Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

October 17, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Integral Domains and Fraction Fields

0.1.1 Theorems

Now what we are going to do is to consider ways in which a ring R can be embedded in a field F. Now we saw previously that if $a \in R$ is a zero divisor then we can't adjoin an inverse without killing some elements. And so we can't embed a ring with zero divisors into a field. This turns out to be the only obstacle though.

Integral Domain

Definition 0.1.1.1. A ring R is an integral domain if it has no zero divisors. I.e. $0 \neq 1$ and if $ab = 0$ then $a = 0$ or $b = 0$.

Cancellation Law

Theorem 0.1.1.2. *If R is an integral domain then it satisfies the cancellation law:*

$$(\forall a, b, c)(a \neq 0) \wedge (ab = ac) \rightarrow (b = c)$$

Proof. We have $ab - ac = a(b - c) = 0$ so $b - c = 0$ as $a \neq 0$. □

Integral Domain of Polynomials

Theorem 0.1.1.3. *Let R be an integral domain. Then $R[x]$ is an integral domain.*

Proof. ********** □

Finite Integral Domain is a Field

Theorem 0.1.1.4. *An integral domain with finitely many elements is a field.*

Proof. ********** □

Field of Fractions

Theorem 0.1.1.5. *Let R be an integral domain. Then there exists an embedding $\phi : R \to F$ into a a field F*

Proof. The way we are going to show this is to mimic how the rational numbers are created from the integers.

Definition of Field of Fractions

Definition 0.1.1.6. A Fraction will be a pair a/b where $a, b \in R$ and $b \neq 0$. Two fractions a_1/b_1, a_2/b_2 are called equivalent $a_1/b_1 \sim a_2/b_2$ if $a_1 b_2 = a_2 b_1$.

First we want to check that $\sim$ is an equivalence relations.

Reflexivity and Symmetry are obvious so all that is left is transitivity.

Suppose $a_1/b_1 \sim a_2/b_2$ and $a_2/b_2 \sim a_3/b_3$. We then have $a_1 b_2 = a_2 b_1$ and $a_2 b_3 = a_3 b_2$. Hence $a_1 b_2 b_3 =$

$a_2b_1b_3 = a_3b_2b_1$ by the assumptions. But because we are in an integral domain we can cancel the b_1 and we get

$$a_2b_3 = a_3b_2$$

and hence $\sim$ is an equivalence relation.

The Field of Fractions of R is defined to be the set of equivalence classes of fractions of R. We define

$$(a/b)(c/d) = ac/bd,\ a/b + c/d = \frac{ad + bc}{bd}$$

We have to check that the axioms of a field are satisfied and that replacing $a/b, c/d$ by equivalent elements doesn't change the answer, but this is easy and we won't do it here. $\square$

As an example consider the the case of the ring $K[x]$ where K is an integral domain. Then in this case the field of fractions is

$K(x) = \{[f/g] :\ f, g$ are polynomials with $g \neq 0$ and $[f/g]$ is the equ

Extending a map onto field of fractions

Theorem 0.1.1.7. *Let R be an integral domain with field of fractions F and let $\varphi : R \to K$ be any injective homomorphism from R into a field K. Then the rule*

$$\Phi(a/b) = \phi(a)\phi(b)^{-}1$$

defines the unique extension of φ to a homomorphism from $F \to R$.

Proof. First we need to check that this extension is well defined. Since the denominator in a/b is not allowed to be zero and since φ is injective we have $\varphi(b) \neq 0$ for all a/b. Hence $\varphi(b)$ is invertible in K. and hence $\varphi(a)\varphi(b)^{-1}$ is an element of K.

Next we need to check that equivalent fractions have the same image. But $a_1/b_1 \sim a_2/b_2 \leftrightarrow a_1b_2 = a_2b_1$

and hence $\varphi(a_1)\varphi(b_2) = \varphi(a_2)\varphi(b_1)$ and $\Phi(a_1/b_1) = \varphi(a_1)\varphi(b_1)^{-1} = \varphi(a_2)\varphi(b_2)^{-1} = \Phi(a_2/b_2)$ as required.

Hence Φ is a homomorphism. And showing that Φ is unique is easy. $\square$

0.2 Maximal Ideals

0.2.1 Definitions

Now lets look at surjective maps from a ring R to a field F. If $\varphi : R \to F$ is such a map then we know by the first isomorphism theorem that $F \cong R/ker(\varphi)$. So in particular we can recover F, φ from $R, ker(\varphi)$.

So we must look at ideals M such that R/M is a field. By the Correspondence Theorem (??4.3??) the ideals of R/M correspond to the ideals of R which contain M. So R/M is a field if R has exactly two ideals containing M.

I.e. M, R.

Maximal Ideal

Definition 0.2.1.1. An ideal M is maximal if $M \neq R$ but M is not contained in any other ideals than M, R.

Quotient by Maximal Ideal

Lemma 0.2.1.2. *An ideal M is maximal if and only if R/M is a field. And the zero ideal is maximal if and only if R is a field.*

Proof. This is immediate from the definition of maximal ideal. □

0.2.2 Examples

Maximal Ideals in Integers

Theorem 0.2.2.1. *The maximal ideals of the ring $\mathbb{Z}$ of integers are the principle ideals generated by the prime integers.*

Proof. If (a) is an ideal and $(a) \subseteq (b)$ an ideal, then a divides b. □

Maximal Ideals in Polynomial rings over $\mathbb{C}$

Theorem 0.2.2.2. *The maximal ideals of the polynomial ring $\mathbb{C}[x]$ are the principle ideals generated by the linear polynomials $x - a$. The ideal generated by $x - a$ is the kernel of the substitution homomorphism $s_a : \mathbb{C}[x] \to \mathbb{C}$ sending $f(x) \rightsquigarrow f(a)$. So there is a bijective correspondence between maximal ideals in $\mathbb{C}[x]$ and $\mathbb{C}$.*

Proof. First notice that if M is a maximal ideal then we know that M is a principle ideal generated by a monic polynomial f of least degree (Because $\mathbb{C}[x]$ is a PID). But since every complex polynomial has a root, f is divisible by some $x-a$. But then f is in the principle ideal $(x-a)$

and hence $M \subseteq (x-a)$ so in fact $M = (x-a)$ as M is maximal.

Next we show that the kernel of the substitution homomorphism s_a is generated by $(x-a)$. To say that a polynomial f is in the kernel of s_a is to say that a is a root of g or that $x-a$ divides g. Thus $(x-a)$ generates s_a. Since the image of s_a is a field this shows that $(x-a)$ is a maximal ideal. □

Hilbert's Nullstellensatz

Theorem 0.2.2.3 (Hilbert's Nullstellensatz)**.** *The maximal ideals of the polynomial ring* $\mathbb{C}[x_1, \ldots, x_n]$ *are in a bijective correspondence with points of complex* n*-dimensional space. A point* $\overline{a} = \langle a_1, \ldots, a_n \rangle$ *in* $\mathbb{C}^n$ *corresponds to the kernel of the substitution map* $s_a : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}$ *which sends* $f(\boldsymbol{x}) \rightsquigarrow f(\overline{a})$*. The*

Kernel M_a of this map is the ideal generated by the linear polynomials

$$x_1 - a_1, \ldots, x_n - a_n$$

Proof. Let $a \in \mathbb{C}^n$ and let M_a be the kernel of the substitution map s_a. Since s_a is surjective and $\mathbb{C}$ is a field M_a is a maximal ideal. Next let us verify that M_a is generated by the linear polynomials as asserted. To do so we expand $f(x)$ in powers of $x_1 - a_1, \ldots, x_n - a_n$ writing

$$f(x) = f(a) + \sum_i c_i(x_i - a_i) + \sum_{i,j} c_{ij}(x_i - a_i)(x_j - a_j) + \cdots$$

The existence of such an expansion can be gotten by letting $x = a + u$ and substituting it into $f(x)$ and then replacing every u with $x - a$. Now notice that every termon the right except $f(a)$ is divisible by at least 1 of $(x_i - a_i)$. So if f is in the kernel of s_a, i.e. $f(a) = 0$ then $f(x)$ is in

the ideal which is generated by $(x_1 - a_1), \ldots, (x_n - a_n)$. Hence $(\{x_i - a_i : i \leq n\})$ generate M_a.

Next we have to prove that every maximal ideal is of the form $(\{x_i - a_i : i \leq n\})$ for some point $a \in \mathbb{C}^n$. To do so lets let M be a maximal ideal and let K denote the field $\mathbb{C}[x_1, \ldots, x_n]/M$. We consider the restrictions of the canonical map $\pi : \mathbb{C}[x_1, \ldots, x_n] \to K$ to the subring $\pi_i : \mathbb{C}[x_i] \to K$

Lemma 0.2.2.4. *The kernel of π_i is either 0 or else it is a maximal ideal.*

Proof. Assume the kernel isn't 0 and $0 \neq f \in ker(\pi_i)$. Now since K isn't the zero ring $\ker(\pi_i)$ isn't the whole ring. So f is non-constant and hence divisible by a linear polynomial. Say $f = (x_i - a_i)g$.

Then $\pi(f) = \pi(x_i - a_i)\pi(g) = 0$ in K. Since K is a field either $\pi(x_i - a_i) = 0$ or $\pi(g) = 0$. So either $(x_i - a_i) \in ker(\pi_i)$ or $g(x_i) \in ker(\pi_i)$. So by induction on the degree of f $ker(\pi_i)$ contains a linear polynomial. □

We are now going to show that $ker(\pi_i)$ isn't the zero ideal and hence M contains a linear polynomial of the form $(x_i - a_i)$.

Because i was arbitrary this will then show that M is contained in the kernel of a substitution map and hence must be equal to the kernel as it is a maximal idea.

Suppose $ker(\pi_i) = 0$. Then π_i maps $\mathbb{C}[x_i]$ isomorphically to its image which is a subring of K. Hence π_i can be extended to the field of fractions of $\mathbb{C}[x_i]$. Hence K contains a subfield isomorphic to $\mathbb{C}(x)$, the field of ratio-

nal functions.

Now the monomials $\mathbf{x}^i = x_1^{i_1} \cdots x_n^{i_n}$ form a basis for $\mathbb{C}[x_1, \ldots x_n]$ as a vector space of $\mathbb{C}$. So in particular $\mathbb{C}[x_1, \ldots, x_n]$ has a countable basis as a vector space over $\mathbb{C}$. And, as K is a quotient of $\mathbb{C}[x_1, \ldots, x_n]$ there is a countable family which spans K (namely the residue of the $\mathbf{x}^i$).

However we will show that there are uncountably many linearly independent elements of $\mathbb{C}(x)$. It will follow that $\mathbb{C}(x)$ can't be isomorphic to a subfield of K.

We need the assumption that $\mathbb{C}$ is uncountable and then the following two lemmas.

Lemma 0.2.2.5. *The uncountably many rational functions* $(x-\alpha)^{-1}, \alpha \in \mathbb{C}$ *are linearly independent.*

Proof. A rational function f/g defines an actual function by evaluation at points of the complex plane where $g \neq 0$. The rational function $(x-\alpha)^{-1}$ has a pole at α, which means that it takes on arbitrarily large values near α. It is also bounded near any other point.

Now consider the following linear combination.

$$\sum_{i=1}^{n} \frac{c_i}{x-\alpha_i}$$

where $\alpha_1, \ldots, \alpha_n$ are distinct complex numbers and say $c_1 \neq 0$. Then the first term is unbounded near α while the other functions are all bounded near it. Hence the linear combination doesn't define the zero function. $\square$

Lemma 0.2.2.6. *Let V be a vector space which is spanned by a countable family $\{v_1, \ldots, v_n, \ldots\}$ of vectors. Then every set L of linearly independent vectors in V is finite or countably infinite.*

Proof. Let L be a linearly independent subset of V and let V_n be the span of the first n vectors and let $L_n = L \cap V_n$. So L_n is a linearly independent subset of a finite dimensional vector space and hence L_n is finite. Moreover,

$$L = \bigcup_n L_n$$

. And, the union of countably many finite sets is finite or countable. □

□

0.3 TODO

- Come up with A BUNCH of examples (more than I can use) so that I don't run out of time.

- Go through Lang's book on the same topics.