LECTURE NOTES FOR 427: PART 2

CHARLES REZK

1. Rings

Recall that a ring is \((R, +, \cdot)\), consisting of a set \(R\) and two binary operations called “addition” and “multiplication”:

\[ +: R \times R \to R, \quad \cdot: R \times R \to R, \]

- \((R, +)\) is an additive group,
- \((R, \cdot)\) is a monoid, and
- multiplication distributes over addition:

\[ a(b + c) = (ab) + (ac), \quad (a + b)c = (ac) + (bc). \]

The identity for + is conventionally called 0, and the inverse of \(a\) under + is called \(-a\). The identity for \(\cdot\) is called 1.

A ring is said to be commutative if multiplication is commutative: \(ab = ba\) for all \(a, b \in R\).

We have already discussed several examples of rings, including matrix rings; fields, including complex numbers; quaternions. Here are some more.

1.1. Example (Rings of functions). For any set \(X\) and ring \(R\), let \(S := \mathcal{F}(X, R) = \{f: X \to R\}\) be the set of all functions. Then \(S\) is a ring, with operations given by “pointwise” addition and multiplication:

\[ (f + g)(x) := f(x) + g(x), \quad (fg)(x) := f(x)g(x). \]

(Exercise: check that this is a ring.) For instance, the set \(\mathcal{F}(\mathbb{R}, \mathbb{R})\) of real valued functions on \(\mathbb{R}\) is a ring.

If \(S\) is a ring, a multiplicative inverse of an element \(a \in S\) is an element \(b \in S\) such that \(ab = 1 = ba\).

Clearly not all elements of a ring can have a multiplicative inverse. For instance, \(0 \in \mathbb{R}\) has none.

1.2. Exercise. If \(a \in S\) has a multiplicative inverse, then this inverse is unique. (Same as the proof for inverses in groups.)

We write \(S^\times \subseteq S\) for the set of elements which have multiplicative inverses.

1.3. Exercise. \((S^\times, \cdot)\) is a group.

Examples: \(\mathbb{R}^\times = \mathbb{R} \setminus \{0\}\), \(\mathbb{Z}^\times = \{\pm 1\}\), \((\mathbb{Z}/n)^\times = \Phi(n)\), \(M_{n\times n}(\mathbb{R})^\times = GL_n(\mathbb{R})\).

We say that a ring \(S\) is a division ring if \(S^\times = S \setminus \{0\}\), i.e., every non-zero element has a multiplicative inverse, and 0 does not have one.

A commutative division ring is called a field. For instance, \(\mathbb{R}\) is a field. Also \(\mathbb{Z}/p\) is a field when \(p\) is prime.

Let’s carefully construct some more examples of rings.
2. Subrings

A subring of a ring \( R \) is a subset \( S \subseteq R \) such that (i) the + and \( \cdot \) operations restrict to \( S \), and make \( S \) a ring in its own right, and (ii) \( R \) and \( S \) have the same multiplicative identity. Here is the subring criterion.

2.1. Proposition. A subset \( S \subseteq R \) of a ring is a subring if and only if

1. \( x,y \in S \) implies \( x + y \in S \), i.e., \( S \) is closed under addition,
2. \( x \in S \) implies \( -x \in S \),
3. \( x,y \in S \) implies \( xy \in S \),
4. \( 1 \in S \), where \( 1 \) denotes the multiplicative identity in \( R \).

Proof. Note that by (4) \( S \) is non-empty. Therefore together with (1) and (2) we see that \((S,+)\) is a subgroup of \((R,+)\). Property (3) implies that multiplication is a binary operation on \( S \). It is straightforward to check the remaining properties (that multiplication is associative, that 1 is a multiplicative identity, the distributive law) on \( S \), because they hold in \( R \). \( \square \)

2.2. Example. The integers \( \mathbb{Z} \) are a subring of \( \mathbb{R} \).

2.3. Example. The rational numbers \( \mathbb{Q} \) are a subring of \( \mathbb{R} \).

2.4. Example. The inclusion \( 2\mathbb{Z} \subseteq \mathbb{Z} \) is not a subring. Although closed under the operations the subset does not have a multiplicative identity.

2.5. Example. Let \( S \subseteq M_{2\times2}(\mathbb{R}) \) be the subset consisting of \( 2 \times 2 \) real matrices of the form
\[
\begin{pmatrix}
a & -b \\
b & a
\end{pmatrix}, \quad a, b \in \mathbb{R}.
\]
We can check that \( S \) is a subring of the ring of matrices. (Verify this.)

2.6. Example (Not a subring). Let \( T = \{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \in \mathbb{R} \} \). This is a subset of the ring \( S = M_{2\times2}(\mathbb{R}) \), which is closed under + and \( \cdot \), and in fact as such it is a ring in its own right: it’s multiplicative identity is \( \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \).

However, we will not consider it as a subring, because the multiplicative identity of \( T \) is not the same as the one for \( S = M_{2\times2}(\mathbb{R}) \), which is the identity matrix. (Note: other sources may differ here, and will consider \( T \) a subring. I won’t however.)

Compare with groups, where if \( H \subseteq G \) is a subset closed under multiplication, and \( H \) has an identity element for its product, then the identity element of \( H \) must be the same as that for \( G \). (The proof of this used the existence of inverses in groups, which we do not assume for multiplication in a ring.) Rings are just different.

2.7. Example. The set \( C(\mathbb{R},\mathbb{R}) \) of continuous functions \( f: \mathbb{R} \to \mathbb{R} \) is a subring \( C(\mathbb{R},\mathbb{R}) \subseteq \mathcal{F}(\mathbb{R},\mathbb{R}) \), commutative with identity. This is because of the fact that sums and products of continuous functions are continuous; it has identity because constant functions are continuous.

3. Homomorphisms and isomorphisms of rings

Let \( R \) and \( S \) be rings. A homomorphism \( \phi: R \to S \) is a function such that

- \( \phi(a + b) = \phi(a) + \phi(b) \) for all \( a,b \in R \),
- \( \phi(ab) = \phi(a)\phi(b) \) for all \( a,b \in \mathbb{R} \), and
- \( \phi(1) = 1 \).

Date: November 3, 2018.
Note: in groups we did not need a condition like (3) for the identity element, because it was true anyway. This is because it was implied by the property that a homomorphism preserve products, which was because elements of groups always have inverses.

Easy fact: if \( \phi \) is a homomorphism, then we also have:
\[
\phi(0) = 0, \quad \phi(-a) = -\phi(a),
\]
since \( \phi \) is also a homomorphism of groups \((R, +) \rightarrow (S, +)\).

3.1. Example (The homomorphism from integers). Let \( R \) be a ring. There is a unique homomorphism of abelian groups \( \phi: \mathbb{Z} \rightarrow R \) which sends the generator 1 of \( \mathbb{Z} \) to 1 \( \in R \). Thus, \( \phi(0) = 0 \) (since 0s are identity elements for additive groups); we have \( \phi(-1) = -1 \) since homomorphisms take inverses to inverses; if \( m > 0 \), we have
\[
\phi(m) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = m \cdot 1.
\]
Similarly, \( \phi(-m) = -m \cdot 1 \).

3.2. Remark. In practice, for any ring \( S \) we usually just write the integer \( m \) to also denote the element in \( S \) given by \( m \cdot 1 \) as above. This can be a little confusing. For instance, it is possible to have a non-zero integer \( n \) whose image in \( S \) is 0, for instance in the ring \( \mathbb{Z}/n \).

3.3. Example. Consider the projection map \( \phi: \mathbb{Z} \rightarrow \mathbb{Z}/n \), defined by \( \phi(x) := [x]_n \). This is a ring homomorphism.

We write \( R^\times \subseteq R \) for the subset of a ring consisting of elements which admit a multiplicative inverse. Note that \((R, \cdot)\) is a group. (But it is not a subgroup of \((R, +)\).)

3.4. Proposition. If \( a \) has a multiplicative inverse, then so does \( \phi(a) \), in which case \( \phi(a)^{-1} = \phi(a^{-1}) \).

Proof. Just verify that \( \phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(1) = 1 \) and \( \phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1) = 1 \). \( \Box \)

3.5. Corollary. If \( \phi: R \rightarrow S \) is a homomorphism of rings, then \( \phi \) restricts to a homomorphism \( R^\times \rightarrow S^\times \) of groups.

An isomorphism of rings is a homomorphism which is a bijection. You can show that the inverse map is also a bijection.

3.6. Proposition. If \( \phi: R \rightarrow S \) is a homomorphism of rings, then \( \phi(R) \) is a subring of \( S \). If \( \phi \) is injective then it defines an isomorphism between \( R \) and \( \phi(R) \).

4. Polynomial rings

For any ring \( S \) we can construct a new ring \( P(S) \), whose elements are “polynomials in one variable with coefficients in \( S \)”. Let \( S \) be any ring. A sequence in \( S \) is a function
\[
a: \mathbb{Z}_{\geq 0} \rightarrow S.
\]
I’ll use the notation \( a_n \in S \) for the value of this function at \( n \), i.e., I’m thinking of \( a \) as an infinite sequence.

We define a new ring \( P(S) \) as follows.
- Elements of \( P(S) \) are sequences \( a: \mathbb{Z}_{\geq 0} \rightarrow S \) for which there exists \( N \in \mathbb{Z}_{\geq 0} \) such that \( a_k = 0 \) for all \( k > N \). only finitely many of the values \( a_k \) are non-zero.
- Addition of elements in \( P(S) \) is defined by the “pointwise addition” rule:
\[
(a + b)_n := a_n + b_n.
\]
We need to make sure these operations are well-defined, because of the requirement that sequences are eventually 0. For instance, given \( a, b \in P(S) \) there is an \( N \) such that \( a_k = b_k = 0 \) for all \( k > N \). Then clearly \( (a+b)_k = 0 \) for \( k > N \), while \( (ab)_k = 0 \) for \( k > 2N \).

4.1. Exercise (Tedious). With this structure \( P(S) \) is a ring. I’ll just note some features of this:

- The additive identity is the zero sequence: \( 0_n = 0 \) for all \( n \).
- Additive inverses are computed “termwise”: \( (−a)_n = −(a_n) \).
- The multiplicative identity is the sequence \( 1 \) defined by \( 1_0 = 1, 1_k = 0 \) for \( k > 0 \).
- If \( S \) is commutative, so is \( P(S) \).
- Associativity of multiplication is the hardest part to prove, but is is not too bad if you are good at multiple summations:

\[
((ab)c)_n = \sum_{i=0}^{n} (ab)_i c_{n-i}
\]

\[
= \sum_{i=0}^{n} \sum_{j=0}^{i} a_j b_{i-j} c_{n-i},
\]

\[
(a(bc))_n = \sum_{k=0}^{n} a_k (bc)_{n-k}
\]

\[
= \sum_{k=0}^{n} \sum_{\ell} a_k b_{\ell} c_{n-k-\ell}.
\]

These work out to the same thing, once you reindex the sums (so that \( k = j \) and \( \ell = i - j \), whence \( n - k - \ell = n - i \)). You will actually understand this better by working it out for small values of \( n \), like 1 or 2 or 3.

We use the following notation when dealing with a polynomial ring.

- Given \( c \in S \), we use the same symbol \( c \) to denote the element of \( P(S) \) defined by the sequence:

\( c_0 := c, \quad c_k := 0 \) if \( k \geq 1 \).

- Let \( S' \subseteq P(S) \) be the set of all \( f \in P(S) \) such that \( f_k = 0 \) if \( k \geq 1 \). Then the above defines a bijection \( S \to S' \), and this bijection is an isomorphism of rings.

- We write \( X \in P(S) \) for the sequence

\( X_1 = 1, \quad X_k = 0 \) if \( k \neq 1 \).

- Note that \( X^n \), the product of \( X \) with itself \( n \) times, is the sequence

\( X_n = 1, \quad X_k = 0 \) if \( k \neq n \).

- Using this notation, we can use the ring structure on \( P(S) \) rewrite any sequence \( a \in P(S) \) as an expression

\( f = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n, \quad a_0, \ldots, a_n \in S, \)

assuming \( a_k = 0 \) for \( k > n \). We often choose to denote such an expression as “\( f(X) \)”, rather than “\( a \)”. 

\( \text{M 5 Nov} \)
In other words, $P(S)$ is the ring of polynomials in one unknown with coefficients in $S$.

**Warning.** Polynomials are not defined as functions, and they are not the same thing as functions. I’ll talk about this later.

Another notation for $P(S)$ is $S[X]$. (This is convenient when we want to name the “variable”.)

4.2. **Exercise (On PS ?).** If $D$ is a domain, then $D[X]$ is a domain.

This is also important because we can iterate the construction. Thus we may consider $P(P(S))$, aka $(S[X])[Y]$. Elements $f$ in this ring are expressions

$$f = g_0 + g_1 Y + g_2 Y^2 + \cdots + g_n Y^n,$$

where each $g_k \in S[X]$, so are expressions

$$g_k = a_{0k} + a_{1k} X + a_{2k} X^2 + \cdots a_{mk} X^m$$

with $a_{ij} \in S$. Using the distributive law, we can always rewrite this as

$$f = \sum_{i=0}^{m} \sum_{j=0}^{n} a_{ij} X^m Y^n.$$

We write $S[X, Y]$ for $(S[X])[Y]$, and call it the ring of polynomials in two variables. As we will see soon, the order of the variables isn’t really important: $(S[X])[Y]$ and $(S[Y])[X]$ are the “same” ring (really, they are canonically isomorphic).

You can go on to define $S[X, Y, Z]$, etc.

5. **Center of a ring**

Given a ring $S$ let

$$\text{Cent}(S) := \{ a \in S \mid ab = ba \text{ for all } b \in S \},$$

called the center of $S$.

5.1. **Exercise (On PS ?).** The set $R = \text{Cent}(S)$ is a subring of $S$. As a ring $R$ is commutative.

Note that if $S$ is commutative, then $\text{Center}(S) = S$.

5.2. **Example.** The center of the quaternion algebra $\mathbb{H}$ is the subset $\mathbb{R}1 = \{ \lambda 1 \mid \lambda \in \mathbb{R} \}$ of scalar quaternions. It’s straightforward to check that scalar quaternions are in the center. To see these are the only ones, check commutativity with $i$, $j$, and $k$. For instance, commutativity with $i$ gives

$$(a1 + bi + cj + dk)i = -b1 + ai + dk - cj,$$

$$i(a1 + bi + cj + dk) = -b1 + ai - dk + ck,$$

which means that if $x = a1 + bi + cj + dk$ is in the center then $c = 0 = d$. Checking commutativity with $j$ gives $b = 0$.

5.3. **Exercise (On PS ?).** Let $S = M_{n \times n}(F)$ where $F$ is a field (e.g., $F = \mathbb{R}$). Then

$$\text{Center}(S) = \{ \lambda I \mid \lambda \in F \},$$

the set of diagonal matrices. Thus $\text{Center}(S) \approx F$. 


6. HOMOMORPHISMS OUT OF A POLYNOMIAL RING

The following proposition tells you how to construct homomorphisms out of a polynomial ring $S[X]$.

6.1. Proposition. Let $S$ and $T$ be rings. Suppose given

1. a ring homomorphism $\phi: S \to T$, and
2. an element $c \in T$, such that
3. $\phi(s)c = c\phi(s)$ for all $s \in S$.

Then there exists a unique ring homomorphism

$$\psi: S[X] \to T$$

such that (i) $\psi(X) = c$ and (ii) $\psi(s) = \phi(s)$ for all $s \in S \subseteq S[X]$.

Note that if $T$ is commutative, then (3) is automatically true.

$$\begin{array}{ccc}
S & \to & S[X] \\
\phi & \downarrow & \uparrow \\
& T \quad \ni \quad X & \\
& \downarrow & \\
& c & \\
\end{array}$$

Proof. Existence. We define $\psi$ by the following rule. If $f \in S[X]$ is given by $f = \sum_{i=0}^{n} a_i X^i$ with $a_i \in S$, then set

$$\psi(f) := \sum_{i=0}^{n} \phi(a_i)c^i.$$ 

Verify directly that this is a ring homomorphism: i.e., that it preserves addition, multiplication, and multiplicative identity.

I’ll do the case of multiplication, which is the only part that needs hypothesis (3). Let $f = \sum_{i} a_i X^i$ and $g = \sum_{j} b_j X^j$. We have

$$\psi(fg) = \psi\left(\left(\sum_{i} a_i X^i\right)\left(\sum_{j} b_j X^j\right)\right)$$

$$= \psi\left(\sum_{\substack{n \atop i=0}} \phi\left(\sum_{\substack{n \atop i=0}} a_i b_{n-i} X^n\right)\right)$$

$$= \sum_{n \atop i=0} \phi\left(\sum_{\substack{n \atop i=0}} a_i b_{n-i}\right)c^n$$

$$= \sum_{n \atop i=0} \phi(a_i)\phi(b_{n-i})c^n$$

$\phi$ is a homomorphism,

while

$$\psi(f)\psi(g) = \psi\left(\sum_{i} a_i X^i\right)\psi\left(\sum_{j} b_j X^j\right)$$

$$= \left(\sum_{i} \phi(a_i)c^i\right)\left(\sum_{j} \phi(b_j)c^j\right)$$

$$= \sum_{n \atop i=0} \phi(a_i)c^i\phi(b_j)c^j$$

$$= \sum_{n \atop i=0} \sum_{j} \phi(a_i)\phi(b_j)c^n$$

condition (3).
Uniqueness. Conversely, given any ring homomorphism \( \psi: S[X] \to T \) such that \( \psi(s) = \phi(s) \) for \( s \in S \), and \( \psi(X) = c \), the properties of ring homomorphisms force the formula that we used as the construction of \( \psi \): ring homomorphisms recover the formula:

\[
\psi(\sum a_i X^i) = \sum \psi(a_i) \psi(X)^i = \sum \phi(a_i) c^i.
\]

\( \square \)

6.2. Example (Evaluating a polynomial on an element). Let \( S \) be a commutative ring (e.g., a field), and let \( \phi: S \to S \) be the identity map. Then for any \( c \in S \) we get a homomorphism \( \epsilon_c: S[X] \to S \) defined by

\[
\epsilon_c(\sum a_i X^i) := \sum a_i c^i.
\]

This is the evaluation at \( c \) function.

6.3. Example (Evaluating a polynomial on a matrix). Let \( F \) be a field, and let \( S = M_{n \times n}(F) \). Fix a matrix \( A \in S \). Let \( \phi: F \to M_{n \times n}(F) \) be the homomorphism defined by \( \phi(c) = cI \); note that the image of \( \phi \) is in the center of \( S \), and so every \( \phi(c) \) commutes with \( A \).

Then the proposition gives a homomorphism \( \psi_A: F[X] \to S \), which sends

\[
c_0 + c_1 X + \cdots + c_n X^n \mapsto c_0 I + c_1 A + c_2 A^2 + \cdots + c_n A^n.
\]

In other words, the function \( \psi_A \) is the one that “plugs the matrix \( A \) into a polynomial”. We usually write \( f(A) \) for \( \psi_A(f) \).

The fact that \( \psi_A \) is a ring homomorphism implies that \((f + g)(A) = f(A) + g(A)\) and \((fg)(A) = f(A)g(A)\), which are formulas you have likely used without thinking about it.

6.4. Example (The function defined by a polynomial). Fix a commutative ring \( S \), and let \( T = F(S, S) \), which is also commutative. Let \( \phi: S \to T \) be the map that sends \( a \in S \) to the constant function \( (x \mapsto a) \). Let \( \epsilon = \text{id} \), the identity function of \( S \). Then the proposition tells us that we get a ring homomorphism \( \psi: S[X] \to T \), defined by

\[
\psi(p)(c) = \sum_{k=0}^{n} a_k c^k \quad \text{if} \quad p = \sum_{k=0}^{n} a_k X^k, \ a_k \in S.
\]

6.5. Example (Polynomial functions on \( \mathbb{Z}/p \)). Let \( S = \mathbb{Z}/p \) where \( p \) is a prime number. Let \( p = X^p - X \) in \( S[X] \). Then I claim that \( \psi(p) = 0 \). This amounts to showing that \( c^p - c = 0 \) for all \( c \in \mathbb{Z}/p \), which is Fermat’s little theorem.

Proof of Fermat’s little theorem: either \( c = 0 \) or \( c \neq 0 \). If \( c = 0 \) then obviously \( 0^p - 0 = 0 \). If \( c \neq 0 \) then \( c \) has a multiplicative inverse, i.e., is in the group \( \Phi(p) = (\mathbb{Z}/p)^\times \). Since this group has order \( p - 1 \) we must have \( c^{p-1} = 1 \), and thus \( c^p = c \).

Here’s another proof that \( \psi \) is not injective: \( \mathbb{Z}/p[X] \) is an infinite set (countably infinite), but \( F(\mathbb{Z}/p, \mathbb{Z}/p) \) is a finite set (size \( p^p \)).

This has the following consequence: different polynomials over \( \mathbb{Z}/p \) can give the same function. This is why I insist that polynomials are not just a kind of function.

Department of Mathematics, University of Illinois, Urbana, IL

E-mail address: rezk@math.uiuc.edu