MAT :Algebra III
September 2, 2004

Gabriel C. Drummond-Cole

November 30, 2004

Say A is a commutative ring. an ideal is a subgroup which is invariant under multiplication by ring elements. This is not a subring. A proper ideal $p \subset A$ is called prime if $xy \in p$ implies either $x \in p$ or $y \in p$; equivalently, A/p has no zero divisors (is an ntegral domain).

Say $A = \mathbb{Z}$. Then $p = (f)$ is prime if and only if f is a prime number. We'll see later that prime and irreducible, which are equivalent in $\mathbb{Z}$, are going to generalize slightly differently.

A proper ideal $m \subset A$ is called maximal if it is maximal with respect to inclusion. The first question is, "do I have maximal ideals?" The answer, I hope you have seen, by an easy application of Zorn's lemma, is yes. The union will be an upper bound on any chain. If you apply this fact, that every ring $A \neq 0$ has maximal ideals, you get that every proper ideal is contained in a maximal ideal. If the ideal is I, then A/I has a maximal ideal, and pulling back to its preimage gives a maximal ideal containing I.

Why do I have this? Suppose $f : A \to B$ is a morphism of rings. Then if $J \subset B$ is an ideal, it is implied that $f^{-1}(J)$ is an ideal in A. The image of an ideal is not necessarily an ideal. Since you have the natural quotient morphism $A \to A/I$, and it turns out to be maximal because the morphism is a surjection.

Remark 1 *$p \subset B$ prime implies $f^{-1}(p)$ is also prime. The same is not true for maximal ideals. Look at inclusion $\mathbb{Z} \to \mathbb{Q}$; then $f^{-1}((0)) = (0)$ is not maximal.*

Since the 50s, the collection of prime ideals $\{p \subset A |\ p \text{ is prime}\}$ has been called $Spec(A)$.

There are two other things I meant to say. We have a very simple lemma.

Lemma 1 *The following are equivalent:*

1. *A is a field*
2. *A has only the (0) and (1) ideals*

3. *Every nonzero morphism from A to another ring is injective.*

$1 \to 2$ and $2 \to 3$ are obvious. In a field, an ideal containing anything nonzero also contains 1. A nonzero morphism has to have a proper kernel, which in the case of 2 is (0), forcing injectivity. $3 \to 1$ is also very easy. This is somewhat more complicated in the noncommutative case.

In correspondence to our statement about prime ideals, if $m \subset A$ is maximal then A/m is a field. Again, this is more complicated if A is noncommutative.

Definition 1 *The nilradical of A $N(A) = \{x \in A | \exists n_x \geq 1$ such that $x^{n_x} = 0\}$.*

The miracle of this in the commutative world is that this is an ideal. Of course, if your ring has no zero divisors, it has no nilpotents. But if you take, say, $\mathbb{Z}[x]/(x^2)$, then the class of x is a nilpotent. It's nonzero, but its square is zero.

Why is this an ideal? For products, it's easy. If $x^n = 0$ then $(rx)^n = r^n x^n = 0$. For sums, say $x^n = 0 = y^m$. Then $(x+y)^{n+m-1} = \sum x^i y^{n+m-1-i} \binom{n+m-1}{i}$. If $i < n$, then $n - i > 0$ so $n + m - 1 - i > m - 1$. Now, in a noncommutative ring, this is not an ideal.

There's a nice relationship between this and prime ideals.

Lemma 2 *$N(A) = \cap_{p \in Spec(A)} p$.*

One direction is easy. Since 0 is in a prime ideal, and x is nilpotent, then either $x \in p$ or $x^{n-1} \in p$. By recursion $x \in p$.

The other direction has a very short proof once you know localization; let's give the "ugly" proof today. Say x is not nilpotent. We want to find a prime ideal p with $x \notin p$. Let's look to $\Sigma = \{I$ a proper ideal of $A | \forall n > 0, x^n \notin I\}$. Is this collection empty? It contains 0 since x is not nilpotent. I'm going to be using Zorn's lemma.

Now, this collection is partially ordered by inclusion. Every chain has an upper bound, the union. So this satisfies the condition of Zorn's lemma. The union is an ideal because the collection is a chain. Then there is a maximal ideal p in Σ. So $x^n \notin p$ for all n. We're going to show that p is a prime ideal. Let $ab \in p$, and say that $a, b \notin p$. Now, $p \subset p + (a), p \subset p + (b)$ strictly. Since p was maximal in Σ, this means $p + (a), p + (b) \notin \Sigma$. Then $x^n \in p + (a), x^m \in p + (b)$. Then $x^{m+n} \in p + (ab) = p$ since $(x_p + x_a)(y_p + y_b) = (x_p y_p + x_p y_a + y_p x_a) + (x_a y_b)$, a contradiction.

Exercise 1 *Say A is a commutative ring, and $f \in A[x]$.*

1. *how $f \in N(A[x])$ if and only if every coefficient is nilpotent.*
2. *Show that f is invertible if and only if the first coefficient is invertible and every other a_i is nilpotent.*

Also, what are the analogs for the rings $A[[x]]$ of formal power series.

What else can you do to an ideal?

Definition 2 *The radical of an ideal, denoted $\sqrt{I}$, is $\{f \in A | \exists n \text{ with } f^n \in I\}$.*

We have immediately that $I \subseteq \sqrt{I}$. Now, if I is prime then I is radical, i.e., $I = \sqrt{I}$. The converse is not true.

Exercise 2 *Find a radical ideal which is not prime.*

Why is $\sqrt{I}$ an ideal? Let $\phi : A \to A/I$. Then $\phi^{-1}(N(A/I)) = \sqrt{I}$. So this is an ideal.

Let's amuse ourselves. Let $I = (x^2 + 3xy, y^2 + 3xy) \subset \mathbb{R}[x, y]$. The radical and the ideal have the same zero locus, and in a certain sense the radical will be the largest ideal which can vanish on a given locus. The ideal (y^2) is not radical, we have $\sqrt{(y^2)} = (y)$. These both define the x axis.

Now in our example, $(x + y)^3 = x(x^2 + 3xy) + y(y^2 + 3xy)$ is in the ideal. This ideal is homogeneous, and so is $x + y$. In a homogeneous ideal, any homogeneous element can be written as a homogeneous combination of the generators. Then degree considerations show that $x+y \notin I$, since homogeneous combinations of the generators can't get anything of degree 1.

This is a hard exercise, well, not so hard.

Exercise 3 *Look now to an $n \times n$ matrix. We can see this as $k[x_{11}, x_{12}, \ldots, x_{nn}]$. I want an ideal I which encodes the matrices which are nilpotent. Show that this is not radical. There will be something representing a trace which is not in the ideal.*

A consequence of the lemma is that $\sqrt{I} = \cap_{p \in Spec(A), p \supset I} p$. I'll tell you the trick behind this in a little bit.

What are our operations on ideals?

- $\sqrt{}$
- $\cap_{j \in J} I_j$
- $\sum_{j \in J} I_j$
- $I \cdot J = (ab | a \in I, b \in J)$.
- $\prod_{i=1}^{n} I_i$
- $I^n = \prod_{i=1}^{n} I$.

- Say $I \subset A \to^{\phi} B \supset J$ is inclusion. Then $J^c = f^{-1}(J)$ is called the contraction of J.
- $I^e = (\phi(I))$ is the extension of I.
- This is like shaving in geometry, getting rid of some components. These all have geometric interpretations. If you have two ideals, $(I : J) = \{f \in A | fJ \subset I\}$.

So let's look in $\mathbb{Z}$. We have $(a) \cap (b) = (lcm(a, b)),\ (a) + (b) = (gcd(a, b)),\ (a) \cdot (b) = (ab)$.

What is $((m) : (n))$? This has to be generated by one number. This is $(m/gcd(m, n))$.

Exercise 4 *Prove this, it shouldn't be so hard.*

Let me list some of the properties which these operations have. These are useful but boring. We know that contraction preserves primality. Does extension preserve primality? Look at the injection $\mathbb{Z} \to \mathbb{Q}$. Then we see that $(3)^e = (1)$ so the answer is no.

Look at the more interesting inclusion $\mathbb{Z} \to \mathbb{Z}[i]$.

Exercise 5 *1. What is* $(2)^e$? *It is* $((1 + i)^2)$

2. $p \equiv 1 \mod 4$, *then* $(p)^e$ *is the product of prime ideals.*

3. $p \equiv 3 \mod 4$, *then* $(p)^e$ *is prime.*
You need the fact that an odd prime is the sum of two squares if and only if it is 1 mod 4.

There is a norm in $\mathbb{Z}[i]$, $N(a + bi) = a^2 + b^2$, with $N(zz') = N(z)N(z')$.

Now what about the properties of the operations?

Exercise 6 *1.* $I \cdot (L + M) = I \cdot L + I \cdot M$

2. $I \cap (L + M) = I \cap L + I \cap M$ *if either* $I \supset L$ *or* $I \supset M$.

3. $(I + J) \cdot (I \cap J) \subset I \cdot J$. *In* $\mathbb{Z}$ *equality holds.*

4. $I \cdot J \subset I \cap J$. *If* $I + J = (1)$ *(I and J are coprime) then this is an equality. This is the shortest version of the Chinese Remainder Lemma.*

5. $I \subset (I^e)^c$

6. $J \supset (J^c)^e$

7. $I^e = I^{ece}; J^c = J^{cec}$. *These yield a correspondence between ideals* $I = I^{ec}$ *and ideals* $J = J^{ce}$.

Lemma 3 *Chinese Remainder Theorem*
Let $I_i \subset A, i \in \{1, \dots, n\}$*. Let* $\phi : A \to \prod_{i=1}^n A/I_i,\ \ x \to (x + I_1, \dots, x + I_n)$*, then if* $I_i + I_j = (1)$ *for all* $i \neq j$ *(equivalent to* ϕ *surjective) it is implied that* $\cap_{i=1}^n I_i = \prod_{i=1}^n I_i$*.*

Say $I_1 = (3), I_2 = (5)$. Then $phi : \mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. The kernel is $I_1 \cap I_2 = (15)$. Then $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$