GROUPS, RINGS, AND IDEALS

1. Groups

1.1. **The (very) basics.** You should already be familiar with what a group is. In some sense, you've known what a (commutative) group is ever since you learned how to add! A group is simply a set with an (associative) way (think "addition") of combining two elements to get another element. We also require that this "way" has an identity element (a "zero") and has inverses ("subtraction"). I say "addition" and use the symbol $+$, but for some groups that is misleading. However, for this course, this will not be the case for the groups we're interested in.

Definition 1.1. A *group* is a set G with a map $+ : G \times G \to G$ such that

(1) There is a distinguished element $e \in G$ such that $e + g = g + e = g$ for any $g \in G$.
(2) The operation $+$ is associative. That is, $(a + b) + c = a + (b + c)$.
(3) For each element $g \in G$, there exists an element $g' \in G$ such that $g + g' = e$.

In case $g + h = h + g$ for every $g, h \in G$, then we say that G is a *commutative group* (sometimes called an *Abelian group*).

Here are some easy properties about groups:

(i) The identity element is unique.
(ii) The element guaranteed by part (3) of the definition is unique, and we will denote it by g^{-1} or sometimes $(-g)$. We call it the inverse of g.
(iii) The inverse of g satisfies $g^{-1} + g = g + g^{-1} = e$.

Example 1.2. The set of integers, $\mathbb{Z}$ form a group under addition. The element 0 is the identity element and $-a$ is the inverse of a. This is a commutative group.

Example 1.3. The set of permutations on n elements, S_n, is a group with composition as the operation. This is a (finite) non-commutative group when $n \geq 3$.

Example 1.4. The set of $m \times n$ matrices with real number entries forms a group under addition. In fact, every vector space is a (commutative) group.

Example 1.5. The set of 2×2 matrices with real entries and with non-zero determinant forms a group under multiplication. This is a non-commutative group. It is usually denoted by $GL(2, \mathbb{R})$.

Definition 1.6. Let G be a group. A subset $H \subset G$ is called a *subgroup of G* if whenever $h_1, h_2 \in H$ then $h_1 + h_2 \in H$ and $h_1^{-1} \in H$.

Here is an easy fact:

Lemma 1.7. *A subgroup H of a group G is a group itself.*

Example 1.8. The set of all even numbers is a subgroup of $\mathbb{Z}$. The set of multiples of a given number m is a subgroup of $\mathbb{Z}$. We often refer to this subgroup as $m\mathbb{Z}$.

Example 1.9. The set of all 2×2 matrices with determinant 1 form a subgroup of the set of all invertible matrices.

1.2. **Homomorphisms.** Given two sets, we may talk about functions between them. Given two groups, we study the functions between them. Informally, we only care about those functions which "remember" the fact that both the source and the target of the function have some extra structure - that is, they are both groups.

Definition 1.10. Let G_1 and G_2 be groups. A function $f : G_1 \to G_2$ is called a *homomorphism* (or sometimes *group homomophism*) if for each $g, h \in G_1$, we have $f(g_1 + g_2) = f(g_1) + f(g_2)$.

Remark 1.11. Notice that the $+$ on the left hand side of the equation means something different from the $+$ on the right hand side of the equation!

Lemma 1.12. *If $f : G_1 \to G_2$ is a group homomorphism, then f sends the identity element of G_1 to the identity element of G_2.*

Proof. Let e be the identity element of G_1. Then for any $g \in G_1$, we have $f(e+g) = f(e) + f(g)$. But because $e + g = g$, we see that $f(e + g) = f(g)$. Combining these we see that $f(g) = f(g) + f(e)$. Now add $f(g)^{-1}$ to both sides. □

Similarly we can prove the following Lemma.

Lemma 1.13. *Let $f : G_1 \to G_2$ be a group homomorphism, then $f(g^{-1}) = (f(g))^{-1}$.*

Example 1.14. Taking the determinant gives a group homomorphism from $GL(2, \mathbb{R})$ to the set $\mathbb{R}^* = \{r \in \mathbb{R} | r \neq 0\}$. This latter set is a group with multiplication as the operation.

Example 1.15. If H is as subgroup of G, then the map $H \to G$ which sends an element of H to the same element but considered inside of G is a group homomorphism. Sometimes we call this the inclusion (for obvious reasons).

Example 1.16. The map from $G \to G$ which sends each element $g \in G$ to itself is called the identity homomorphism.

Example 1.17. Fix a group G and an element $g \in G$. The map $L_g : G \to G$ which sends x to $g + x$ is NOT a group homomorphism unless $g = e$.

The following lemma is very easy.

Lemma 1.18. *If $f_1 : G \to H$ and $f_2 : H \to J$ are group homomorphisms, then $f_2 \circ f_1$ is a group homomorphism from G to J.*

Definition 1.19. Two groups G_1 and G_2 are isomorphic if there are group homomorphisms $f_1 : G_1 \to G_2$ and $f_2 : G_2 \to G_1$ such that $f_1 \circ f_2$ and $f_2 \circ f_1$ are both the identity homomorphism.

Definition 1.20. A group homomorphism $f : G_1 \to G_2$ is called *injective* if $f(a) = f(b)$ implies that $a = b$. The homomorphism f is called *surjective* if for every $y \in G_2$, there is an $x \in G_1$ such that $f(x) = y$.

Lemma 1.21. *A group homomorphism $f : G_1 \to G_2$ is injective if and only if $f(x) = e$ (here e denotes the identity in G_2) implies that x is the identity in G_1.*

Proof. The "only if" part is clear. Suppose then that the second condition holds and $f(a) = f(b)$. Using the properties of a group homomorphism shown above, this means that $f(a + b^{-1}) = e$. By the condition then $a + b^{-1}$ is the identity in G_1; in other words, $a = b$. □

The following lemma is now pretty easy. You just have to define the "reverse" map and show it is a group homomorphism.

Lemma 1.22. *A group homomorphism $f : G \to H$ is an isomorphism if and only if f is both injective and surjective.*

Definition 1.23. Let $f : G_1 \to G_2$ be a group homomorphism. We define the *kernel* of f to be the set of elements $x \in G_1$ such that $f(x)$ is the identity in G_2. We define the *image* of f to be the set of elements $y \in G_2$ such that there is some $x \in G_1$ with $f(x) = y$. We denote these $Ker(f)$ and $Im(f)$ respectively.

The following Lemma is now an unwinding of all the definitions and basic properties.

Lemma 1.24. *Let $f : G_1 \to G_2$ be a group homomorphism. Then $Ker(f)$ is a subgroup of G_1 and $Im(f)$ is a subgroup of G_2; in particular, both are groups.*

Example 1.25. The determinant map from $GL(2, \mathbb{R})$ to $\mathbb{R}^*$ has kernel the set of two by two matrices with determinant one. These form a group, as already mentioned.

1.3. **Cosets and Quotient Groups.** The general mantra of this section is: it can be useful to consider two elements of a group as "the same" if they differ by a subgroup. For example, if we are only concerned whether a number is odd or even, then we consider any two numbers (elements of $\mathbb{Z}$) the same if they differ by an element of the subgroup $2\mathbb{Z}$.

Definition 1.26. Let G be a group and H a subgroup. Then given $g \in G$, the (left) *coset* $g + H$ is $\{g + h | h \in H\}$.

This is no longer a subgroup of G usually, but we think of it as H haven been "translated" inside G. There is also a notion of right coset but we will not have need to distinguish in this course. The set of all cosets partition G in the following sense.

Lemma 1.27. *Two cosets are either disjoint or equal.*

Proof. Suppose $g + H$ and $g' + H$ are not disjoint. Then there are elements $h, h' \in H$ such that $g + h = g' + h'$. This implies $g = g' + h' - h$. Now let $g + h'' \in g + H$. Then this element is also equal to $g' + h - h' + h''$ and is an element of $g' + H$. The same argument shows every element of $g' + H$ is contained in $g + H$ and so the two are equal. □

We would like to turn the set of cosets $(g + H)$ for each $g \in G$ into a group. How would we do this? Well we would like to say that $(g + H) + (g' + H)$ is the coset $g + g' + H$. That seems natural enough - but it doesn't always work! The problem is that what if $g + H = g'' + H$. We saw in the proof above that this happens if (and only if) $g - g'' \in H$. Well then we would certainly need to have $(g+H)+(g'+H) = (g''+H)+(g'+H)$. This would mean $g+g'+H = g''+g'+H$. This would mean $g + g' - g'' - g'$ would have to be in H! But from what we have assumed, it isn't obvious (and it's not always true) that this holds.

Definition 1.28. A subgroup N of G is called *normal* if for every $g \in G$, we have $g + N = N + g$ or equivalently $g + N + g^{-1} = N$ (as sets).

This is exactly the condition we need to fix the problem above.

Proposition 1.29. *Given a normal subgroup N of a group G, the set of cosets of N do form a group under the above rule.*

Proof. With the notation from before, we must show that if $g + H = g'' + N$ then $(g + g') + N = (g'' + g') + N$. The set $g + g' + N$ is equal to $g + N + g'$ because N is normal. This set in turn is equal to $g'' + N + g'$ which is equal to $g'' + g' + N$ again by normality. This shows that the operation is well-defined. Proving that it's a group now is easy. □

Definition 1.30. If N is a normal subgroup of G, we call the group of left cosets the *quotient group* of G by N and write it G/N.

To emphasize: two elements of the quotient group $a + N$ and $b + N$ and are equal if and only if a and b differ by an element of N.

Here are some basic facts about normal subgroups and quotient groups. I won't go through the proofs.

Theorem 1.31.
1. *Every subgroup of a commutative group is normal. If G is commutative and N is a subgroup, then G/N is also commutative. This will be key for us.*
2. *If N is normal in G, there is a group homomorphism $p : G \to G/N$. This map sends g to $g + N$ and is often called the quotient homomorphism. The kernel of this homomorphism is exactly N.*
3. *Conversely (to the point above), the kernel of any group homomorphism $f : G \to G'$ is a normal subgroup. The image of f is isomorphic to $G/Ker(f)$. This shows us that the normal subgroups of a given group G in some sense "control" how G maps to other groups.*

This brings us to the most important example of this course.

Example 1.32. Let G be the group of integers $\mathbb{Z}$ and N be the normal subgroup $n\mathbb{Z}$ (remember, every subgroup of a commutative group is normal). Then the quotient group is $\mathbb{Z}/n\mathbb{Z}$, and we often say that this is "the group of integers modulo/mod n". There is a homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$. It sends an integer to that integer mod n.

For concreteness, suppose that $n = 5$. Then the elements of $\mathbb{Z}/5\mathbb{Z}$ are $0 + \mathbb{Z}, 1 + \mathbb{Z}, 2 + \mathbb{Z}, 3 + \mathbb{Z}, 4 + \mathbb{Z}$. After a while, we won't write this all out and just refer to the elements as $0, 1, 2, 3, 4$. Then we say that, for example, $3+4 \equiv 2$ (or sometimes $3 + 4 \equiv 2(mod5)$ to emphasize that we're working in the quotient group) because $3+\mathbb{Z}+4\mathbb{Z} = 7+\mathbb{Z} = 2+\mathbb{Z}$. If $p : \mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ is the quotient map, then $p(a) = p(b)$ if and only if a and b differ by a multiple of 5, or what amounts to the same thing, that 5 divides $a - b$. Again, we denote this by $a \equiv b(mod5)$.

2. Rings

Informally, a ring is a set with two operations - addition and multiplication - which interact in the "usual" ways.

Definition 2.1. A set R is called a *ring* if there are two maps $+ : R \times R \to R$ and $\cdot : R \times R \to R$ such that

(1) R is a commutative group with the operation $+$.
(2) The operation $\cdot$ is associative.
(3) There is an element, 1, which is the identity for multiplication. That is, $1 \cdot r = r \cdot 1 = r$ for each $r \in R$.
(4) The distributive law holds; that is $r \cdot (x + y) = r \cdot x + r \cdot y$ and $(x + y) \cdot r = x \cdot r + y \cdot r$.

If in addition, we have $r \cdot s = s \cdot r$ for each $r, s \in R$, then R is called a *commutative ring*. We will now refer to the identity for $+$ in a ring as 0, instead of e. We will refer to the additive inverse for $r \in R$ as $-r$.

Here are a couple easy properties.

Lemma 2.2. *The multiplicative identity is unique. We have the formula* $0 \cdot r = r \cdot 0 = 0$ *for each* $r \in R$. *We also have* $-1 \cdot r = -r$.

Proof. Suppose that $1'$ was another identity. Then $1' = 1 \cdot 1' = 1$. For the second, we have $0 \cdot r + r = 0 \cdot r + 1 \cdot r = (0+1) \cdot r = 1 \cdot r = r$. Adding $-r$ to both sides proves the formula. For the third, we have $-1 \cdot r + r = -1 \cdot r + 1 \cdot r = (-1+1) \cdot r = 0 \cdot r = 0$ by the second formula. This shows that $-1 \cdot r = -r$. □

Example 2.3. The integers $\mathbb{Z}$ form a ring. So do the rational numbers, $\mathbb{Q}$, the real numbers, $\mathbb{R}$, and the complex number, $\mathbb{C}$.

Example 2.4. The groups we talked about in the previous section $\mathbb{Z}/n\mathbb{Z}$ also form a ring. Here, as with addition, we use "multiplication mod n".

Example 2.5. The set of polynomials in one variable with complex coefficients form a ring, $\mathbb{C}[x]$.

Example 2.6. Not every ring is commutative. Consider the set of all 2×2 matrices with usual addition and multiplication.

Example 2.7. Let $\mathbb{Z}[i] = \{a+bi|a, b \in \mathbb{Z}\}$. Here $i^2 = -1$. This is a ring, called the ring of Gaussian integers. Similarly we have rings like $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2}|a, b \in \mathbb{Z}\}$.

Notice that an element of a ring need not have an inverse for the operation of multiplication!

There is a notion of a subring of a ring just like of a subgroup of a group. Instead we'll be interested in what are called ideals, which we'll talk about in the next section.

There is also the notion of a ring homomorphism.

Definition 2.8. A map between rings $f : R \to S$ is a ring homomorphism if $f(1) = 1$, $f(x+y) = f(x) + f(y)$, and $f(x \cdot y) = f(x) \cdot f(y)$.

Again the $+$ and $\cdot$ on the left hand side of the equations can be different than their counterparts on the right hand side of the equation. Notice that a ring homomorphism is also a group homomorphism when we forget about the extra structure of $\cdot$.

Example 2.9. When is there a ring homomorphism $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$? (In fact we'll also answer when there is a group homomorphism between these two groups).

Well, since we must have $f(1) = 1$, we must also have $f(1) + \ldots + f(1) = 0$ (sum taken n times). This implies that m divides n. Think about why this has to be true.

This shows that, for example, there is no ring (or group) homomorphism from $\mathbb{Z}/3\mathbb{Z}$ to $\mathbb{Z}/5\mathbb{Z}$ or to $\mathbb{Z}/6\mathbb{Z}$. But there is one from $\mathbb{Z}/6\mathbb{Z}$ to $\mathbb{Z}/3\mathbb{Z}$.

We can define injective, surjective, isomorphism, kernel, and image just as in the case of groups. We must warn you though, the kernel of a ring homomorphism will not usually be a ring! This is because 1 will not map to 0.

3. Ideals

In the setting of groups, we had normal subgroups which allowed us to define quotient groups. In the setting of rings, the analogues are called ideals. Ideals are important in both algebra and number theory. After defining them we will finally directly address some number theory!

Definition 3.1. A subset $I \subset R$ of a ring is called an *ideal* if $0 \in I$ and for every $a, b \in I$ and $r, s \in R$ we have $r \cdot a + s \cdot b \in I$ also.

Here are some easy to prove properties:

Lemma 3.2. *(1) An ideal I is a subgroup of R with respect to addition.*
(2) If $r \in R$ and $i \in I$ then $r \cdot i \in I$.
(3) If $r_1, \ldots, r_k \in R$ and $i_1, \ldots, i_k \in I$ then $r_1 \cdot i_1 + \ldots + r_k \cdot i_k \in I$.

Proof. (1) If $a, b \in I$ we must show that $a + b \in I$. This follows from the definition by taking $r = s = 1$. If $a \in I$ we must also show that $-a \in I$. This follows by taking $r = -1$ and $b = s = 0$ in the definition.
(2) This follows by taking $a = i$, $b = 0$, $r = 1$ and $s = 0$ in the definition of an ideal.

(3) Part (2) is the case $k = 1$. This fact then can easily be proven by induction on k. I.e., assume it's true for $k - 1$, then $r_1 \cdot i_1 + \ldots + r_{k-1} \cdot i_{k-1} \in I$ and $r_k \cdot i_k \in I$ by part (2) again. So then by the definition of an ideal, $r_1 \cdot i_1 + \ldots + r_k \cdot i_k \in I$ also.

□

Example 3.3. If R is any ring, and $a \in R$. Then the set $(a) = \{r \cdot a | r \in R\}$ is an ideal of R. Think about this, it's not hard!

Definition 3.4. An ideal $I \subset R$ is called *principal* if it is of the form (a) for some $a \in R$.

Example 3.5. The set of all multiples of 7 in $\mathbb{Z}$ is a principal ideal. Of course, this works for any integer n.

Example 3.6. Not every ideal is principal. Here is an example. Let R be the ring of polynomials with complex coefficients in two variables, x and y. We write $R = \mathbb{C}[x, y]$. Then the ideal $I = \{p(x, y) \in R | p(0, 0) = 0\}$ is a non-principal ideal. Think about why!

Finally we come to the first main application of all this theory to the study of integers.

Theorem 3.7. *Every ideal of $\mathbb{Z}$ is principal.*

Proof. If $I = (0)$, we are finished. So assume that I contains positive integers. Let a be the smallest integer in I. Then by the ideal properties, we have $(a) \subset I$. So we just need to show $I \subset (a)$. Suppose $b \in I$ is a positive number. Since $a < b$, by the division algorithm, we can write $b = n \cdot a + r$ with $0 \leq r < a$. But then $r = b - n \cdot a$ would be in I. Since a is the smallest positive integer in I, we must have $r = 0$, and so b is a multiple of a. If $b \in I$ is negative, then $-b$ is also in I and is positive, and by the above argument, also a multiple of a. This shows that $I \subset (a)$. □

There are at least two applications of this fact. The first is a combination of Theorem 1.3 and 1.4 in our book.

Theorem 3.8. *Suppose that $a, b \in \mathbb{Z}$ are two integers. Then there is an integer d such that $d|a$ and $d|b$ which satisfies the following property. Further, $e|a$ and $e|b$ if and only if $e|d$. This integer d may be expressed as $m \cdot a + n \cdot b$ for some integers m, n. We call d the greatest common divisor of a and b.*

Proof. Consider the set $I = \{m \cdot a + n \cdot b | m, n \in \mathbb{Z}\}$. This is an ideal in $\mathbb{Z}$, which is easy to check. Then $I = (d)$ for some integer d by the previous theorem. Since $a \in I$, we must have that a is a multiple of d; in other words, $d|a$. Similarly for b. By definition we can write $d = m \cdot a + n \cdot b$ for some $m, n \in \mathbb{Z}$. Suppose that $e|a$ and $e|b$. Then $e|m \cdot a + n \cdot b$ so e divides d also. If $e|d$ then e divides any multiple of d, so in particular a and b. □

The second application is Theorem 1.15 in our book.

Theorem 3.9. *Suppose that p is a prime number and $p|ab$. Then $p|a$ or $p|b$.*

Proof. Consider the set $I = \{m \cdot a + n \cdot b | m, n \in \mathbb{Z}\}$. This is an ideal, so we may write $I = (c)$ with c positive. Now, p must be a multiple of c, so either $c = 1$ or $c = p$. If $c = 1$, then we may write $1 = ma + np$ for some integers, and so $b = mab + npb$. Since p divides the right hand side it must also divide the left hand side, b. If $c = p$, then because a is a multiple of c have that p divides a. □

Now just as promised, let's just remember that we can take quotients of rings by ideals just like we could with groups by normal subgroups.

Theorem 3.10. *Suppose that R is a ring and $I \subset R$ is an ideal. Then there is a quotient ring R/I, and a surjective ring homomorphism $R \to R/I$. The kernel of this map is exactly I. If R is commutative, so is R/I.*

Proof. Actually we have already almost proved this when we talked about groups. Since I is a normal subgroup of R with respect to $+$ (every ideal in a ring is a normal subgroup because rings are required to be commutative groups with respect to $+$), then the quotient group R/I makes sense. We simply must make sure multiplication makes sense on the set of cosets, R/I.

Let $a, b \in R$. We define $(a + I) \cdot (b + I)$ to be $a \cdot b + I$. Now, does this make sense? Suppose that $a + I = c + I$ as cosets. This means $a - c \in I$ as before. We better have that $a \cdot b + I = c \cdot b + I$. Well, $a \cdot b - c \cdot b = (a - c) \cdot b$ which is indeed in I. So our definition makes sense. The rest of verifying that R/I is a ring is pretty easy. So is verifying that $R \to R/I$ the group homomorphism projection is a ring homomorphism. It is clear that if R is commutative then so is R/I. □

Example 3.11. Our main example, is again, $I = (n) \subset \mathbb{Z}$. Then $\mathbb{Z}/I$ is the ring that we already discussed, $\mathbb{Z}/n\mathbb{Z}$.