A Few Notes on Group, Ring and Field Theory (WIP)

David Meyer

dmm@{1-4-5.net,uoregon.edu}

Last update: January 21, 2020

1 Introduction

Group Theory is the study of symmetry. Symmetry takes many different forms. Here we'll focus on the basic theory and use that to motivate a few examples

2 Definitions

The pair $(G, \circ)$ with the following four properties is called a group:

1. **Closure:** $x, y \in G \implies x \circ y \in G$
   In words: A group is closed under the group operation $\circ$. $\circ$ is sometimes called "group multiplication" (or even "multiplication") even though it might be some other operation (such as addition).

2. **Associativity:** $x, y, z \in G \implies (x \circ y) \circ z = x \circ (y \circ z)$

3. **Identity:** $\exists e \in G$ s.t. $\forall x \in G \; x \circ e = e \circ x = x$

4. **Inverse:** $\forall x \in G \; \exists x^{-1} \in G$ s.t. $x \circ x^{-1} = x^{-1} \circ x = e$

The point here is that a group is a device that measures symmetry.

Before doing an example, we need to define the *order* of a group element. Specifically, the order of a group element[1] is the smallest integer n, if it exists, such that $x^n = e$. Note that the relationship between the order of an element and the order of a group is that the order of the subgroup $\langle x \rangle$ generated by x is n. That is, $x^n = e \implies |\langle x \rangle| = n$.

[1] Not to be confused with the order of a group, which for finite $G =\mid G \mid$.

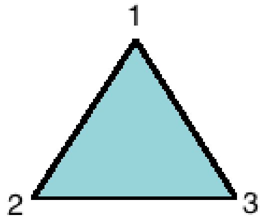

Figure 1: Symmetries of a Triangle

Now, consider the symmetries of a triangle shown in Figure 1. This forms a group called S_3 where the group operation $\circ$ is function composition. Here we name the vertices of the triangle with "labels" from the set $\{1, 2, 3\}$. In this case our group has six elements, as shown using cyclic notation in Table 1.

Element	Type	Action	Inverse	Order
e	No Op	No Op	e	1
(1 2)	Reflection	Fix 3, swap 1 & 2	(1 2)	2
(2 3)	Reflection	Fix 1, swap 2 & 3	(2 3)	2
(1 3)	Reflection	Fix 2, swap 1 & 3	(1 3)	2
(1 2 3)	Rotation	Rotate CW by $\frac{2\phi}{3}$	(1 3 2)	3
(1 3 2)	Rotation	Rotate CCW by $\frac{2\phi}{3}$	(1 2 3)	3

Table 1: The Group S_3

A group is called *Abelian* or *commutative* if the group operation $\circ$ commutes. That is, $\forall x, y \in G\ x \circ y = y \circ x$. Note that in our example above, S_3 is not Abelian. You can see this if you consider: Let $x = (12)$ and $y = (23)$. Then $x \circ y \neq y \circ x$ since

$$(12) \circ (23) = (123)$$
$$(23) \circ (12) = (132)$$

So S_3 is not Abelian.

One other example: Let X be any set and $G = \{\text{bijections } f : X \to X\}$ with group operation function composition. Then $(G, \circ)$ is a group. To show this, we need to show the following four things:

1. **Closure under $\circ$:** The composition of bijections is a bijection

2. **Associativity:** $(f \circ g) \circ h = f \circ (g \circ h)$
3. **Identity:** $I(x) = x$
4. **Inverse:** $y = f(x) \Leftrightarrow f^{-1}(y) = x$

One other definition we'll need here: A non-empty subset $H \subseteq G$ is a *subgroup*, denoted $H \leq G$, iff

1. **Closure:** $x, y \in H \implies x \circ y \in H$
2. **Inverses:** $x \in H \implies x^{-1} \in H$
3. **Identity:** $e \in H$ (implies H non-empty)

3 Subgroups, Equivalence Relations, and Cosets

Let $H \leq G$. H induces an equivalence relation $\sim$ on G as follows: For a group G and a subgroup $H \leq G$

$$x \sim y \text{ iff } x = yh \text{ for some } h \in H \tag{1}$$

The equivalence relation $\sim$ implies H partitions G. In particular, fix some $x \in G$. Then

$$E_x = \{y \in G \mid x \sim y\}$$

E_x is sometimes denoted $[x]$. In this case the notation $[x] = \{y \in G \mid x \sim y\} \implies x^{-1}y \in H$ or $y \in xH$.

Note that the E_x's form a disjoint union: $\underset{x \in G}{\cup} E_x = G$ and either $E_x = E_y$ or $E_x \cap \mathbb{E}_y = \emptyset$. This will become important later when we consider Lagrange's Theorem (Theorem 3.1).

More generally,

$$\begin{aligned}
E_x &= \{y \in G \mid x \sim y\} && \text{\# definition of } E_x \\
&= \{y \in G \mid y = xh \text{ for some } h \in H\} && \text{\# definition of } \sim \\
&= \{xh \mid h \in H\} && \text{\# simplify} \\
&= xH && \text{\# } xH \text{ is the left } \textit{coset} \text{ of H for x}
\end{aligned}$$

Summary: $E_x = [x] = \{xh \mid h \in H\} = xH$. xH is called a *left coset* of H for x.

Somewhat surprisingly, H and all of its cosets have the same cardinality. That is, $|H| = |xH| \; \forall x \in G$. The proof of this is pretty straightforward. Here we just need to construct a bijection $H \to xH$. We can do this by fixing a $x \in G$ and considering $l_x : H \to xH$ by the map $h \mapsto xh$. Then we need to show that l_x is one-to-one and onto.

- **one-to-one**
  For one-to-one we want to show that $l_x(h_1) = l_x(h_2) \implies h_1 = h_2$. In this case we can cancel on the left: $l_x(h_1) = l_x(h_2) \implies xh_1 = xh_2 \implies h_1 = h_2$. So one-to-one.
- **onto**
  Consider some $z \in xH$. Then $z = xh$ for some $h \in H$, so $l_x(x) = z$ and l_x is onto.

So $l_x : H \to xH$ is a bijection and therefore H and all of its cosets xH have the same cardinality, namely, $|H|$.

A couple useful definitions:

- $|G|$ is the *order* of G. If G is finite then $|G| = \#$ of elements in G.
- $|x|$ is the *order* of x. $|x|$ is the smallest positive integer n, if it exists, such that $x^n = e$.
- $[G : H]$ is the *index* of H in G. $[G : H] = \#$ of cosets for H (left or right) in G.

With this machinery we can state and prove Lagrange's Theorem:

Theorem 3.1. ***Lagrange's Theorem:*** *Let G be a finite group and let H be a subgroup of G. Then $|H|$ divides $|G|$.*

Proof: Recall that the left cosets of H in G form a disjoint union of G. We also know that $|H| = |xH|$. Now suppose that there are k cosets. Then $|G| = k \cdot |H|$. Since $|G|$, $|H|$, and k are integers $|H|$ divides $|G|$. $\square$

Note that if G is finite, $[G : H] = \frac{|G|}{|H|}$. A nice corollary of Lagrange's Theorem is that if $x \in G$, then $|x|$ divides $|G|$.

4 Normal and Quotient Subgroups

Let G be any group. Then a subgroup $N \subseteq G$ is called *normal*, written $N \lhd G$, iff $\forall x \in G \; xN = Nx$. Equivalently, $\forall x \in G \; N = xNx^{-1}$ (multiply on the right by x^{-1}). Also equivalently $\forall x \in G \; \forall n \in N \; xnx^{-1} \in N$. The last expression is called conjugation by x.

5 Group Actions

The action of a group is a formal way of interpreting the manner in which the elements of the group correspond to (usually linear) transformations of some space in a way that preserves the structure of that space. Common examples of spaces that groups act on are sets, vector spaces, and topological spaces. Actions of groups on vector spaces are called representations of the group (this is the subject of representation theory).

Definition: An *action* of the group G on the set X is a map $G \times X \to X$ by $(g, x) \mapsto \phi(g)x$ such that

- $\phi(e)x = x$
- $\phi(g_1 g_2) = \phi(g_1)\big[\phi(g_2)x\big]$

Examples of actions include

- $G = (S_n, \circ)$ and $X = \{1, \ldots, n\}$. Then for permutation σ, $\phi(\sigma)i = \sigma(i)$.
- $G = (\mathbb{Z}, +)$ and $X = \mathbb{R}$. Then the translations $\phi(n)x = x + n$ are an action.
- $(S^1, +)$ and $X = \mathbb{C}$. Then the rotations $\phi(e^{i\theta})z = e^{i\theta}z$ are an action.

Another definition of group action is that we say that the group G acts on the set X if there is a homomorphism $\phi : G \to \mathrm{Sym}(X)$.

5.1 Group Actions and Equivalence Relations

Perhaps surprisingly, it turns out that $x \sim y \Leftrightarrow \exists g \in G$ s.t. $\phi(g)x = y$, where ϕ is as defined above. So all the machinery developed for the equivalence relations E_x apply to actions, except that in the context of group actions what we called equivalence classes above are called orbits. Orbits are denoted O_x and $O_x = E_x$. In particular

$$\begin{aligned} O_x &= \{y \in X \mid x \sim y\} \\ &= \{y \in X \mid \phi(g)x = y\} \\ &= \{\phi(g)x \mid g \in G\} \end{aligned}$$

6 Group Homomorphism

Let $(G, \diamond)$ and $(H, \circ)$ be groups. Common usage is to use G to refer to $(G, \diamond)$. Similarly, H will refer to $(H, \circ)$. Then a mapping $\phi : G \to H$ is called a *homomorphism* iff

$$\phi(x \diamond y) = \phi(x) \circ \phi(y) \; \forall x, y \in G$$

Essentially, a homomorphism $\phi : G \to H$ is a way of exploring the structure of H by varying G using structure preserving transformations. That is, ϕ preserves the group operation.

Example: Define a map

$$\phi : G \to H$$

where $G = \mathbb{Z}$ and $H = \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$ is the standard group of order two. Then define $\phi : \mathbb{Z} \to \mathbb{Z}_2$ by the rule

$$\phi(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd} \end{cases}$$

It is easy to check that ϕ is a homomorphism. Suppose that x and y are two integers. Then there are four cases:

- x and y are both even

  In this case $\phi(x + y) = 0$ (even + even = even). Here $\phi(x) + \phi(y) = 0 + 0 = 0$ so $\phi(x + y) = \phi(x) + \phi(y) = 0 + 0 = 0$.

- x and y are both odd

  In this case $\phi(x + y) = 0$ (odd + odd = even). Here $\phi(x) + \phi(y) = 1 + 1 = 2 \mod 2 = 0$, so $\phi(x + y) = \phi(x) + \phi(y) = 1 + 1 = 2 \mod 2 = 0$.

- x is even and y is odd or x is odd and y is even

  In this case one is even and the other is odd and $x + y$ is odd. Here $\phi(x + y) = 1$ and $\phi(x) + \phi(y) = 1 + 0 = 1$ so $\phi(x + y) = \phi(x) + \phi(y)$.

Thus ϕ is a homomorphism. Note that in this example $\diamond = +$ (normal addition in $\mathbb{Z}$) and $\circ = +$ (addition mod 2 in $\mathbb{Z}_2$).

Example: Let $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}_{>0}, \cdot)$ and let $\phi(x) = e^x$. To see that ϕ is a homomorphism consider $\phi(x + y)$:

$$\begin{array}{rcll} \phi(x+y) & = & e^{(x+y)} & \text{\# definition of } \phi \\ & = & e^x \cdot e^y & \text{\# } a^{(b+c)} = a^b \cdot a^c \\ & = & \phi(x) \cdot \phi(y) & \text{\# definition of } \phi \\ \phi(x+y) & = & \phi(x) \cdot \phi(y) & \text{\# therefore } \phi \text{ is a homomorphism} \end{array}$$

Note that in this example $\diamond = +$ (normal addition) and $\circ = \cdot$ (normal multiplication).

Frequently the group operation is the same for G and H (like, for example, if $\phi : G \to G$). So in many cases we see the homomorphism property expressed as follows:

$$\phi(xy) = \phi(x)\phi(y) \; \forall x, y \in G$$

Example: Let G be a group with $N \lhd G$ (N is a normal subgroup of G). Define the *quotient homomorphism* q as

$$q : G \to G/N$$

and let $x \mapsto xN$ by $q(x) = xN$. To show that q is a homomorphism, let $x, y \in G$ and consider $q(xy)$:

$$\begin{array}{rcll} q(xy) & = & xyN & \text{\# definition of } q \\ & = & xyNN & \text{\# } NN = N \text{ for } N \text{ a subgroup in } G \\ & = & x(yN)N & \text{\# group multiplication is associative} \\ & = & x(Ny)N & \text{\# } N \text{ normal so } xN = Nx \\ & = & (xN)(yN) & \text{\# group multiplication is associative} \\ & = & q(x)q(y) & \text{\# definition of } q \\ q(xy) & = & q(x)q(y) & \text{\# therefore } q \text{ is a homomorphism} \end{array}$$

Lemma 6.1. Let G and H be groups where e is the identity in G and f is the identity in H and define a homomorphism $\phi : G \to H$. Then

1. $\phi(e) = f$. That is, ϕ maps the identity in G to the identity in H. In particular
   - $\phi(0) = 0$
   - $\phi(1) = 1$
2. $\phi(a^{-1}) = (\phi(a))^{-1}$. That is, ϕ maps inverses to inverses.
3. If K is subgroup of G, then $\phi(K)$ is a subgroup of H.

Proof: To show 1. above let $a = \phi(e)$. Then

$$\begin{array}{lll}
a = & \phi(e) & \text{\# by assumption} \\
= & \phi(e \cdot e) & \text{\# } x \cdot e = e \cdot x = x \text{ so } e = e \cdot e \\
= & \phi(e) \cdot \phi(e) & \text{\# } \phi \text{ is a homomorphism} \\
= & a \cdot \phi(e) & \text{\# } a = \phi(e) \text{ (by assumption)} \\
= & a \cdot a & \text{\# } \ldots \\
\Longrightarrow & a \cdot a^{-1} = (a \cdot a) \cdot a^{-1} & \text{\# multiply on the right by } a^{-1} \\
\Longrightarrow & a \cdot a^{-1} = a \cdot (a \cdot a^{-1}) & \text{\# multiplication is associative} \\
\Longrightarrow & a \cdot a^{-1} = a \cdot f & \text{\# } a \cdot a^{-1} = f, \text{ where } f \text{ is the identity in } H \\
\Longrightarrow & a \cdot a^{-1} = a & \text{\# } a \cdot f = a \\
\Longrightarrow & f = a & \text{\# } a \cdot a^{-1} = f \text{ by definition of inverse} \\
\Longrightarrow & \phi(e) = f & \text{\# } \phi \text{ maps the identity in } G \text{ to the identity in } H
\end{array}$$

So ϕ maps the identity in G to the identity in H which shows 1. above.

Another approach is to recognize that if the group operation is $+$, then 0 is the (additive) identity, that is, $0 + x = x + 0 = x$. Then

$$\begin{array}{rll}
0 + x = & x & \text{\# 0 is the additive identity} \\
\Longrightarrow & \phi(0 + x) = \phi(x) & \text{\# apply } \phi \\
\Longrightarrow & \phi(0) + \phi(x) = \phi(x) & \text{\# } \phi \text{ is a homomorphism} \\
\Longrightarrow & (\phi(0) + \phi(x)) - \phi(x) = \phi(x) - \phi(x) & \text{\# subtract } \phi(x) \text{ from both sides} \\
\Longrightarrow & (\phi(0) + \phi(x)) - \phi(x) = 0 & \text{\# } \phi(x) - \phi(x) = 0 \\
\Longrightarrow & \phi(0) + (\phi(x) - \phi(x)) = 0 & \text{\# addition is associative} \\
\Longrightarrow & \phi(0) + 0 = 0 & \text{\# } \phi(x) - \phi(x) = 0 \\
\Longrightarrow & \phi(0) = 0 & \text{\# } \phi(x) \text{ maps 0 to 0}
\end{array}$$

So $\phi(0) = 0$. A similar argument can be used where the group operation is multiplication:

$$\begin{array}{rll}
1 \cdot x = & x & \text{\# 1 is the multiplicative identity} \\
\Longrightarrow & \phi(1 \cdot x) = \phi(x) & \text{\# apply } \phi \\
\Longrightarrow & \phi(1) \cdot \phi(x) = \phi(x) & \text{\# } \phi \text{ is a homomorphism} \\
\Longrightarrow & (\phi(1) \cdot \phi(x)) \cdot (\phi(x))^{-1} = \phi(x) \cdot (\phi(x))^{-1} & \text{\# multiply on the right by } (\phi(x))^{-1} \\
\Longrightarrow & (\phi(1) \cdot \phi(x)) \cdot (\phi(x))^{-1} = 1 & \text{\# } \phi(x) \cdot (\phi(x))^{-1} = 1 \\
\Longrightarrow & \phi(1) \cdot (\phi(x) \cdot (\phi(x))^{-1}) = 1 & \text{\# multiplication is associative} \\
\Longrightarrow & \phi(1) \cdot 1 = 1 & \text{\# } \phi(x) \cdot (\phi(x))^{-1} = 1 \\
\Longrightarrow & \phi(1) = 1 & \text{\# } x \cdot 1 = x
\end{array} \tag{2}$$

So we have $\phi(0) = 0$ and $\phi(1) = 1$.

To show 2., note that since G is a group, $x^{-1} \in G$ and $x \cdot x^{-1} = 1$ for $x, x^{-1} \in G$. Then

$$\begin{array}{rcll} x \cdot x^{-1} & = & 1 & \text{\# definition of inverse} \\ & \implies & \phi(x \cdot x^{-1}) = \phi(1) & \text{\# apply } \phi \\ & \implies & \phi(x \cdot x^{-1}) = 1 & \text{\# } \phi(1) = 1 \text{ (see Equation 2 above)} \\ & \implies & \phi(x) \cdot \phi(x^{-1}) = 1 & \text{\# } \phi \text{ is a homomorphism} \\ & \implies & \phi(x^{-1}) = 1/\phi(x) & \text{\# divide both sides by } \phi(x) \\ & \implies & \phi(x^{-1}) = (\phi(x))^{-1} & \text{\# hence } \phi \text{ maps inverses to inverses} \end{array} \tag{3}$$

Finally, to show 3., let $X = \phi(K)$. Then it suffices to show that X is non-empty and closed under products and inverses. X contains f, the identity of H, by 1. above. We also know that X is closed under inverses by 2. above. Finally, we know that X and is closed under products (almost) by definition. Thus X is a subgroup. □

Theorem 6.1. *Let G and H be groups and let $f : G \to H$ be a group homomorphism. Then f is one-to-one iff the kernel of f is trivial, that is,* $\ker f = \{e\}$ *where e is the identity element of G.*

Proof: Here we'll show that f is one-to-one $\iff \ker f = \{e\}$:

- f is one-to-one $\implies \ker f = \{e\}$

  Suppose the homomorphism $f : G \to H$ is one-to-one. Then since f is a group homomorphism, the identity element e of G is mapped to the identity element e' of H. That is, $f(e) = e'$ (see Equation 2 above).

  Now let $g \in \ker f$, so $f(g) = e'$, recalling that $\ker f = \{g \in G \mid f(g) = e'\}$. So now $f(e) = e'$ and $f(g) = e'$ which implies that $f(g) = f(e)$.

  Since f is one-to-one[2] we know that $(g) = f(e) \implies g = e$, so $g = e$. But g was an arbitrary element of $\ker f$ so f maps every $g \in \ker f$ to e. Hence $\ker f = \{e\}$.

- $\ker f = \{e\} \implies f$ is one-to-one

  On the other hand, suppose that $\ker f = \{e\}$ and that there exists $g_1, g_2 \in G$ such that

  $$f(g_1) = f(g_2) \tag{4}$$

  Now consider an element $g_1 g_2^{-1} \in G$. Then

[2] Recall that saying f is one-to-one means that $f(x) = f(y) \implies x = y$.

$$
\begin{array}{rcll}
f(g_1g_2^{-1}) & = & f(g_1)f(g_2^{-1}) & \#\ f \text{ is a homomorphism} \\
& = & f(g_1)(f(g_2))^{-1} & \#\ f(g_2^{-1}) = (f(g_2))^{-1} \text{ (Equation 3)} \\
& = & f(g_1)(f(g_1))^{-1} & \#\ f(g_2) = f(g_1) \text{ (Equation 4)} \\
& = & e' & \#\ f(g_1)(f(g_1))^{-1} = e'
\end{array}
\tag{5}
$$

So $f(g_1g_2^{-1}) = e'$ which implies that $g_1g_2^{-1} \in \ker f$. But by assumption $\ker f = \{e\}$ so $g_1g_2^{-1} = e$.

If you multiply $g_1g_2^{-1} = e$ on the right by g_2, you notice that

$$
\begin{array}{rcll}
g_1g_2^{-1} & = & e & \#\ \text{Equation 5} \\
& \Longrightarrow & (g_1 \cdot g_2^{-1}) \cdot g_2 = e \cdot g_2 & \#\ \text{multiply on the right by } g_2 \\
& \Longrightarrow & g_1 \cdot (g_2^{-1} \cdot g_2) = e \cdot g_2 & \#\ \text{multiplication is associative} \\
& \Longrightarrow & g_1 \cdot e = e \cdot g_2 & \#\ g_2^{-1} \cdot g_2 = e \\
& \Longrightarrow & g_1 = g_2 & \#\ e \cdot g = g \cdot e = g
\end{array}
$$

So $f(g_1) = f(g_2)$ (Equation 4) implies that $g_1 = g_2$ and so f is one-to-one.

This shows that f is one-to-one $\iff \ker f = \{e\}$.

7 The First Isomorphism Theorem

The First Isomorphism Theorem (FIT) is a handy piece of machinery for many problems in group theory. Before getting to all of that, recall the following:

- A mapping $\phi : G \to G'$ is called a **group homomorphism** if it preserves the group operation: $\phi(ab) = \phi(a)\phi(b)$.
- The **image of G:** $\phi(G) = \{\phi(g) \mid g \in G\}$.
- The **kernel of ϕ**: $\ker \phi = \{g \in G \mid \phi(g) = e'\}$ (e' is the identity in G').
- $\phi(a) = \phi(b)$ iff $a \ker \phi = b \ker \phi$.
- If $\phi(g) = g'$ then $\phi^{-1}(g') = g \ker \phi$.

So here's a theorem: Let $\phi : G \to G$ be a group homomorphism. Then $\ker \phi \lhd G$.

In other words: The kernel of ϕ is a normal subgroup of G.

To show this, first let $k \in \ker \phi$ and let $g \in G$. Then we want to show[3] that $gkg^{-1} \in \ker \phi$ or equivalently that $g \ker \phi g^{-1} = \ker \phi$. So now consider $\phi(gkg^{-1})$:

[3] Recall that for normal subgroups $xN = Nx$ which implies that $xnx^{-1} \in N$.

$$\begin{aligned}
\phi(gkg^{-1}) &= \phi(g)\phi(k)\phi(g^{-1}) && \#\ \phi \text{ is a homomorphism}\\
&= \phi(g)\phi(k)(\phi(g))^{-1} && \#\ \phi(g^{-1}) = (\phi(g))^{-1} \text{ (see (3) above)}\\
&= \phi(g)e(\phi(g))^{-1} && \#\ k \in \ker\phi \implies \phi(k) = e \text{ (e is the identity in G)}\\
&= \phi(g)(\phi(g))^{-1} && \#\ \phi(g)e = \phi(g) \text{ and } e\phi(g)^{-1} = \phi(g)^{-1}\\
&= e && \#\ xx^{-1} = x^{-1}x = e \text{ (where } x \neq 0)\\
\phi(gkg^{-1}) &= e && \#\ \implies gkg^{-1} \in \ker\phi
\end{aligned}$$

So $gkg^{-1} \in \ker\phi \implies g\ker\phi g^{-1} = \ker\phi \implies \ker\phi \lhd G$.

Example: Consider the group $(\mathbb{Z}_{12}, +)$ and let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_{12}$ by $\phi(x) = 3x$. First, we need to show that ϕ is a homomorphism. But this is an easy one: $\phi(x+y) = 3(x+y) = 3x + 3y = \phi(x) + \phi(y)$. So ϕ is a homomorphism. Next consider the mapping ϕ on $\mathbb{Z}_{12}$:

$$\begin{tikzcd}
\mathbb{Z}_{12} : & 0 \arrow[d] & 1 \arrow[d] & 2 \arrow[d] & 3 \arrow[d] & 4 \arrow[d] & 5 \arrow[d] & 6 \arrow[d] & 7 \arrow[d] & 8 \arrow[d] & 9 \arrow[d] & 10 \arrow[d] & 11 \arrow[d] \\
\phi(x) : & 0 & 3 & 6 & 9 & 0 & 3 & 6 & 9 & 0 & 3 & 6 & 9
\end{tikzcd}$$

We can see that the image of $\mathbb{Z}_{12}$, $\phi(\mathbb{Z}_{12}) = \{0, 3, 6, 9\}$ and that $\ker\phi = \{0, 4, 8\}$.

Grouping the elements of $\mathbb{Z}_{12}$ with their images we see that

$$\begin{tikzcd}
\mathbb{Z}_{12} : & \{0,4,8\} \arrow[d] & \{1,5,9\} \arrow[d] & \{2,6,10\} \arrow[d] & \{3,7,11\} \arrow[d] \\
\phi(x) : & 0 \arrow[d] & 3 \arrow[d] & 6 \arrow[d] & 9 \arrow[d] \\
\phi(x)^{-1} : & \{0,4,8\} \arrow[d, equal] & \{1,5,9\} \arrow[d, equal] & \{2,6,10\} \arrow[d, equal] & \{3,7,11\} \arrow[d, equal] \\
 & 0 + \ker\phi & 1 + \ker\phi & 2 + \ker\phi & 3 + \ker\phi
\end{tikzcd}$$

This is a nice example of the property that $\phi(a) = x \implies \phi^{-1}(x) = a\ker\phi$. To see this, choose, for example, $a = 5$. Then $\phi(5) = 3 \cdot 5 = 15$ and $15 \mod 12 = 3$, so $x = 3$. This implies that $\phi(3)^{-1} = 5 + \ker\phi = \{5+0, 5+4, 5+8\} = \{5, 9, 13\} = \{1, 5, 9\}$, noting that $13 \mod 12 = 1$.

Now we can state the **First Isomorphism Theorem:** Let $\phi : G \to H$ be an onto homomorphism. Then $H \simeq G/N$, where $N = \ker\phi$.

Though technical this is really an amazing theorem. So here's one way to prove this. We need to construct an isomorphism $\widetilde{\phi} : G/N \to H$ by $\widetilde{\phi}(gN) = \phi(g)$. To show this, we need to show three things: that $\widetilde{\phi}$ is well-defined, that $\widetilde{\phi}$ is a homomorphism, and that $\widetilde{\phi}$ is one-to-one and onto.

- To show that $\widetilde{\phi}$ is well-defined[4]. That is, if $gN = hN$ then $\widetilde{\phi}(gN) = \widetilde{\phi}(hN)$. Now, if $gN = hN$ then since N is the the identity in G/N, $g = hn$ for some $n \in N$. This means

$$\begin{array}{rcll}
\widetilde{\phi}(gN) & = & \phi(g) & \# \text{ definition of } \widetilde{\phi}(gN) \\
 & = & \phi(hn) & \# \; g = hn \text{ since } gN = hN \text{ by assumption} \\
 & = & \phi(h)\phi(n) & \# \; \phi \text{ is a homomorphism} \\
 & = & \phi(h)e & \# \; n \in N = \ker\phi = \{x \in G \mid \phi(x) = e\} \\
 & = & \phi(h) & \# \; x \cdot e = x \\
 & = & \widetilde{\phi}(hN) & \# \text{ definition of } \widetilde{\phi} \\
\widetilde{\phi}(gN) & = & \widetilde{\phi}(hN) & \# \text{ so } \widetilde{\phi} \text{ is well-defined}
\end{array}$$

- Next, we need to show that $\widetilde{\phi}$ is a homomorphism. To see this, consider

$$\begin{array}{rcll}
\widetilde{\phi}(gNhN) & = & \widetilde{\phi}(ghNN) & \# \text{ definition of group multiplication} \\
 & = & \widetilde{\phi}(ghN) & \# \; NN = N(N \text{ a subgroup}) \\
 & = & \phi(gh) & \# \text{ definition of } \widetilde{\phi} \\
 & = & \phi(g)\phi(h) & \# \; \phi \text{ is a homomorphism} \\
 & = & \widetilde{\phi}(gN)\widetilde{\phi}(hN) & \# \text{ definition of } \widetilde{\phi} \\
\widetilde{\phi}(gNhN) & = & \widetilde{\phi}(gN)\widetilde{\phi}(hN) & \# \text{ therefore } \widetilde{\phi} \text{ is a homomorphism}
\end{array}$$

  So $\widetilde{\phi}$ is a homomorphism.

- For one-to-one, we need to show that $\widetilde{\phi}(gN) = \widetilde{\phi}(hN) \implies gN = hN$. We know that if $\widetilde{\phi}(gN) = e_H$, then $\phi(g) = e_H$. So $g \in \ker\phi$ (recalling that $N = \ker\phi$). This implies that $gN \in N$ (N is the identity in G/N). Similarly for $\widetilde{\phi}(hN)$, so $\widetilde{\phi}$ is one-to-one. [ed: this isn't complete]

- Finally, to show onto, choose a h in H. We want to show that $\exists gN \in G/N$ with $\widetilde{\phi}(gN) = h$. Well, we know that ϕ is onto so $\exists g \in G$ with $\phi(g) = h$. This means that $\widetilde{\phi}(gN) = \phi(g) = h$, so $\widetilde{\phi}$ is onto.

This shows that $H \simeq G/\ker\phi$.

[4] Well-defined is kind of the opposite of one-to-one where we show that if $f(x) = f(y)$ then $x = y$.

8 Rings, Ideals and Homomorphisms

This section provides a few notes on Ring Theory. To start, a few definitions

Definition 8.1. A ring R is an abelian group with a multiplication operation

$$(a, b) \mapsto ab$$

which is associative and satisfies the distributive laws $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$ and has identity element 1.

Here there is a group structure with the addition operation but not necessarily with the multiplication operation. Thus an element of a ring may or may not be invertible with respect to the multiplication operation.

Definition 8.2. Let a, b be in a ring R. If $a \neq 0$ and $b \neq 0$ but $ab = 0$, then we say that a and b are *zero divisors*. If $ab = ba = 1$, we say that a is a *unit* or that a is invertible.

For example, consider the ring $\mathbb{Z}_n$. Notice that if n is not prime then $\mathbb{Z}_n$ has zero divisors. For a concrete example, consider the ring $\mathbb{Z}_{10}$ and let $a = 2$ and $b = 5$. Then $ab = 2 \cdot 5 = 10$ and $10 \mod 10 = 0$, so 2 and 5 are zero divisors in $\mathbb{Z}_{10}$. On the other hand, if $n = p$ is prime then the only factors of p are 1 and p, so $\mathbb{Z}_p$ has no zero divisors.

Definition 8.3. Let R be a ring. Then if $ab = ba$ for any $a, b \in R$ then R is said to be *commutative.*

In general, for a given ring R the addition operation is commutative, but the the multiplication operation may or may not be commutative. There are two particular kinds of rings where the multiplication operation is well-behaved:

Definition 8.4. An *integral domain* is a commutative ring with no zero divisors. A *division ring* or skew field is a ring in which every non-zero element a has an inverse a^{-1}.

For example, the integers $\mathbb{Z}$ form an integral domain. The quaternions (more on this later) form a division ring.

Definition 8.5. The characteristic of a ring R, denoted by $\text{char}(R)$, is the smallest positive integer n such that

$$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$$

One more definition then we'll look at a few examples.

Definition 8.6. A subring of a ring R is a subset S of R that forms a ring under the operations of addition and multiplication defined in R.

8.1 Examples

Before diving into examples, it is worthwhile to notice that the concepts of subrings and ideals, while related, have subtle and important differences. Both an ideal I and a subring S of a ring R are subsets of R which are subgroups under addition and are closed under multiplication. However, each has an additional property:

- An ideal I has the absorption property ($\forall r \in R \; rI \subset I$), while a subring is only required to be closed under multiplication.
- A subring S is usually required to contain the multiplicative identity 1, while an ideal is not required to contain 1.

For example, consider the integers $\mathbb{Z}$. $\mathbb{Z}$ is a subring of the rational numbers $\mathbb{Q}$ but is not an ideal since $\frac{1}{2} \cdot 1 = \frac{1}{2}$ and $\frac{1}{2} \notin \mathbb{Z}$ (that is, $\mathbb{Z}$ does not *absorb* $\mathbb{Q}$). On the other hand, the subset $2\mathbb{Z} \subset \mathbb{Z}$, where $2\mathbb{Z} = \{2n \mid n \in Z\}$ is an ideal of $\mathbb{Z}$ but is not a subring (since $1 \notin 2\mathbb{Z}$). A few other examples:

- $\mathbb{Z}$ is an integral domain but not a field since only $\{-1, 1\} \in \mathbb{Z}$ have inverses in $\mathbb{Z}$.
- As we saw above, the integers modulo n, $\mathbb{Z}_n$, form a ring which is an integral domain if and only if n is prime.
- The $n \times n$ matrices $\mathcal{M}_n(\mathbb{R})$ with coefficients in $\mathbb{R}$ are a ring, but not an integral domain if $n \geq 2$.
- The quaternions are the smallest and perhaps the most famous example of a division ring. To see this, first take $1, i, j, k$ to be basis vectors for a 4-dimensional vector space over R, and define multiplication by

$$\begin{aligned} i^2 = j^2 = k^2 &= -1, \\ ij &= k, \\ jk &= i, \\ ki &= j, \\ ji &= -ij, \\ kj &= -jk, \\ ik &= -ki \end{aligned}$$

  Then we can define the quaternions $\mathbb{H} = \{a + bi + cj + dk, \text{ for } a, b, c, d \in R\}$. $\mathbb{H}$ forms a division ring called the quaternions [1]. To show that $\mathbb{H}$ is a division ring, we need to show that every non-zero element is invertible. To do this, consider the *conjugate* of an element $h = a + bi + cj + dk \in H$ to be $\bar{h} = a - bi - cj - dk$; note that this is analogous to the complex conjugates we saw for complex numbers in $\mathbb{C}$. It is pretty easy to see (multiply it out) that

$$q\bar{q} = a^2 + b^2 + c^2 + d^2$$

Next, take

$$q^{-1} = \frac{q}{q\bar{q}} \tag{6}$$

Then $qq^{-1} = q^{-1}q = 1$ and the denominator in Equation 6 cannot be 0 unless $a = b = c = d = 0$.

As we saw with groups, we can define a map from a ring to another which has the property of carrying one ring structure to the other.

Definition 8.7. Let R and S be rings. A map $f : R \to S$ satisfying

1. $f(a + b) = f(a) + f(b)$ (so f is a group homomorphism under $+$)
2. $f(ab) = f(a)f(b)$
3. $f(1_R) = 1_S$

for $a, b \in R$ is called *ring homomorphism*

8.2 Ideals

The concept of an ”ideal number” was introduced by the mathematician Kummer as being some special numbers (well, today we call them groups) having the property of unique factorization, even when considered over more general rings than $\mathbb{Z}$. Today's definition of *ideals* looks more like:

Definition 8.8. Let I be a subset of a ring R. Then an additive subgroup of R having the property that

$$ra \in I \text{ for } a \in I,\ r \in R$$

is called a left ideal of R. Similarly

$$ar \in I \text{ for } a \in I,\ r \in R$$

is called a right ideal of R. If an ideal is both a right and a left ideal then we call it a two-sided ideal of R, or simply an ideal of R.

We say that an ideal I of R is proper if $I \neq R$. We say that is it non-trivial if $I \neq R$ and $I \neq 0$.

I've seen several different notations for ideals including, among others: $rI = \{ri \mid r \in R, i \in I\}$ and $rI \subset I\ \forall r \in R$.

So in words: An ideal I is a subset of a ring R such that

- I is a subgroup of R under addition (so $0 \in I$ and so $I \neq \emptyset$)
- I is not only closed under multiplication but also satisfies the *stronger property* that it "absorbs" all of the elements of R under multiplication: $\forall r \in R\ rI \subset I$

In addition, if $f : R \to S$ is a ring homomorphism we define the kernel of f in the expected way, namely, $\ker f = \{r \in R \mid f(r) = 0\}$. Since a ring homomorphism is a group homomorphism, we already know that f is one-to-one iff $\ker f = \{0\}$. $\ker f$ is a proper two-sided ideal since

- $\ker f$ is an additive subgroup of R
- Take $a \in \ker f$ and $r \in R$. Then $f(ra) = f(r)f(a) = 0$ and $f(ar) = f(a)f(r) = 0$ so both ra and ar are in $\ker f$.

Quick proof: Since $\ker f$ is a two-sided ideal of R, then either $\ker f = \{0\}$ or $\ker f = R$. But $kerf \neq R$ since $f(1) = 1$ by definition. In words, $\ker f$ is a proper ideal.

It is worth noticing the analogy between rings and their two-sided ideals and groups and their normal subgroups:

- Two-sided ideals are stable when the ring acts on them by multiplication, either on the right or on the left, and so

  $$rar^{-1} \in I \text{ for } a \in I \text{ and } r \in R$$

  while normal subgroups are stable when the groups act on them on them by conjugation:

  $$ghg^{-1} \in H \text{ for } h \in H, g \in G$$

  That is $H \lhd G$.
- Groups with only trivial normal subgroups are called simple. We will not see it formally here, but rings with only trivial two-sided ideals as in the above lemma are called simple rings.

- The kernel of a group homomorphism is a normal subgroup, while the kernel of a ring homomorphism is an ideal.
- Normal subgroups allowed us to define quotient groups. We will see now that two-sided ideals will allow to define quotient rings.

8.3 Quotient rings

Let I be a proper two-sided ideal of R. Since I is an additive subgroup of R by definition, it makes sense to speak of cosets $r+I$ of I where $r \in R$. Furthermore, a ring has a structure of abelian group for addition, so I satisfies the definition of a normal subgroup. From group theory we know that of the quotient group is

$$R/I = \{r + I \text{ for } r \in R\}$$

9 Acknowledgements

Thanks to Joel Bion for pointing out a typo in an early version of these notes.

References

[1] Berthold K.P. Horn. Some Notes on Unit Quaternions and Rotation. `https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-801-machine-vision-fall-2004/readings/quaternions.pdf`, 2001. [Online; accessed 21-Feb-2019].