Math146 - Lecture notes

George McNinch

2025-02-03 18:15:09 EST (george@valhalla)

Contents

1 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 $R \times R \to R$ 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 $a_i \in R$.

---

[1] As 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).

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

[3] Usually 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 $R = \mathrm{Mat}_2(\mathbb{R})$.

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

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

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

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

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

2 Properties of rings

2.1 Ring Homomorphisms

Definition 2.1.1. If R and S are rings, a function $\phi : R \to S$ 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 $\phi : R \to S$ 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 $\phi : R \to S$ 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 $ay, xb, xy \in I$ henc $ay + xb + xy \in I$. 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 $\phi : R \to S$ be a ring homomorphism. Assume that ϕ is* surjective *(i.e.* onto*). Then ϕ determines an isomorphism $\overline{\phi} : R/I \to S$ where $I = \ker \phi$, where $\overline{\phi}$ is determined by the rule*

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

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

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

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

2.6 A Homorphism from the polynomial ring to the scalars

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

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

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 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 $a_1, \cdots, a_n \in R$ we can consider the ideal

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

defined as

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

It is straightforward to check that $\langle a_1, \cdots, a_n \rangle$ 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 An important result on polynomial rings

Proposition 3.2.1. *Let R and S be rings, let $\phi : R \to S$ be a ring homomorphism, and let $\alpha \in S$ be an element. There is a unique ring homomorphism*

$$\Psi : R[T] \to S$$

such that $\Psi(T) = \alpha$ and such that $\Psi_{|R} = \phi$.

Proof. Let $f, g \in R[T]$, say

$$f = \sum_{i=0}^{n} a_i T^i \quad \text{and} \quad g = \sum_{i=0}^{m} b_i T^i$$

be elements of $R[T]$.

To see that Ψ is an additive homomorphism, note that $f + g = \sum_{i=0}^{\max(n,m)} (a_i + b_i)T^i$ so that

$$\Psi(f + g) = \sum_{i=0}^{\max(n,m)} (a_i + b_i)\alpha^i = \sum_{i=0}^{n} a_i\alpha^i + \sum_{i=0}^{m} b_i\alpha^i = \Psi(f) + \Psi(g)$$

Similarly, to see that Ψ is multiplicative, note that $fg = \sum_{i=0}^{n+m} c_i T^i$ where $c_i = \sum_{s+t=i} a_s b_t$. Now,

$$\Psi(fg) = \sum_{i=0}^{n+m} \phi(c_i)\alpha^i = \left(\sum_{i=0}^{n} \phi(a_i)\alpha^i\right)\left(\sum_{i=0}^{m} \phi(b_i)\alpha^i\right) = \Psi(f) \cdot \Psi(g)$$

$\square$

3.3 The degree of a polynomial

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

Definition 3.3.1. 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 3.3.2. *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 3.3.3. *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 3.3.4. *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 $F[T]/\langle f \rangle$.*

3.4 The division algorithm

Theorem 3.4.1. *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

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

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

Corollary 3.4.2. *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 3.4.3. *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 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 results is immediate. Thus we may suppose $I \neq 0$.

Consider the set $\{\deg(g) | 0 \neq g \in I\}$. 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. □

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 0* [5]*.*

(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 $\langle f, g \rangle$. □

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

[5] Note 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)

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 divison 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.

4.3 PIDs and greatest common divisors

Let R be a PID.

The results about gcd in the polynomial ring proved in Section 4.1 actually hold in the generality of the PID R. We quickly give the statements:

Definition 4.3.1. 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")

Lemma 4.3.2. *If R is a PID and if d and d' are* gcd*s of a and b then d and d' are associates.*

Proof. This follows from Proposition 3.1.9 □

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 $u, v \in R^\times$. □

Remark 4.3.3. 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 4.3.4. *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 4.3.4 proceed as in the proof of Proposition 4.1.4.

5 Prime elements and unique factorization

5.1 Irreducible elements

Let R be a principal ideal domain.

Definition 5.1.1. 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 5.1.2. Assume that $p, a \in R$ with p irreducible. Then either $\gcd(p, a) = 1$ or $\gcd(p, a) = p$.

Proposition 5.1.3. *$p \in R$ is irreducible if and only if (♣): 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 (♣) 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 (♣) 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. □

Remark 5.1.4. For any integral domain R, we can speak of *irreducible elements* defined as in Definition 5.1.1. And we can speak of *prime elements*, where an element $p \in R$ is *prime* if it satisfies condition (♣) of Proposition 5.1.3. In this language, Proposition 5.1.3 shows that in a PID, an element is prime iff it is irreducible.

Corollary 5.1.5. *Let R be a PID, let $p, a_1, \cdots, a_n \in R$ with p prime, and suppose that $p \mid a_1 a_2 \cdots a_n = \prod_{i=1}^n a_i$. Then $p \mid a_i$ for some $1 \le i \le n$.*

Example 5.1.6. Let F a field and let $f \in F[T]$ be a non-constant polynomial; i.e. $\deg(f) > 0$. If f is reducible there are polynomials $g, h \in F[T]$ for which $f = gh$ and $\deg(g), \deg(h) > 0$.

Example 5.1.7. 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 3.3.2. According to Proposition 3.3.4, 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

The Fundamental Theorem of Arithmetic says that any integer $n > 1$ may factored uniquely as a product of primes. This result holds for any PID, as follows:

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* $p_1, p_2, \cdots, p_n \in R$ *such that* $a = p_1 \cdot p_2 \cdots p_n$.

(b) *if* $q_1, \cdots, q_m \in R$ *are irreducibles such that* $a = q_1 \cdots q_m$ *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 $a_1, a_2, \cdots \in R \setminus R^\times$ with the property that for each $i \geq 1$ we have: (i) $a_{i+1} \mid a_i$ and (ii) a_{i+1} and a_i are not associate.

To prove ($*$), let $x_1 = a$. Now suppose we have found elements $a_1, a_2, \cdots, a_n$ such that for each $1 \leq i \leq n$ conditions (i) and (ii) hold, and such that the conclusion of (a) fails for a_n. In particular, a_n is reducible, so we may write $a_n = xy$ with $x, y \in R$ and $x, y \notin R^\times$. Without loss of generality, we may suppose that the conclusion of (a) fails for x and we set $a_{n+1} = x$. By construction, $a_{n+1} \mid a_n$; moreover a_{n+1} and a_n are not associates. Thus we have proved by induction that ($*$) holds.

To prove (a), we will now show that ($*$) leads to a contradiction.

Let $\{a_i\}$ be a sequence of elements as in ($*$) and let I be given by

$$I = \bigcup_{i \geq 1} \langle a_i \rangle.$$

Since

$$\langle a_1 \rangle \subset \langle a_2 \rangle \subset \langle a_3 \rangle \subset \cdots$$

it is straightforward to see that I is an ideal. Since R is a PID, we may write $I = \langle d \rangle$ for some $d \in R$. By the definition of I, we may find an index N for which $d \in \langle a_j \rangle$ for each $j \geq N$.

Fix $j \geq N$. We may write $d = x \cdot a_j$ for $x \in R$.

On the other hand, $\langle a_j \rangle \subseteq \langle d \rangle$, we we may write $a_j = y \cdot d$ for $y \in R$.

We now see that $d = x \cdot a_j = xyd$ so that $x, y \in R^\times$ by cancellation (Lemma 3.1.8). Thus d and a_j are *associates* so that $\langle d \rangle = \langle a_j \rangle$. In particular, we have proved that

$$\langle d \rangle = \langle a_N \rangle = \langle a_{N+1} \rangle = \langle a_{N+2} \rangle = \cdots$$

contradicting the assumption (ii) that a_{j+1} and a_j are not associates. This contradiction proves (a).

We now prove (b). We are given an equality

$$p_1 \cdots p_n = q_1 \cdots q_m$$

with p_i, q_j irreducible and $n, m \geq 1$.

We proceed by induction on the minimum $\min(n, m)$, and without loss of generality we suppose that $n \leq m$ so that $n = \min(n, m)$.

In case $n = 1$, our assumption is $p_1 = q_1 \cdots q_m$. Applying Corollary 5.1.5 we see that $p_i \mid q_j$ for some $1 \leq j \leq m$. Since p_i and q_j are irreducible, we see that $q_j = u \cdot p_1$ for some unit $u \in R^\times$ Thus

$$p_1 = u \cdot p_1 \cdot \prod_{i \neq j} q_i.$$

Applying cancellation (Lemma 3.1.8) we see $u \cdot \prod_{i \neq j} q_i = 1$ so that $q_i \in R^\times$ for $i \neq j$. Thus $m = 1$ and p_1 and q_1 are associates, as required. This confirms the base-case of the induction.

Now suppose that $n > 1$ and that the result is known when the element has an expression as a product of $< n$ irreducibles.

Thus we have

$$p_1 \cdots p_n = q_1 \cdots q_m$$

and $m \geq n$. Now $p_n \mid q_1 \cdots q_m$ and as before we see for some $1 \leq j \leq m$ that $q_j = up_n$ for a unit $u \in R^\times$. Without loss of generality we may suppose that $j = m$. We find

$$p_1 \cdots p_{n-1} \cdot p_n = u \cdot p_n \cdot q_1 \cdots q_{m-1}$$

Applying cancellation (Lemma 3.1.8) we find that

$$p_1 \cdots p_{n-1} = uq_1 \cdots q_{m-1}$$

Replacing q_1 by the irreducible uq_1, we can view the right-hand side as a product of $m - 1$ irreducibles. Since $m - 1 \geq n - 1$ we may apply the induction hypothesis to find that $m - 1 = n - 1$ and that after re-ordering we have p_i associate to q_i for $1 \leq i \leq m - 1$. Since p_n and q_m are associate as well, this proves (b). $\square$

6 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 $i(b)^{-1} = \dfrac{1}{i(b)}$ 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 $\dfrac{1}{i(b)}$ in F to form the *fraction* $\dfrac{i(a)}{i(b)}$. If we choose to identify R with the image $i(R)$, we might simply write $\dfrac{a}{b} = \dfrac{i(a)}{i(b)}$ for this *fraction*.

So if the field F *exists*, it must contain all fractions $\dfrac{a}{b}$ 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 6.0.1. $\sim$ *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.

$\square$

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 $\dfrac{a}{b} = [(a, b)]$ 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:

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

Theorem 6.0.2. *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 $\dfrac{a}{b} = \dfrac{a'}{b'}$ and $\dfrac{s}{t} = \dfrac{s'}{t'}$, we must check that $\dfrac{a}{b} + \dfrac{s}{t} = \dfrac{a'}{b'} + \dfrac{s'}{t'}$; 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 $0 = \dfrac{0}{1}$ is an identity for the binary operation $+$ on Q.
- One readily checks that $+$ is commutative for Q.
- One readily checks that $\dfrac{-a}{b}$ is an additive inverse for $\dfrac{a}{b}$.
- 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 $\diamondsuit)$ of multiplication.

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

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

- One readily checks that $1 = \dfrac{1}{1}$ 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! $\square$

Remark 6.0.3. 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 $i : R \to Q(R)$ given by $r \mapsto i(r) = \dfrac{r}{1}$ for $r \in R$. This homomorphism is one-to-one: indeed, if $\dfrac{r}{1} = 0 = \dfrac{0}{1}$, then $r \cdot 1 = 0 \cdot 1 \implies r = 0$. Thus, we may identify R with a subring of $Q(R)$.

Proposition 6.0.4. *Let R be an integral domain, let $\phi : R \to S$ 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 $\widetilde{\phi} : Q(R) \to S$ with the property that $\widetilde{\phi}_{|R} = \phi$.*

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

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

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

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

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

which confirms the uniqueness.

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

Example 6.0.5. The field of rational functions

Let F be a field, and consider $R = F[T]$ the ring of polynomials. This is in 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

$$F(T) = \left\{ \frac{f}{g} \mid f, g \in F[T], g \neq 0 \right\};$$

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

7 Irreducible polynomials over a field

7.1 Fields as quotient rings

Proposition 7.1.1. *Let R be a PID and let $p \in R$ be an irreducible element. Then the quotient ring $A = R/\langle p \rangle$ is a field.*

Proof. Let $\alpha \in A$ be non-zero. To prove that A is a field, we must show that α has a multiplicative inverse. Thus α has the form $h + \langle p \rangle$ and since $\alpha \neq 0$ we know that $p \nmid h$. Since p is irreducible, Remark 5.1.2 shows that $\gcd(p, h) = 1$.

Thus according to Proposition 4.3.4 there are elements $x, y \in R$ for which

$$1 = xp + yh$$

Let $\beta = y + \langle p \rangle \in A$. Then

$$\alpha\beta = yh + \langle p \rangle = 1 + \langle p$$

since $yh \equiv 1 \pmod{p}$. Thus β is the multiplicative inverse of α in A. □

Example 7.1.2. • $\mathbf{Z}/p\mathbf{Z}$ is a field for a prime number p.

As a special case of Proposition 7.1.1, we have:

Corollary 7.1.3. *Let F be a field and let f be an irreducible polynomial in $F[T]$. Then $A = F[T]/\langle f \rangle$ is a field.*

For small degree polynomials, one can confirm irreducibility just by considering roots, as follows:

Proposition 7.1.4. *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.*

Proof. Suppose that f is reducible, say $f = gh$ with $\deg(g), \deg(h) > 0$. Since $\deg(f) \leq 3$ and since $\deg(g) + \deg(h) = \deg(f)$ by Proposition 3.3.2, we see that at least one of g or h must have degree 1; without loss of generality we suppose $\deg(g) = 1$.

Thus $g = aT + b$ for $a, b \in F$ with $a \neq 0$. Set $\alpha = \dfrac{-b}{a} \in F$ and observe that $f(\alpha) = g(\alpha)h(\alpha) = 0$; thus f has the root $\alpha \in F$. □

Example 7.1.5. Let p be a prime number. Then the polynomial $T^2 - p \in \mathbf{Q}[T]$ is *irreducible.* In particular,

$$\mathbf{Q}(\sqrt{p}) = \mathbf{Q}[T]/\langle T^2 - p \rangle$$

is a field.

7.2 The Gauss Lemma

Let R be a PID with field of fractions F. The polynomial ring $R[T]$ is the subring of $F[T]$ consisting of polynomials whose coefficients lie in R. In particular $R[T]$ is itself an integral domain.

Remark 7.2.1. Note that in the case where R is *already* a polynomial ring $F[X]$, we introduce a *new* variable T different from X.

Definition 7.2.2. The *content* content$(f)$of the element $f = \sum_{i=0}^{N} a_i T^i \in R[T]$ where $a_i \in R$ is defined to be

$$\text{content}(f) = \gcd(a_0, a_1, \cdots, a_N).$$

We say that the polynomial $f \in R[T]$ is *primitive* if content$(f) = 1$.

Lemma 7.2.3. *Let $p \in R$ be irreducible and consider the assignment*

$$h \mapsto \overline{h} : R[T] \to (R/\langle p \rangle)[T]$$

defined as follows: for $h = \sum_{i=0}^{N} c_i T^i \in R[T]$ with $c_i \in R$, the polynomial $\overline{h} \in (R/\langle p \rangle)[T]$ is given by

$$\overline{h} = \sum_{i=0}^{N} [c_i] T^i$$

where $[c_i] = c_i + pR$ is the class of c_i modulo pR.

(a) This assignment is a ring homomorphism.

(b) For $h \in R[T]$, $\overline{h} = 0$ if and only if $p \mid \text{content}(h)$.

Proof. (a) follows from Proposition 3.2.1. For (b), just observe that $\overline{h} = 0$ if and only if $p \mid c_i$ for every i. □

Proposition 7.2.4. *("The Gauss Lemma") If $f, g \in R[T]$ are primitive, then the product fg is primitive.*

Proof. Suppose on the contrary that there are primitive polynomials $f, g \in R[T]$ for which fg is not primitive. Writing $d = \text{content}(fg)$ for the content of the product, we know that $\langle d \rangle \neq R$ so that d is divisible by some prime $p \in R$.

Consider the ring homomorphism $h \mapsto \overline{h}$ of Lemma 7.2.3.

Now, $p \mid \text{content}(fg) \implies 0 = \overline{fg} = \overline{f} \cdot \overline{g}$. Since R/pR is a field, the ring $(R/pR)[T]$ is an integral domain, so we may conclude that either $\overline{f} = 0$ or $\overline{g} = 0$.

But according to Lemma 7.2.3 (b), $\overline{f} = 0 \implies p \mid \text{content}(f)$ and $\overline{g} = 0 \implies p \mid \text{content}(g)$. This contradicts our assumption that $1 = \text{content}(f) = \text{content}(g)$. Thus indeed $\text{content}(fg) = 1$. □

Theorem 7.2.5. *Suppose that $f \in R[T]$ is a primitive polynomial, and that $g, h \in K[T]$ are polynomials for which $f = gh$ in $K[T]$. Then there are polynomials $g_1, h_1 \in R[T]$ with $\deg g = \deg g_1$ and $\deg h = \deg h_1$ for which $f = g_1 h_1$ in $R[T]$.*

Proof. We may write $g = \dfrac{x}{y} g_1$ and $h = \dfrac{z}{w} h_1$ where $g_1, h_1 \in R[T]$ are *primitive* and $x, y, z, w \in R$ with $y, w \neq 0$. We now see that

$$(\heartsuit) \quad yw \cdot f = xz \cdot g_1 h_1.$$

Since f is primitive, notice that $yw = \text{content}(ywf)$. Moreover,the Gauss Lemma – i.e. Proposition 7.2.4 – shows that $g_1 h_1$ is primitive; thus, we have $\text{content}(xzg_1h_1) = xz$.

It follows that

$$\langle yw \rangle = \langle xz \rangle$$

i.e. that $(\clubsuit) \quad u \cdot yw = xz$ for a unit $u \in R^\times$ – see Proposition 3.1.9.

But then $(\heartsuit)$ and $(\clubsuit)$ together show that $yw \cdot f = u \cdot yw \cdot g_1 h_1$ and now the cancellation law Lemma 3.1.8 in the integral domain $R[T]$ implies $f = (ug_1) \cdot h_1$ which proves the Theorem. □

7.3 Eisenstein's irreducibility criterion

Theorem 7.3.1. *Let $p \in R$ be irreducible, and let*

$$f = \sum_{i=0}^{n} a_i T^i \in R[T], \quad (\textit{where } a_i \in R,\ 0 \le i \le n)$$

be a polynomial with $a_n \neq 0$. Suppose that $p \nmid a_n$, that $p \mid a_i$ for $0 \le i \le n-1$ and that $p^2 \nmid a_0$. Then f is irreducible when viewed as an element of $F[T]$.

Proof. Let $c = \mathrm{content}(f)$. Then $c \not\equiv 0 \pmod{p}$ since $p \nmid a_n$. Observe now that the polynomial $\widetilde{f} = \dfrac{1}{c} f \in R[T]$ still satisfies the assumptions of the Theorem. Since $\widetilde{f}$ is irreducible in $K[T]$ if and only if the same is true for f, it suffices to prove the Theorem when $f = \widetilde{f}$ is primitive.

Now, according to Theorem 7.2.5 the irreducibility of $f \in F[T]$ will follow once we show that if $f = gh$ for $g, h \in R[T]$ then either $\deg g = 0$ or $\deg h = 0$. So suppose $f = gh$ for $g, h \in R[T]$.

Consider the ring homomorphism $f \mapsto \overline{f} : R[T] \to (R/pR)[T]$ as in Lemma 7.2.3. Assumptions on the coefficients a_i show $\overline{f} = \overline{g}\overline{h}$ to be a non-zero multiple of T^n. Using unique factorization in the principal ideal domain $(R/pR)[T]$, it follows that $\overline{g}$ is a non-zero multiple of T^i and $\overline{h}$ is a non-zero multiple of T^j where $i + j = n$ and $0 \le i, j \le n$. Moreover $i = \deg g$ and $j = \deg h$.

Now the Theorem follows since if $i, j > 0$ then p divides the constant term of both g and h, and then $p^2 \mid a_0$ contradicting our assumption. $\square$