of a subgroup under a homomorphism; so gHg^{-1}, the image of H under conjugation by g, is always a subgroup of the same cardinality as H. Thus, if H is the only one of that cardinality, then $gHg^{-1} = H$. (Counterexample to the converse: V has three subgroups of order 2, namely $\langle a \rangle$, $\langle b \rangle$ and $\langle c \rangle$, all normal because V is abelian.)//

Examples:

(a) The quaternion group Q_8 is one of the few nonabelian groups all of whose subgroups are normal. Specifically, $\langle -I \rangle$ is normal because it is the center of Q_8. The elements of the factor group $Q_8/\langle -I \rangle$ are the cosets of $\langle -I \rangle$:

$$\overline{I} = \langle -I \rangle = \{I, -I\} = \overline{-I}\ , \quad \overline{J} = \langle -I \rangle J = \overline{-J}\ , \quad \overline{K} = \overline{-K}\ , \quad \overline{L} = \overline{-L}\ .$$

And we can build the multiplication table for these elements. For example, it is pretty clear that $\overline{I}$ acts as an identity for these factor group. Now the product $(\overline{J})(\overline{K})$ is defined to be $\overline{JK}$, which is $\overline{L}$; and the product in the other order, $(\overline{K})(\overline{J})$, is $\overline{KJ} = \overline{-L} = \overline{L}$. Thus, even though the elements J and K do not commute in Q_8, their images $\overline{J}$ and $\overline{K}$ do commute in $Q_8/\langle -I \rangle$. In fact, the factor group is abelian, and we can see by the correspondence

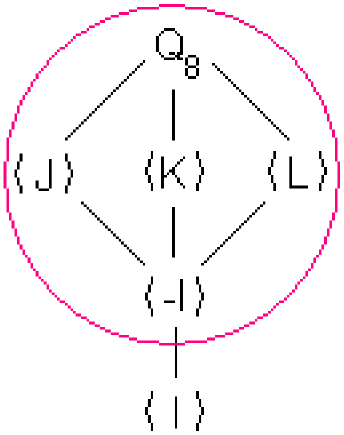
$$\overline{I} \leftrightarrow e\ , \quad \overline{J} \leftrightarrow a\ , \quad \overline{K} \leftrightarrow b\ , \quad \overline{L} \leftrightarrow c$$

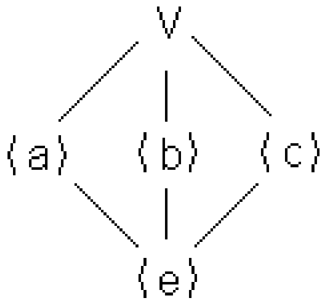
that its operation table looks just like that of the Klein 4-group:

	$\overline{I}$	$\overline{J}$	$\overline{K}$	$\overline{L}$
$\overline{I}$	$\overline{I}$	$\overline{J}$	$\overline{K}$	$\overline{L}$
$\overline{J}$	$\overline{J}$	$\overline{I}$	$\overline{L}$	$\overline{K}$
$\overline{K}$	$\overline{K}$	$\overline{L}$	$\overline{I}$	$\overline{J}$
$\overline{L}$	$\overline{L}$	$\overline{K}$	$\overline{J}$	$\overline{I}$

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Before we leave this example, let's note that the lattice of subgroups of Q_8 from $\langle -I \rangle$ looks like the lattice of subgroups of V (which looks like the lattice of subgroups of $Q_8/\langle -I \rangle$ because the last two groups “look alike” — more on that below).





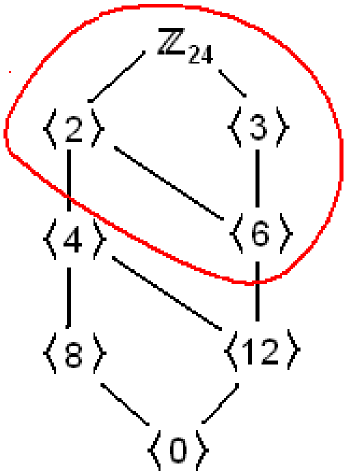
Also, $\langle J\rangle$ is normal in Q_8 because it contains half the elements of $\mathbb{Q}_8$. But there are only two cosets, so the operation table is pretty simple and looks just like that of $\mathbb{Z}_2$ under the correspondence:

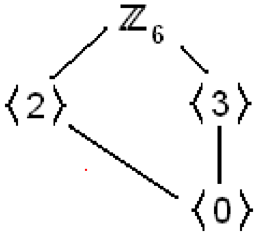
$$\overline{I} = \langle J\rangle \leftrightarrow 0\ , \qquad \overline{K} = \langle J\rangle K \leftrightarrow 1\ .$$

(b) In the abelian group $\mathbb{Z}_{24}$, all the subgroups, including $\langle 6\rangle$, are normal. There are 4 elements in this subgroup, and hence there are 6 cosets, i.e., elements of $\mathbb{Z}_{24}/\langle 6\rangle$, namely

$\overline{0} = \langle 6\rangle = \{0, 6, 12, 18\} = \overline{6} = \overline{12} = \overline{18}\, , quad\overline{1} = \langle 6\rangle \oplus 1 = \{1, 7, 13, 19\} = \overline{7}\, , \quad \overline{2} = \langle 6\rangle \oplus 2\, , \quad \overline{3}\, , \quad \overline{4}\, , \quad \overline{5}\, .$

It is not hard to check that $\mathbb{Z}_{24}/\langle 6\rangle$ looks like $\mathbb{Z}_6$, and the subgroup lattice of $\mathbb{Z}_{24}$ from $\langle 6\rangle$ looks like that of $\mathbb{Z}_6$:





(c) As additive groups, $\mathbb{Z}$ is normal in $\mathbb{Q}$ or in $\mathbb{R}$. As an element of $\mathbb{Q}/\mathbb{Z}$, $\overline{1} = \overline{0}$, so $\overline{1/2}$ has order 2, and $\overline{3/5}$ has order 5. In fact, every element of $\mathbb{Q}/\mathbb{Z}$ has finite order, so $\mathbb{Q}/\mathbb{Z}$ is a “torsion” abelian group. Moreover, it is also “divisible”: Given any element x (say $x = \overline{2/9}$) and any positive integer n (say $n = 5$), there is an element y of $\mathbb{Q}/\mathbb{Z}$ for which $ny = x$ (in this case $y = \overline{2/(45)}$). But the larger group $\mathbb{R}/\mathbb{Z}$ has lots of elements of infinite order, like $\overline{\sqrt{2}}$ or $\overline{\pi}$. We can think of $\mathbb{R}/\mathbb{Z}$ as the set of points on a circle of circumference 1: $\overline{r}$ denotes the point r units around the circle from some fixed point on it, where $\overline{r} = \overline{s}$ if r and s differ by an integer.

Terrible example: It is true that gHg^{-1} is always a subgroup of G of the same cardinality as H; but if H is infinite, then it is possible that gHg^{-1} is a proper subgroup of H for a particular g in G. (In such a case, as the proof shows, $g^{-1}H(g^{-1})^{-1}$ properly contains H, so H is not normal.) Here is an example: Let $G = \mathcal{S}(\mathbb{Z})$, $H = \{f \in G : f(x) = x \ \forall x \in \mathbb{Z}^+\}$, and $g : \mathbb{Z} \to \mathbb{Z}$ be the "subtract 1" function $g(x) = x - 1$. Then $gHg^{-1} = \{f \in G : f(x) = x \ \forall x \in \mathbb{Z}^+ \cup \{0\}\}$, a proper subset of H. Here is an element of H that is not in gHg^{-1}:

$$(0, -1) \circ (-2, -3) \circ (-4, -5) \circ \cdots \ .$$

Loose end: Earlier we claimed that $\mathcal{A}_4$, a group with $4!/2 = 12$ elements had no subgroup of 6 elements. We can now prove that: Assume by way of contradiction that there is a subgroup G of 6 elements; then because it has exactly half the elements of $\mathcal{A}_4$, $G \triangleleft \mathcal{A}_4$. The disjoint cycle decompositions of non-identity elements of $\mathcal{A}_4$ are 3-cycles and two disjoint 2-cycles; there are only $4!/(2 \cdot 2 \cdot 2) = 3$ of the latter form, and one identity, so G must have at least one 3-cycle — in fact, two of them, say some (a, b, c) and its inverse, i.e., its square, (a, c, b). We want to show that all the 3-cycles in $\mathcal{A}_4$ are in G; because $\mathcal{A}_4$ is generated by 3-cycles, that will mean that $G = \mathcal{A}_4$, the desired contradiction. To see this, take any 3-cycle (p, q, r). Because we have only four elements to choose from, there must be an overlap of at least two numbers between a, b, c and p, q, r; and because we have both (a, b, c) and (a, c, b) in G, we may assume that $a = p$ and $b = q$. Of course if $c = r$, then $(p, q, r) = (a, b, c) \in G$. If $c \neq r$, then because $(a, b)(c, r) \in \mathcal{A}_4$ and $G \triangleleft \mathcal{A}_4$, we have

$$(p, q, r) = (q, p, r)^2 = (b, a, r)^2 = [((a, b)(c, r))(a, b, c)((a, b)(c, r))^{-1}]^2 \in G \ .$$

Thus, every 3-cycle is in G, and we have the desired contradiction. So $\mathcal{A}_4$ has no 6-element subgroup.

Section 12: Homomorphisms

Recall from the notes and from the first exam:

Def: Let $(G, *)$ and $(H, \circ)$ be groups. Then a function $\varphi : G \to H$ is a *homomorphism (of groups)* if it "respects the operations," i.e., for all g_1, g_2 in G, $\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2)$. The subset $K = \{g \in G : \varphi(g) = e_H\}$ is the *kernel* of φ. If φ is a one-to-one function, it is called a *monomorphism;* if it is onto H, it is called an *epimorphism;* if both, it is an *isomorphism.*

We can adjust the diagram of which we saw a special case in the notes for Section 4: Starting with any pair (g_1, g_2) in the upper left, we get the same result if we go across and then down, or down (side-by-side) and then across:

$$\begin{tikzcd}
G \arrow[d, "\varphi"] & \times & G \arrow[d, "\varphi"] \arrow[r, "*"] & G \arrow[d, "\varphi"] \\
H & \times & H \arrow[r, "\circ"] & H
\end{tikzcd} \ .$$

From now on we will again write group operations as juxtaposition unless it may cause confusion. Let's list the immediate results of this definition:

Prop: Let $\varphi : G \to H$ be a homomorphism. Then:

(a) $\varphi(e_G) = e_H$.

(b) For all n in $\mathbb{Z}$ and g in G, $\varphi(g^n) = \varphi(g)^n$.

(c) The kernel of φ is a normal subgroup of G.

(d) φ is a monomorphism if and only if its kernel is $\{e_G\}$.

(e) For any g in G for which $o(g)$ is finite, $o(\varphi(g))$ is a factor of $o(g)$. If φ is a monomorphism, then the orders are equal.

Pf: (a) $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$, but also $\varphi(e_G) = \varphi(e_G)e_H$, so $\varphi(e_G)\varphi(e_G) = \varphi(e_G)e_H$ and we can cancel $\varphi(e_G)$.

(b) For positive integers this is an induction, trivial for $n = 1$, the definition of homomorphism for $n = 2$, and easy to step from n to $n + 1$. For $n = 0$ this is (a). For $n < 0$, let's start with $n = -1$:

$$\varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_G) = e_H \ ,$$

so $\varphi(g^{-1}) = (\varphi(g))^{-1}$. Thus, for larger negative n, say $n = -m$, we have $\varphi(g^n) = \varphi((g^m)^{-1}) = (\varphi(g^m))^{-1} = (\varphi(g)^m)^{-1} = \varphi(g)^n$.

(c) By (a), the kernel K contains e_G, so it is not empty. Suppose $a, b \in K$; then $\varphi(ab) = \varphi(a)\varphi(b) = e_H e_H = e_H$, so $ab \in K$. Suppose $a \in K$; then $\varphi(a^{-1}) = \varphi(a)^{-1} = e_H^{-1} = e_H$, so $a^{-1} \in K$. Finally, suppose $a \in K$ and $g \in G$; then $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(g)e_H\varphi(g)^{-1} = e_H$, so $gag^{-1} \in K$.

(d) We know that e_G goes to e_H; if φ is one-to-one, e_G must be the only element of G that goes to e_H, i.e., $K = \{e_G\}$. Conversely, suppose $K = \{e_G\}$ and $\varphi(g_1) = \varphi(g_2)$. Then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H$, so $g_1 g_2^{-1} \in K$. By hypothesis, $g_1 g_2^{-1} = e_G$, and hence $g_1 = g_2$.

(e) Because $\varphi(g)^{o(g)} = \varphi(g^{o(g)}) = \varphi(e_G) = e_H$, we have that $o(\varphi(g))$ divides $o(g)$. If φ is a monomorphism, then because none of $g, g^2, \ldots, g^{o(g)-1}$ are e_G, none of $\varphi(g), \varphi(g)^2, \ldots, \varphi(g)^{o(g)-1}$ are e_H, so $o(\varphi(g)) = o(g)$.//

Exs of homomorphisms: (1) The identity function $G \to G$ is an isomorphism. In general, any isomorphism from a group onto itself is called an *automorphism.* For a cyclic group $G = \langle x \rangle$, if y is another generator of G, then $x^n \mapsto y^n$ gives an automorphism of G. Thus, in particular, $n \mapsto -n$ is an automorphism of $\mathbb{Z}$. And because 1 and 2 are both generators of $\mathbb{Z}_5$, the function $\mathbb{Z}_5 \to \mathbb{Z}_5$ given by

$$0 \mapsto 0, \quad 1 \mapsto 2, \quad 2 \mapsto 4, \quad 3 \mapsto 1, \quad 4 \mapsto 3$$

is an automorphism. For a general group G and an element g of G, "conjugation by g", $x \mapsto gxg^{-1}$, is an automorphism of G; the conjugations by elements of G are called *inner automorphisms.* (Of course, in an abelian group, all the inner automorphisms are the identity function.) And all of the one-to-one correspondences of V to itself that take e to e turn out to be automorphisms of V.

(2) The determinant is an epimorphism $GL(n, \mathbb{R}) \to \mathbb{R} - \{0\}$. Its kernel, the set of matrices with determinant 1, is called $SL(n, \mathbb{R})$. (We mentioned this group earlier; now we can interpret it as a kernel.)

(3) The "signum" function $\operatorname{sgn} : \mathcal{S}_n \to \{1, -1\}$, defined by $\varphi \mapsto (-1)^b$ where b is the number of backward pairs in φ, is a epimorphism with kernel $\mathcal{A}_n$.

(4) The function $\mathbb{Z} \to \mathbb{Z}_5 : a \mapsto a \mod 5$ is an epimorphism with kernel $5\mathbb{Z}$ (provided, of course, that the addition in $\mathbb{Z}_5$ is done mod 5).

(5) Differentiation is a homomorphism from the additive group of differentiable functions on a fixed interval in $\mathbb{R}$ into the additive group of all functions on that interval. Because some functions are not the derivative of anything, it is not an epimorphism, and because constant functions all go to 0, it is not a monomorphism.

(6) Physicists and geologists (crystallographers) make use of "group representations", by which they mean homomorphisms from groups (usually the ones inspired by geometric objects, like the D_n's) into $GL(n, \mathbb{R})$ for various n's. For example, Dean Roelofs asked me for a group representation for a group of order 10. I assumed that he would not have asked about the only abelian group of order 10, namely $\mathbb{Z}_{10}$, so he meant D_5. I gave him the function

$$f \mapsto \begin{pmatrix} \cos 72^\circ & -\sin 72^\circ \\ \sin 72^\circ & \cos 72^\circ \end{pmatrix}, \qquad g \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad .$$

In straightforward ways we can show the following:

Prop: Let $\varphi : G \to H$ be a homomorphism. Then:

(a) For every subgroup L of G, $\varphi(L) = \{\varphi(x) : x \in L\}$ is a subgroup of H. If $L \lhd G$, then $\varphi(L) \lhd \varphi(G)$ (though $\varphi(L)$ may not be normal in all of H).

(b) For every subgroup M of H, $\varphi^{-1}(M) = \{x \in G : \varphi(x) \in M\}$ is a subgroup of G that contains the kernel of φ. If $M \lhd H$, then $\varphi^{-1}(M) \lhd G$.

(c) For every subgroup L of G, $\varphi^{-1}(\varphi(L)) = LK$ where K is the kernel of φ. (Because $K \lhd G$, LK is a subgroup of G.) In particular, if $K \subseteq L$, then $\varphi^{-1}(\varphi(L)) = L$.

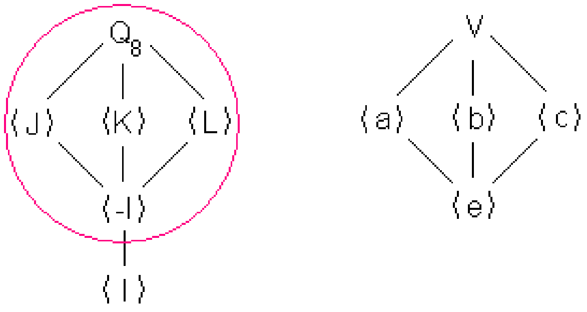
(d) For every subgroup M of H, $\varphi(\varphi^{-1}(M)) = M \cap \varphi(G)$. In particular, if $M \subseteq \varphi(G)$, then $\varphi(\varphi^{-1}(M)) = M$.

(e) There is a one-to-one correspondence, which preserves inclusion both ways, between the lattice of subgroups of G that contain the kernel of φ and the lattice of subgroups contained in the image of φ. The inverse correspondences are given by φ and φ^{-1} on subgroups, and the normal subgroups in G correspond to the normal subgroups in $\varphi(G)$ (though they may not be normal in all of H).

We can see this in our earlier example: Recall the function $\varphi : Q_8 \to V$ defined by

$$\varphi : \qquad \pm I \mapsto e, \quad \pm J \mapsto a, \quad \pm K \mapsto b, \quad \pm L \mapsto c \qquad .$$

Because φ is an epimorphism with kernel $\langle -I \rangle$, we get a natural one-to-one correspondence between the subgroups of Q_8 that contain $\langle -I \rangle$ and the subgroups of V:



Here is an example of a homomorphism $\varphi : G \to H$ and $L \triangleleft G$, but $\varphi(L)$ is not normal in H: Let $H = D_6$, $L = \langle g \rangle$, $G = \{e, g, f^3, f^3g\}$ and $\varphi : G \to H$ be the inclusion monomorphism $a \mapsto a$. Then L is normal in the abelian group G, but in the larger group H, conjugation by f takes g to $fgf^{-1} = f^2g$, outside of L.

We can finally make sense of the phrase that I have been using since early in the course, saying that one group "behaves just like" another group. What I mean by that is that there is an isomorphism from one group onto the other. Using this isomorphism, we see that the operation table of one group transforms into the operation table of the other. Thus, whatever group-theoretic property holds in one of these groups must also hold in the other: the abelian property, numbers of elements of each given order, number of subgroups of each given order, etc., etc. Of course, the isomorphism does not reflect properties that aren't related to the group structure. For example, there is an obvious isomorphism of the additive groups $M_{2\times 2}(\mathbb{R})$ and $\mathbb{R}^4$, given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (a, b, c, d)$; but $M_{2\times 2}(\mathbb{R})$ has a familiar multiplication of matrices that has no obvious parallel in $\mathbb{R}^4$. (Because the isomorphism is a one-to-one correspondence, we could artificially define a multiplication in $\mathbb{R}^4$ to match the one in $M_{2\times 2}(\mathbb{R})$, but it would not make a lot of sense.) So that extra multiplication is not a "group-theoretic property." As additive groups, they are essentially the same.

Because an isomorphism is a one-to-one correspondence, it has an inverse function, also a one-to-one correspondence. The composition of two isomorphisms is again a one-to-one correspondence. And it is not hard to see that the inverse of an isomorphism or the composition of two isomorphisms is again an isomorphism. As a result, the relation "there is an isomorphism from G to H" is an equivalence relation on the family of all groups. That family is so huge, however, that to work with it as a whole would take us into the deep forests of set theory. So let us let us give a useful name and symbol to that equivalence relation and then turn back to our well-traveled road of individual groups: If there is an isomorphism from G onto H, then we say "G is *isomorphic* to H" and write $G \cong H$. So for example, we have seen that every cyclic group of order n is isomorphic to $\mathbb{Z}_n$, every infinite cyclic group is isomorphic to $\mathbb{Z}$, and $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

The following result is easy to prove, and we'll return to it later.

Prop and Def: The set of all automorphisms from a group G onto itself is a subgroup of $\mathcal{S}(G)$, denoted $\mathrm{Aut}(G)$. The conjugations by elements of G, i.e., the inner automorphisms of G, form a subgroup of $\mathrm{Aut}(G)$ denoted $\mathrm{Inn}(G)$.

Here is a theorem that may be interesting but is not very useful, because $\mathcal{S}(G)$ is so much larger than G itself. But at least it justifies the claim that every group is essentially a subgroup of a symmetric group:

Cayley's Thm: Let G be any group. Then the function $\varphi : G \to \mathcal{S}(G)$ that is defined by: $\varphi(g)$ is the function $G \to G : x \mapsto gx$ (in symbols, $(\varphi(g))(x) = gx$), is a monomorphism (and hence an isomorphism onto its image, so G is isomorphic to a subgroup of $\mathcal{S}(G)$).

Pf: That $\varphi(g)$ is a one-to-one function $G \to G$ is proved by cancellation of g. That it is onto G follows from the fact that, for any y in G, $(\varphi(g))(g^{-1}y) = y$. So φ is indeed a function from G into $\mathcal{S}(G)$. To see it is a homomorphism, we must show that, for g, h in G, we have $\varphi(g) \circ \varphi(h) = \varphi(gh)$. But two functions are equal if they take each element of their common domain to the same element of of their common codomain, so: For all x in G,

$$(\varphi(g) \circ \varphi(h))(x) = (\varphi(g))((\varphi(h))(x)) = g(hx) = (gh)x = (\varphi(gh))(x) \ ,$$

and the result follows. Finally, to see that it is a monomorphism, suppose $\varphi(g) = \varphi(h)$; then applying these two functions to the element e of G, we see $g = h$.//

Section 13: Homomorphisms and Normal Subgroups

We have seen that the kernel of a homomorphism is a normal subgroup. Now we complete the connection between the two:

Def, Prop and the "First Isomorphism Thm (of Groups)": (1) Let K be a normal subgroup of G. Then the "canonical" function from G onto the factor group G/K, given by $g \mapsto Kg$, is an epimorphism.

(2) Let $\varphi : G \to H$ be a group homomorphism. Then the kernel K of φ is a normal subgroup of G, and G/K is isomorphic to the subgroup $\varphi(G)$ of H via the well-defined isomorphism $\overline{\varphi} : Kg \mapsto \varphi(g)$.

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d, "\mathrm{can}"'] & H \\
G/K \arrow[r, "\overline{\varphi}", "\cong"'] & \varphi(G) \arrow[u, hook, "\mathrm{incl}"']
\end{tikzcd}$$

In this diagram the vertical maps are the canonical homomorphism $G \to G/K : g \mapsto Kg$ and the inclusion function $\varphi(G) \to H : x \mapsto x$.

Pf: (1) Because K is a normal subgroup of G, we know that G/K makes sense, and the definition of multiplication in this group makes the canonical map, which is clearly onto G/K, an epimorphism: $(Ka)(Kb) = K(ab)$.

(2) We show that $\overline{\varphi}$ is well-defined and one-to-one with the same string of implications, going in two directions: For g_1, g_2 in G,

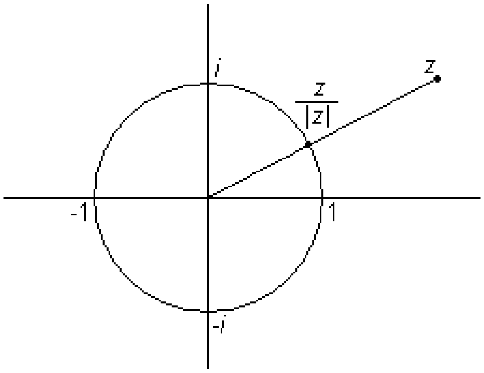
$$Kg_1 = Kg_2 \quad \Longleftrightarrow \quad g_1 g_2^{-1} \in K \quad \Longleftrightarrow \quad \varphi(g_1 g_2^{-1}) = e_H \quad \Longleftrightarrow \quad \varphi(g_1) = \varphi(g_2) \ .$$

Because φ and $\overline{\varphi}$ hit the same elements in H, $\overline{\varphi}$ is onto $\varphi(G)$, so across the bottom of the diagram above $\overline{\varphi}$ is an isomorphism.//

Ex: 1. Because $\mathbb{Z} \to \mathbb{Z}_5 : k \mapsto k \mod 5$ is an additive group epimorphism (where the addition in $\mathbb{Z}_5$ is mod 5), and $5\mathbb{Z}$ is the kernel, we have $\mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}_5$.

2. Because determinant is a multiplicative epimorphism from $GL(n, \mathbb{R})$ to $\mathbb{R} - \{0\}$, and $SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) : \det(A) = 1\}$ is the kernel, we see that $GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R} - \{0\}$.

3. You may not know much about absolute value of complex numbers: For $x, y \in \mathbb{R}$, if $z = x+yi$, then $|z| = |x + yi| = \sqrt{x^2 + y^2}$. But you can check that, for $z, w \in \mathbb{C}$, $|zw| = |z||w|$. Thinking about drawing complex numbers in the plane (an "Argand diagram"), we see that, for each nonzero z in $\mathbb{C}$, $z/|z|$ is the point on the unit circle $\mathcal{U}$ (the set of points one unit away from the origin) that makes the same angle with the positive real axis as z does.



We get two homomorphisms of multiplicative groups:

$$(\mathbb{C}-\{0\}) \to \mathbb{R}-\{0\} : z \mapsto |z| \qquad (\mathbb{C}-\{0\}) \to (\mathbb{C}-\{0\}) : z \mapsto z/|z|$$

The first of these has kernel $\mathcal{U}$ and image $\mathbb{R}^+$ (the positive real axis), so $\mathcal{U}$ is a subgroup of $\mathbb{C}-\{0\}$ (necessarily normal, because $\mathbb{C}-\{0\}$ is abelian), and $(\mathbb{C}-\{0\})/\mathcal{U} \cong \mathbb{R}^+$. The second has kernel $\mathbb{R}^+$ and image $\mathcal{U}$, so $(\mathbb{C}-\{0\})/\mathbb{R}^+ \cong \mathcal{U}$.

The Second and Third Isomorphism Theorems are not really all that important, and are simple consequences of the Fundamental Theorem:

Second Isomorphism Thm: Let H, K be subgroups of G with $K \triangleleft G$. Then HK is a subgroup of G and

$$\frac{H}{H \cap K} \cong \frac{HK}{K} .$$

Pf: It is immediate that $H, K \subseteq HK = \{hk : h \in H, k \in K\}$ and, once we have shown that HK is a subgroup of G, that $K \triangleleft HK$. It is left to the reader to show that HK is closed under inverses, and that $H \cap K$ is normal in H. We show that HK is closed under the operation: Let $h_1, h_2 \in H$ and $k_1, k_2 \in K$; then $(h_1k_1)(h_2k_2) = (h_1h_2)((h_2^{-1}k_1h_2)k_2)$; of course, $h_1h_2 \in H$, and because, by the normality, the conjugate $h_2^{-1}k_1h_2$ of k_1 by h_2^{-1} is in K, we have $(h_2^{-1}k_1h_2)k_2 \in K$. So $(h_1k_1)(h_2k_2) \in HK$.

Now consider the canonical epimorphism $G \to G/K : g \mapsto Kg$, with its domain restricted to H. It is of course still a homomorphism, its kernel is the set of elements of K that are also in H, i.e., $H \cap K$, and its image is HK/K, the cosets of K in G that include elements of H. By the Fundamental Theorem, the result follows.//

Third Isomorphism Thm: Let $K \subseteq H$ be normal subgroups of G. Then H/K is a normal subgroup of G/K and

$$\frac{G/K}{H/K} \cong \frac{G}{H} .$$

Pf: For any Kh in H/K and Kg in G/K, we have $ghg^{-1} \in H$, so $(Kg)(Kh)(Kg)^{-1} \in H/K$. Now consider the composition of the canonical epimorphisms $G \to G/K : g \to Kg$ and $G/K \to (G/K)/(H/K) : Kg \mapsto (H/K)(Kg)$. This composition is still an epimorphism, and its kernel is the set of elements g in G for which $Kg \in H/K$, which is just H. By the Fundamental Theorem, the result follows.//

Ex: Consider the subgroup $\langle 10 \rangle$ in $\mathbb{Z}_{20}$. What does $\mathbb{Z}_{20}/\langle 10 \rangle$ look like? Well, $\mathbb{Z}_{20} \cong \mathbb{Z}/20\mathbb{Z}$ and

$\langle 10 \rangle$ is the image of $10\mathbb{Z}$ under the epimorphism $\mathbb{Z} \to \mathbb{Z}_{20}$, so $Z_{20}/\langle 10 \rangle \cong (\mathbb{Z}/20\mathbb{Z})/(10\mathbb{Z}/20\mathbb{Z}) \cong \mathbb{Z}/10\mathbb{Z} \cong \mathbb{Z}_{10}$.