Topics in Algebra

Mendel Keller

November 17, 2017

All the rings we'll be working with will be commutative.

0 Zorn's lemma

Before we begin, it is helpful to state a very confusing and extremely useful mathematical fact. This strictly speaking cannot actually be proven (in some subtle understanding of the word), but there are other ways to state it that make it sound more reasonable.

Lemma 1. *If in a set with some ordering (i.e. we sometimes have $x > y$, and in that case we dont also have $y > x$, but we can have neither), every* chain*, a subset where every pair of elements x, y has either $x > y$, $y > x$, $x = y$ has an* upper bound*, an element z of the set such that $z \geq x$ for any x in the chain, then the whole set has a* maximal *element, an element m such that for every other element x of the set we have $x \not> m$.*

There is not really any simpler way to put it, and it's not immediately clear that this makes sense or is useful, but we shall see that it is in fact both useful and important. It is in fact among the most important mathematical facts we have.

Theorem. *Every ring has a maximal ideal.*

Proof. We show that every chain of ideals in a ring has an upper bound, the theorem then follows. Here the order we are considering is inclusion. Given a chain of ideals $C = \{I_0, I_1, \ldots\}$, we take their union $I = \bigcup_{I_n \in C} I_n$ to be their upper bound. First this is an ideal, because if $a \in I$, then we have that $a \in I_n$ for some n, so that $ra \in I_n$ for any ring element r, and thus $ra \in I$. Similarly, if $a, b \in I$, we have each of these in some minimal I_n, take the greater of the two, then $a, b \in I_n \Rightarrow a + b \in I_n \Rightarrow a + b \in I$, so that this is in fact an ideal. It is an upper bound for the chain since by definition it will contain any ideal in the chain. Thus every ring has a maximal element. ■

1 The nilradical

The nilradical $\mathfrak{N}$ of a ring A is the set of elements a, some power of which is 0. If we take the intersection of all the prime ideals of a ring we get the nilradical, a fact we now prove.

Proof. The first direction is somewhat easier. Given a nilpotent element a (i.e. an element in the nilradical), and a prime ideal $\mathfrak{p}$, we show that $a \in \mathfrak{p}$. But $a^n = 0 \in \mathfrak{p}$, so we must have that $a \in \mathfrak{p}$. For the reverse direction, say that a^n is not equal to 0 for any n, then consider the ideals not containing any a^n, and we show that at least one such ideal is prime. We have that there is at least one such ideal, namely (0). Every chain of such ideals has an upper bound, namely its union, and since no a^n is in anything in the chain, it also cannot be in the union, so that the union is in fact in the set under consideration. Thus this set has a maximal element I. If there's another ideal J with $I \subset J$, it must be the case that $a^n \in J$ for some n. Now, we show that I is prime. Given $x, y \notin I$ we have that $I \subset I + (x)$ and $I \subset I + (y)$, so that $a^n \in (x)$ and $a^m \in (y)$ and thus $a^{n+m} \in (xy)$ so that $xy \notin I$ and so I is prime, as desired. This tells us that a cannot be in the intersection of all prime ideals. ■

2 Nullstellensatz

Not all polynomials over the real numbers have a solution, namely, some quadratics have their roots in the complex numbers $\mathbb{C}$. But any polynomial $f(x)$ with coefficients in the complex numbers has all its roots in $\mathbb{C}$, so we can write $f(x) = (x - a_1) \cdots (x - a_n)$. This polynomial will then be divisible by each of the $(x - a_i)$, so that in particular the ideal (f) is contained in each of the ideals $(x - a_i)$, and isn't maximal, or even prime. In fact the maximal ideals of $\mathbb{C}[x]$ are exactly the ideals $(x - a)$ for any $a \in \mathbb{C}$. Hilbert's nullstellensatz states that this holds for rings in many variables over $\mathbb{C}$ as well.

Theorem. *(Nullstellensatz) The maximal ideals of* $\mathbb{C}[x_1, \ldots, x_n]$ *are exactly* $(x_1 - a_1, \ldots, x_n - a_n)$ *for* $a_i \in \mathbb{C}$.

The nullstellensatz in fact says something more, about any ideal. First we must present the idea of a *variety*. Given an ideal I in a polynomial ring of n variables over a ring A, the corresponding variety $V(I)$ is the set of points in A^n that is zero for every polynomial $f \in I$. In fact, given a set S of polynomials, the set of polynomials, denoted $Z(S)$, that are zero at every point where every $f \in S$ is zero is an ideal, because multiplying by a polynomial keeps the polynomial at 0, and adding gives $0 + 0 = 0$. What would be particularly nice is if we had $Z(V(I)) = I$, but this is not the case, we do however have something similar $Z(V(I)) = \sqrt{I} = \{f : f^n \in I, n \in \mathbb{N}\}$ (this is called the strong Nullstellensatz). Note, that in this light the weak nullstellensatz is saying that maximal ideals have variety a point, although the converse doesn't really hold.

3 Different kinds of quotients

Notice the vast difference between quotients of $\mathbb{Z}$ by maximal ideals (p) and of $\mathbb{C}[x]$ by maximal ideals $(x - a)$. Namely, for $\mathbb{Z}$, we obtain something different, depending on which (p) we quotiented out by, but for $\mathbb{C}[x]/(x - a) \cong \mathbb{C}$, what we obtain looks the same no matter which ideal gave us that quotient. In fact, in studying these rings and ideals, it generally makes sense to study (p) by looking at the quotient by it, or some similar construction, deriving properties of p by the way $\mathbb{Z}/(p)$ behaves. Conversely, the way that $\mathbb{C}[x]/(x - a) \cong \mathbb{C}$ behaves is rather uniform, and in fact what we end up studying is specifically ideals that aren't maximal, generally in rings of several variables. Contrastingly, in $\mathbb{Z}$, much of what's interesting is simply in studying various primes, and their properties.

4 Modules

A module M is something satisfying the vector space axioms over a ring A. Namely, M has a + operation, and module elements can be multiplied by ring elements to obtain another module element, a module also has a 0 element which is the identity for +. We also have that for any $a, b \in A$ and $m, n, k \in M$,

1. $m + n = n + m$
2. $m + (n + k) = (m + n) + k$
3. $\exists - m : m + (-m) = 0$
4. $0m = 0$
5. $1m = m$
6. $a(bm) = (ab)m$
7. $(a + b)m = am + bm$
8. $a(m + n) = am + an$

Here, 1-3 are axioms relating to addition in the module, 4-6 tell us about multiplication by ring elements, and 7-8 are distributivity axioms. A better way to thing about this is that M is a commutative group, with the ring A acting on it by multiplication, in an appropriate way to make things compatible. Although the axioms here are somewhat similar to a vector space, the behavior of modules turns out to be quite different.

An example of a module is an ideal $I \subset A$ where the action by A is multiplication by an element of A as usual. Or a quotient ring A/I, where the operation is done by quotienting an element of A by I and then multiplying in A/I. Or what's called a free module A^n with elements being $(a_1, \ldots, a_n)$ for ring elements $a_1, \ldots, a_n \in A$ here the addition is component-wise, as is the multiplication.

For modules we also have a concept of quotient modules and module homomorphisms. A module homomorphism $f : M \to N$ satisfies $f(m+n) = f(m) + f(n)$ and $f(am) = af(m)$. Instructive to consider is a case where the module homomorphism doesn't work. Namely, consider $\mathbb{C}[x]/(x) \cong \mathbb{C}$ and $\mathbb{C}[x]/(x-1) \cong \mathbb{C}$, as fields these two are isomorphic, but this doesn't work as modules. In the first case, for $c \in \mathbb{C}$ we have $xc = 0$, while in the second case $xc = c$. This is a way in which studying quotient rings in modules differs from studying the quotient ring alone. Although I don't know many examples of this being interesting, it is used in some theorems.

5 Tensor products

Given three modules over A, which we name M, N and P. We can have a map $f : M \times N \to P$, such that, for any fixed $m \in M$ the map $f : \{m\} \times N \to P$ is a homomorphism, and similarly for a fixed $n \in N$. This isn't a homomorphism itself, because we must have that $f(0,n) = f(m,0) = 0$ so that if this were a homomorphism we would have $f(m,n) = f(m,0) + f(0,n) = 0 + 0 = 0$. But we would like this to be a homomorphism, and so in order to do that, we define a new module $M \otimes N$, this is given by $M \times N$, with the following relations: $(m+m',n) = (m,n) + (m',n), (m,n+n') = (m,n) + (m,n'), (am,n) = a(m,n) = (m,an)$. This is a somewhat more complicated object, but the correct way to think about it is that given a map $f : M \times N \to P$ for any A-module P, satisfying that fixing an element of M or N gives a homomorphism, we can then send this map through $M \otimes N$ to get a homomorphism $f^* : M \otimes N \to P$. Interesting to note is the existence of non-simple tensors, elements of $M \otimes N$ that cannot be simply expressed as $m \otimes n$, but rather need to be expressed as a sum. One example can be obtained by considering $M[x] \cong A[x] \otimes M$.

For any two algebraic objects A, B, the Hom-set $Hom(A,B)$ is the set of homomorphisms from A to B. We have the following interesting module isomorphism. $Hom(M \otimes N, P) \cong Hom(M, Hom(N,P))$. This is simply true by the way we defined the tensor product.

Tensoring by the 0 module turns any module into 0. Tensoring by A just gives the module back, as there's a natural isomorphism $M \otimes A \cong M$. We can also add modules using the direct sum, $M \oplus N$ is just ordered pairs (m,n), with the coordinates not interacting. We have a distributive law $M \otimes (N \oplus P) \cong (M \otimes N) \oplus (M \otimes P)$. These two operations (direct sum and tensor product), both have associative and commutative laws as well (up to isomorphism). Here we see the beginning of defining a ring structure on modules. There are a bunch of fun proofs we can do using these facts, but I will omit them here.

6 More about varieties

One thing to consider about varieties, is polynomials on the variety. We call this the coordinate ring of the variety and denote it by A (this is done when using R to denote the whole polynomial ring). It turns out, somewhat unsurprisingly, that $A \cong R/I$. This statement essentially says that if we have 3 polynomials, f, g, h with $f(x) = 0$ everywhere on $V(I)$ (i.e. $f \in I$) and $g = f + h$ then plugging in a value from $V(I)$ gives the same thing for g and h. A somewhat unsurprising assertion.

Another point of interest is a point which is a "multiple root" of an ideal. The following is a little difficult to motivate without a much more in depth look at algebraic geometry, but is not too difficult to understand on its own. If we consider for example, in $\mathbb{C}[x,y]$ the ideal (x^2, y), we can imagine having obtained this from a limit process, where we took $\lim_{t \to 0}(x(x-t), y)$. Now the variety of $(x(x-t), y)$ is just 2 points, $\{(0,0), (t,0)\}$ so that from this perspective, the variety of (x^2, y) is the collision of two points at $(0,0)$ in the horizontal direction. We think of this as the point $(0,0)$ thickened infinitesimally in the horizontal direction. If we consider (x^2, y^2), we can think of this as the origin thickened with a small neighborhood in all directions.

If we think about $(x, x^2 + y)$, this will be a line at $x = 0$ with the origin somewhat thickened. We can also consider (x^2) as a line at the origin thickened slightly in the horizontal direction. We can also think of (x^5, y^8) as the origin thickened a bit more, perhaps with a slightly bigger infinitesimal neighborhood.

7 Localization

The same way that the quotient by an ideal kills all the ideal lying below it i.e. contained in it, we have a process for killing all the ideals above a given ideal. In this case instead of sending the to (0) we will be sending them to (1), and we will do this by turning them into units. This is a more powerful method of zooming into an ideal, and seeing exactly what's going on under the hood. We call this process localization. Typically we will do this to a maximal or prime ideal, and so I will only bother discussing those cases.

Given a prime ideal $\mathfrak{p}$ (recall that maximal ideals are prime as well), we have a multiplicatively closed subset S, the complement of $\mathfrak{p}$, which can be denoted $S = A - \mathfrak{p}$. Localizing A at $\mathfrak{p}$ is the process of inverting all of S, we denote this by $S^{-1}A$ in the general case of any multiplicatively closed subset, and by $A_{\mathfrak{p}}$ in the case of localization at a prime ideal. To be a bit precise about things, elements of $S^{-1}A$ are defined as ordered pairs (s, a) with $s \in S$ and $a \in A$, and equality is defined as $(s, a) \sim (s', a') \Leftrightarrow (s, a) = (ts, ta)$ for some $t \in S$. Note that if $0 \in S$ then everything is equal to (0,0). Also in order for our definition of equality not to be extremely silly, we want to have $1 \in S$. Now we think of this ring as comprised of fractions, often writing (s, a) as a/s. It turns out that only ideals inside $\mathfrak{p}$ stay ideals in $A_{\mathfrak{p}}$, and then $\mathfrak{p}A_{\mathfrak{p}}$ (which is the ideal in $A_{\mathfrak{p}}$ generated by $\mathfrak{p}$, which is given as the set of elements $\{p/1 : p \in \mathfrak{p}\}$) is the unique maximal ideal of $A_{\mathfrak{p}}$. We generally call rings with a unique maximal ideal local rings.

8 Noetherian and Artinian

A Noetherian ring is a ring where every ideal has only finitely many ideal between it and (0), for example $\mathbb{Z}$ is such a ring, as is any polynomial ring in finitely many variables over a Noetherian ring, or the quotient of a Noetherian ring. An Artinian ring is one with a similar condition, but this time for (1) instead of (0). It turns out that Artinian rings are really close to fields.

Theorem 2. *In an artinian ring, every prime ideal is maximal.*

Proof. For a prime $\mathfrak{p}$ we have that $A/\mathfrak{p}$ is an artinian integral domain. For a nonzero $x \in A/\mathfrak{p}$ we must have that the ideal powers of x eventually stabilize, or we'd get an infinite descending chain. So we have $x^n = yx^{n+1}$ canceling x^n yields $xy = 1$. So $A/\mathfrak{p}$ is a field, and thus $\mathfrak{p}$ is maximal. ■

It turns out we have a better theorem, we can express an Artinian ring as a direct sum of artinian local rings. We won't prove this fact.

9 DVR

The next least complicated ring has dimension 1, that means there is some containment of prime ideals (the dimension of a ring is the highest number of prime ideals of the ring contained in each other, minus one). If A is a domain and Noetherian, then all its nonzero primes are maximal. An example of this is $\mathbb{Z}$.

A discrete valuation is a surjective function v from a field to $\mathbb{Z}$, such that $v(xy) = v(x) + v(y)$ and $v(x + y) \geq min\{v(x), v(y)\}$. given a valuation, we can define a DVR, the set of elements with $v(x) \geq 0$. It turns out this is local, and all ideals in it are powers of the maximal ideal.

Another simple type of ring is a Dedekind domain, satisfying that every localization of it is a DVR. The integers are a Dedekind domain.