

Math146 - Lecture notes

George McNinch

2025-01-29 13:17:24 EST (george@calliope)

Contents

| | | |
|----------|---|-----------|
| 1 | 2025-01-15 - Commutative rings | 3 |
| 1.1 | Definitions | 3 |
| 1.2 | Polynomial rings | 3 |
| 2 | 2025-01-22 - Properties of rings | 5 |
| 2.1 | Ring Homomorphisms | 5 |
| 2.2 | Ideals of a ring | 5 |
| 2.3 | Quotient rings | 5 |
| 2.4 | Principal ideals | 6 |
| 2.5 | Isomorphism Theorem | 6 |
| 2.6 | A Homomorphism from the polynomial ring to the scalars | 7 |
| 3 | 2025-01-27 - Polynomials over a field and the division algorithm | 8 |
| 3.1 | Some general notions for commutative rings | 8 |
| 3.2 | The degree of a polynomial | 9 |
| 3.3 | The division algorithm | 9 |
| 4 | 2025-01-29 - ideals of the polynomial ring | 11 |
| 4.1 | Ideals of the polynomial ring $F[T]$ | 11 |
| 4.2 | Principal ideal domains (PIDs) and gcds | 12 |
| 5 | 2025-02-03 - prime elements and unique factorization | 13 |
| 5.1 | Prime elements in a PID | 13 |
| 5.2 | Unique factorization in a PID | 14 |
| 6 | Irreducible polynomials over a field | 15 |
| 6.1 | Fields as quotient rings | 15 |
| 6.2 | Some criteria for irreducibility | 15 |
| 7 | The Field of fractions of an Integral Domain | 16 |
| 7.1 | Another field of fractions | 19 |
| 7.2 | Eisenstein's criteria | 19 |

1 2025-01-15 - Commutative rings

See [Stewart, chapter 16] ¹ for general results about commutative rings.

1.1 Definitions

Definition 1.1.1. A ring R is an additive abelian group together with an operation of multiplication $R \times R \rightarrow R$ given by $(a, b) \mapsto a \cdot b$ such that the following axioms hold:

- multiplication is *associative*
- multiplication *distributes* over addition: for every $a, b, c \in R$ we have ²

$$a(b + c) = ab + ac$$

and

$$(b + c)a = ba + ca$$

We say that the ring R is *commutative* if the operation of multiplication is commutative; i.e. if $ab = ba$ for all $a, b \in R$.

And we say that R has identity if multiplication has an identity, i.e. if there is an element $1_R \in R$ such that $a \cdot 1_R = 1_R \cdot a = a$ for every $a \in R$. ³

In the course, we will consider (almost?) exclusively rings which are commutative and have identity.

Here are some examples of commutative rings:

Example 1.1.2. (a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$

(b) if X is a set and if R is a commutative ring, the set X^R of all R -valued functions on X can be viewed as a commutative ring in a natural way.

1.2 Polynomial rings

If R is a commutative ring, the collection of all polynomials in the variable T having coefficients in R is denoted $R[T]$.

Notice that the set of *monomials* $S = \{T^i \mid i \in \mathbb{N}\}$ has the following properties:

(M1) every element of $R[T]$ is an R -linear combination of elements of S . This just amounts to the statement that every polynomial $f(T) \in R[T]$ has the form

$$f(T) = \sum_{i=0}^N a_i T^i$$

for a suitable $N \geq 0$ and suitable coefficients $a_i \in R$.

¹As noted in the course syllabus, Tisch library has an entry for this item here; click to find online access to the text *Galois Theory*, Ian Stewart. (CRC Press, 4th edition 2022).

²We often just denote multiplication by juxtaposition: i.e. we may write ab instead of $a \cdot b$ for $a, b \in R$

³Usually we write 1 for 1_R . The idea is that 1_R is the multiplicative identity of R . For example, the identity matrix $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the multiplicative identity 1_R of the matrix ring $R = \text{Mat}_2(\mathbb{R})$.

(M2) the elements of S are linearly independent i.e. if

$$\sum_{i=0}^N a_i T^i = 0 \quad \text{for } a_i \in R,$$

then $a_i = 0$ for every i .

Polynomials in $R[T]$ can be added in a natural way. (This is just like adding vectors in a vector space).

And there is a product operation on polynomials, as follows:

if $f(T) = \sum_{i=0}^N a_i T^i$ and $g(T) = \sum_{i=0}^M b_i T^i$ then

$$f(T) \cdot g(T) = \sum_{i=0}^{N+M} c_i T^i \quad \text{where } c_i = \sum_{s+t=i} a_s b_t.$$

Proposition 1.2.1. $R[T]$ is a commutative ring with identity.

2 2025-01-22 - Properties of rings

2.1 Ring Homomorphisms

Definition 2.1.1. If R and S are rings, a function $\phi : R \rightarrow S$ is called a *ring homomorphism* provided that

- (a) ϕ is a homomorphism of *additive groups*,
- (b) ϕ preserves multiplication; i.e. for all $x, y \in R$ we have $\phi(xy) = \phi(x)\phi(y)$, and
- (c) $\phi(1_R) = 1_S$.

Definition 2.1.2. The *kernel* of the ring homomorphism $\phi : R \rightarrow S$ is given by

$$\ker \phi = \phi^{-1}(0) = \{x \in R \mid \phi(x) = 0\};$$

thus $\ker \phi$ is just the kernel of ϕ viewed as a homomorphism of additive groups.

Here are some properties of the kernel:

- (K1) $\ker \phi$ is an additive subgroup of R
- (K2) for every $r \in R$ and every $x \in \ker \phi$ we have $rx \in \ker \phi$.

2.2 Ideals of a ring

For simplicity suppose that the ring R (and S) are *commutative* rings.

Definition 2.2.1. A subset I of R is an *ideal* provided that

- (a) I is an additive subgroup of R , and
- (b) for every $r \in R$ and every $x \in I$ we have $rx \in I$.

We sometimes describe condition (b) by saying that " I is closed under multiplication by every element of R ".

The proof of the following is immediate from definitions:

Proposition 2.2.2. *If $\phi : R \rightarrow S$ is a ring homomorphism, then $\ker \phi$ is an ideal of R .*

2.3 Quotient rings

Let R be a commutative ring and let I be an ideal of R .

Since I is a subgroup of the (abelian) additive group R , we may consider the quotient group R/I . Its elements are (additive) cosets $a + I$ for $a \in R$.

It follows from the definition of cosets that the $a + I = b + I$ if and only if $b - a \in I$.

The additive group can be made into a commutative ring by defining the multiplication as follows:

For $a + I, b + I \in R/I$ (so that $a, b \in R$), the product is given by

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

In order to make this definition, one must confirm that this rule is well-defined. Namely, if we have equalities $a + I = a' + I$ and $b + I = b' + I$, we need to know that

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

Applying the definition, we see that we must confirm that

$$ab = I = a'b' + I.$$

For this, we need to argue that $a'b' - ab \in I$.

Since $a + I = a' + I$, we know that $a' - a = x \in I$ and since $b + I = b' + I$ we know that $b' - b = y \in I$.

Thus $a' = a + x$ and $b' = b + y$. Now we see that

$$a'b' = (a + x)(b + y) = ab + ay + xb + xy$$

Since I is an ideal, we see that $ay, xb, xy \in I$ hence $ay + xb + xy \in I$. Now conclude that $a'b' + I = ab + I$ as required.

It is now straightforward to confirm that the ring axioms hold for the set R/I with these operations.

Proposition 2.3.1. *If I is an ideal of the commutative ring R , then R/I is a commutative ring with the addition and multiplication just described.*

2.4 Principal ideals

Definition 2.4.1. If R is a commutative ring and $a \in R$, the *principal ideal generated by a* – written Ra or $\langle a \rangle$ – is defined by

$$Ra = \langle a \rangle = \{ra \mid r \in R\}.$$

Proposition 2.4.2. *For $a \in R$, Ra is an ideal of R .*

Example 2.4.3. Let $n \in \mathbb{Z}_{>0}$ and consider the principal ideal $n\mathbb{Z}$ of the ring \mathbb{Z} generated by $n \in \mathbb{Z}$.

As an additive group, $n\mathbb{Z}$ is the infinite cyclic group generated by n .

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is the finite commutative ring with n elements; these elements are precisely the *congruence classes* of integers modulo n .

2.5 Isomorphism Theorem

Theorem 2.5.1. *Let R, S be commutative rings with identity and let $\phi : R \rightarrow S$ be a ring homomorphism. Assume that ϕ is surjective (i.e. onto). Then ϕ determines an isomorphism $\bar{\phi} : R/I \rightarrow S$ where $I = \ker \phi$, where $\bar{\phi}$ is determined by the rule*

$$\bar{\phi}(a + I) = \phi(a) \quad \text{for } a \in R.$$

Proof. First, you must confirm that $\bar{\phi}$ is *well-defined*; i.e. that if $a + I = a' + I$ then $\bar{\phi}(a + I) = \bar{\phi}(a' + I)$.

Next, you must confirm that $\bar{\phi}$ is a ring homomorphism (this is immediate from the definition of ring operations on R/I).

Finally, you must confirm that $\ker \bar{\phi} = \{0\}$, where here 0 refers to the additive identity of the quotient ring R/I . This additive identity is of course the trivial coset $I = 0 + I \in R/I$. \square

2.6 A Homomorphism from the polynomial ring to the scalars

Let F is a field and let $a \in F$. consider the mapping

$$\Phi : F[T] \rightarrow F$$

given by $\Phi(f(T)) = f(a)$. Namely, applying Φ to a polynomial $f(T)$ results in the value $f(a)$ of $f(T)$ at a .

The definition of multiplication in $F[T]$ guarantees that Φ is a ring homomorphism.

3 2025-01-27 - Polynomials over a field and the division algorithm

3.1 Some general notions for commutative rings

Definition 3.1.1. If R is a commutative ring with 1 and if $u \in R$ we say that u is a *unit* - or that u is *invertible* - provided that there is $v \in R$ with $uv = 1$; then $v = u^{-1}$.

We write R^\times for the units in R .

A commutative ring R is a *field* provided that every non-zero element is invertible. Thus R is a field if $R^\times = R \setminus \{0\}$.

Proposition 3.1.2. *If R is a commutative, then R^\times is an abelian group (with operation the multiplication in R).*

For any commutative ring R and elements $a, b \in R$ we say that a **divides** b - written $a \mid b$ - if $\exists x \in R$ with $ax = b$.

Proposition 3.1.3. *For $a, b \in R$ we have $a \mid b$ if and only if $b \in \langle a \rangle$.*

Recall that we introduced the principal ideal $\langle a \rangle = aR$ for any commutative ring R and any $a \in R$. In fact, given $a_1, \dots, a_n \in R$ we can consider the ideal

$$\langle a_1, \dots, a_n \rangle = \sum_{i=1}^n a_i R$$

defined as

$$\langle a_1, \dots, a_n \rangle = \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R \right\}.$$

It is straightforward to check that $\langle a_1, \dots, a_n \rangle$ is indeed an ideal of R .

Definition 3.1.4. A non-zero element $a \in R$ is said to be a *0-divisor* provided that there is $0 \neq b \in R$ with $ab = 0$.

Example 3.1.5. Let n be a composite positive integer, so that $n = ij$ for integers $i, j > 0$. Consider the elements $[i] = i + n\mathbf{Z}, [j] = j + n\mathbf{Z}$ in the quotient ring $\mathbf{Z}/n\mathbf{Z}$.

Then $[i]$ and $[j]$ are both non-zero since $0 < i, j < n$ so that $n \nmid i$ and $n \nmid j$. But $[i] \cdot [j] = [n] = 0$ so that $[i]$ and $[j]$ are 0-divisors of the ring $\mathbf{Z}/n\mathbf{Z}$.

Definition 3.1.6. A commutative ring R is said to be an *integral domain* provided that it has no zero-divisors.

Example 3.1.7. (a) Any field is an integral domain.

(b) The ring \mathbf{Z} of integers is an integral domain.

(c) Any subring of an integral domain is an integral domain.

For example, the ring $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$ of gaussian integers is an integral domain.

(d) $\mathbf{Z}/n\mathbf{Z}$ is not an integral domain whenever n is composite.

(e) If R and S are commutative rings, the direct product $R \times S$ is *never* an integral domain. Indeed, the elements $(1, 0)$ and $(0, 1)$ are 0-divisors.

Lemma 3.1.8. (Cancellation) Let R be an integral domain and let $a, b, c, \in R$ with $c \neq 0$. If $ac = bc$ then $a = b$.

Proof. The equation $ac = bc$ implies that $ac - bc = 0$ so that $(a - b)c = 0$ by the distributive property. Since R has no zero divisors and since $c \neq 0$ by assumption, conclude that $a - b = 0$ i.e. that $a = b$. \square

Proposition 3.1.9. Let R be an integral domain and let $d, d' \in R \setminus \{0\}$. If $\langle d \rangle = \langle d' \rangle$ then d and d' are associate.

Proof. Since $d \in \langle d' \rangle$ we may write $d = xd'$ and since $d' \in \langle d \rangle$ we may write $d' = yd$. Now we see that $d = xd' = xyd$. Since $d \neq 0$ cancellation (Lemma 3.1.8) implies that $xy = 1$. Thus $x, y \in R^\times$ and indeed d, d' are associate. \square

3.2 The degree of a polynomial

Let F be a field and consider the ring of polynomials $F[T]$.

Definition 3.2.1. The *degree* of a polynomial $f = f(T) \in F[T]$ is defined to be $\deg(f) = -\infty$ if $f = 0$, and otherwise $\deg(f) = n$ where

$$f = \sum_{i=0}^n a_i T^i \quad \text{with each } a_i \in F \text{ and } a_n \neq 0.$$

We have some easy and familiar properties of the degree function:

Proposition 3.2.2. Let $f, g \in F[T]$.

- (a) $\deg(fg) = \deg(f) + \deg(g)$.
- (b) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ and equality holds if $\deg(f) \neq \deg(g)$.
- (c) $f \in F[T]^\times$ if and only if $\deg(f) = 0$. In particular, $F[T]^\times = F^\times$.

Corollary 3.2.3. For a field F , the polynomial ring $F[T]$ is an integral domain.

Proof. Let $f, g \in F[T]$ and suppose that $fg = 0$. We must argue that either $f = 0$ or $g = 0$. \square

Proposition 3.2.4. Let $f, g \in F[T]$. If $g \neq 0$ and $\deg g < \deg f$ then $[g] = g + \langle f \rangle$ is a non-zero element of $F[T]/\langle f \rangle$.

3.3 The division algorithm

Theorem 3.3.1. Let F be a field, and let $f, g \in F[T]$ with $0 \neq g$. Then there are polynomials $q, r \in F[T]$ for which

$$f = qg + r$$

and $\deg r < \deg g$.

Proof. First note that we may suppose f to be non-zero. Indeed, if $f = 0$, we just take $q = r = 0$. Clearly $f = qg + r$, and $\deg(r) = -\infty < \deg(g)$ since g is non-zero.

We now proceed by induction on $\deg(f) \geq 0$.

For the base case in which $\deg(f) = 0$, we note that $f = c$ is a constant polynomial; here $c \in F^\times$.

If $\deg(g) = 0$ as well, then $g = d \in F^\times$ and then $c = (c/d)d + 0$ so we may take $q = c/d$ and $r = 0$. Now $\deg(r) = -\infty < \deg(g)$ as required.

If $\deg(g) > 0$, we simply take $q = 0$ and $r = f$: we then have $f = 0 \cdot g + f$ and $\deg(f) = 0 < \deg(g)$ as required.

We have now confirmed the Theorem holds when $\deg(f) = 0$.

Proceeding with the induction, we now suppose $n > 0$ and that the Theorem holds whenever f has degree $< n$. We must prove the Theorem holds when f has degree n .

Since f has degree n , we may write $f = a_n T^n + f_0$ where $a_n \in F^\times$ and $f_0 \in F[T]$ has $\deg(f_0) < n$.

Let us write $g = \deg(g)$; we may write $g = b_m T^m + g_0$ where $b_m \in F^\times$ and $g_0 \in F[T]$ has $\deg(g_0) < m$.

If $n < m$ we take $q = 0$ and $r = f$ to find that $f = qg + r$ and $\deg(r) < \deg(g)$.

Finally, if $m \leq n$ we set

$$f_1 = f - (a_n/b_m)T^{n-m}g = a_n T^n + f_0 - \left(\frac{a_n}{b_m} b_m T^n + \frac{a_n}{b_m} T^{n-m} g_0 \right) = f_0 - \frac{a_n}{b_m} T^{n-m} g_0.$$

We have $\deg(f_0) < n$ by assumption, and $\deg\left(\frac{a_n}{b_m} T^{n-m} g_0\right) < n$ by the Proposition together with the fact that $\deg(g_0) < m$.

Thus $\deg(f_1) < n$. Now we apply the induction hypothesis to write

$$f_1 = q_1 g + r_1 \quad \text{with } \deg(r_1) < \deg(g).$$

Finally, we have

$$f = f_1 + (a_n/b_m)T^{n-m}g = q_1 g + r_1 + (a_n/b_m)T^{n-m}g = (q_1 + (a_n/b_m)T^{n-m})g + r_1$$

so we have indeed written $f = qg + r$ in the required form. \square

Corollary 3.3.2. *Let F be a field and let $f \in F[T]$. For $a \in F$, there is a polynomial $q \in F[T]$ for which*

$$f = q(T - a) + f(a).$$

Corollary 3.3.3. *For $f \in F[T]$ an element $a \in F$ is a **root** of the polynomial f if and only if $T - a \mid f$ in $F[T]$.*

4 2025-01-29 - ideals of the polynomial ring

4.1 Ideals of the polynomial ring $F[T]$

Corollary 4.1.1. *Let F be a field and let I be an ideal of the ring $F[T]$. Then I is a principal ideal; i.e. there is $g \in I$ for which*

$$I = \langle g \rangle = g \cdot F[T].$$

Proof. If $I = \{0\}$ ⁴ the result is immediate. Thus we may suppose $I \neq 0$.

Consider the set $\{\deg(g) \mid 0 \neq g \in I\}$. This is a non-empty set of natural numbers, hence it contains a minimal element by the **well-ordering principle**.

Choose $g \in I$ such that $\deg(g)$ is this minimal degree; we claim that $I = \langle g \rangle$.

Clearly $\langle g \rangle \subseteq I$. To complete the proof, it remains to establish the inclusion $I \subseteq \langle g \rangle$. Let $f \in I$ and use the **Division Algorithm** to write $f = qg + r$ for $q, r \in F[T]$ with $\deg r < \deg g$.

Observe that $f - qg \in I$ so that $r \in I$. Since $\deg r < \deg g$ conclude that $r = 0$. This shows that $f = qg \in \langle g \rangle$ as required, completing the proof. \square

Let F be a field, $F[T]$ be the ring of polynomials with coefficients in F , let $f, g \in F[T]$ be polynomials which are not both 0.

Definition 4.1.2. The **greatest common divisor** $\gcd(f, g)$ of the pair f, g is a monic polynomial d such that

- (a) $d \mid f$ and $d \mid g$,
- (b) if $e \in F[T]$ satisfies $e \mid f$ and $e \mid g$, then $e \mid d$.

Remark 4.1.3. If d, d' are two gcds of f, g then $d \mid d'$ and $d' \mid d$. In particular, $\deg(d) = \deg(d')$ and $d' = \alpha d$ for some $\alpha \in F^\times$. It is then clear that there is no more than one monic polynomial satisfying i. and ii.

Proposition 4.1.4. *Let $f, g \in F[T]$ not both 0⁵.*

(a) $\langle f, g \rangle$ is an ideal. According to the previous corollary, there is a monic polynomial $d \in F[T]$ with

$$\langle d \rangle = \langle f, g \rangle.$$

Then $d = \gcd(f, g)$

(b) In particular, $d = \gcd(f, g)$ may be written in the form $d = uf + vg$ for $u, v \in F[T]$.

Proof. For a., write $I = \langle f, g \rangle = \langle d \rangle$. Since $f, g \in I$, the definition of $\langle d \rangle$ shows that $d \mid f$ and $d \mid g$.

Now suppose that $e \in F[T]$ and that $e \mid f$ and $e \mid g$. Then $f, g \in \langle e \rangle$ which shows that $\langle f, g \rangle \subseteq \langle e \rangle$.

But this implies that $\langle d \rangle \subset \langle e \rangle$ so that $e \mid d$ as required. Thus we see that d is indeed equal to $\gcd(f, g)$.

Since $d \in \langle d \rangle = \langle f, g \rangle$, assertion b. follows from the definition of $\langle f, g \rangle$. \square

⁴We will write simply 0 for the ideal $\{0\}$.

⁵Note that f, g are not both 0 if and only if the ideal $\langle f, g \rangle$ is not 0.

4.2 Principal ideal domains (PIDs) and gcds

Definition 4.2.1. An integral domain R is said to be a **principal ideal domain** (abbreviated PID) provided that every ideal I of R has the form

$$I = \langle a \rangle \quad \text{for some } a \in R;$$

i.e. provided that every ideal of R is principal.

Example 4.2.2. (a) The ring \mathbf{Z} of integers is a PID.

(b) For any field F , the ring $F[T]$ of polynomials is a PID - this follows from the Corollary to the division algorithm, above.

(c) The rings $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{2}]$ are PIDs - to see this one can argue that these rings are Euclidean domains and then one proves that any Euclidean domain is a PID.

5 2025-02-03 - prime elements and unique factorization

5.1 Prime elements in a PID

Let R be a PID.

For $a_1, \dots, a_n \in R$ write $\langle a_1, \dots, a_n \rangle = Ra_1 + \dots + Ra_n$ for the ideal generated by the a_i , as before.

Our results about gcd in the polynomial ring actually hold in the generality of the PID R . We quickly give the statements:

Definition 5.1.1. Let $a, b \in R$ such that $\langle a, b \rangle \neq 0$. A gcd of a and b is an element $d \in R$ such that

- (i) $d \mid a$ and $d \mid b$ (in words: " d is a common divisor of a and b ")
- (ii) if $e \mid a$ and $e \mid b$ then $e \mid d$. (in words: "any common divisor of a and b divides d ")

Definition 5.1.2. Two elements $d, d' \in R$ are said to be *associates* provided that there is a unit $u \in R^\times$ for which $d = ud'$.

It is straightforward to check that the property " d and d' are associates" defines an equivalence relation on R .

Lemma 5.1.3. *Let R be an integral domain and let $d, d' \in R$.*

- (a) *If $\langle d \rangle = \langle d' \rangle$ then d and d' are associates.*
- (b) *If R is a PID and if d and d' are gcds of a and b then d and d' are associates.*

Proof. Using the definition of gcd we see that $d \mid d'$ and $d' \mid d$. Thus $d' = dv$ and $d = d'u$ for $u, v \in R$.

This shows that $d' = dv = d'uv$. Using cancellation, find that $1 = uv$ so that $u, v \in R^\times$. \square

Remark 5.1.4. This definition of course covers the cases when $R = \mathbf{Z}$ and when $R = F[T]$. The main thing to point out is that when $R = \mathbf{Z}$, there is a unique **positive** gcd for any pair $a, b \in \mathbf{Z}$ and when $R = F[T]$ there is a unique **monic** gcd for any pair $f, g \in F[T]$.

For a general PID there need not be a natural choice of gcd, so for $x, y \in R$ we can only speak of $\gcd(x, y)$ up to multiplication by a unit of R .

Proposition 5.1.5. *Let R be a PID and let $x, y \in R$ with $\langle x, y \rangle \neq 0$.*

- (a) *Since R is a PID, we may write find $d \in R$ with*

$$\langle d \rangle = \langle x, y \rangle.$$

Then $d = \gcd(x, y)$.

- (b) *In particular, $d = \gcd(x, y)$ may be written in the form $d = ux + vv$ for $u, v \in R$.*

To prove Proposition 5.1.5 proceed as in the proof of Proposition 4.1.4.
Let R be a PID.

Definition 5.1.6. A non-zero element $p \in R$ is said to be **irreducible** provided that $p \notin R^\times$ and whenever $p = xy$ for $x, y \in R$ then either $x \in R^\times$ or $y \in R^\times$.

Remark 5.1.7. Assume that $p, a \in R$ with p irreducible. Then either $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

Proposition 5.1.8. $p \in R$ is irreducible if and only if (\clubsuit): whenever $a, b \in R$ and $p \mid ab$ then either $p \mid a$ or $p \mid b$.

Proof. (\Rightarrow): Assume that p is irreducible, suppose that $a, b \in R$ and that $p \mid ab$. We must show that $p \mid a$ or $p \mid b$.

For this, we may as well suppose that $p \nmid a$; we must then prove that $p \mid b$. Since $p \nmid a$, we see that $\gcd(a, p) = 1$ by the Remark above. Then $ua + vp = 1$ for elements $u, v \in R$.

Now we see that

$$b = 1 \cdot b = (ua + vp) \cdot b = uab + vpb.$$

Since $p \mid ab$ we see that $p \mid uab + vpb$ which proves that $p \mid b$, as required.

(\Leftarrow): Assume that condition (\clubsuit) holds for p . We must show that p is irreducible. For this, assume $p = xy$ for $x, y \in R$; we must show that either $x \in R^\times$ or $y \in R^\times$.

Since $p = xy$, in particular $p \mid xy$ and we may apply (\clubsuit) to conclude without loss of generality that $p \mid x$.

Write $x = pa$. We now see that $p = xy = pay$; by cancellation, find that $1 = ay$ so that $y \in R^\times$. We conclude that p is irreducible, as required. \square

Example 5.1.9. If $f \in F[T]$ is reducible (i.e. not irreducible) then the quotient ring $F[T]/\langle f \rangle$ is not an integral domain.

Indeed, write $f = gh$ for $g, h \in F[T]$ non-units. Thus $\deg f > \deg g, \deg h > 0$ by Proposition 3.2.2. According to Proposition 3.2.4, the classes $[g], [h] \in F[T]$ are non-zero, but $[g] \cdot [h] = [f] = 0$. Thus $F[T]/\langle f \rangle$ has zero divisors and is not an integral domain.

5.2 Unique factorization in a PID

Theorem 5.2.1. Let R be a PID, let $0 \neq a \in R$, and suppose that a is not a unit.

- (a) There are irreducible elements $p_1, p_2, \dots, p_n \in R$ such that $a = p_1 \cdot p_2 \cdot \dots \cdot p_n$.
- (b) if $q_1, \dots, q_m \in R$ are irreducibles such that $a = q_1 \cdot \dots \cdot q_m$ then $n = m$ and – after possibly reordering the q_i – there are units $u_i \in R^\times$ for which $q_i = u_i p_i$ for each i .

Proof. We first prove (a).

For this, we first prove the following claim:

(*): if the conclusion of (a) fails, there is a sequence of elements $a_1, a_2, \dots \in R$ with the property that for each $i \geq 1$ we have:

- $a_{i+1} \mid a_i$ and
- a_i and a_{i+1} are not associate.

Note that if a is irreducible, we are done. Otherwise, we can write $a = xy$ with $x, y \in R$ and $x, y \notin R^\times$. \square

6 Irreducible polynomials over a field

6.1 Fields as quotient rings

Proposition 6.1.1. *Let F be a field and let f be an irreducible polynomial in $F[T]$. Then $F[T]/\langle f \rangle$ is a field.*

6.2 Some criteria for irreducibility

Proposition 6.2.1. *Let F be a field and let $f \in F[T]$ be a polynomial with $\deg(f) \leq 3$. If f has no root in F then f is irreducible.*

7 The Field of fractions of an Integral Domain

Recall Example 3.1.7 that any subring of a field is an integral domain. We now want to argue that the *converse* to this statement is true, as well. Namely, an integral domain R is a subring of a field. In fact, we are essentially going to give a *construction* of such a field from R .

Let's fix an integral domain R . To confirm the suggested converse to the above Corollary, we must construct a field F and an inclusion $i : R \subset F$.

Of course, if we have such a mapping i , then for any $0 \neq b \in R$, the element $i(b)$ is non-zero in F and hence $i(b)^{-1} = \frac{1}{i(b)}$ should be an element of F (even though $i(b)^{-1}$ is possibly not an element of R). For any $a \in R$ we should be able to multiply $i(a)$ and $\frac{1}{i(b)}$ in F to form the fraction $\frac{i(a)}{i(b)}$. If we choose to identify R with the image $i(R)$, we might simply write $\frac{a}{b} = \frac{i(a)}{i(b)}$ for this fraction.

So if the field F exists, it must contain all fractions $\frac{a}{b}$ for $a, b \in R$ with $0 \neq b$.

In fact, we are going to construct a field F by formally introducing such fractions.

Consider the set $W = \{(a, b) \mid a, b \in R, b \neq 0\}$ and define a relation \sim in W by the condition

$$(a, b) \sim (s, t) \iff at = bs.$$

This relation is motivated by the observation that for *fractions* in a field F we have

$$\frac{a}{b} = \frac{s}{t} \iff at = bs.$$

One needs to check the following:

Proposition 7.0.1. \sim defines an equivalence relation on W .

Proof. We must confirm properties of \sim :

(*reflexive*) if $(a, b) \in W$, then $ab = ba \implies (a, b) \sim (a, b)$.

(*symmetric*) if $(a, b), (s, t) \in W$ then

$$(a, b) \sim (s, t) \implies at = bs \implies sb = ta \implies (s, t) \sim (a, b).$$

(*transitive*) Let $(a, b), (s, t), (u, v) \in W$ and suppose that $(a, b) \sim (s, t)$ and $(s, t) \sim (u, v)$.

The assumptions mean that $at = bs$ and $sv = tu$.

Multiplying the equation $at = bs$ by v on each side, we see that

$$atv = bsv \implies atv = btu \implies (av)t = (bu)t;$$

since $t \neq 0$ and since the cancellation law holds in an integral domain, conclude $av = bu$.

Hence $(a, b) \sim (u, v)$ which confirms the transitive law.

□

We are now going to show that the fractions - i.e. the equivalence classes in W - form a field. We define $Q = Q(R)$ to be the set of equivalence classes of W under the equivalence relation \sim .

We write $\frac{a}{b} = [(a, b)]$ for the equivalence class of $(a, b) \in W$. Thus Q is the set of (formal) fractions of elements of R , and

$$\frac{a}{b} = \frac{s}{t} \iff (a, b) \sim (s, t) \iff at = bs$$

It remains to argue that Q has the structure of a field. To do this, we must define binary operations $+$ and \cdot on the set Q and check that they satisfy the correct axioms.

Define addition of fractions: for $a, b, s, t \in R$ with $b, t \neq 0$,

$$(\clubsuit) \quad \frac{a}{b} + \frac{s}{t} = \frac{at + bs}{bt}.$$

And define multiplication of fractions:

$$(\diamond) \quad \frac{a}{b} \cdot \frac{s}{t} = \frac{as}{bt}.$$

Theorem 7.0.2. *For an integral domain R , the set $Q(R)$ of fractions of R forms a field with the indicated addition and multiplication.*

Sketch of proof. What must be checked??

- must first confirm that (\clubsuit) is *well-defined!* i.e. if $a', b', s', t' \in R$ with $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{s}{t} = \frac{s'}{t'}$, we must check that $\frac{a}{b} + \frac{s}{t} = \frac{a'}{b'} + \frac{s'}{t'}$; i.e. that

$$\frac{at + bs}{bt} = \frac{a't' + b's'}{b't'}.$$

This is straightforward if a bit tedious.

- One readily checks that $0 = \frac{0}{1}$ is an identity for the binary operation $+$ on Q .
- One readily checks that $+$ is commutative for Q .
- One readily checks that $\frac{-a}{b}$ is an additive inverse for $\frac{a}{b}$.
- With some more effort, one confirms that $+$ is *associative* on Q ; i.e. for $\alpha, \beta, \gamma \in Q$

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma).$$

Thus $(Q, +)$ is an abelian group. Now consider the operation \diamond of multiplication.

- must again confirm that (\diamond) is *well-defined!* i.e. if $a', b', s', t' \in R$ with $\frac{a}{b} = \frac{a'}{b'}$ and $\frac{s}{t} = \frac{s'}{t'}$, we must check that $\frac{a}{b} \cdot \frac{s}{t} = \frac{a'}{b'} \cdot \frac{s'}{t'}$; i.e. that

$$\frac{as}{bt} = \frac{a's'}{b't'}.$$

- One readily checks that $1 = \frac{1}{1}$ is an identity for the binary operation \cdot on Q .
- One readily checks that \cdot is commutative for Q .
- With some more effort, one confirms that \cdot is *associative* on Q ; i.e. for $\alpha, \beta, \gamma \in Q$

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma).$$

- Next, one must confirm the *distributive law*: for $\alpha, \beta, \gamma \in Q$,

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma.$$

Phew! □

Remark 7.0.3. Despite the details of the preceding proof, all that is happening is confirming properties of operations of fractions that you have used since grade-school. . .

Now, we want to emphasize a crucial property of the field of fractions of an integral domain.

Let $Q(R)$ be the field constructed above, and note that there is a natural ring homomorphism $i : R \rightarrow Q(R)$ given by $r \mapsto i(r) = \frac{r}{1}$ for $r \in R$. This homomorphism is one-to-one: indeed, if $\frac{r}{1} = 0 = \frac{0}{1}$, then $r \cdot 1 = 0 \cdot 1 \implies r = 0$. Thus, we may identify R with a subring of $Q(R)$.

Proposition 7.0.4. *Let R be an integral domain, let $\phi : R \rightarrow S$ be any ring homomorphism, and suppose that for all $0 \neq d \in R$, $\phi(d) \in S^\times$ - i.e. $\phi(d)$ is a unit in S . Then there is a unique homomorphism $\tilde{\phi} : Q(R) \rightarrow S$ with the property that $\tilde{\phi}|_R = \phi$.*

Proof. Let $x \in Q(R)$ be any element. Thus $x = \frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b}$ for $a, b \in R$ with $b \neq 0$.

Let's first argue that uniqueness of $\tilde{\phi}$. If $\tilde{\phi}$ is a ring homomorphism, then

$$1 = \tilde{\phi}(1) = \tilde{\phi}(b \cdot \frac{1}{b}) = \phi(b)\tilde{\phi}(\frac{1}{b}) \implies \tilde{\phi}(\frac{1}{b}) = \phi(b)^{-1}$$

Since $\tilde{\phi}$ is a ring homomorphism, we must have

$$(\clubsuit) \quad \tilde{\phi}(x) = \tilde{\phi}(\frac{a}{1})\tilde{\phi}(\frac{1}{b}) = \phi(a) \cdot \phi(b)^{-1}$$

which confirms the uniqueness.

It now only remains to check that the rule (\clubsuit) determines a ring homomorphism, which is straightforward. □

Example 7.0.5. The field of rational functions

Let F be a field, and consider $R = F[T]$ the ring of polynomials. This is an integral domain, and its field of fractions $Q(R)$ is usually written $F(T)$ and is known as the field of rational functions over F .

Note that

$$F(T) = \left\{ \frac{f}{g} \mid f, g \in F[T] \right\};$$

thus elements of $F(T)$ are fractions $\frac{f}{g}$ whose numerator and denominator are *polynomials*; we usually call such expressions *rational functions*.

7.1 Another field of fractions

Let p be a prime number and consider the field $F = \mathbf{Q}(\alpha)$ obtained by adjoining a cube root $\alpha = p^{1/3}$ of p to \mathbf{Q} .

Since $T^3 - p \in \mathbf{Q}[T]$ is irreducible, results reviewed earlier show that F has a \mathbf{Q} -basis consisting of $\{1, \alpha, \alpha^2\}$ – i.e. every element can be expressed uniquely in the form

$$a + b\alpha + c\alpha^2 \quad \text{for } a, b, c \in \mathbf{Q}$$

Consider the subset

$$R = \mathbb{Z}[\alpha] = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}\} \subset F$$

Lemma 7.1.1. *R is a subring of F . In particular, since F is a field, R is an integral domain.*

Sketch of proof. One must check the following:

- R is an additive subgroup of F
- R is closed under the multiplication of F .

□

Since R is an integral domain, we can construct its field of fractions $Q = Q(R)$.

In fact, we have

`{lem:field-isom}`

Proposition 7.1.2. *There is an isomorphism of fields $Q(R) \simeq F = \mathbf{Q}(\alpha)$.*

Proof. Write $\phi : R \rightarrow F$ for the inclusion mapping given by $\phi(x) = x$ (this looks confusing; the point is that $x = a + b\alpha + c\alpha^2$ with $a, b, c \in \mathbb{Z}$, and to view $x \in F$ we just view $a, b, c \in \mathbf{Q}$).

Since ϕ is one-to-one, if $0 \neq x \in R$ then $0 \neq \phi(x)$; since F is a field $\phi(x) \in F^\times$. Thus the Proposition above implies that there is a ring homomorphism $\tilde{\phi} : Q(R) \rightarrow F$.

Of course, since $Q(R)$ is a field, $\tilde{\phi}$ is one-to-one. So it only remains to check that $\tilde{\phi}$ is onto.

Let $x = s + t\alpha + u\alpha^2 \in F$ for $s, t, u \in \mathbf{Q}$.

Now find $a, b, c, d \in \mathbb{Z}$ so that $s = \frac{a}{d}, t = \frac{b}{d}, u = \frac{c}{d}$.

Then $x = s + t\alpha + u\alpha^2 = \frac{a + b\alpha + c\alpha^2}{d} \in Q(R)$ is a fraction of elements in $\mathbb{Z}[\alpha] = R$ – i.e. is in the image of $\tilde{\phi}$. □

7.2 Eisenstein's criteria

Let A be a PID and let $p \in A$ be *irreducible*. Write F for the *field of fractions* of A .

Theorem 7.2.1. *Let $f = T^n + \sum_{i=0}^{n-1} a_i T^i \in A[T]$, where $a_i \in A$. Suppose that $p \mid a_i$ for all i and that $p^2 \nmid a_0$. Then f is irreducible in $F[T]$.*