Math 457: Honros Algebra 4

Jacob Reznikov

January 24, 2021

Abstract

My course notes for Math 457

1 Rings

1.1 Ring basics

Definition 1.1.1. *A set R with operations $+$ and $\cdot$ is called a* ***Ring*** *if:*

- $(R, +)$ *is an abelian group*
- $(R, \cdot)$ *is a semigroup (an associative operation). we write* $a \cdot b = ab$
- $\cdot$ *distributes over* $+$ *I.e:*
$$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca$$

Remark 1.1.2. In most cases, $(R, +)$ is finitely generated and so we have

$$R \cong \mathbb{Z}^n \times \mathbb{Z} / n_1\mathbb{Z} \ldots$$

This comes from a fundamental theorem for abelian groups. If

$$R \cong \mathbb{Z}^n$$

We call R 'torsion free'. In that case giving R a multiplication is equivalent to bestowing an integer tuple, a distributive multiplication.

Remark 1.1.3. If $n = 1$, i.e $R \cong \mathbb{Z}$ then the ring structure is essential unique, this is not true in general.

We now list some useful properties

- 0 is absoring, in that $0 \cdot r = r \cdot 0 = 0$

Definition 1.1.4. *A ring R is unital if $(R, \cdot)$ has a unit 1 (was assume $1 \neq 0$)*

Remark 1.1.5. In a ring, $(R, +)$ is necessarily abelian (proof requires a unit)

Definition 1.1.6. *A ring is commutative if $(R, \times)$ is abelian, i.e. $rs = sr, \forall r, s \in R$*

Example 1.1.7. The Gaussian integers:

$$\mathbb{Z}[i] = \{a + ib, a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

Example 1.1.8. The Eisenstein's integers:

$$\mathbb{Z}[w] = \{a + bw, a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$$

where w solves $w^3 = 1$ and $w \neq 1$

These aer two *different* examples of ring structures $\mathbb{Z}^2$. An interesting question about these could be if they have Euclidean division (later).

Example 1.1.9. We also have

$$H_{\mathbb{Z}} = \{a + bi + cj + dk, a, b, c, d \in \mathbb{Z}\}$$

where i, j, k are **quaternions**.

Example 1.1.10. Let K be a field and G a group, then $R = KG$ is a group ring.

$$KG = f : G \longrightarrow K \text{ f has finite support}$$

We can then define the operation on this ring as

$$(f \cdot g)(z) = \sum_{xy \in z} f(x) g(y)$$

This operation is called a convolution.

1.2 Group Ring

Recall the previous definition of a group ring KG.
We often denote an element of this ring as

$$f = \sum_{s \in G} a_s s$$

Where this means $f(s) = a_s$.
The strength of this notation is that multiplication of the polynomials matches multiplication of the elements

Example 1.2.1. Take for an example $e - s \in KG$ where $s \in G$ and e is the identity.
Now suppose that s is of finite order, i.e. $\exists n : s^n = e$. We can then see that

$$(e - s)(e + s + s^2 + \ldots + s^{n-1}) = e - s^n = e - e = 0$$

Then $(e - s)$ is a zero divisor.

This then presents us with an open problem:

Conjecture 1.2.2. *Suppose G is torsion free (no elements of finite order) then KG has no nonzero zero divsiors.*

1.3 Ring Homomorphism

Remark 1.3.1. Rings may not be unital. However, you can always add a unit formally to every ring.

Example 1.3.2. Let $R = C_0(\mathbb{R})$ which are the continuous functions on $\mathbb{R}$ which converge to 0 at ∞.
Now clearly R does not have a unit since the multiplicative 1 does not converge to 0 at ∞.
So if we do add a unit to R what does that give us?

$$\hat{R} = \mathbb{R}1 \oplus C_0(\mathbb{R})$$

And it turns out that $\hat{R}$ is equivalent to $C(S')$ which are the continuous functions over a circle.

Now we define a Homomorphism on Rings

Definition 1.3.3. *Let R, S be rings. A map $f : R \longrightarrow S$ is a ring homomorphism if it preserves and multiplication:*

$$f(r \pm s) = f(r) \pm f(s)$$
$$f(rs) = f(r)f(s)$$

Remark 1.3.4. f may or may not preserve the units. However, if we assume R has a unit then $f(1)$ is indempotent since $f(1)f(1) = f(1 \cdot 1) = f(1)$.

Example 1.3.5. Define a function $f : M_2(K) \longrightarrow M_4(K)$ that maps

$$M \mapsto \begin{bmatrix} M & 0 \\ 0 & M \end{bmatrix}$$

This function is unital.

Let R, S be a unital ring and $f : R \longrightarrow S$ be a unital homorphism.
Then f is an isomorphism if it is bijective.

Definition 1.3.6. *The kernal of $f : R \longrightarrow S$ is*

$$\ker(f) := \{r \in R, f(r) = 0\}$$

$\ker(f)$ *is an ideal*

Definition 1.3.7. *A left ideal is a subring $I \subseteq R$ such that $rI \subseteq I$ for every $r \in R$. Similarly a right ideal is a subring $I \subseteq R$ such that $Ir \subseteq I$ for every $r \in R$.*

We then get a smiliar concept to a quotient group called a quotient ring

Definition 1.3.8. *Let R be a ring and I be an ideal of this ring then if we think of $(R, +)$ and $(I, +)$ as a groups. This gives us R / I as a quotient group.*
Now elements of this group can be written as $s + I$ for $s \in R$ and so we can define a multiplication on this quotient group,

$$(s + I)(t + I) = st + I$$

This defines a new ring which we call the quotient ring.

Now in order to really check this multiplication is well defined we need to check that if $s' \in s+I$ and $t' \in t + I$ then

$$(s' + I)(t' + I) = (s + I)(t + I)$$

And we get this by

$$(s' + I)(t' + I) = s't' + I = (s + i_1)(t + i_2) + I = st + si_1 + i_2 t + i_1 i_2 + I$$

And since I is a two sided ideal then $si_1, i_2 t, i_1 i_2$ are all in I and so

$$(s' + I)(t' + I) = st + I = (s + I)(t + I)$$

1.4 Isomorphisms Theorem

Theorem 1.4.1 (First Isomorphism Theorem). *$f : R \twoheadrightarrow S$ then* $\ker f$ *is an ideal, and f induces an isomorphism*

$$\Phi : R / \ker f \longrightarrow S$$

Where

$$s + I \mapsto f(s)$$

Theorem 1.4.2 (Second Isomorphism Theorem). *Let R be a ring with $S \subseteq R$ a subring and $I \subseteq R$ an ideal then*

$$S + I = \{s + r, s \in S, r \in R\}$$

Is a subring, and I is an ideal in $S + I$.
On top of that

$$S \twoheadrightarrow S + I / I$$

Is surjective with kernal $S \cap I$ and so

$$S / S \cap I \cong S + I / I$$

Theorem 1.4.3 (Third Isomorphism Theorem). *Let $I \subseteq J \subseteq R$ and I, J are ideals then*

$$R / I \twoheadrightarrow R / J$$

With kernal J / I

$$R / J \cong \frac{(R / I)}{(J / I)}$$

Theorem 1.4.4 (Fourth Isomorphism Theorem). *Let $f : R \twoheadrightarrow S$ be a surjective homorphism, then there is a bijection between Subrings of R containing $\ker f$ and Subrings of S.*

1.5 Characteristic Ring

Theorem 1.5.1. *Let R be a unital ring then there exists a unique homomorphism $f : \mathbb{Z} \longrightarrow R$*

$$f(n) = f(1 + 1 + \cdots + 1) = f(1) + f(1) + \cdots + f(1) = n \cdot 1$$

Definition 1.5.2. *The non negative integer such that $\ker f \cong n\mathbb{Z}$ is called the Characteristic of R.*

Definition 1.5.3. $\operatorname{Im} f$ *is called the Characteristic subring of $\mathbb{Z}$*

Example 1.5.4. $\operatorname{Char}(\mathbb{Z} / n\mathbb{Z}) = n$

Remark 1.5.5. Suppose that every subring of R is an ideal, then $R \cong \mathbb{Z}$ or $R \cong \mathbb{Z} / n\mathbb{Z}$. Notice that if the characteristic subring is an ideal, then since it contains 1 then $x \cdot 1$ is in the Characteristic subring for any x and so R is its own characteristic ideal, which means it is generated by 1 additively and so it is isomorphic to $\mathbb{Z}$ or $\mathbb{Z} / n\mathbb{Z}$.

Proposition 1.5.6. Suppose that R contains no zero divisors. Then $\operatorname{Char}(R) = 0$ or a prime number.

Proof. If $\operatorname{Char}(R) = n$ and n is composite then

$$\mathbb{Z} / n\mathbb{Z} \hookrightarrow R$$

And so since $\mathbb{Z} / n\mathbb{Z}$ contains zero divisors for n composite then so does R □

1.6 Algebra over a ring

Definition 1.6.1. *Let R be a commutative ring. An Algebra over R is a ring A together with a ring homomorphism $\eta : R \longrightarrow A$ such that $\eta(s)$ commutes multiplicatively with all elements of A.*

We think of this as scalar multiplication of A by R as it acts exactly like it (mainly the commutativity part).
To further cement this, notice that if R is a field then this is exactly a vector space, with scalar multiplication being

$$R \times A \longrightarrow A : (s, a) \mapsto \eta(s) \cdot a$$

Remark 1.6.2. A ring can always be viewed as an algebra over $\mathbb{Z}$(add multiple times) or over its Characteristic subring, or over its center.

Example 1.6.3. $A = Map(X, \mathbb{R})$ which is the sets of all functions from $\mathbb{R}$, it is an algebra over $\mathbb{R}$ using $\eta(n) = n$

Example 1.6.4. The group ring KG is an algebra over K.

2 Units and Zero divisors

2.1 Invertible elements

Definition 2.1.1. *An element $r \in R$ is invertible if there exists $s \in R$ such that*

$$rs = sr = 1$$

the set of invertible elements is a group $R^\times$ called, the group of units

Example 2.1.2. Recall the Gaussian integers $\mathbb{Z}[i]$, then its group of units is

$$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\} \cong \mathbb{Z} / 4\mathbb{Z}$$

Example 2.1.3. Recall the Eisenstein integers $\mathbb{Z}[w]$, its group of units is

$$\mathbb{Z}[w]^\times = \{\pm w, 1\} \cong \mathbb{Z} / 3\mathbb{Z}$$

Notice that this proves that these two rings are not isomorphic

Example 2.1.4. If $R = M_n(K)$ then $R^\times = GL_n(K)$

Now the main point of this chapter is to adjoin inveres to certain elements in a ring

Example 2.1.5. $n \in \mathbb{Z}$ and we can find its inverse in $\frac{1}{n} \in \mathbb{Q}$

Fields are the rings with the largest possible set of invertible elements, i.e. in a field $\mathbb{F}$ we have

$$F^\times = F \setminus \{0\}$$

2.2 Adding inverses to non invertible elements

Let $R = K[X]$ where k is a field be the ring of polynomials over this field, we have two constructions of the inverse for the elements of R.

We have $K[x] \subseteq K(x)$ where

$$K(x) = \left\{ \frac{f}{g}, f, g \in K[x] \wedge g \neq 0 \right\}$$

But we also have

$$K[x] \subseteq K[[x]]$$

Where $K[[x]]$ is called the ring of formal power series.

Definition 2.2.1. *Let K be a field then $K[[x]]$ is called the ring of formal power series. An element of this ring is of the form*

$$f = \sum_{n=0}^{\infty} a_n x^n$$

Remark 2.2.2. This addition is not real addition, we never compute the value at a certain input x. We only treat this as a construct for a sequence of coefficients a_n

Where addition is

$$(a_n)_n + (b_n)_n = (a_n + b_n)_n$$

And multiplication is

$$(a_n)(b_n) = \left(\sum_{k=0}^{n} a_k b_{n-k} \right)_n$$

We can see then that $\sum x^n$ is the inverse of $1 - x$ in this wrong and so this ring does add extra inverses we didn't have before. However, this is not a field, since x doesn't have an inverse in this ring (a simple proof of this is noticing that x shifts all coefficients by 1).

An interesting question then, is what is the group $K[[x]]^\times$ this is left as a question

Definition 2.2.3. *We define $K((x))$, the field of formal laurent series to be*

$$K((x)) = \{(a_n)_{n\in\mathbb{Z}} \text{ such that } a_n = 0 \text{ if } n < N \text{ for some } N \in \mathbb{Z}\}$$

2.3 Zero Divisors

For a ring to be embed into a field, it should not contain zero divisors.

Definition 2.3.1. *An element $r \in R$ is a* ***zero divisor*** *if $\exists s \neq 0$ such that $rs = 0$*

Proposition 2.3.2. If $R \hookrightarrow K$ where K is a field, then R does not contain nonzero zero divisors.

Proof.

$$\frac{1}{r} = \frac{s}{rs} = \frac{s}{0}$$

□

Remark 2.3.3. The set of zero divisors is not a subring, for example take two fields K, L then $K \times L$ has the following zero divisors

$$\{(0,0)\} \cup \{(k,0), k \in K\} \cup \{(0,l), l \in L\}$$

On the other hand the complement of this set, the set of non zero divisors is multiplicative and is stable under product, and is thus a submonoid of $(R, \cdot)$

A nilpotenent element ($s^n = 0, n \geq 1$) is a zero divisor.

Proposition 2.3.4. An element $r \in R$ is not a zero divisor iff it can be cancelled,

$$rs = rt \implies s = t$$

Definition 2.3.5. *A ring is* ***left cancellative*** *if it does not contain left zero divisors.*

Definition 2.3.6. *An* ***integral domain*** *is a ring which is unital, commutative, and cancellative.*

Proposition 2.3.7. Every integral domain R embeds naturally into a field K called the field of fractions of R which is denoted $Q = Frac(R)$.

2.4 Field of fractions

Definition 2.4.1. *Let R be an integral domain then we define*

$$Frac(R) = \left\{ \frac{p}{q}, p, q \in \mathbb{R} \; : \; q \neq 0 \right\}$$

Where a fraction $\frac{p}{q}$ is an equivalance calss of pairs (p, q) where

$$(p, q) \sim (p', q') \iff p'q = q'p$$

Proof. Now we need to check that this is an equivalence relationship. Transitivity is the only non trivial property

$$p_1 q_2 = p_2 q_1 \implies p_1 q_3 q_2 = p_2 q_1 q_3 = p_3 q_2 q_1$$

Now since R is cancellative we can write

$$p_1 q_3 q_2 = p_3 q_2 q_1 \implies p_1 q_3 = p_3 q_1$$

And thus this relation is transitive.

We can then define addition and multiplication on this new set

$$\frac{p}{q} + \frac{p'}{q'} = \frac{pq' + p'q}{qq'}$$

$$\frac{p}{q} \cdot \frac{p'}{q'} = \frac{pp'}{qq'}$$

□

There is a canonical embedding $R \hookrightarrow Frac(R) \; : \; r \mapsto \frac{r}{1}$

A similar construction works if R is commutative. In fact, we can always embed a ring R into a larger ring in which every nonzero divisor is invertible.

We can describe this in a more general fashion

Definition 2.4.2. *Let S be a multiplicative subset of R (submonoid). We construct*

$$S^{-1}R = \left\{ \frac{p}{q} : p \in R, q \in S \right\}$$

With all elements of S inverted. This is a ring.

Proof. We first define a new equivalence relation on pairs

$$(r, s) \sim (r', s') \iff \exists t \in S : t(rs' - r's) = 0$$

The equivalence class is denoted

$$\frac{r}{s}$$

We still have a homomorphism

$$\begin{aligned} R &\longrightarrow S^{-1}R \\ r &\longmapsto \frac{r}{1} \end{aligned}$$

□

Remark 2.4.3. Suppose S contains a zero divisor, i.e. $\exists s \in S : \exists r \in R : rs = 0$ then

$$r \longmapsto \frac{r}{1} = \frac{rs}{s} = 0$$

So this map is no longer injective.

If S contains 0 then the condition of equivalence is always true and so there is only 1 equivalence class and so this is the zero ring $1 = 0$.

$$\ker(R \longrightarrow S^{-1}R) = \{r \in R : \exists s \in S : rs = 0\}$$

And so $R \longmapsto S^{-1}R$ is injective if S does not contain zero divisors of R.

Proposition 2.4.4. Let S be a multiplicative set of nonzero divsiors in R. Then there exists a natural ring $S^{-1}R$ and an embedding $R \hookrightarrow S^{-1}R$ in which every element in S becomes a unit in $S^{-1}R$

Example 2.4.5. We want to adjoin an inverse for 2 in the ring $\mathbb{Z} / 6\mathbb{Z}$ but then since $3 \cdot 2 = 0$ then the homomorphism between then $\langle 2 \rangle^{-1}\mathbb{Z} / 6\mathbb{Z}$ does not have an injection from $\mathbb{Z} / 6\mathbb{Z}$. This also becomes clear since $\frac{1}{1} = \frac{3}{1}$ in this ring.

Example 2.4.6. Let P be a set of only primes and $S \langle P \rangle$.

Proposition 2.4.7. The set of unital subrings in $\mathbb{Q}$ is the cantor space of all subsets of the set of prime numbers.

2.5 A comment on the 4-th isom theorem

$f : R \twoheadrightarrow R'$, the 4-th isomoprhism theorem only works for surjective homomorphism. If f is not a surjective then $f(I)$ may not be an ideal.

Example 2.5.1. $\mathbb{Z} \hookrightarrow \mathbb{Q}$ then $n\mathbb{Z}$ is not an ideal.

In general, $f : R \longrightarrow R'$ can be decomposed:

$$R \overset{f}{\twoheadrightarrow} \operatorname{Im} f \hookrightarrow R'$$

But then this changes our problem into, what happens to ideals under inclusion?

Definition 2.5.2. *Let $f : R \longrightarrow R'$ be a homomorphism and $I \triangleright R$ an ideal. Then the extension of I by f is the ideal,*

$$I^f = R'(f(I))$$

which is an ideal in R'.

Example 2.5.3. $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ has

$$(n\mathbb{Z})^f = \mathbb{Q}$$

Proposition 2.5.4. Suppose that $f : R \longrightarrow S^{-1}R$ and S is a multiplicative set of nonzero divisors then

1. $I \longmapsto If$ is surjective onto the set of ideals in $S^{-1}R$
2. $J \longmapsto f^{-1}(J)$ is injective

Remark 2.5.5. If J is an ideal then the ideal $f^{-1}(J)$ is called the contraction of J. The standard notation is I^e for extension and J^c for contraction.

Remark 2.5.6. In fact every ideal J in $S^{-1}R$ is of the form I^f where

$$I = J \cap R = f^{-1}(J)$$

3 Ideals.

3.1 Dedekind.

Dedekind defined real numbers using "Dedekind cuts".

Example 3.1.1. We define $\sqrt{2}$

$$\sqrt{2} = \left\{ r \in Q, r > 0, r^2 > 2 \right\}$$

Dedekind also introduced ideals in a ring, "ideal numbers" (following Kummer), They are also subsets of R. Kummer wanted to fix the lack of prime decomposition in rings. This also has some connections with Fermat's Last Theorem.

3.2 Ideals generated by subsets

Let R be a unital ring.

Definition 3.2.1. *The ideal* (S) *generayed by a set* $S \subseteq R$ *is the intersection of all the ideals that contain* S*.*

Example 3.2.2. If $r \in R$ then

$$(r) = RrR = \left\{ \sum_{i \in E} s_i r t_i, s_i, t_i \in R \right\}$$

Example 3.2.3. If R is commutative then

$$(r) = Rr = sr, s \in R$$

Proof. Rr is an ideal containing r. Every ideal containing r must containin Rr and so $(r) = Rr$. □

These ideals are called principal ideal (simply generayted).

Definition 3.2.4. *A ring is called a principal ring if it only has principal ideals.*

Definition 3.2.5. *A principal ideal domain, is an integral domain where every ideal is principal*

Example 3.2.6. In $\mathbb{Z}$ all ideals are $n\mathbb{Z} = (n)$. Inclusion of ideals

$$(n) \subseteq (m) \iff m|n$$

This is true for principal ideals in a general commutative ring.

Proof. In an integral domain, the principal ideals determine their generator up to a unit.

$$(r) = (s) \implies r = as \wedge s = br \implies r = abr \implies r(1 - ab) = 0$$

And so in an integral domain we have $(1 - ab) = 0$ and so $ab = 1$. □

Definition 3.2.7. *Let* $r, s \in R$ *then if* $r = as$ *for some unit* a *then we call* r *and* s *unit associate.*

Example 3.2.8. In $\mathbb{Z}$ we have the set of all ideals be $\mathbb{N}$, through $n \mapsto n\mathbb{Z}$

Remark 3.2.9. In a principal ideal domain (PID) the set of ideals is the quotient of R by the action of the group $R^\times$ through $a : r \mapsto ar$.

This action is free on $R \setminus \{0\}$

$$(1 - a)r = 0 \implies (1 - a)r = 0$$

Definition 3.2.10. *Stabilisers are trivial*