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 \(+: R \times R \to R, \quad \cdot : R \times R \to R,\) called “addition” and “multiplication”,

- \((R, +)\) 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 \( S \subseteq M_{2 \times 2}(\mathbb{R}) \) 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 \( S = M_{2 \times 2}(\mathbb{R}) \), which is closed under + and \( \cdot \), and in fact as such it is a ring in its own right: its 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 \( S = M_{2 \times 2}(\mathbb{R}) \), 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 9, 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

\[
\phi(m) = \phi(1 + \cdots + 1) = \underbrace{\phi(1) + \cdots + \phi(1)}_{m\text{-times}} = m1.
\]

Similarly, \( \phi(-m) = -m1 \).

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 \( m1 \) 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 \( R^x \subseteq R \) 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 \( \phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1) = 1 \)

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

\[
(ab)_n := \sum_{i=0}^{n} a_i b_{n-i} = a_n b_0 + a_{n-1} b_1 + \cdots + a_1 b_{n-1} + a_0 b_n.
\]

E.g., \((ab)_0 = a_0 b_0\), \((ab)_1 = a_1 b_0 + a_0 b_1\), \((ab)_2 = a_2 b_0 + a_1 b_1 + a_0 b_2\), etc.

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:

\[
c_0 := c, \quad c_k := 0 \quad \text{if} \ k \geq 1.
\]

- 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 \( S \rightarrow S' \), and this bijection is an isomorphism of rings.
- We write \( X \in P(S) \) for the sequence

\[
X_1 = 1, \quad X_k = 0 \quad \text{if} \ k \neq 1.
\]

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

\[
X_n = 1, \quad X_k = 0 \quad \text{if} \ k \neq n.
\]

- 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 11).** 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

\[
g_k = a_{0k} + a_{1k}X + a_{2k}X^2 + \cdots a_{2m}X^m
\]

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

\[
(a1 + bi + cj + dk)i = -b1 + ai + dk - cj,
\]

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 11).** 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.

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

$$
\psi(fg) = \psi\left(\left(\sum_{i} a_i X^i\right)\left(\sum_{j} b_j X^j\right)\right)
= \psi\left(\sum_{n} \left(\sum_{i} a_i b_{n-i}\right)X^n\right)
= \sum_{n} \phi\left(\sum_{i} a_i b_{n-i}\right)c^n
= \sum_{n} \left(\sum_{i} \phi(a_i)\phi(b_{n-i})\right)c^n
$$

while

$$
\psi(f)\psi(g) = \psi\left(\sum_{i} a_i X^i\right)\psi\left(\sum_{j} b_j X^j\right)
= \left(\sum_{i} \phi(a_i)c^i\right)\left(\sum_{j} \phi(b_j)c^j\right)
= \sum_{n} \left(\sum_{i} \phi(a_i)c^i\phi(b_j)c^j\right)
= \sum_{n} \sum_{i=0}^{n} \phi(a_i)\phi(b_j)c^n
$$

$\phi$ is a homomorphism,
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:

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

\( \Box \)

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 \( T = \mathcal{F}(S,S) \), 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 \( c = id \), the identity function of \( S \). Then the proposition tells us that we get a ring homomorphism \( \psi : S[X] \to T \), defined by

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

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 \( \mathcal{F}(\mathbb{Z}/p, \mathbb{Z}/p) \) 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.

7. Ideals

An ideal of a ring \( R \) is a subset \( I \subseteq R \) such that

1. \( I \) is a subgroup of \((R,+)\),
2. if \( r, r' \in R \) and \( x \in I \), then \( r xr' \in I \). (You can write this condition as \( RIR \subseteq I \).)

Note that an ideal, under our definition of ring, is not usually a subring. (This differs from books where rings are allowed to not have a multiplicative identity.)

Note that since \( 1 \in R \), the condition implies \( r x, x r \in I \) if \( x \in I, r \in R \).

Warning. The notion of ideal we have defined is sometimes called a two-sided ideal, to distinguish it from the notions of left-ideal and right-ideal.
7.1. **Example.** In any ring $R$, the subsets $R$ and $\{0\}$ are ideals of $R$.

7.2. **Example.** In $R = \mathbb{Z}$, the subsets $\mathbb{Z}n = \{nx \mid x \in \mathbb{Z}\}$ are ideals for every $n$.

The **kernel** of a ring homomorphism $\phi: R \to S$ is the set $\text{Ker} \phi := \{ r \in R \mid \phi(r) = 0 \}$. In other words, it is the same as the kernel of $\phi$ thought of as a homomorphism of abelian groups.

7.3. **Proposition.** The kernel $\text{Ker} \phi \subseteq R$ of a ring homomorphism $\phi: R \to S$ is an ideal of $R$.

**Proof.** Straightforward.

This implies that a ring homomorphism $\phi$ is injective iff $\text{Ker} \phi = \{0\}$ (because $\phi$ is also a homomorphism of abelian groups).

7.4. **Exercise (On PS ?).** Let $F$ be a field, $c \in F$ an element. Let $I := \{ f \in F[X] \mid f(c) = 0 \}$. Show that $I$ is an ideal of $F[X]$.

---

8. **Quotient Rings**

Given an ideal $I$ of a ring $R$, there is a **quotient ring** $R/I$. Elements of $R/I$ are cosets $a + I = \{ a + x \mid x \in I \} \subseteq R$ of the additive group $(R, +)$ with respect to the subgroup $(I, +)$. Thus, it is automatic that $R/I$ is an abelian group, with

$$(a + I) + (b + I) = (a + b) + I.$$

**Note.** Sometimes I will use the notation $\overline{a} \in R/I$ for the coset $a + I$.

8.1. **Proposition.** If $I \subseteq R$ is an ideal, then $R/I$ is a ring, with addition as above and multiplication defined by

$$(a + I)(b + I) := ab + I.$$

If $R$ has multiplicative identity $1$, then $R/I$ has multiplicative identity $1 + I$.

Furthermore, the obvious projection map $\pi: R \to R/I$ defined by $\pi(a) := a + I$ is a ring homomorphism.

**Proof.** Check that the formula for product is well defined. Suppose $a + I = a' + I$ and $b + I = b' + I$, which implies

$$a' = a + x, \quad b' = b + y, \quad x, y \in I.$$

Then

$$a'b' = (a + x)(b + y) = ab + (ay + xb + xy) \in ab + I,$$

since $ay + xb + xy \in I$. Therefore $a'b' + I = ab + I$.

Checking the various axioms for $R/I$ to be a ring is straightforward, using that they are true for $R$. □

8.2. **Example.** $\mathbb{Z}/n = \mathbb{Z}/(n)$, the quotient of integers by the ideal $(n) = \mathbb{Z}n$. We already know this is a quotient group (under addition). In fact, it is a quotient ring.

8.3. **Example.** Let $R \subseteq M_{n \times n}(F)$ be the set of **upper triangular matrices**: so $A = (A_{ij}) \in R$ if and only if $a_{ij} = 0$ when $i > j$. For example, if $n = 2$ then $R = \{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid a, b, d \in F \}$. It is easy to check that $R$ is a subring of the matrix ring: if $i > j$, then $I \subseteq R$, and

$$(A + B)_{i,j} = A_{i,j} + B_{i,j}, \quad (-A)_{i,j} = -A_{i,j}, \quad (AB)_{i,j} = \sum_{k=1}^{n} A_{i,k}B_{k,j},$$

and since $i > j$ then for each $k = 1, \ldots, n$ either $i > k$ or $k > j$. (I.e., you can’t have $k \geq i > j \geq k$.)

Now let $J \subseteq R$ be the set of **strictly upper triangular matrices**: so $A = (A_{ij}) \in J$ if and
only if \( a_{ij} = 0 \) when \( i \geq j \). For example, if \( n = 2 \) then \( R = \{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \mid b \in F \} \).

You can check that \( J \) is an ideal in \( R \).

The quotient ring \( R/J \approx R^n = \underbrace{R \times \cdots \times R}_{\text{n copies}} \).

9. IDEALS GENERATED BY SUBSETS

**Observation.** We have the following equivalent formulation of the definition of an ideal \( I \) in \( R \).

1. \((1')\) 0 \in I, and if \( x, y \in I \) then \( x + y \in I \).
2. If \( r, r' \in R \) and \( x \in I \), then \( rrx' \in I \).

(\(1') \) replaces (1), which said that \((I, +) \) is a subgroup of \((R, +)\). This is because \(-1 \in R \), so \( x \in I \) and (2) implies \(-x = (-1)x \in I \).

Let \( R \) be a ring and \( S \subseteq R \) a subset. The ideal generated by \( S \) is

\[
(S) := \bigcap_{S \subseteq J \leq R} J
\]

the intersection of all ideals of \( R \) which contain the subset \( S \). That this is an ideal is because of the following.

9.1. **Proposition.** If \( \{ J_i \} \) is any collection of ideals in \( R \), then \( J = \bigcap_i J_i \) is an ideal.

**Proof.** Straightforward.

We also have an explicit description of \((S)\).

9.2. **Proposition.** We have that

\[
(S) = \{0\} \cup \{ a_1s_1b_1 + \cdots + a_ks_kb_k \mid \text{for all } k \geq 1, a_i, b_i \in R, s_i \in S \}.
\]

**Proof.** First, note that if \( J \leq R \) is any ideal and \( S \subseteq R \), then the RHS is a subset of \( J \), by the closure properties of the ideal \( J \).

Next, check that the RHS is an ideal: Show \((1')\) 0 is in it and it is closed under addition (immediate), and (2) if \( r, r' \in R \) and \( x \in (S) \) then \( rrx' \in S \): if \( x = a_1s_1b_1 + \cdots + a_ks_kb_k \) then

\[
rrx' = (ra_1)s_1(b_1r') + \cdots + (ra_k)s_k(b_kr').
\]

**Note.** The ideal \((S)\) contains the subgroup \((S)\) of \((R, +)\) generated by \( S \), but is usually bigger than it.

When \( R \) is a commutative ring, this simplifies a bit.

9.3. **Proposition.** If \( R \) is commutative, then

\[
(S) = \{0\} \cup \{ a_1s_1 + \cdots + a_ks_k \mid \text{for all } k \geq 1, a_i \in R, s_i \in S \}.
\]

**Proof.** \( \text{asb} = (ab)s \).

A principal ideal is an ideal which can be generated by a single element. For \( x \in R \) we write \((x) := (\{x\})\). Thus

\[
(x) = \{ a_1xb_1 + \cdots + a_nxb_n \mid a_i, b_i \in R \}.
\]

When \( R \) is commutative, we can always rearrange:

\[
a_1xb_1 + \cdots + a_nxb_n = (a_1b_1)x + \cdots + (a_nb_n)x = (a_1b_1 + \cdots + a_nb_n)x.
\]

Thus, for commutative \( R \), principal ideals have the form

\[
(x) = Rx = \{ rx \mid r \in R \}.
\]

Sometimes I’ll write \( Rx \) (or \( xR \)) for principal ideals in commutative rings.
We are going to say a lot about principal ideals in commutative rings. Here is an important fact: principal ideals in commutative rings correspond to elements “up to units”.

9.4. Exercise (On PS ?). Let $R$ be a commutative ring, and let $a, b \in R$. Then $(a) = (b)$ if and only if there exists a unit $u \in R^\times$ such that $b = ua$, $a = u^{-1}b$.

10. IDEALS IN POLYNOMIAL RINGS

We recall some exercises from the homework. Let $R$ be a domain, and let $P = R[X]$ the polynomial ring. We defined the **degree function**

$$\deg: R[X] \to \mathbb{Z}_{\geq 0} \cup \{-\infty\}$$

which had the properties

- $\deg(f) = -\infty$ if and only if $f = 0$.
- $\deg(f) = 1$ if and only if $f$ is non-zero and “constant”.
- $\deg(fg) = \deg(f) + \deg(g)$.
- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

As a consequence, $R[X]$ is a domain: if $f \neq 0$ and $g \neq 0$, then $fg \neq 0$ since $\deg(fg) = \deg(f)\deg(g)$.

In the following, I’ll assume $R = F$ is a field. The following is a statement of “polynomial long division” for polynomials with coefficients in a field.

10.1. **Proposition** (Division algorithm for polynomials). Let $f, g \in F[X]$ with $g \neq 0$. Then there exists a unique pair $q, r \in F[X]$ such that

- $f = gq + r$ and
- $\deg(r) < \deg(g)$.

In other words, “$f \div g$” has quotient $q$ and remainder $r$, where $\deg(r) < \deg(g)$.

Before proving this, let’s think about some consequences.

10.2. **Example** (Important). Let $F$ be a field, $c \in F$ an element, and $f \in F[X]$. Then, $f(c) = 0$ implies that $f = (X - c)f_1$ for some polynomial $f_1 \in F[X]$.

**Proof.** Use polynomial division for $f \div g$ with $g = X - c$, giving

$$f = gq + r = (X - c)q + r,$$

$\deg(r) < \deg(g) = 1$.

Because “evaluation at $c$” is a ring homomorphism $F[X] \to F$, this implies

$$0 = f(c) = g(c)q(c) + r(c) = (c - c)q(c) + r(c) = r(c).$$

But $\deg(r) < 1$, so $r \in F \subseteq F[X]$ is a constant polynomial. So $r(c) = 0$ means $r = 0$, so we get

$$f = (X - c)q$$

as desired.

10.3. **Corollary.** If $F$ is a field and $f \in F[X]$ is a polynomial of degree $n \geq 0$, then $f$ has at most $n$ distinct roots in $F$.

**Proof.** By induction on degree. **Basis step.** If $\deg(f) = 0$, then $f$ is a non-zero constant polynomial so has no roots.

**Induction step.** Suppose $\deg(f) = n \geq 1$. If $f$ has no roots we are done. If $c \in F$ is a root, then $f = (X - c)g$ with $\deg(g) = n - 1$. By induction, $g$ has at most $n - 1$ roots, so $f$ has at most $n$ roots.
A **monic polynomial** is a polynomial with coefficient of the leading degree term equal to 1. That is, \( f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \). Note that the zero polynomial cannot be a monic polynomial; however, the constant polynomial 1 is monic.

We can classify all ideals in \( F[X] \). The proof is very much like the classification of subgroups/ideals in \( \mathbb{Z} \).

10.4. **Proposition.** Let \( F \) be a field. Then all ideals in \( F[X] \) are principal. In particular, every ideal \( I \leq F[X] \) is of the form \( I = (f) = R[X]f \) for exactly one polynomial \( f \) which is either 0 or a monic polynomial.

**Proof.** The subset \( (0) = \{0\} \) is an ideal, and 0 is the only single element which generates it.

Suppose \( I \leq K[X] \) such that \( I \neq \{0\} \). Since \( I \) contains non-zero elements, it must contain a non-zero element \( f \) of minimal degree \( d \geq 0 \) (by the Well-Ordering Principle of \( \mathbb{Z}_{\geq 0} \)). We are going to show that every \( h \in I \) is of the form \( f(q) \) for some \( q \in F[X] \), i.e., that \( I = (f) \).

The proof is the division algorithm. Given \( h \in I \) consider the division algorithm for \( h \div f \): there exist \( q, r \in F[X] \) with \( \deg(r) < \deg(f) \) such that \( h = f(q) + r \). But by hypothesis \( \deg(f) \) is minimal for non-zero elements, so \( r = 0 \), so \( h = f(q) \in (f) \).

Given \( I = (f) \), write \( f = cX^d + \text{(lower degree)} \) with \( c \neq 0 \). Then \( f' = c^{-1}f \) is monic and \( I = (f) = (f') \). This is the only monic polynomial of degree \( d \) in \( I \), since if there are two such \( f', f'' \), then \( \deg(f' - f'') < d \) so \( f' = f'' \). \( \square \)

10.5. **Exercise.** Given a field \( F \) and \( c \in F \), let \( I = \{ f \in F[X] \mid f(c) = 0 \} \). What is the monic polynomial which generates \( I? \)

**Proof of the division algorithm. Uniqueness.** I'll do uniqueness first. Suppose there are two solutions, i.e.,

\[
\begin{align*}
f &= gq_1 + r_1 = gq_2 + r_2, \\
\deg(r_1), \deg(r_2) &< \deg(g).
\end{align*}
\]

Then taking differences gives

\[
\begin{align*}
g(q_2 - q_1) &= r_1 - r_2, \\
\deg(r_1 - r_2) &< \max\{\deg(r_1), \deg(r_2)\} < \deg(g).
\end{align*}
\]

Set \( q = q_2 - q_1 \) and \( r = r_1 - r_2 \), so this becomes \( gq = r \). If \( r \neq 0 \), then also \( q \neq 0 \), and we would have \( \deg(r) = \deg(g) + \deg(q) \). Since \( \deg(q) \geq 0 \) this contradicts \( \deg(r) < \deg(g) \), so this is impossible. Thus we must have \( r = 0 \) and thus \( q = 0 \), whence \( r_1 = r_2 \) and \( q_1 = q_2 \).

**Existence.** Suppose \( \deg(g) = n \geq 0 \).

In general, prove this by induction on \( \deg(f) = m \): assume the proposition has been proved for \( fs \) with degree \( < m \).

If \( \deg(f) = -\infty \) then \( f = 0 \), so just take \( q = r = 0 \).

If \( \deg(f) < \deg(g) \), set \( q = 0 \) and \( r = f \), so that

\[
f = 0g + r.
\]

Now suppose \( \deg(f) \geq \deg(g) \). That is, \( \deg(f) = m \geq n \). Write

\[
\begin{align*}
f &= a_mX^m + \cdots, \\
g &= b_nX^n + \cdots, \\
a_m, b_n &\in F \setminus \{0\},
\end{align*}
\]

and let

\[
u = \frac{a_mX^m}{b_nX^n} = a_mb_n^{-1}X^{m-n},
\]

(the fraction in quotes isn't generally well-defined because \( b_nX^n \) may not have a multiplicative inverse, but the expression of the right is defined since \( b_n \neq 0 \) and \( m \geq n \)). Thus

\[
(b_nX^n)u = a_mX^m.
\]

Now let \( f' := f - gu \). Looking at the terms of highest degree (= \( m \)) we have

\[
f' = f - gu = (a_mX^m + \cdots) - (b_nX^n + \cdots)(a_mb_n^{-1}X^{m-n} + \cdots) = 0X^m + \text{(lower deg)}.
\]
Therefore \( f' \) has degree strictly less than \( m \), so \( \deg(f') < \deg(f) \). By the induction on degree we know that there exist \( q' \) and \( r' \) such that

\[
f' = gq' + r', \quad \deg(r') < \deg(g).
\]

Then

\[
f = f' + gu = gq' + r' + gu = g(q' + u) + r'
\]

so \( q' + u \) and \( r' = r \) is a solution.

\[
\square
\]

11. Quotient rings of polynomials

An important example are quotients of polynomial rings by principal ideals.

11.1. Example. Let \( S = \mathbb{Q}[X]/J \) where \( J = (f) = (X^2 - 2) \). Any element of \( S \) has the form

\[
g + J = (a_nX^n + \cdots + a_1X + a_0) + J, \quad a_n, \ldots, a_n \in \mathbb{Q},
\]

but not uniquely. We can use the division algorithm to find a “canonical form”: a canonical form for \( g + J \) is an expression \( r + J \) such that \( r + J = g + J \) and \( \deg(r) < \deg(f) \). The division algorithm for “\( g \div f' \)” tells us that there is a unique canonical form, given by the remainder.

For instance, doing \( (X^3 + 4X^2 + 5X - 3) \div f \) gives

\[
X^3 + 4X^2 + 5X - 3 = (X + 4)(X^2 - 2) + (7X + 5) = Xf + (7X + 5)
\]

so

\[
(X^3 - 2X^2 + 5X - 3) + J = (7X + 5) + J.
\]

11.2. Remark. Here is another way to think about this. Still assuming \( f = X^2 - 2 \in \mathbb{Q}[X] \) and \( J = (X^2 - 2) \subseteq \mathbb{Q}[X] \), note that for \( n \geq 2 \),

\[
X^n = X^2X^{n-2} = (X^2 - 2)X^{n-2} + 2X^{n-2} + 2X^{n-2} + J.
\]

In other words, “modulo \( J \)” we replaced an instance of “\( X^{2n} \)” with “2”. So by induction, we have

\[
X^{2k} + J = 2^k + J, \quad X^{2k+1} + J = 2^k X + J.
\]

In general, every element of \( S \) is represented uniquely as

\[
a + bX + J, \quad a, b \in \mathbb{Q}.
\]

In particular, the set \( \{a + J \mid a \in \mathbb{Q}\} \) is a subring of \( S \) which is isomorphic to \( \mathbb{Q} \).

Addition of canonical forms gives a canonical form:

\[
((a + bX) + J) + ((a' + b'X) + J) = ((a + a') + (b + b')X) + J.
\]

Multiplication doesn’t automatically give a canonical form, so we have to work:

\[
((a + bX) + J)((a' + b'X) + J) = (a + bX)(a' + b'X) + J
\]

\[
= (aa' + (ab' + a'b)X + bb'X^2) + J
\]

\[
= (aa' + (ab' + a'b)X + bb'X^2 - bb'(X^2 - 2)) + J
\]

\[
= ((aa' + 2) + (ab' + a'b)X) + J.
\]

In practice we use the following notational tricks to deal with this:

- Given \( a \in \mathbb{Q} \), we use the same symbol “\( a \)” to represent the element \( a + J \in S \).
- We pick a symbol like \( X \) or \( \alpha \) to represent the coset \( X + J \in S \).
- Then any element \( u \in S \) can be written uniquely as

\[
u = a + b\alpha, \quad a, b \in \mathbb{Q}.
\]
• The symbol $\alpha$ satisfies the “reduction rule” $\omega^2 = 2$. We use this rule whenever we need to put expressions in “canonical form”:

$$\omega^3 + 4\omega^2 + 5\omega - 3 = 2\omega + 4(2) + 5\omega - 3 = 7\omega + 5.$$  

11.3. Example (Continued). Let $T \subseteq \mathbb{R}$ denote the following subset of $\mathbb{R}$:

$$T := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$  

Exercise: $T$ is a subring of $\mathbb{R}$.

We can define a function $\phi: S \to T$ by

$$\phi(g + J) := g(\sqrt{2}).$$

That this is well defined relies on the following observation: if $g + J = g' + J$, then $g' = g + hJ$, and therefore

$$g'(\sqrt{2}) = g(\sqrt{2}) + h(\sqrt{2})f(\sqrt{2}) = g(\sqrt{2}) + f(0) = g(\sqrt{2}),$$

since $\sqrt{2}$ is a root of the polynomial $f = x^2 - 2$.

As we will soon see, $\phi$ is an isomorphism of rings.

11.4. Example. Let $S = \mathbb{R}[X]/(X^2 + 1)$. If we define $i := X$, then $i^2 = -1$, and an element of $S$ has a unique representation $a + bi$ with $a, b \in \mathbb{R}$. Of course, $S \approx \mathbb{C}$.

Here is the general principle about canonical form for elements in a quotient of a polynomial ring on one variable:

11.5. Proposition. Given $S = F[X]/J$ with $J = (f)$ for a monic polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$, then every element of $S$ can be written uniquely as

$$c_0 + c_1X + \cdots + c_{n-1}X^{n-1}, \quad c_0, \ldots, c_{n-1} \in F,$$

where we identify elements $c \in F$ with elements $c + J \in S$, and $X = X + J$.

Furthermore, any expression $c_0 + c_1X + \cdots + c_mX^m$ can be reduced to a canonical form by repeated applications of replacing $X^n$ with $-(a_0 + a_1X + \cdots + a_{n-1}X^{n-1})$.

Proof. Division algorithm. The process for finding canonical forms for elements in $S$ is exactly the division algorithm in $R[X]$ for $f$. \qed

It is not necessarily the case that $F[X]/(f)$ will be a field.

11.6. Example. Let $S = \mathbb{Q}[X]/(X^2 - 4)$. Then the elements $\alpha = X - 2$ and $\beta = X + 2$ are non-zero in $S$, but satisfy $\alpha\beta = 0$, because $\alpha\beta = (X - 2)(X + 2) = X^2 - 4 = 0$.

You can think of it this way: the ring $S$ is obtained from $\mathbb{Q}$ by “formally adjoining” an element $X$ which is a square root of 4, since $X^2 = 4$. But $\mathbb{Q}$ already has a square root of 4 (in fact two: $\pm 2$), so $S$ has “too many” square roots of 4 if it is going to be a field. (In a field, there are at most $d$ roots of a polynomial of degree $d$.)

11.7. Example. Let $S = \mathbb{Q}[X]/J$ with $J = (f) = (X^3 - 2)$. Write $\omega := [X] = X + J \in S$, and identify elements $a \in \mathbb{Q}$ with $a + J \in S$. Then every element of $S$ can be written uniquely as

$$a + b\omega + c\omega^2, \quad a, b, c \in \mathbb{Q}.$$  

You can carry out calculations using the “reduction” formula $\omega^3 = 2$.

Exercise: $S$ is a field. (This is not obvious, and we will return to this.)
12. Homomorphism theorems

12.1. Theorem (Homomorphism theorem for rings). Let $\phi: R \to S$ be a surjective homomorphism of rings with $I = \ker \phi$. Let $\pi: R \to R/I$ be the quotient homomorphism. Then there exists a unique ring isomorphism $\bar{\phi}: R/I \to S$ such that $\bar{\phi}(\pi(r)) = \phi(r)$ for all $r \in R$.

Proof. If you understand the proof of the homomorphism theorem of groups, then you understand the proof of the homomorphism theorem for rings. □

If $\phi: R \to S$ isn’t surjective, its image $S' := \phi(R) \subseteq S$ is a subring, and you can apply the homomorphism theorem to $R \to S'$, so $S' = \phi(R) \approx R/I$.

12.2. Example. Let $\phi: \mathbb{R}[x] \to \mathbb{C}$ be the homomorphism defined by evaluation at $i \in \mathbb{C}$, and using the usual inclusion $\mathbb{R} \subset \mathbb{C}$. Thus $\phi(g) := g(i)$. This is surjective because $a + bi = \phi(a + bx)$.

$\ker \phi$ is set of all polynomials $g$ such that $g(i) = 0$. Clearly $x^2 + 1 \in \ker(\phi)$, therefore $(x^2 + 1) \subseteq \ker(\phi)$.

Given an arbitrary $g \in \mathbb{R}[x]$, by polynomial division we have $g = (x^2 + 1)q + (a + bx)$ for some $q \in \mathbb{R}[x]$. We have

$$\phi(g) = \phi(x^2 + 1)\phi(q) + (a + bx) = a + bi.$$

This is 0 iff $a = 0 = b$, so we see that $\ker(\phi) = (x^2 + 1)$.

The homomorphism theorem gives a unital isomorphism $\mathbb{R}[x]/(x^2 + 1) \approx \mathbb{C}$ of rings.

12.3. Example. Let $\psi: \mathbb{R}[X] \to \mathbb{C}$ be the homomorphism defined by evaluation at $\omega = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$.

This is surjective. Both $\mathbb{R}[X]$ and $\mathbb{C}$ are, in particular, real vector spaces over $\mathbb{R}$, and $\psi$ is, in particular, an $\mathbb{R}$-linear map. The set $\{\psi(1) = 1, \psi(x) = \omega\}$ in $\mathbb{C}$ is linearly independent over $\mathbb{R}$. Since $\dim_{\mathbb{R}} \mathbb{C} = 2$, this means $\psi$ is surjective.

Write $\ker(\psi) = (f)$. The homomorphism theorem gives an isomorphism

$$\mathbb{R}[X]/(f) \sim \mathbb{C}$$

of rings. By counting dimensions, we see that deg $f = 2$. The set $(f)$ is the collection of all polynomials over $\mathbb{R}$ which have $\omega$ as a root.

There is a degree 2 polynomial with $\omega$ as a root, for instance $f = X^2 + X + 1$. We get an isomorphism $\mathbb{R}[x]/(X^2 + X + 1) \approx \mathbb{C}$ of rings.

13. Domains

Let $R$ be a commutative ring with 1.

An domain (sometimes called an integral domain) is a commutative ring $R$ with 1 such that $1 \neq 0$, and such that $xy = 0$ implies either $x = 0$ or $y = 0$.

As we have noted, this is the same as: a commutative ring $R$ such that $R \setminus \{0\}$ is non-empty and closed under multiplication.

13.1. Example. Examples of domains are $\mathbb{Z}$, fields $F$.

Also, the polynomial ring $D[x]$ with $D$ a domain (because $\deg(fg) = \deg(f)\deg(g)$).

13.2. Proposition. Any subring of a domain is a domain.

Proof. Easy. □

For instance, the Gaussian integers

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

13.3. Example. Let $f_1, f_2 \in F[x]$ be two non-constant polynomials, and let $g = f_1f_2$ and $I = (g)$.

The ring $F[x]/I$ is not a domain, since $\overline{f_1} = f_1 + I, \overline{f_2} = f_2 + I$ are non-zero, but $\overline{f_1}\overline{f_2} = 0$.

For instance, $\mathbb{Q}[X]/(g)$ with $g = X^2 - 4 = (X - 2)(X + 2)$.
Domains have cancellation of non-zero elements.

13.4. **Proposition** (Cancellation). If \( R \) is a domain, and \( a, b, c \in R \) such that \( a \neq 0 \), then \( ab = ac \) implies \( b = c \).

**Proof.** \( a(b - c) = 0 \) implies either \( a = 0 \) or \( b - c = 0 \). \( \square \)

14. **Fields of fractions**

Every domain is a subring of a field, called its **field of fractions**.

Given a domain \( R \), consider the set

\[
S := \{ (a, b) \in R \times R \mid b \neq 0 \}.
\]

Define a relation on \( S \) by

\[
(a, b) \sim (a', b') \quad \text{iff} \quad ab' = ba'.
\]

(Remember that in \( \mathbb{Q} \), we have \( a/b = a'/b' \) if and only if \( ab' = ba' \).)

14.1. **Lemma.** This is an equivalence relation on \( S \).

**Proof.**

- **Reflexive.** To see that \((a, b) \sim (a, b)\), note that \( ab = ba \).
- **Symmetric.** If \((a, b) \sim (a', b')\), then \( ab' = ba' \). But this means \( a'b = b'a \), so \((a', b') \sim (a, b)\).
- **Transitive.** If \((a, b) \sim (a', b')\) and \((a', b') \sim (a'', b'')\), then

\[
ab' = ba', \quad a'b'' = b'a''.
\]

We can combine these to get

\[
ab'b'' = (ab')b'' = (ba')b'' = b(a'b'') = b(b'a'') = bb'a''.
\]

Because the ring is commutative, we can rewrite this as \( b'(ab'') = b'(ba'') \). Because \( b' \neq 0 \) and \( R \) is a domain, we can cancel to get \( ab'' = ba'' \), which implies \((a, b) \sim (a'', b'')\).

\( \square \)

Let \( F = \text{Frac}(R) := \) the set of equivalence classe under this relation. We write \( "(a/b)" \) in \( \text{Frac}(R) \) for the equivalence class of \((a, b)\). Note that the equivalence relation then says that \((a/b) = (a'/b')\) iff \( ab' = ba' \).

14.2. **Exercise.** If \( c \in R \setminus \{0\} \), then \((ac/bc) = (a/b)\).

Define operations \(+\) and \(\cdot\) on \( F \) by

\[
(a/b) + (c/d) := ((ad + bc)/bd), \quad (a/b)(c/d) = (ac/bd).
\]

Check that these are compatible with the equivalence relation (Exercise!), and so are well-defined operations on \( F \).

14.3. **Proposition.** If \( R \) is a domain, then \( F = \text{Frac}(R) \) is a field. The function \( \phi : R \to F \) given by \( \phi(a) := (a/1) \) defines an isomorphism of rings from \( R \) to the subring \( \phi(R) = \{ (a/1) \mid a \in \mathbb{R} \} \) of \( F \).

**Proof.** This is just straightforward, and is partially an exercise. Note: the 0 element is \((0/1)\), the 1 element is \((1/1)\).

I’ll do multiplicative inverses (or leave as exercise?) If \( x \in F \) is not equal to 0, write \( x = (a/b) \). Because \( x \neq 0 \), we have \((a/b) \neq (0/1)\), i.e., \( a1 \neq b0 \), i.e., \( a \neq 0 \). So set \( y = (b/a) \in F \) (this makes sense exactly because \( a \neq 0 \), and check that \((a/b)(b/a) = (ab/ab) = (1/1) = 1 \).

Typically we identify \( R \) with its image in \( F = \text{Frac}(R) \), so we can say that the domain \( R \) is a subring of its fraction field.
14.4. Example. If $R = \mathbb{Z}$, then $\text{Frac}(\mathbb{Z}) = \mathbb{Q}$.

14.5. Example. If $R = F[X]$, then $F(X) := \text{Frac}(F[X])$ is called the field of rational functions in one variable. Elements are $f/g$ where $f, g$ are polynomials.

Note that polynomial long division of the form $f ÷ g$ for $g \neq 0$ gives $f = gq + r$ with $\deg(r) < \deg(g)$, which in $F(X)$ gives

$$
\frac{f}{g} = q + \frac{r}{g}.
$$

14.6. Example. $\text{Frac}(\mathbb{Z}[i]) = \mathbb{Q}[i]$. To see this, note that every element in $\mathbb{Q}[i]$ is a ratio of elements in $\mathbb{Z}[i]$. In fact, if $x \in \mathbb{Q}[i]$ we can write it as $x = (a/b) + (c/d)i$ with $a, b, c, d \in \mathbb{Z}$. Then

$$
x = (bd)^{-1}(ad + bci), \quad bd, ad + bci \in \mathbb{Z}[i].
$$

The claim follows from the following proposition.

14.7. Proposition. Let $F$ be a field, and $F \subseteq R$ a subring (which is thus a domain). If every element of $F$ has the form $ab^{-1}$ with $a, b \in R$, $b \neq 0$, then $F$ is isomorphic to the fraction field of $R$.

Proof. (Don’t spend much time on this.)

(1) Define a function $\phi : \text{Frac}(R) \to F$ by $\phi((a/b)) := ab^{-1}$. First check that this is well-defined: if $(a/b) = (a'/b')$ represent the same element in $\text{Frac}(R)$, then $ab' = ba'$ in $R$, and thus $a' = ab'b^{-1}$ in $F$, whence $a'b^{-1} = (ab'b^{-1})b'^{-1} = ab^{-1}$.

(2) Check that $\phi$ is a ring homomorphism. This is a straightforward exercise:

$$
\phi((a/b) + (a'/b')) = \phi((ab' + ba')/ab) = (ab' + ba')(bb')^{-1} = ab^{-1} + a'b^{-1} = \phi((a/b)) + \phi((a'/b')),
$$

$$
\phi((a/b)(a'/b')) = \phi((aa'/bb')) = aa'(bb')^{-1} = (ab^{-1})(a'b^{-1}) = \phi((a/b))\phi((a'/b')),
$$

$$
\phi((1/1)) = 1.
$$

(3) The function $\phi$ is surjective, because of the hypothesis that every element of $F$ has the form $ab^{-1}$ with $a, b \in R$. To see that $\phi$ is surjective, consider $\text{Ker } \phi$ which is an ideal in $F$. Since $F$ has only two ideals, and $1 \notin \text{Ker } \phi$, we have $\text{Ker } \phi = \{0\}$ so $\phi$ is injective.

\[\]