Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

October 3, 2006

TALK SLOWLY AND WRITE NEATLY!!

0.1 Rings

Today we are going to introduce a new structure which you haven't seen before. They are called Rings and they are a generalization of the integers.

0.1.1 Definitions

Definition of Ring

Definition 0.1.1.1. We say $\langle R, +, \times, 0, 1\rangle$ is a Ring if

- R is a set with $0, 1 \in R$
- $+, \times : R \times R \to R$
- $R^+ = \langle R, +, 0\rangle$ is an abelian group
- $$(\forall x, y, z \in R)(x \times y) \times z = x \times (y \times z)$$

- $$(\forall x \in R)x \times 1 = 1 \times x$$

(Distributive Laws)

$$(\forall x, y, z \in R)x \times (y + z) = x \times y + x \times z$$

$$(\forall x, y, z \in R)(y + z) \times x = y \times x + z \times x$$

We say a ring is Commutative if

$$(\forall a, b \in R)$$

Definition of Subring

Definition 0.1.1.2. Let $\langle R, +, \times, 0, 1\rangle$ be a ring. We say that $S \subseteq R$ is a Subring of $\langle R.+, \times, 0, 1\rangle$ if $0, 1 \in S$

$$(\forall x, y \in S)x + y \in X \wedge (-x) \in S \wedge x \times y \in S$$

0.1.2 Examples

Integers

Integers:

One of the most important examples of a commutative ring is the ring of integers $\mathbb{Z}$.

Some properties of the ring of integers which are interesting are

- $\mathbb{Z}$ is commutative.
- $\mathbb{Z}$ has no subrings.

  This is because if $S \subseteq \mathbb{Z}$ is a subring then it contains $0, 1$ and hence contains $1 + 1 + \cdots + 1$ n times for all n. And similarly contains $-(1 + \cdots + 1)$ and hence contains all the integers.

Gaussian Integers

Gaussian Integers:

Definition 0.1.2.1. We say that

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

is the ring of Gaussian Integers

The Gaussian integers are the points of a square lattice in the complex plane. DRAW THE COMPLEX PLANE WITH THE POINTS OF THE GAUSSIAN INTEGERS.

Subring of $\mathbb{C}$ generated by α:

Similar to the ring of Gaussian integers, given any complex number $\alpha \in \mathbb{C}$ we can form

$$\mathbb{Z}[\alpha] = \{\Sigma_{i \leq n} a_i \alpha^i : (\forall i) a_i \in \mathbb{Z} \text{ and } n \in \{0, 1, 2, \dots\}\}$$

Notice that $\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{C}$ containing α. We call $\mathbb{Z}[\alpha]$ the subring generated by α.

ASK IF THEY WANT ME TO PROVE THA

Algebraic/Transcendental Number

Definition 0.1.2.2. We say that $\alpha \in \mathbb{C}$ is algebraic if

$$(\exists a_0, a_1, \ldots, a_n \in \mathbb{Z}) a_0 + a_1\alpha^1 + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$$

We say that α is transcendental if it is not algebraic.

Some examples of algebraic numbers are i, $\sqrt{2}$, $\sqrt{\sqrt{2}+17}$ while some examples of transcendental numbers are e, π.

If α is transcendental then there is a bijection

$$p(\alpha) \rightsquigarrow p(x)$$

From the ring generated by α to the ring of polynomials with coefficients in $\mathbb{Z}$.

Polynomial Rings

Ring of Polynomials over a Ring:

In general we have that if R is a ring then

$$R[x] = \{\Sigma_{i \leq n} a_i x^i : a_i \in R\}$$

is also a ring.

Zero Ring

Zero Ring:

Definition 0.1.2.3. We define $\langle \{0\}, +, *, 0, 0 \rangle$ to be the Zero Ring

We then have that

Theorem 0.1.2.4. *If R is a ring such that $0 = 1$ then R is the zero ring.*

Proof. First note that $0a = 0$ for any element of a ring. This is because $0a + 0a = (0 + 0)a = 0a$ so subtracting $0a$ from both sides we see $0a = 0$. Now assume $0 = 1$ in a ring R. Then for all $a \in R$, $a = 1a = 0a = 0$. □

Fields

Fields:

Every field is also a ring. In fact fields are special types of rings because every element other than 0 has a multiplicative inverse. There is a special name for such elements.

Definition of Unit

Definition 0.1.2.5. Let $\langle R, \times, +, 0, 1\rangle$ be a ring. We say that $u \in R$ is a unit of R if

$$(\exists u^{-1} \in R) u \times u^{-1} = u^{-1} \times u = 1$$

So a field is a commutative ring where every element other than 0 is a unit.

Matrixes

Real Matrixes:

Our last example of a ring are the real $n \times n$ matrixes. This is an important example of a ring because it is an example of a non-commutative ring.

0.2 Homomorphisms and Ideals

0.2.1 Definitions

Ring Homomorphism

Definition 0.2.1.1. Let $\langle R, \times, +, 0, 1\rangle, \langle R', \times', +', 0', 1'\rangle$ be rings. A Homomorphism from R to R' is a map $\phi : R \to R'$ such that

$$\phi(0) = 0', \phi(1) = 1', \phi(a+b) = \phi(a)+'\phi(b), \phi(a\times b) = \phi(a)\times'\phi(b)$$

for all $a, b \in R$.

We say that ϕ is an isomorphism if it is a bijective homomorphism. If there is an isomorphism between R, R' then we say R and R' are isomorphic

0.2.2 Theorems

The most important ring homomorphisms are those which are obtained by evaluating a polynomial at a value. For example, if $a \in \mathbb{R}$ then we have

$$\phi : p(x) \rightsquigarrow p(a)$$

is a homomorphism $\phi : \mathbb{R}[x] \to \mathbb{R}$.

This leads to the following theorem.

Substitution Principle

Theorem 0.2.2.1 (Substitution Principle)**.** *Let* $\varphi : R \to R'$ *be a ring homomorphism.*

(a) Given an element $\alpha \in R'$ *there is a unique homomorphism* $\Phi : R[x] \to R'$ *which agrees with the map* φ *on constant polynomials and sends*

$$x \rightsquigarrow \alpha$$

(b) More generally, given elements $\alpha_1, \ldots, \alpha_n \in R'$ *there is a unique homomorphism* $\Phi : R[x_1, \ldots, x_n] \to R'$ *from the polynomial ring in* n *over* R *to* R' *which agrees with* φ *on constant polynomials and which sends*

$$x_i \rightsquigarrow \alpha_i$$

Proof. First note that the proof of (b) is obtained by simply repeatedly applying (a).

Note that if Φ exists then we must for each polynomial that

$$\Phi(\Sigma r_i x^i) = \Sigma \varphi(r_i)\alpha^i$$

because we have determined where Φ send coefficients of the polynomial as well as where it sends x (and it is a ring homomorphism. Hence, if Φ exists it must be unique.

To prove its existence lets take the above formulas as the definition for Φ and show that it is in fact a homomorphism from $R[x]$ to R'.

- Note that $\Phi(1) = \varphi(1) = 1$.
- It is obviously true that Φ commutes with addition
- Let $f = \Sigma_i a_i x^i, g = \Sigma_j b_j x^j$. Then

  $\Phi(fg) = \Phi(\Sigma_{i,j} a_i b_j x^{i+j}) = \Sigma_{i,j} \varphi(a_i)\varphi(b_j)\alpha^{i+j} = (\Sigma_i \varphi(a_i)\alpha^i)(\Sigma_j \varphi$

□

Corollary 0.2.2.2. *Let* $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_m)$ *denote sets of variables. Then there is a unique morphism*

$$\varphi : R[x, y] \to R[x][y]$$

which is the identity on $R \cup \boldsymbol{x} \cup \boldsymbol{y}$.

Proof. Note that R is a subring of $R[x]$ and $R[x]$ is a subring of $R[x][y]$ so R is a subring of $R[x][y]$. Let $\varphi : R \to R[x][y]$ be the inclusion map. The substitution principle tells us that there is a unique extension of φ to a map from $\Phi : R[x, y] \to R[x][y]$ sending x to x and y to y while agreeing with φ on R.

However, we also know that there is an inclusion map $\psi : R[x] \to R[x, y]$. And so by the substitution principle there must be a unique extension $\Psi : R[x][y] \to R[x, y]$ sending y to y and agreeing with ψ on $R[x]$.

But then $\Psi\Phi$ and $\Phi\Psi$ are both the identity on R and on x, y so they must be the identity on their respective domains. And hence inverse isomorphisms. □

We also have a relationship between polynomials as elements of $\mathbb{R}[x]$ and polynomials as functions via the above substitution maps. This can be seen by the following theorem.

Theorem 0.2.2.3. *Let $\mathcal{R}$ denote the ring of continuous real-valued functions on $\mathbb{R}^n$. The map*

$$\varphi : \mathbb{R}[x_1, \cdots, x_n] \to \mathcal{R}$$

sending a polynomial to its associated polynomial function is an injective homomorphism.

Proof. Immediate. □

Another set of important ring homomorphisms comes from the following

Integers are an Initial Object

Theorem 0.2.2.4. *For every ring R there is exactly one homomorphism*

$$\varphi : \mathbb{Z} \to R$$

It is the map which takes $\varphi(n) = 1_R + 1_R + \cdots + 1_R$ n times if $n > 0$ and $\varphi(-n) = -\varphi(n)$.

Proof. First we will show uniqueness. Suppose there are two homomorphisms $\varphi, \psi\mathbb{Z} \to R$. Then we must have $\varphi(1) = 1_R = \psi(1)$. Now lets assume φ and ψ agree on all numbers between x, $-n \leq x \leq n$. Then $\varphi(n+1) = \varphi(n) + \varphi(1) = \psi(n) + \psi(1) = \psi(n+1)$. And so by induction $\varphi = psi$ on $\mathbb{Z}$.

Now lets consider the map defined by

- $\varphi(1) = 1_R$
- $\varphi(n+1) = \varphi(n) + 1$
- $\varphi(-n) = -\varphi(n)$

This is the only possible homomorphism from $\mathbb{Z} \to R$. So all that is left is to show that it is an actual homomorphism.

Addition:

First notice that $\varphi(1+1) = \varphi(1) + \varphi(1)$.

Now assume that if $m + n = r$ (and both are positive) then $\varphi(m+n) = \varphi(m) + \varphi(n)$. Now let $s + t = r + 1$. Then we have

$$\varphi(s+t) = \varphi(r+1) = \varphi(r)+\varphi(1) = \varphi(s+(t-1))+\varphi(1) = \varphi(s)+\varphi(t-1)$$

And so by induction we have φ commutes with addition.

Multiplication:

First notice that $\varphi(1 * r) = \varphi(1) * \varphi(r) = \varphi(r)$.

Now assume that $\varphi(m * n) = \varphi(m) * \varphi(n)$. We then have

$$\varphi((m+1)*n) = \varphi(m*n+m) = \varphi(m)*\varphi(n)+\varphi(m) = (\varphi(m)+\varphi(1))*\varphi$$

And so by induction (and the previous result concerning addition) we have φ commutes with multiplication and hence is a homomorphism. □

0.3 Ideals and Kernels

0.3.1 Definitions

Kernel of a Homomorphism

Definition 0.3.1.1. Let

$$\phi : R \to R'$$

be a ring homomorphism. We the define the Kernel of ϕ to be

$$\{r \in R : \phi(r) = 0\}$$

Definition of Ideal

Definition 0.3.1.2. An Ideal of a ring R is a set I such that

- $(I, +, 0)$ is a subgroup of $(R, +, 0)$

- If $a \in I$ and $r \in R$ then $ra \in I$

Lemma 0.3.1.3. *$I \subseteq R$ is an ideal if and only if $I \neq \emptyset$ and*

$$(\forall a_i \in I, r_i \in R)\Sigma_i r_i a_i \in I$$

Proof. Immediate □

Lemma 0.3.1.4. *If $a \in R$ then the set $\{ra : r \in R\}$ is an ideal. This ideal is denoted (a) or Ra or aR. It is called a Principle Ideal*

Proof. Immediate. □

Lemma 0.3.1.5. *Let $\varphi : R \to R'$ be a homomorphism. Then $ker(\varphi)$ is an ideal.*

Proof. *********HOMEWORK********* □

MAYBE:

Give examples of kernels in the polynomial ring, or the

ring $\mathbb{Z}/(n)$.

Zero, Unit and Proper Ideals

Definition 0.3.1.6. Let R be a ring. Then the set $\{0\}$ is an ideal of R called the zero ideal and denoted (0).

R is also an ideal called the unit ideal and denoted (1). It is the only idea which contains a unit.

An ideal is called a proper ideal if it is not (0) or (1).

Theorem 0.3.1.7. *(a) Let F be a field. Then the only ideals of F are (0) and (1)*

(b) If a ring R has exactly two ideals then it is a field.

Proof. (a): HOMEWORK

(b): The two facts we need to prove about R to show that it is a field are

(1) R is not the zero ring

(2) Every non-zero element of R has an inverse.

To show (1) observe that if R is the zero ring then it has only one element. As such the zero ring has only one ideal and so our ring isn't the zero ring.

This means that $0 \neq 1$ and so $(0) \neq (1)$ and hence these must be the only two ideals of our ring.

Let $a \in R$ be a non-zero element. Then $(a) \neq (0)$ because $a \in (a)$. Therefore $(a) = (1)$. This implies that $1 \in (a)$ and hence $1 = ra$ for some $r \in R$. Hence a has an inverse and we are done. □

Corollary 0.3.1.8. *Let F be a field and R a non-zero ring. Then every homomorphism $\varphi : F \to R$ is injective.*

Proof. We know that either $ker(\varphi) = (0)$ or $ker(\varphi) = (1)$.

But we can't have $ker(\varphi) = (1)$ because then φ is the constant function and in particular we have $\varphi(0) = \varphi(1)$ and so R must be the zero ring.

Now $\varphi(a) = \varphi(b)$. Then $\varphi(a - b) = 0$ and so $a - b \in ker(\varphi) = (0)$ and hence $a = b$ and φ is injective. □

Theorem 0.3.1.9. *Every ideal in the ring $\mathbb{Z}$ is principle.*

Proof. We know that every subgroup of the additive group $\mathbb{Z}^+$ is of the form $n\mathbb{Z}$ (by previous theorems from last semester). Hence every ideal must be of this form and hence principle. □

Characteristic of a Ring

Definition 0.3.1.10. The Characteristic of a ring R is the generator of the kernel of the unique homomorphism $\varphi : \mathbb{Z} \to R$

Notice that for instance the characteristic of $\mathbb{Z}/(p)$ is p

Remainder Theorem for Polynomials

Theorem 0.3.1.11. *Let R be a ring and let f, g be polynomials in $R[x]$. Assume that the leading coefficients of f is a unit in R. Then there are polynomials $q, r \in R[x]$ such that*

$$g(x) = f(x)q(x) + r(x)$$

such that the degree of r is less than the degree of f or $r = 0$

Proof. **********HOMEWORK Proposition 10.3.19 ********** □

Division by Roots of a Polynomial

Corollary 0.3.1.12. *Let $g(x)$ be a monic polynomial in $R[x]$ and let α be an element of R such that $g(\alpha) = 0$. Then $x - \alpha$ divides $g \in R[x]$*

Proof. We know that $g(x) = f(x)(x - \alpha) + \beta$ where $\beta \in R$. But then $g(\alpha) = \beta = 0$. □

Ideals of Polynomial Ring over a Field are Pri

Theorem 0.3.1.13. *Let F be a field. Every ideal in the ring $F[x]$ is principle*

Proof. Let I be an ideal of $F[x]$. Since (0) is principle we can assume that $I \neq (0)$. Next lets choose an non-zero polynomial $f(x) \in F(x)$ of minimal degree. Now we want to show that $I = (f)$.

First observe that we must have $(f) \subseteq I$. Now let let $g(x) \in I - f(x)$. We then have by the remainder theo-

rem that $g(x) = f(x)q(x) + r(x)$ where $r(x)$ has degree less than that of $f(x)$ (because otherwise $r(x) = 0$ and so $g(x) \in (f)$). But then we have $g(x) - f(x)q(x) \in I$ and has degree less than that of $f(x)$. $\Rightarrow\Leftarrow$

Hence $I = (f)$ $\square$

Greatest Common Divisor of Polynomials ove

Corollary 0.3.1.14. *Let F be a field and let $f, g \in F[x]$ which are both non-zero. Then there is a unique monic $d(x) \in F[x]$ called the greatest common divisor of f and g such that*

(a) d generates the ideal (f, g) of $F[x]$ generated by f and g

(b) d divides f and g

(c) If h is any divisor of f and g then h divides d

(d) There are polynomials $p, q \in F[x]$ such that $d = pf + qg$

Proof. Let d be such that $(f, g) = (d)$. □

0.4 TODO

- Flush out the outline of math.
- Go through Lang's book on the same topics.