# Lecture Notes Math 371: Algebra (Fall 2006)

by Nathanael Leedom Ackerman

October 10, 2006

**TALK SLOWLY AND WRITE NEATLY!!**

## 0.1 Quotient Rings and Relations

### 0.1.1 Theorems

**Definition 0.1.1.1.** Let $\langle R, +, \times \rangle$ be a ring and let $I \subseteq R$ be an ideal. Define $R/I$ = cosets of $R$ as a group under $+$.

**Theorem 0.1.1.2.** *Let $I$ be an ideal of a ring $R$*

*(a) There is a unique ring structure on the set $R/I$ such that the canonical map $\pi : R \to R/I$ sending $a \rightsquigarrow a + I$ is a homomorphism.*

*(b) The kernel of $\pi$ is $I$*

*Proof.* Part (a):

The first thing to note is that $R^+$ is an abelian group and $I$ is a normal subgroup of $R^+$ and so given co set

$\overline{a} = a + I$ and $\overline{b} = b + I$ we can define the coset

$$\overline{a} + \overline{b} = \{r + s : r \in a + I, s \in b + I\}$$

just as we did in the case of groups.

So all that is left is to define $\overline{a}\overline{b}$. The problem is that in general

$$P = \{rs : r \in a + I, s \in b + I\}$$

is not an ideal. But, it is contained in a single ideal $ab+I$. To see this note that if we let $r = a + u$ and $s = b + v$ then

$$rs = (a + u)(b + v) = ab + (av + bu + uv) \in ab + I$$

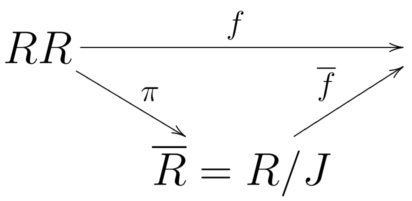
Further, this is the unique coset which $P$ is a subset of because the cosets partition $R$. Hence we can let $\pi(ab) = ab + I$. And the rest of the proof of part (a) is the same as the case for groups.

<u>Part (b):</u>

So obviously $I \subseteq ker(\pi)$. Now suppose $x \in ker(\pi)$. We then have $x + I = 0 + I = I$ and so $x \in I$. □

**Theorem 0.1.1.3** (Mapping Property of Quotient Rings)**.** *Let $f : R \to R'$ be a ring homomorphism with kernel $I$ and let $J$ be an ideal which is contained in $I$. Denote $R/J$ by $\overline{R}$.*

*(a) There is a unique homomorphism $\overline{f} : \overline{R} \to R'$ such that $\overline{f}\pi = f$:*




*(b) <u>First Isomorphism Theorem</u>: If $J = I$ then $\overline{f}$ maps $\overline{R}$ isomorphically to the image of $f$.*

*Proof.* *************TODO Theorem 10.4.2 *************MAYBE GIVE AS HOMEWORK □

**Theorem 0.1.1.4** (Correspondence Theorem)**.** *Let $\overline{R} = R/J$ and let $\pi$ denote the canonical map $R \to \overline{R}$.*

*(a) There is a bijective correspondence between the set of ideals of $R$ which contain $J$ and the set of all ideals of $\overline{R}$, given*

$$I \rightsquigarrow \pi(I) \text{ and } \overline{I} \rightsquigarrow \pi^{-1}(\overline{I})$$

*(b) (Third Isomorphism Theorem) If $I \subset R$ corresponds to $\overline{I} \subset \overline{R}$, then $R/I$ and $\overline{R}/\overline{I}$ are isomorphic rings.*

*Proof.* Part (a):

We need to check

(i) If $I$ is an ideal of $R$ which contains $J$ then $\pi(I)$ is an ideal of $\overline{R}$

(ii) If $\overline{I}$ is an ideal of $\overline{R}$ then $\pi^{-1}(I)$ is an ideal of $R$.

(iii) $\pi^{-1}(\pi(I)) = I$ and $\pi(\pi^{-1}(\overline{I})) = \overline{I}$

Item (i)

Now we know the image of a subgroup is a subgroup so to show that $\pi(I)$ is an ideal we just need to show that $\pi(I)$ is closed under multiplication by elements of $\overline{R}$. Let $\overline{r} \in \overline{R}$ and let $\overline{x} \in \overline{I}$. We can write $\pi(r) = \overline{r}$ and $\pi(x) = \overline{x}$ for some $x \in I, r \in R$. But then $\overline{rx} = \pi(rx)$ and $rx \in I$ (because $x$ is). Notice that we haven't used the assumption that $I \subseteq J$ yet however the fact that $\pi$ is surjective is essential.

Item (ii)

Let $\varphi : \overline{R} \to \overline{R}/\overline{I}$. Now since $\varphi$ is surjective so is $\varphi \circ \pi$. Further, $ker(\varphi \circ \pi) = \{r \in R : \pi(r) \in ker(\varphi) = I\} = \pi^{-1}(I)$. Hence $\pi^{-1}(I)$ is an ideal.

Part (b):

The first isomorphism theorem also shows us that $R/\pi^{-1}(I)$

is isomorphic to $\overline{R}/\overline{I}$.

<u>Item (iii)</u>

First note that for any map of sets $\pi^{-1}(\pi(I)) \supset I$ and $\pi(\pi^{-1}(\overline{I})) \subset \overline{I}$. And further, for any surjective map $\pi$, $\pi(\pi^{-1}(\overline{I})) = \overline{I}$.

To see $\pi^{-1}(\pi(I)) \subset I$ we need that $I \supset J$. Let $x \in \pi^{-1}(\pi(I))$. Then $\pi(x) \in \pi(I)$ and so there is an element $y \in I$ such that $\pi(y) = \pi(x)$. Since $\pi$ is a homomorphism we have $\pi(x - y) = 0$ and hence $x - y \in J = ker(\pi)$. Since $y \in I$ and $J \subseteq I$ this means that $x \in I$ and we are done. □

### 0.1.2 Examples

One intuitive way to think about what is going on when we take the map $\pi : R \to R/I$ is that we are setting all the elements of $I$ "equal to 0". This is witnessed by the fact that $I = Ker(\pi)$.

One easy example is consider the ring $\mathbb{Z}/(p)$. This ring has characteristic $p$ and can be gotten from the ring $\mathbb{Z}$ by setting every element of $(p)$ or equivalently every multiple of $p$ to 0.

Another example is consider the map $\zeta_\alpha : \mathbb{R}[x] \to \mathbb{R}$ which is evaluation of $x$ at $\alpha$. Then

$\Sigma_i a_i x^i \in Ker(\zeta_\alpha) \Leftrightarrow \zeta_\alpha(\Sigma_i a_i x^i) = 0 \Leftrightarrow (\Sigma_i a_i \alpha^i) = 0 \Leftrightarrow (x-\alpha)|(\Sigma_i a_i x$

## 0.2 Adjoining an element

Another procedure we will now study for creating rings is to adjoin an element to the ring.

**Definition 0.2.0.1.** Let $R$ be a ring such that $R \subseteq R'$

where $R'$ is a ring. Then we say that $R'$ is a ring extension of $R$.

**Definition 0.2.0.2.** Let $R'$ be a ring extension of $R$ and let $\alpha \in R' - R$. We then define

$$R[\alpha] = \{\Sigma_{i \leq n} r_i \alpha^i : r_i \in R\}$$

We say that $R[\alpha]$ is generated by $R$ and $\alpha$

Now the by the substitution principle we have

**Theorem 0.2.0.3.** *Let $R \subseteq R'$ and let $\alpha \in R'$. Then there is a unique map*

$$\varphi : R[x] \to R'$$

*such that $\varphi$ is the identity on $R$ and takes $x \rightsquigarrow \alpha$. Further, $R[\alpha] = im[\varphi]$*

*Proof.* Immediate from the Substitution Theorem. □

So, we have that $R[x]$ is a universal solution to the problem of adjoining a new element.

### 0.2.1 Examples

## Construction of Complex Numbers

The example which we want to keep in mind when considering adjoining new elements is case of the complex numbers over the reals. Specifically we find that

$$\mathbb{C} = \mathbb{R}[i]$$

So we know that there is a map

$$\varphi : \mathbb{R}[x] \to \mathbb{C}$$

which is constant on $\mathbb{R}$ and takes $x \rightsquigarrow i$. But we also know that $\varphi$ is surjective and so $\mathbb{C} = im(\varphi) = \mathbb{R}[x]/ker(\varphi)$.

But $p(x) = \Sigma_{j<n} r_j x^j \in ker(\varphi)$ if and only if $p(i) = \Sigma_{j<n} r_j i^j = 0$ and so $p(x) \in ker(\varphi) \leftrightarrow (x^2+1)$ divides $p(x)$.

Hence $ker(\varphi) = (x^2+1)$ and we see that $\mathbb{C} \cong \mathbb{R}[x]/(x^2+$

1).

**Construction of Infinitesimals** Similar to the constriction of the complex numbers we can just the previous results to add infinitesimals to our ring.

**Definition 0.2.1.1.** Let $R$ be a ring. $\epsilon \in R$ is called an Infinitesimal or nilpotent element if $\epsilon^2 = 0$.

**Theorem 0.2.1.2.** *If $R$ is a ring and $R'$ is a ring extension of $R$ such that there is an $\epsilon \in R' - R$ which is nilpotent then $R[\epsilon] \cong R[x]/(x^2)$*

*Proof.* This is immediate from the Substitution Principle. □

### 0.2.2 Theorems

This leads to the following theorem.

**Theorem 0.2.2.1.** *Let $R$ be a ring and let $f(x)$ be a monic polynomial of positive degree $n$ with coeffi-*

*cients in R. Let $R[\alpha]$ denote the ring obtained by adjoining an element satisfying $f(\alpha) = 0$. The elements of $R[\alpha]$ are in bijective correspondence with vectors $(r_0, \dots, r_{n-1}) \in R^n$ via a map $\eta$. Where*

$$\eta(r_0, \dots, r_{n-1}) = r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{n-1}\alpha^{n-1}$$

*Proof.* *************TODO Theorem 10.5.7 *************

□

It is more difficult to analyze the structure of rings obtained by adjoining an element satisfying a non-monic polynomial. Now we will consider a special case of adjoining an element satisfying a non-monic polynomial, that of adjoining an inverse.

Let $R$ be a ring and let $a \in R$. $a$ has an inverse $\alpha$ if and only if $a\alpha - 1$. So, in the ring $R[x]/(ax - 1)$ $x$ is an inverse to $a$. Let us call ring $R[x]/(ax - 1) = R[\alpha]$

Now while $R[\alpha]$ doesn't have a basis in the sense of the previous theorem we do know that every element $b \in R$ is of the form

$$b = \Sigma_{i \leq n} r_i \alpha^i$$

However, this does up a new questions. If we adjoin an element $x$ with some relation to our ring $R$ when is $R$ a subring of $R[x]/I$?

Now we know that there is a canonical map

$$\psi : R \rightarrow R[x] \rightarrow R[x]/I$$

And it is clear that the $ker(\psi) = R \cap I$.

It then follows from the previous theorem that if $I = (p(x))$ where $p(x)$ is a monic polynomial then $ker(\psi) = 0$ and so $\psi$ is injective.

However, this is not always the case. For example suppose we wanted to adjoin an element $\alpha$ which was the inverse of 0. Then in this case we must have $R[\alpha] = 0$ the 0 ring, because that is the only ring in which 0 has an inverse.

To be precise this gets us

**Theorem 0.2.2.2.** *Let $R$ be a ring and let $a, b \in R$ such that $ab = 0$. Further let $c \in R[\alpha]$ be such that $\psi(a)c = 1$ where $\psi : R \to R[\alpha]$. Then if $R[\alpha] \neq 0$ we must have $\psi(b) = 0$.*

*Proof.* We have

$$R[x]/(ax - 1) \cong R[c] \rightarrowtail R[\alpha]$$

But $b = -b(ax - 1) \in (ax - 1)$ (the ideal) and hence $\psi(b) = 0$ □

**Definition 0.2.2.3.** We say an element $b$ of a ring $R$ is a Zero Divisor if there is a non-zero element $a$ such that $ab = 0$

## 0.3 TODO

- Flush out the outline of math.
- 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.