More ring theory

Mendel Keller

November 14, 2017

1 Ring homomorphism

A ring homomorphism is a function $f : A \to B$ from one ring to another, satisfying the three properties: (1) $f(a+b) = f(a) + f(b)$, and (2) $f(ab) = f(a)f(b)$ i.e. the function is compatible with the ring operations. Some immediate consequences are that $f(1) = 1$ and $f(0) = 0$ i.e. f takes the identities in A to identities in B (we do not consider the possibility that f takes everything in A to 0 in B, even though this satisfies the above properties, sometimes people state this condition explicitly in the definition of homomorphism). Similarly, f takes inverses to inverses, because $0 = f(0) = f(a + (-a)) = f(a) + f(-a)$ so that $-f(a) = f(-a)$. These are the sort of properties that make homomorphisms easy to work with.

The *kernel* of a homomorphism $Ker(f)$ is the set of elements in A which map to 0 in B. The kernel is an ideal, because $f(a) = 0$ and $f(b) = 0$ gives that $f(a + b) = f(a) + f(b) = 0 + 0 = 0$, similarly $f(a) = 0$ gives that $f(ra) = f(r)f(a) = f(r) * 0 = 0$. This explains why we would bother caring about an ideal in the first place.

An example of a ring homomorphism is $f : \mathbb{Z} \to \mathbb{Q}$ gives by $f(x) = x$, here the kernel is just the zero ideal. This example may not seem very interesting, and we will introduce more complicated examples once we've introduced some more ring constructions.

2 Special ideals

There are in general two special types of ideals, that we can consider: prime ideals and maximal ideals. A prime ideal is an ideal I satisfying that if a product is in it $xy \in I$ then at least one of $x \in I$ or $y \in I$ (this is somewhat similar to prime numbers, where if a prime number divides a product, it must divide one of the factors, in fact prime numbers generate prime ideals, for exactly this reason). A maximal ideal is an ideal that isn't the unit ideal i.e. doesn't contain all of the ring, but there are no other ideals between it and the whole ring. For example, the zero ideal is maximal in a field, because the only ideal containing it is the whole ring. A non-example is the ideal (4) in $\mathbb{Z}$, since it is contained in the ideal (2).

Theorem 1. *Every maximal ideal is prime.*

Proof. Given a maximal ideal I, if we had $xy \in I$ and $x \in I$, we can show that $y \in I$. Since if we take I and add x to it along with everything that adding x forces us to add, we can write this as $I + (x) = \{a + b : a \in I, b \in (x)\}$ (see section 6), we have that this must equal the whole ring, since it is an ideal containing I, in particular, it contains 1, so that we get an equation $i + xz = 1$ where $i \in I$ and z is anything in the ring. We can then multiply this equation by y to get $iy + xyz = y$. But since $i \in I$ we have that $iy \in I$, and since $xy \in I$ we also have $(xy)z \in I$, so that $iy + xyz = y \in I$, so that I is in fact prime. ■

The other inclusion doesn't hold however, consider the zero ideal in $\mathbb{Z}$, consisting of just 0, clearly if a product of integers is 0, one of the factors is 0, so that it is prime. It is not maximal however, as it is contained in the ideal (2).

3 Quotient rings

Given an ideal I, we can define a new ring A/I (we call this A mod I), one way to understand this is that we set everything in the ideal I equal to zero. This gives that $a = b + i$ for $a, b \in A$ and $i \in I$, notice how the properties of an ideal make this quotient construction sensible. The ideals of a quotient ring $J \subset A/I$ correspond exactly to the ideals J in A that contain I.

A good set of examples can be given by $\mathbb{Z}/(n)$ for an integer n. for example $\mathbb{Z}/(4) = \{0, 1, 2, 3\}$ with addition and multiplication being mod 4, this ring contains a ideal $\{0, 2\}$ corresponding to the ideal (2) in $\mathbb{Z}$. A ring mod the zero ideal is just the ring again, and a ring mod the unit ideal is the zero ring.

Given a ring homomorphism $f : A \to B$ we can turn this into a homomorphism $\overline{f} : A/Ker(f) \to B$, which contains the same information as the original homomorphism (we are simply dividing the homomorphism into two parts, first sending everything that ends up at 0 to 0, then sending it over to B).

4 Quotient properties

We define a new type of ring, and call it an integral domain. A ring A is an *integral domain* if having $ab = 0$ implies that $a = 0$ or $b = 0$ (does this remind you of something?). This basically means there are no complicated ways to get 0 as a product, only the simple way we already had for any ring, by multiplying by zero. We can think of these as nicely behaved rings, as the following theorem shows.

Theorem 2. *In an integral domain $ab = ac$ implies that $a = 0$ or $b = c$.*

Proof. We have that $ab = ac \Rightarrow a(b - c) = ab - ac = 0$ so either $a = 0$ or $b - c = 0$, in the first case, the theorem is proved, but if $a \neq 0$ then we get $b - c = 0 \Rightarrow b = c$, which again proves the theorem. ■

Integral domains correspond to a certain type of quotient ring, in particular, to quotients by a prime ideal. We also have a similar fact for maximal ideals and fields, as we now show with a theorem.

Theorem 3. *A quotient ring A/I is a integral domain if and only if I is prime. Similarly, a quotient ring is a field if and only if I is maximal.*

Proof. We first show that a quotient by a prime ideal is an integral domain. We have that everything in the quotient ring A/I that is equal to zero is an element of I in A, so that if $xy = 0 \in A/I$ then $xy \in I \subset A$ and either $x \in I$ or $y \in I$ so that one of these is equal to 0 in A/I, and thus A/I is a integral domain. Similarly, if I isn't prime, then some xy is in I, with neither of x or y being in I. so that $xy = 0$ in A/I, with neither of these being 0.

The quotient obtained from a maximal ideal is a field, because the only ideal containing it is the whole ring. This gives us that the only ideals of the quotient are the zero ideal and the whole ring, thus the quotient ring is a field. Similarly, if we quotient by an ideal I that isn't maximal, there is another ideal J such that $I \subset J \subset (1)$, so that the quotient A/I contains a corresponding ideal $(0) \subset J \subset (1)$, so that A/I cannot be a field. ■

In light of this theorem, we have another way of showing that a maximal ideal is prime, namely by showing that a field is an integral domain. We can however demonstrate this, because if $xy = 0$ and $x \neq 0$, then since x is invertible we get $y = 1 * y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0$.

5 Polynomial rings

Given a ring A, we can define another ring, which we call $A[x]$, the ring of polynomials over x. This field is formed by polynomials $a_0x^n + \cdots a_{n-1}x + a_n$ where $a_0, \ldots, a_n \in A$ i.e. the coefficients are in A. We add polynomials term-wise, as usual, and multiply them as usual. This gives that the multiplicative identity is 1 and additive identity is 0, so that $A[x]$ inherits its identity elements from A, inverses remain inverses, and the additive inverse of a polynomial is the polynomial obtained by taking the additive inverses of all its coefficients. Note that if A is an integral domain, so is $A[x]$ (this is **not** true for fields).

Since the polynomial ring is also a ring, we can again take the polynomial ring of this ring. This gives us $(A[x])[y]$ where the polynomial coefficients are themselves polynomials, this is the same as taking the ring $A[x, y]$ of polynomials in two variables over A.

We can quotient a polynomial ring by the ideal generated by any polynomial. For example we can take the ideal (x) generated by x, this ideal will contain exactly all polynomials without a constant term. The quotient by (x) is equivalent to evaluating the polynomials at $x = 0$, namely sending a polynomial to its constant term. Similarly the quotient by $(x - a)$ is equal to evaluation the polynomials at $x = a$ (since we then get $x - a = 0$ so we can add a to both sides of that equation). Both of these will just give us our original ring (the polynomial $f(x) = b$ will just evaluate to b, and every sum and product of ring elements is another ring element).

We can also take the quotients of higher degree polynomials, and this in general may give us something more complicated. For example taking $\mathbb{Z}[x]/(x^2 + 1)$ gives us the ring of Gaussian integers $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i = \{a + bi : a, b \in \mathbb{Z}\}$. The idea here is that any polynomial with degree higher than 1 can be cut down to something of degree 1 by replacing each x^2 with -1 because $x^2+1 = 0 \Rightarrow x^2 = -1$. Then given a polynomial of degree 1 it will look like $a + bx$ (where a and b can also be 0) but we have that $x^2 = -1$ so that x acts like i, the square root of negative 1.

6 Some ideal properties

The ideal sum $I + J$ is defined as $\{i + j : i \in I, j \in J\}$. This is an ideal, and contains both I and J. It's an ideal because given $a, b \in I + J$ we have that $a + b = (i + j) + (i' + j') = (i + i') + (j + j') = i'' + j''$ where $i, i', i'' \in I$, similarly for J. On a similar note, for $a \in I + J$ and $r \in A$ we have that $ra = r(i + j) = ri + rj$, which is still in the ideal using the ideal properties from I and J. This contains both I and J because we can take in the sum one of the summands to be 0, which is in every ideal since $a0 = 0$. This allows us to define ideals such as $(a, b) = (a) + (b)$, or similarly for any number of elements, we then call these elements *generators*.

Another ideal we can take is the intersection of two ideals $I \cap J$. Since if two elements are in the intersection, they are in both ideals, so their sum must also be in both. Similarly for a product by any ring elements. However, he union of ideals is in general **not** an ideal. For example in $\mathbb{Z}$ the union $(2) \cup (3)$ contains both 2 and 3 but doesn't contain $2 + 3 = 5$. What we can take instead is $(2) + (3)$ which ends up being the whole ring, since $-2 + 3 = 1$, so we can get any number by multiplying it by 1.

We can also take the product of two ideals $IJ = \{i_1j_1 + \cdots i_nj_n : i_1, \ldots, i_n \in I, j_1 \ldots, j_n \in J\}$, this is again an ideal. It is closed under addition by definition, as we can just extend the sum to get a longer one, and closed under multiplication because the original ideals are. Notice that this definition is a bit more complicated than the others, but this is necessary to ensure closure under addition. The product of two ideals is contained in their intersection.

We also have a distributive law, namely for ideals I, J and K we have that $I(J + K) = IJ + IK$. We demonstrate this by showing inclusion in both directions. If something is in $I(J + K)$ we can write it as a sum $i_1(j_1 + k_1) + \cdots + i_n(j_n + k_n)$ but we can then distribute the products and get something in $IJ + IK$. In the other direction, we certainly have $IJ \subset I(J + K)$, because we can simply always take the element from K to be 0, similarly $IK \subset I(J + K)$ but since the ideals themselves are contained, any sum with one term coming from each must be in $I(J + K)$, since ideals are closed under addition, giving the second inclusion and thus equality.