BASIC NOTIONS FROM RING THEORY

LEO GOLDMAKHER

ABSTRACT. A brief overview of the basic concepts from ring theory.

1. RINGS

The most important concept in ring theory, unsurprisingly, is that of a ring.

Definition (tl;dr)**.** *A (commutative)* ***ring*** *is like a field, except without requiring the existence of multiplicative inverses.*

Definition (Formal definition)**.** *A* ***ring*** *is a set R, endowed with two binary operations $+$ and $\times$, such that*

(1) *R is an abelian group under $+$, with identity denoted 0 and additive inverse of x denoted $-x$;*
(2) *R under $\times$ satisfies closure and associativity, and possesses an identity (denoted 1); and*
(3) *the two operations satisfy the distributive property: for any $x, y, z \in R$ we have*

$$x(y+z) = xy + xz \qquad \text{and} \qquad (x+y)z = xz + yz.$$

In Galois theory, we will be dealing exclusively with a particularly nice type of ring:

Definition. *A* ***commutative ring*** *is a ring in which multiplication is commutative.*

Example 1.1. $\mathbb{Z}$ is a classical example of a commutative ring.

Example 1.2. For any field K, the set $K[t]$ of polynomials with coefficients in K is a commutative ring. (The strong similarities between $\mathbb{Z}$ and $K[t]$ we discussed in class are the reason the concept of ring was invented in the first place.)

Example 1.3. The set $\mathbb{Z}_6 := \{[0], [1], [2], [3], [4], [5]\}$ under addition and multiplication (mod 6) is a commutative ring.

By definition, not every element of a ring is invertible under multiplication. Those elements which *are* are quite special; for example, the only invertible elements of $\mathbb{Z}$ are ± 1. For this reason, invertible elements are called *units*. Formally:

Definition. *Given a ring R, we say $x \in R$ is a* ***unit*** *if and only if there exists $y \in R$ such that $xy = yx = 1$. The collection of all units of R is denoted $R^\times$.*

Example 1.4. $\mathbb{Z}^\times = \{\pm 1\}$.

Example 1.5. For any field K, $K[t]^\times = K \setminus \{0\}$.

Example 1.6. $\mathbb{Z}_6^\times = \{[1], [5]\}$.

Note that $R^\times$ gains multiplicative structure over R, but this comes at a cost: $R^\times$ loses the additive structure of R.

2. SUBRINGS

Inspired by our experience with groups, we know that once one defines an object, it's useful to define the notion of a sub-object.

Definition. *A subset S of a ring R is a **subring** iff S is a ring under the same operations as R and the multiplicative identity of S is the same as that of R.*

Example 2.1. $\mathbb{Z}$ is a subring of $\mathbb{Q}$.

Example 2.2. $2\mathbb{Z}$ is **not** a subring of $\mathbb{Z}$.

The last example is very important. Even though $2\mathbb{Z}$ isn't a subring of $\mathbb{Z}$, it's still rather well-structured: it exhibits almost all the properties of a ring. However $2\mathbb{Z}$ has another trick up its sleeve: the quotient set $\mathbb{Z}/2\mathbb{Z}$ is itself a ring. This property is so nice that we call such subsets *ideal*. We explore ideal subsets in the next section.

3. IDEALS

Definition. *Given a ring R and a normal subgroup $I \trianglelefteq R$, we say I is an **ideal** subset iff the group R/I forms a ring under the multiplication inherited from R.*

In practice, people generally say *ideal* rather than *ideal subset*. Life's too short.

Let's unpack the notion of ideal a bit more. Given $I \trianglelefteq R$, we can form the quotient group

$$R/I = \{[x] : x \in R\}$$

where $[x]$ consists of all elements of R which are congruent to x mod I. More formally,

$$[x] := \{r \in R : r - x \in I\}.$$

(This is sometimes expressed in the form $[x] = x + I$.) In particular, recall that any given element of R/I is actually a *subset* of R, and that we have a well-defined operation on how to add two of these subsets:

$$[x] + [y] := [x + y].$$

If we want R/I to be a ring, we also need to be able to multiply. The most natural definition is

$$[x][y] := [xy].$$

As was the case with quotient groups, this operation might not be well-defined. To better appreciate this point, we consider the following non-example.

Example 3.1 (Non-example)**.** Consider the ring $K[t]$. Inside this ring lives a very nice subgroup: the field K. So we can form a quotient group

$$K[t]/K := \{[f(t)] : f \in K[t]\}$$

where $[f] = [g]$ iff $f - g \in K$, or in other words iff f and g differ by a constant. Note that $K[t]/K$ is group, since $K \trianglelefteq K[t]$ (why?). It also seems like a perfectly decent ring, with $[0]$ as the additive identity and $[1]$ as the multiplicative identity. But there's a problem: $[t] = [t + 1]$, whence $[t^2] = [t][t] = [t][t + 1] = [t^2 + t]$. But this implies $[t] = [0]$, which is false since t isn't a constant. Thus, we see that trying to define multiplication naively as $[a][b] := [ab]$ doesn't work. In other words, **the inherited multiplication operation isn't well-defined** in this example.

Example 3.2. $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Playing around a bit with the non-example above, one is quickly led to discover the following:

Proposition 3.1. *A subset I of a ring R is **ideal** iff*

(1) *viewed as sets under $+$, we have $I \trianglelefteq R$ and*
(2) *both RI and IR are subsets of I.*

Remark. This proposition is usually given as the definition of an ideal. However, it's somewhat technical, and obscures the reason we actually care about ideals!

The second condition means that for any $x \in I$, all multiples of x live in I as well; this property is often colloquially described as I 'swallowing' multiplication.

Example 3.3. Given a field K, pick any $f \in K[t]$. Then the set $fK[t]$ (consisting of all multiples of f) is an ideal of $K[t]$. This ideal is usually denoted (f) or $\langle f \rangle$.

Example 3.4. Given a field K, pick any $\alpha \in K$. The set of all $f \in K[t]$ such that $f(\alpha) = 0$ forms an ideal of $K[t]$.

In examples 3.2 and 3.3 we formed an ideal by starting with a single element of the ring and then generating all multiples of it. More generally, any ideal generated by a single element is called a **principal** ideal; a principal ideal generated by x is denoted (x). In the context of a commutative ring R, we can describe (x) explicitly as

$$(x) := xR.$$

(Why can't we describe a principal ideal this way in a noncommutative ring R?) We can similarly form ideals generated by two elements $x, y \in R$; again assuming R is commutative, such an ideal can be expressed

$$(x, y) := xR + yR.$$

As I pointed out above, the reason we care about ideals is the same reason we care about normal subgroups: when we form the quotient of a ring by an ideal, we get a ring. However, there's a crucial difference between the group setting and the ring setting – ideals aren't necessarily subrings, as the example of $2\mathbb{Z}$ shows. Nonetheless, there are various parallels between normal subgroups and ideals. An important example of this is the first isomorphism theorem, which (in the group setting) characterizes normal subgroups as the kernels of group homomorphisms. Similarly, ideals are characterized by being the kernel of some ring homomorphism. To discuss this meaningfully, we first need to define the notion of a ring homomorphism.

4. Ring homomorphisms and the 1st isomorphism theorem

Definition. *Given two rings R and S, we say a map $\varphi : R \to S$ is a **ring homomorphism** iff addition and multiplication are preserved under φ* and $\varphi(1) = 1$.

Note in particular that we require the multiplicative identity to be mapped to the multiplicative identity. Problem **3.1** will demonstrate why this hypothesis is desirable.

Next we recall two important notions connected to homomorphisms: the **image** of a ring homomorphism $\varphi : R \to S$ is defined

$$\text{im } \varphi := \{\varphi(x) : x \in R\}$$

and the *kernel* of φ is defined

$$\ker \varphi := \{x \in R : \varphi(x) = 0\}.$$

It is straightforward to verify that $\ker\varphi$ is always an ideal of R. Less obvious is that the converse holds: any ideal is the kernel of some ring homomorphism. We will return to this point. First, we prove a fundamental result about ring homomorphisms:

Theorem 4.1 (First Isomorphism Theorem)**.** *Given any two rings R and S and a ring homomorphism $\varphi : R \to S$, we have*

- $\operatorname{im}\varphi$ *is a subring of* S
- $\ker\varphi$ *is an ideal of* R
- $R/\ker\varphi \simeq \operatorname{im}\varphi$

The first two claims are straightforward exercises (which you should do!), which leaves us with

Claim. $R/\ker\varphi \simeq \operatorname{im}\varphi$.

Proof. We started by drawing a diagram of all the rings we're dealing with, and the connections between them.

$$\begin{array}{ccc} R & \xrightarrow{\ \varphi\ } & \operatorname{im}\varphi \leq S \\ {\scriptstyle\pi}\downarrow & \nearrow_{\Delta} & \\ R/\ker\varphi & & \end{array} \tag{1}$$

The function $\pi : R \to R/\ker\varphi$ is the natural projection map defined by $\pi(x) = [x]$. Note that φ maps R surjectively onto $\operatorname{im}\varphi$, and π maps R surjectively onto $R/\ker\varphi$. The dotted line is the isomorphism we wish to find between $R/\ker\varphi$ and $\operatorname{im}\varphi$. Actually, it's not obvious how to find any such map, isomorphism or otherwise. To do so, we need to specify where to send a typical element $[x] \in R/\ker\varphi$; all we know is it has to end up somewhere in $\operatorname{im}\varphi$. Staring at the diagram above, we come up with the following guess:

$$\begin{aligned} \Delta : R/\ker\varphi &\longrightarrow \operatorname{im}\varphi \\ [x] &\longmapsto \varphi(x) \end{aligned}$$

Right away we should be suspicious of this definition: $[x]$ is a set, whereas $\varphi(x)$ is a function of the single element x. Why is this a problem? Suppose $a \in [x]$. Then $[a] = [x]$. So how do we define $\Delta([x])$ – as $\varphi(x)$ or as $\varphi(a)$? In other words, is Δ well-defined?

Turns out it is! Let's see why this is. First, recall that $[x] = x + \ker\varphi$. Applying the homomorphism φ to the set (i.e. to each element of the set), we find that

$$\varphi([x]) = \varphi(x + \ker\varphi) = \varphi(x) + \varphi(\ker\varphi) = \{\varphi(x)\}.$$

Note that $\varphi([x])$ is a set, since we are applying a function to a set; the above calculation shows that this set has only one element in it! It follows that

$$\begin{aligned} [x] = [y] &\implies \varphi([x]) = \varphi([y]) \\ &\implies \{\varphi(x)\} = \{\varphi(y)\} \\ &\implies \varphi(x) = \varphi(y) \\ &\implies \Delta([x]) = \Delta([y]) \end{aligned}$$

Thus Δ is well-defined after all.

Great, so we've come up with a function from $R/\ker\varphi$ to $\operatorname{im}\varphi$. But this wasn't actually our goal: what we're really after is an isomorphism between these two. Is Δ an isomorphism? It's easily verified that it is. (Do this.) We've proved the theorem! $\square$

The diagram (1) is helpful for visualizing (and coming up with!) the proof. It's called a *commutative diagram*, because you can get from R to im φ in two different ways – directly by applying φ, or indirectly by first applying π and then applying Δ – and each way gives the same result. In other words: $\varphi = \Delta \circ \pi$. In fact, our whole proof boils down to finding a function Δ which makes this hold (i.e. which makes the diagram commute.)

The above proof is yet another illustration of a general principle we've run across in class: the most natural map between two isomorphic rings (or groups, or...) usually turns out to be an isomorphism. So if you're ever trying to prove that two rings are isomorphic, just construct any map you can from one to the other. Chances are, it will be an isomorphism.

Exercise 1. Prove that any ideal of a ring R is the kernel of some homomorphism out of R.

5. Maximal and prime ideals

In this final section we discuss two types of ideals which are particularly nice: maximal ideals and prime ideals.

5.1. **Maximal ideals.** If you don't remember the definition of a maximal ideal, that's OK – just take a moment and come up with a notion for which the name would make sense. Chances are, you've come up with the correct definition! Here's the formal version:

Definition. *An ideal I of a ring R is **maximal** iff the only ideal containing I is R itself.*

Colloquially, this says that a maximal ideal is as large as possible.

Example 5.1. If $f \in K[t]$ is irreducible, then the ideal generated by f is maximal. To see this, pick any ideal I containing (f), so that we have

$$(f) \subseteq I \subseteq K[t].$$

What can we say about I? Recall from class that any ideal generated by two polynomials is also generated by their greatest common divisor. More generally, it is a straightforward consequence of the division-with-remainder theorem that *any* ideal of $K[t]$ must be generated by a single polynomial. In other words, we see that I must be principal; say $I = (g)$. Since $f \in I$, we deduce that $f = gh$. But f is irreducible, whence one of g or h must be a unit in $K[t]$. Either way, we have $I = (f)$ or $I = K[t]$, which proves that (f) is maximal.

In addition to being awesomely large, maximal ideals have another very nice property:

Proposition 5.1. *If M is a maximal ideal of a commutative ring R, then R/M is a field.*

Proof. Given $[f] \neq [0]$ in R/M, it suffices to show that $[f]$ is invertible. By definition, $[f] \neq [0]$ means that $f \notin M$, whence the ideal generated by f and M must be the entire ring R. In particular, 1 is a linear combination of f and some element of M. It follows that there exists $g \in R$ such that $[f][g] = [1]$. □

Example 5.2. We deduce that if $f \in K[t]$ is irreducible, then $K[t]/(f)$ must be a field. In fact, as we saw in Kronecker's theorem, $K[t]/(f)$ is a field extension of K containing a root of f.

5.2. **Prime ideals.** In $\mathbb{Z}$, we usually think of a prime as a number which does not factor as the product of two integers of smaller magnitude:

$$p = ab \qquad \Longrightarrow \qquad |p| = |a| \quad \text{or} \quad |p| = |b|.$$

However, there is an equivalent characterization of primes, which is the one used to prove the Fundamental Theorem of Arithmetic:

$$p \mid ab \qquad \Longrightarrow \qquad p \mid a \quad \text{or} \quad p \mid b.$$

Although both of these characterizations are familiar and seem obvious, the proof that they are equivalent is not so easy, and with good reason: these two statements are not equivalent in a general ring! Elements which enjoy an analogue of the first assertion are called *irreducible*; those satisfying an analogue of the second are called *prime*. Here's the formal definition:

Definition. *An ideal I is **prime** iff $ab \in I$ implies that either $a \in I$ or $b \in I$.*

Example 5.3. It's not hard to show that any ideal of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some n. Observe that $n\mathbb{Z}$ is a prime ideal iff n is prime.

Unpacking definitions shows that any maximal ideal must be prime. What about the converse?

Proposition 5.2. *In the polynomial ring $K[t]$, an ideal is maximal if and only if it is prime.*

Proof. Let P be a prime ideal of $K[t]$, and pick any ideal I containing P. In other words,

$$P \subseteq I \subseteq K[t].$$

As we know from above, every ideal in $K[t]$ is principal, so we can write

$$P = (f) \qquad\qquad I = (g).$$

$P \subseteq I$ immediately implies $f = gh$ for some $h \in K[t]$. But this means that $gh \in P$, and since P is prime, one of g or h must live in P. We analyze these cases individually.

- If $g \in P$, then $I = P$.

- If $h \in P = (f)$, then $f \mid h$. On the other hand, $f = gh$, whence $h \mid f$. These two divisibility conditions together imply $h = \alpha f$ for some unit $\alpha \in K^\times$, which in turn yields $g = \alpha^{-1} \in K^\times$. We conclude that $I = (g) = K[t]$.

We've therefore shown that any ideal containing P must either be P or the entire ring $K[t]$. In other words, P is maximal. □

Needless to say, there's a lot more to be said about ring theory! But the results described above will tide us over for this semester.

DEPT OF MATHEMATICS & STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA, USA
E-mail address: leo.goldmakher@williams.edu