Chapter 4

Factorization

01/22/19

Throughout this chapter, R stands for a commutative ring with unity, and D stands for an integral domain, unless indicated otherwise.

The most important theorem in this course, after the Fundamental Theorem of Galois Theory, can be briefly stated as follows.

Theorem 4.0.1 *Field* $\Rightarrow$ *ED* $\Rightarrow$ *PID* $\Rightarrow$ *UFD* $\Rightarrow$ *ID*

In other words, every field is an Euclidean Domain; every Euclidean Domain is a Principal Ideal Domain; every Principal Ideal Domain is a Unique Factorization Domain; and every Unique Factorization Domain is an Integral Domain. So far, we only have the definition for the first, third, and last of these expressions. In the following sections we will give the appropriate definitions of the other terms, prove each of the implications, and show, by counterexample, that all implications are strict. See Propositions 4.1.2, 4.2.1, 4.4.3, as well as Examples 4.1.1.2, 4.4.1.2, 4.4.2 and Exercise 4.6.1.

4.1 Euclidean Domain

Theorem 4.1.1 [Gallian 16.2] *let F be a field, and $F[x]$ the ring of polynomials with coefficients in F. For any $f(x), g(x) \in F[x]$ with $g(x) \neq 0$, there are unique $q(x), r(x) \in F[x]$ such that*

$$f(x) = q(x)g(x) + r(x) \text{ and } r(x) = 0 or \deg(r(x)) < \deg(g(x).$$

Proof. ∎

Definition 4.1.1. An Euclidean Domain consists of an integral domain D and a function $\delta : D - \{0\} \to \mathbb{N}$, satisfying the following conditions:
For any $f, g \in D$ with $g \neq 0$, there exist $q, r \in D$ s.t.

$$f = gq + r \quad \text{and,} \quad \text{either} \quad r = 0, \quad \text{or} \quad \delta(r) < \delta(g). \tag{4.1}$$

Notes 4.1.1.

The function δ is referred to as *division function*, or *measure*, or *degree*.

Some authors require the function δ to satisfy $\delta(a) \leq \delta(ab)$ for all $a, b \in D - \{0\}$. However, it can be shown that this extra requirement is superfluous.

The q and r are not required to be unique. In fact, in some EDs they are not unique, as we will see below in Example **??**.

Examples 4.1.1. 1. $\mathbb{Z}$ with $\delta(n) = |n|$.

2. Theorem 4.1.1 above shows that for a field F, the ring $F[x]$ of polynomials over F with $\delta(f) = \deg(f)$ forms an Euclidean Domain.

Proposition 4.1.2 *If F is a field, then it is an Euclidean Domain, with $\delta(a) = 1$ for all $a \neq 0$.*

Note that the function δ is never used here, since the residue is always 0. In other words, a field has *exact* division.

We get the following corollaries from Theorem 4.1.1.

Corollary 4.1.3 *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.* multiplicity

Corollary 4.1.4 *Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a root or a zero of $f(x)$ iff $x - a$ is a factor of $f(x)$.*

Definition 4.1.2. Let F be a field, $a \in F$, $f(x) \in F[x]$, and $m \in \mathbb{N}_0$. We say that a is a root of $f(x)$ of ***multiplicity*** m, if there is $g(x) \in F[x]$ such that $f(x) = (x-a)^m g(x)$, and $(x-a)$ is not a factor of $g(x)$. In other words, the multiplicity of a as a root of $f(x)$ is the largest $m \in \mathbb{N}_0$ such that $(x-a)^m$ is a factor of $f(x)$. To say that a is a root of multiplicity 0, simply means that a is **NOT** a root.

Theorem 4.1.5 [Gallian 16.3] *A polynomial of degree n over a field F has at most n zeros, counting multiplicity.*

01/23/19

Proposition 4.1.6 *The ring of Gaussian integers*

$$\mathbb{Z}[i] = \{m + ni \in \mathbb{C} | m, n \in \mathbb{Z}\}$$

with $\delta(m + ni) = m^2 + n^2 = N(m + ni)$, is an Euclidean Domain.

Proof. ■

4.2 Principal Ideal Domain

Definition 4.2.1. A *Principal Ideal Domain* (PID) is an integral domain in which every ideal is principal, i.e. generated by a single element.

Example 4.2.1. $\mathbb{Z}$ is an PID.

We get more examples of PIDs from the following proposition.

Proposition 4.2.1 [Gallian 18.4] *If D is an Euclidean Domain, then it is a PID. Moreover, every non-zero ideal I is generated by a non-zero element of I with smallest δ value.*

Proof. Let $I \trianglelefteq D$. If $I = \{0\}$ then $I = \langle 0 \rangle$.
Assume $I \neq \{0\}$. Let $0 \neq a \in I$, such that $\delta(a)$ is smallest among non-zero elements of I.
Claim: $I = \langle a \rangle$. Clearly $\langle a \rangle \subseteq I$. Let $b \in I$. Since D is an ED there exist $q, r \in D$ such that

$$b = aq + r \quad \text{and,} \quad \text{either } r = 0, \quad \text{or} \quad \delta(r) < \delta(a).$$

Since $a, b \in I$, we that $r = b - aq \in I$. Minimality of $\delta(a)$ force $r = 0$, so $b = aq \in \langle a \rangle$. ■

We get from this proposition and Examples 4.1.1 that in addition to $\mathbb{Z}$, the ring $\mathbb{Z}[i]$ of Gaussian integers is a PID, and for any field F, the ring $F[x]$ of polynomials over F is also a PID.

Corollary 4.2.2

$$\mathbb{R}[x]/\langle x^2 + 1 \rangle \approx \mathbb{C}$$

Proof. Consider the evaluation map

$$\begin{array}{rccc} ev_i : & \mathbb{R}[x] & \to & \mathbb{C} \\ & f(x) & \mapsto & f(i) \end{array}$$

It is an epimorphism, and its kernel is generated by a non-zero element of lowest degree. Clearly $ev_i(x^2 + 1) = 0$, and the kernel has no elements of degree 1. Now apply the first isomorphism theorem. ■

Definition 4.2.2. Let $a, b \in D$. We say that a *divides* b if there is $c \in D$ such that $b = ac$, i.e. $b \in \langle a \rangle$. We may also say that a is a *divisor* of b, or that b is a *multiple* of a.

Lemma 4.2.3 *Let $a, b, b_1, b_2, c, r \in R$.*

1. $a|a$

2. $a|0$

3. $1|a$

4. $a|b$ *and* $b|c \Rightarrow a|c$

5. $a|b_1, a|b_2 \Rightarrow a|(b_1 + b_2)$

6. $a|b \Rightarrow a|rb$

7. $\{b \in R \mid a|b\}$ *is an ideal of* R*. In fact, it is non other than* $\langle a \rangle$*.*

01/25/19

Definition 4.2.3. a, b are said to be *associates* in D if $a|b$ and $b|a$. We write $a \sim b$.

Note 4.2.1. Note that the binary relation "*is associate of*" is an equivalence relation. We'll use the expression "*up to associates*" to refer to elements in the same equivalence class. For example, in Lemma 4.4.7 we will prove that greatest common divisors are unique, up to associates.

Lemma 4.2.4 *Let* $a \in R$*.*

1. $a \sim 0$ *iff* $a = 0$*.*

2. $a \sim 1$ *iff* a *is a unit.*

Proposition 4.2.5 *Let* $a, b \in D$*. TFAE:*

1. a, b *are associates in* D

2. *there is a unit* $u \in D^*$ *such that* $a = ub$

3. $\langle a \rangle = \langle b \rangle$

Proof. (1) ⇒(2) ⇒(3) ⇒(1) ■

4.3 Irreducible and Prime Elements

Recall that for $p \in \mathbb{Z}$, not zero, not ± 1, TFAE:

1. $p = ab \Rightarrow a = \pm 1$ or $b = \pm 1$.

irreducible
prime

2. $p|ab \Rightarrow p|a$ or $p|b$, i.e. $ab \in \langle p\rangle \Rightarrow a \in \langle p\rangle$ or $b \in \langle p\rangle$.

We extend these two ideas to an arbitrary ID D. In general they are not equivalent, like they are in $\mathbb{Z}$. We have an example of that in Examples 4.3.1 below.

Definition 4.3.1. Let $p \in D$ be a non-zero non-unit element (*nznu* for short).

1. We say p is *irreducible* if

$$p = ab \Rightarrow a \quad is\ a\ unit, or \quad b \quad is\ a\ unit.$$

2. We say p is *prime* if

$$p|ab \Rightarrow p|a \text{ or } p|b, \quad \text{i.e.} \quad ab \in \langle p\rangle \Rightarrow a \in \langle p\rangle \text{ or } b \in \langle p\rangle.$$

Notes 4.3.1. 1. Note that the condition for *irreducible* is equivalent to

$$p = ab \Rightarrow p \sim a \text{ or } p \sim b.$$

2. The condition "p is *prime*" is equivalent to "$\langle p\rangle$ *is a prime ideal*".

3. When checking that p is a prime, it suffices to consider the case when a and b are nznu. Otherwise, the condition is trivially satisfied.

Exercise 4.3.1. Show that the properties of being *irreducible* or being *prime* are shared by associates. Given $a, b \in D$, such that $a \sim b$, then

1. a is irreducible iff b is irreducible.

2. a is prime iff b is prime.

Proposition 4.3.1 [Gallian 18.1, 18.2] *Let $p \in D$ be nznu.*

1. *If p is prime then p is irreducible.*

2. *Assume D is a PID. If p is irreducible then p is prime.*

Proof. 1. Assume p is prime. WTS p is irreducible. Suppose $p = ab$. Then $p|ab$ and by primality $p|a$ or $p|b$. WLOG $p|a$, so $a = pc$ for some $c \in D$, and $p = ab = pcb$. Since D is an ID, and $p \neq 0$ we get $1 = cb$, so b is a unit.

2. Assume now that D is a PID and p is irreducible. WTS p is prime. Suppose $p|ab$, where $a, b \in D$. Let

$$I = \{xa + yp | x, y \in D\} = \langle a \rangle + \langle p \rangle \trianglelefteq D$$

Since D is a PID, there is $d \in D$ such that $I = \langle d \rangle$. Now we have $p \in I$ so there is $z \in D$ such that $p = zd$. Since p is irreducible, either d is a unit or $p \sim d$. If d is a unit then $I = D$, and $1 \in D$, so there are $x, y \in D$ such that $1 = xa + yp$. We get $b = xab + ypb$, and since $p|ab$, we get $p|b$. On the other hand, if $p \sim d$ then $\langle p \rangle = \langle d \rangle = I$, and since $a \in I$ we get $p|a$. ■

Examples 4.3.1. 1. The norm function, $N(z)$, defined as the square of the absolute value for any $z \in \mathbb{C}$, is a multiplicative function, i.e. $N(zw) = N(z)N(w)$. In the domain of Gaussian integers, $\mathbb{Z}[i]$, the norm function takes non-negative integer values. It follows that the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$, i.e. the elements with norm 1.

01/28/19 Now, since $N(1 + i) = 2$, it follows that $1 + i$ is irreducible. Since $\mathbb{Z}[i]$ is PID, $1 + i$ is also prime.

2. Consider now the subring of $\mathbb{C}$,

$$\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}.$$

Clearly, it is an ID since it is a subring of an ID. The norm is given by $N(a+b\sqrt{-5}) = a^2 + 5b^2$, and it takes non-negative integer values. The units are ± 1, the only elements with norm 1. The elements $1 \pm \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ have norm $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$. Since there are no elements in $\mathbb{Z}[\sqrt{-5}]$ with norm equal to 2 or 3, it follows that the elements $1 \pm \sqrt{-5}$ are irreducible. However, $1 + \sqrt{-5}$ is not a prime since $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$ but $N(2) = 4$, $N(3) = 9$, and therefore $1+\sqrt{-5}$ cannot divide either 2 or 3. From Proposition 4.3.1.2, we conclude that $\mathbb{Z}[\sqrt{-5}]$ is not a PID. A similar argument shows that 2 and 3 are irreducible but not prime in $\mathbb{Z}[\sqrt{-5}]$. It also shows that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. See Definition 4.4.1 below.

Unique Factorization Domain

Recall that for a field F, the ring of polynomials $F[x]$ is a PID. Hence, *irreducible* and *prime* are equivalent. Deciding whether a polynomial is irreducible or not, is not always an easy task. The following is the first of several irreducibility criteria we will use for that purpose.

Proposition 4.3.2 [Irreducibility Criterion in $F[x]$, Gallian 17.1] *Let F be a field.*

1 Every linear polynomial in $F[x]$ is irreducible.

2 For $f \in F[x]$, with $\deg(f) > 1$, if f has a root in F then it is reducible in $F[x]$.

3 For $f \in F[x]$, with $\deg(f) = 2$ or 3, f is reducible in $F[x]$ iff it has a root in F.

Proof. This follows immediately from the definition of irreducible and Corollary 4.1.4. ■

The result of this proposition does not extend beyond degree 3.

Example 4.3.2. The polynomial $x^4 + 5x^2 + 6 \in \mathbb{Q}[x]$ is reducible, yet it has no root in $\mathbb{Q}$. It factors as $x^4 + 5x^2 + 6 = (x^2 + 2)(x^2 + 3)$.

4.4 Unique Factorization Domain

Definition 4.4.1. An integral domain D is called a *Unique Factorization Domain* (UFD), if every nznu $a \in D$ can be factored as a product of irreducible elements, in a unique way up to order and associates. The uniqueness means that if

$$a = p_1 \cdots p_r = q_1 \cdots q_s,$$

with all the p_is and q_js irreducible, then $r = s$, and, after some possible reordering, we get $p_i \sim q_i$ for $i = 1, \ldots, r$.

By definition, every UFD is an integral domain, so we get for free the implication UFD ⇒ID in Theorem 4.0.1.

To show that an integral domain D is a UFD, we usually break the argument into two parts. For any nznu $a \in D$,

Ascending Chain Condition

Noetherian

Existence: there exists a factorization of a into irreducible factors;

Uniqueness: two such factorizations have the same number of factors, and differ only on the order of the factors, and up to associates.

That is what we will do in the proof of Proposition 4.4.3 below.

Examples 4.4.1. 1. Since $\mathbb{Z}$ is a PID, primes and irreducible elements are the same. The Fundamental Theorem of Arithmetic tells us that $\mathbb{Z}$ is a UFD.

2. Example 4.3.1.2 above shows that in $R = \mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

The four factors have norms 4, 9, 6 and 6, respectively. Therefore, they are irreducible in $\mathbb{Z}[\sqrt{-5}]$. Since the units of R have norm 1, associate elements in R must have the same norm. Therefore, the two factorizations of 6 are not the same up to associates. In conclusion, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. This shows that the implication UFD $\Rightarrow$ID in Theorem 4.0.1 is strict.

3. We will show in Proposition 4.4.3 below, that every PID is a UFD. It follows that for any field F, the ring $F[x]$ is a UFD.

Definition 4.4.2. We say that a ring R satisfies the *Ascending Chain Condition* (ACC), if every ascending chain of ideals

$$I_1 \leq I_2 \leq \cdots$$

has to become constant after a finite number of steps. That is, there is $n \geq 1$, such that $I_n = I_{n+1} = \cdots$. A ring that satisfies the ACC is called *Noetherian*.

Proposition 4.4.1 *Every PID satisfies the ACC, i.e. it is Noetherian.*

Proof. Let D be a PID, and let $I_1 \leq I_2 \leq \cdots$ be an ascending chain of ideals of D. Let $A = \bigcup_{i=1}^{\infty} I_i$.
We first claim that A is an ideal of D. Given $a, b \in A$, there are $i, j \in \mathbb{N}$ such that $a \in I_i$, and $b \in I_j$. WLOG we may assume $j \leq i$. Since the ideals satisfy $I_j \leq I_i$, we have $a, b \in I_i$, and I_i being an ideal, yields $a + b \in I_i$, so $a + b \in A$. For $r \in D$, we have $ra \in I_i$, so $ra \in A$.
Since D is a PID, there is $a \in A$ such that $A = \langle a \rangle$. But then there is $i \in \mathbb{N}$ such that $a \in I_i$, and therefore

$$\langle a \rangle \leq I_i \leq A = \langle a \rangle,$$

which yields $I_i = A$. For any $k \geq i$, we have

$$I_i \leq I_k \leq A = I_i,$$

so $I_k = I_i$. ■

01/29/19

Lemma 4.4.2 *Let D be an integral domain, $a, b, c, u, v, p, q, a_1, \ldots, a_n \in D$.*

1. *uv is a unit iff u and v are units.*
2. *If p is a prime, and $p | a_1 \cdots a_n$ then $p | a_i$ for some $i = 1, \ldots, n$.*
3. *If p is irreducible, q is nznu, and $q | p$ then $p \sim q$.*
4. *If a is nznu, $a = bc$ and $a \sim b$ then c is a unit.*

Proposition 4.4.3 *Let D be an integral domain satisfying:*

1. *ACC, i.e D is Noetherian,*
2. *Every irreducible in prime.*

Then D is a UFD.

Proof. Let $a \in D$ be a nznu. We want to show that a has a factorization into irreducible factors, unique up to order and associates.
Existence: We first prove the following
Claim: Any nznu a has at least one irreducible factor. If a is irreducible, we are done. Otherwise, it can be factored as $a = b_1c_1$ with b_1, c_1 nznu. If b_1 is irreducible, we are done. Otherwise, note that $\langle a\rangle \subsetneqq \langle b_1\rangle$ since c_1 is not a unit, and b_1 can be factored as $b_1 = b_2c_2$ with b_2, c_2 nznu. If b_2 is irreducible, we are done. Otherwise, note that $\langle b_1\rangle \subsetneqq \langle b_2\rangle$ since c_2 is not a unit, and b_2 can be factored as $b_2 = b_3c_3$ with b_3, c_3 nznu. This process has to stop, for otherwise we would have an infinite strictly ascending chain of ideals

$$\langle a\rangle \subsetneqq \langle b_1\rangle \subsetneqq \langle b_2\rangle \subsetneqq \cdots$$

contradicting the ACC assumption.
Now we use the claim above to prove that any nznu a is a product of irreducible factors. If a is irreducible, we are done. Otherwise, write $a = p_1d_1$ where p_1 is irreducible and d_1 a nznu. Note that $\langle a\rangle \subsetneqq \langle d_1\rangle$. If d_1 is irreducible, we are done. Otherwise, write $d_1 = p_2d_2$ where p_2 is irreducible and d_2 a nznu. Note that $a = p_1p_2d_2$, and $\langle d_1\rangle \subsetneqq \langle d_2\rangle$. If d_2 is irreducible, we are done. Otherwise, write $d_2 = p_3d_3$ where p_3 is irreducible and d_3 a nznu. Note that $a = p_1p_2p_3d_3$, and $\langle d_2\rangle \subsetneqq \langle d_2\rangle$. This process has to stop for otherwise we would have an infinite strictly ascending chain of ideals

$$\langle a\rangle \subsetneqq \langle d_1\rangle \subsetneqq \langle d_2\rangle \subsetneqq \cdots$$

Uniqueness: Suppose $a = p_1p_2\cdots p_r = q_1q_2\cdots q_s$, with p_i, q_j irreducible, and prime by the second assumption. WLOG consider $r \leq s$, and proceed by induction on r.
Base case ($r = 1$) We have $a = p_1 = q_1q_2\cdots q_s$. By Lemma 4.4.2, $p_1 \sim q_1$, and if we had $s > 1$ the product $q_2\cdots q_s$ would be a unit, contradicting the assumption that all q_j's are irreducible. Hence $s = 1$.
Inductive step From $a = p_1p_2\cdots p_r = q_1q_2\cdots q_s$, and Lemma 4.4.2.2 we have $p_1|q_j$ for some $1 \leq j \leq s$. Switch q_j with q_1 to have $p_1|q_1$, and by Lemma 4.4.2.3, we get $p_1 \sim q_1$. There is a unit $u \in D$ such that $q_1 = p_1u$.

$$p_1p_2p_3\cdots p_r = p_1uq_2q_3\cdots q_s.$$

Note that $uq_2 \sim q_2$, so, replacing q_2 with uq_2, and using the cancellation property of D we obtain

$$p_2p_3\cdots p_r = q_2q_3\cdots q_s.$$

By inductive hypothesis $r = s$ and, after some possible reordering, $p_i \sim q_i$ for $i = 2, \ldots, r$. ■

From this proposition, together with Propositions 4.4.1 and 4.3.1.2, we get the following corollary.

Corollary 4.4.4 [Gallian 18.3] *Every PID is a UFD.*

This is the last implication needed to complete the proof of Theorem 4.0.1. The following example shows that this implication is strict.

Example 4.4.2. $\mathbb{Z}[x]$ is not a PID. It follows from Theorem 4.4.5 below, that it is a UFD. Let

$$I = \{f(x) \in \mathbb{Z}[x] | \text{ constant term is even}\}.$$

It is easy to see that I is an ideal of $\mathbb{Z}[x]$, but there is no polynomial $f \in \mathbb{Z}[x]$ that generates I. A non-constant f would not have the constant 2 as a multiple in $\mathbb{Z}[x]$. A constant f would have to be even to be in I, and would not have x as a multiple in $\mathbb{Z}[x]$.

We have already seen that when D is an integral domain, the ring $D[x]$ of polynomials over D is also an integral domain. One may ask what properties of D survive when we move to the larger ring $D[x]$. We have seen (see Example 4.1.1.2) that when F is a field, $F[x]$ even though it is not a field, it is an Euclidean Domain. Example 4.4.2 above shows that the properties ED and PID do not survive in general. We will prove that the property of UFD does survive.

Theorem 4.4.5 [Gallian 18.5] *If D is a UFD, then the ring $D[x]$ of polynomials over D is a UFD.*

Based on this theorem, and the fact that $\mathbb{Z}$ is an Euclidean Domain, but $\mathbb{Z}[x]$ is not a PID, the best we can say for the polynomial ring of an integral domain is summarized in the following table.

greatest common divisor

D	$D[x]$
ID	ID
UFD	UFD
PID	UFD
ED	UFD
Field	ED

Corollary 4.4.6 *If D is a UFD then the ring $D[x_1, \dots, x_n]$ of polynomials in several variables over D is a UFD.*

We will need several lemmas and propositions before we can prove Theorem 4.4.5.

Definition 4.4.3. Let $a, b, d \in D$. We say that d is a *greatest common divisor* of a and b provided:

- d is a common divisor, i.e.

$$d|a \text{ and } d|b,$$

- if d' is a common divisor of a and b then $d'|d$, i.e.

$$d'|a \text{ and } d'|b \Rightarrow d'|d.$$

Lemma 4.4.7 *Greatest common divisor of a and b is unique, up to associates, when it exists.*

We will denote by g.c.d.(a, b) "*the*" greatest common divisor of a and b when it exists, understanding that it is well-defined up to associates.

01/30/19

Lemma 4.4.8 *Let D be an ID, $a, b, u \in D$.*

1. g.c.d.$(a, b) \sim$ g.c.d.(b, a), *whenever one of them exists,*
2. g.c.d.$(a, 0) \sim a$,
3. *if u is a unit* g.c.d.$(a, u) \sim 1$,
4. *if $a|b$ then* g.c.d.$(a, b) \sim a$.

In general, g.c.d.(a, b) does not have to exist. We will show that in a UFD it does always exist. Because of Lemma 4.4.8 we only need to consider the case when a and b are nznu.

Example 4.4.3. Consider the ring $R = \mathbb{Z}\left[\sqrt{-5}\right]$ from Example 4.3.1.2. Note that

$$\begin{aligned} (1+\sqrt{-5})(1-\sqrt{-5}) &= 6 = 2\cdot 3 \\ (1+\sqrt{-5})(1+2\sqrt{-5}) &= -9+3\sqrt{-5} = 3(-3+\sqrt{-5}) \end{aligned}$$

We claim that 6 and $-9+3\sqrt{-5}$ do not have a g.c.d. in R. Suppose otherwise, and let $d \sim$ g.c.d.$(6, -9+3\sqrt{-5})$. Since 3 and $1+\sqrt{-5})$ are both common divisors of 6 and $-9+3\sqrt{-5}$, we must have $3|d$ and $1+\sqrt{-5})|d$. The norm is a multiplicative function R taking integer values. Therefore, we must have $N(3)|N(d)$ and $N(1+\sqrt{-5})|N(d)$ in $\mathbb{Z}$. This means $9|N(d)$ and $6|N(d)$, and $18|N(d)$. On the other hand, we have $d|6$ and $d|-9+3\sqrt{-5}$, so $N(d)|36$ and $N(d)|126$. This yields $N(d)|18$, and since $N(d)$ is a non-negative integer, we must have $N(d) = 18$. But the equation $a^2 + 5b^2 = 18$ has no integer solutions.

Lemma 4.4.9 *Let D be an ID, $a, b, c \in D$. We have* g.c.d.$(a,$ g.c.d.$(b, c)) \sim$ g.c.d.(g.c.d.$(a, b), c)$ *whenever one side exists.*

Lemmas 4.4.9 and 4.4.8.1 tell us that g.c.d., as a binary operation when defined, is associative and commutative, up to associates. Therefore, the expression g.c.d.$\{a_1, \ldots, a_n\}$ is well-defined, up to associates.

Lemma 4.4.10.1 gives us a converse to Proposition 4.3.1.1 for UFDs. Proposition 4.3.1.1 already gave us the converse for PIDs. This converse is not true for IDs in general, as Example 4.3.1.2 shows.

Lemma 4.4.10 *Let D be a UFD, $a, p \in D$, nznu.*

1. *If p is irreducible, then it is prime.*
2. *There are finitely many (up to associates) irreducible divisors of a.*

Proof. (1) Assume $p \in D$ is irreducible and let $b, c \in D$ be nznu such that $p|bc$. There is $d \in D$ such that $pd = bc$. Write each b, c, d as a product of irreducibles,

$$\begin{aligned} b &= p_1 \cdots p_j \\ c &= q_1 \cdots q_k \\ d &= r_1 \cdots r_l \end{aligned}$$

so we have $pr_1 \cdots r_l = p_1 \cdots p_j q_1 \cdots q_k$. By uniqueness of the factorization, we must have either $p \sim p_i$ for some $1 \leq i \leq j$ or $p \sim q_i$ for some $1 \leq i \leq k$. It then follows that either $p|a$ or $p|b$. So, p is prime.
(2) Write a as a product of irreducibles $a = p_1 \cdots p_j$. If p is an irreducible that divides a, by Part(4.4.10.1), $p|p_i$ for some $1 \leq i \leq j$. Since p_i is irreducible and p is a nznu, by Lemma 4.4.2.3 we get $p \sim p_i$. Therefore, up to associates, the only irreducible factors of a are $p_1, \ldots, p_j$. ■

Proposition 4.4.11 *Let D be a UFD, $a, b \in D$ nznu.*
Let $p_1, \ldots, p_r$ be the list, without repetitions, of all irreducible factors of either a or b, up to associates. Write

$$\begin{aligned} a &= p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \quad \alpha_i \geq 0, \\ b &= p_1^{\beta_1} \cdots p_r^{\beta_r}, \quad \beta_i \geq 0. \end{aligned}$$

Then a and b have a greatest common divisor, given by

$$\text{g.c.d.}(a, b) = p_1^{\gamma_1} \cdots p_r^{\gamma_r}, \quad \textit{where} \qquad \gamma_i = \min\{\alpha_i, \beta_i\}$$

Proof. Let $d = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$. Since $\gamma_i \leq \alpha_i$, we have $\alpha_i - \gamma_i \geq 0$, so

$$a = dp_1^{\alpha_1 - \gamma_1} \cdots p_r^{\alpha_r - \gamma_r}$$

and $d|a$. Similarly, $d|b$, so d is a common divisor of a and b. If d' is also a common divisor of a and b, then every irreducible factor of d' divides a, and, up to associates, it has to be one of $p_1, \ldots, p_r$. Therefore, we write d' as a product irreducibles, it must take the form $d' = p_1^{\delta_1} \cdots p_r^{\delta_r}$ with $\delta_i \geq 0$. Since d' divides a, there is $e \in D$ such that $a = d'e$. Now, $e|a$, so the same argument used with d', shows that the factorization of e into irreducible factors must have the form $e = p_1^{\mu_1} \cdots p_r^{\mu_r}$ with $\mu_i \geq 0$. Now we have

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r} = d'e = p_1^{\delta_1 + \mu_1} \cdots p_r^{\delta_r + \mu_r}$$

Since $p_1, \ldots, p_r$ are pairwise non-associates, the uniqueness of factorization forces $\alpha_i = \delta_i + \mu_i$, so $\delta_i \leq \alpha_i$. A similar argument shows that $\delta_i \leq \beta_i$, so $\delta_i \leq \min\{\alpha_i, \beta_i\} = \gamma_i$. Therefore, $d = p_1^{\gamma_1} \cdots p_r^{\gamma_r} = d' p_1^{\gamma_1 - \delta_1} \cdots p_r^{\gamma_r - \delta_r}$, and $d'|d$. ■

least common multiple

Corollary 4.4.12 *In any PID and in any ED the operation* g.c.d. *is well-defined, up to associates.*

Note that Proposition 4.4.11 gives us a procedure to find the g.c.d. of two elements in a UFD. The following exercise shows alternative ways to find the g.c.d. of two elements in a PID, and in an ED.

Exercise 4.4.1. 1. Let D be a PID, $a, b \in D$. Let d be a generator of the ideal $\langle a\rangle + \langle b\rangle$. Show that $d \sim \text{g.c.d.}(a, b)$.

2. Let D be an ED, $a, b \in D$, with $b \neq 0$. Consider the sequence $r_0, r_1, r_2, \dots, r_n$ defined recursively as follows: $r_0 = a, r_1 = b$, and using Property 4.1 of an Euclidean Domain, until obtaining a residue 0,

$$\begin{array}{rcllll} r_0 & = & q_1 r_1 + r_2 & \text{and} & \delta(r_2) < \delta(r_1), \\ r_1 & = & q_2 r_2 + r_3 & \text{and} & \delta(r_3) < \delta(r_2), \\ & \vdots & & & \\ r_{n-3} & = & q_{n-2} r_{n-2} + r_{n-1} & \text{and} & \delta(r_{n-1}) < \delta(r_{n-2}), \\ r_{n-2} & = & q_{n-1} r_{n-1} + r_n & \text{and} & r_n = 0. \end{array}$$

Why does the sequence $r_1, r_2, \dots, r_n$ have to eventually attain the value $r_n = 0$? Prove that the last non-zero entry in the residues list, i.e. $r_{n-1} \sim \text{g.c.d.}(a, b)$.

02/01/19

Corollary 4.4.13 *Let* $a, b, c \in D$. $\text{g.c.d.}(ac, bc) \sim c \cdot \text{g.c.d.}(a, b)$.

Definition 4.4.4. Let $a, b, m \in D$. We say that m is a *least common multiple* of a and b provided:

- m is a common multiple, i.e.

$$a|m \text{ and } b|m,$$

- if m' is a common multiple of a and b then $m|m'$, i.e.

$$a|m' \text{ and } b|m' \Rightarrow m|m'.$$

Note that the "*least common multiple*" of a and b is unique, up to associates, when it exists. We denote it by l.c.m.(a,b), understanding that it is well-defined up to associates.

Lemma 4.4.14 *Let D be an ID, $a, b, u \in D$.*

1. l.c.m.$(a,b) \sim$ l.c.m.(b,a), *whenever one of them exists,*
2. l.c.m.$(a,0) \sim 0$,
3. *if u is a unit* l.c.m.$(a,u) \sim a$,
4. *if $a|b$ then* l.c.m.$(a,b) \sim b$.

In general, l.c.m.(a,b) does not have to exist. We will show that in a UFD it does always exist. Because of Lemma 4.4.14 we only need to consider the case when a and b are nznu.

Lemma 4.4.15 *Let D be an ID, $a, b, c \in D$. We have* l.c.m.$(a,$ l.c.m.$(b,c)) \sim$ l.c.m.(l.c.m.$(a,b), c)$ *whenever one side exists.*

Lemmas 4.4.15 and 4.4.14.1 tell us that l.c.m., as a binary operation when defined, is associative and commutative, up to associates. Therefore, the expression l.c.m.$\{a_1, \ldots, a_n\}$ is well-defined, up to associates.

Exercise 4.4.2. 1. Let D be an UFD, $a, b \in D$. Prove that a and b have a least common multiple, and

$$\text{g.c.d.}(a,b) \cdot \text{l.c.m.}(a,b) = a \cdot b,$$

so that when at least one of a and b is non-zero, then

$$\text{l.c.m.}(a,b) = \frac{a \cdot b}{\text{g.c.d.}(a,b)}.$$

2. Let D be an ID, $a, b \in D$. Prove that if a and b have a least common multiple l in D, then $\dfrac{ab}{l}$ is a greatest common divisor of a and b.

content
primitive

4.5 Factorization in $D[x]$

Recall that for any ring R, R is a subring of the ring of polynomials $R[x]$, consisting of all constant polynomials. When D is an ID, the units of $D[x]$ are all constant, and precisely the units of D.

Example 4.5.1. The previous statement about units, requires D to be an ID. In $\mathbb{Z}_4[x]$, the polynomial $1+2x$ is a non-constant unit, as $(1+2x)^2 = 1$.

Definition 4.5.1. Let D be a UFD, $0 \neq f \in D[x]$ with

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

The ***content*** of $f(x)$, denoted $c(f(x))$, is defined as g.c.d.$\{a_0, \ldots, a_n\}$. We'll often write $c(f)$ instead of $c(f(x))$. Note that $c(f)$ is well-defined, up to associates. We say that $f(x)$ is ***primitive*** if $c(f) \sim 1$.

Example 4.5.2. If we take $f(x) = 3x^2 - 12x + 9 \in \mathbb{Z}[x]$ then $c(f) \sim 3$. Note that $f(x) = 3(x^2 - 4x + 3)$ and the second factor is primitive. This holds in general.

Lemma 4.5.1 *Let D be a UFD, $0 \neq f(x), g(x) \in D[x]$, $0 \neq a \in D$.*

1. *$c(af(x)) \sim a \cdot c(f(x))$.*
2. *There is a primitive $\widehat{f}(x) \in D[x]$ such that $f(x) = c(f) \cdot \widehat{f}(x)$. This primitive is unique, up to associates, and $\deg(\widehat{f}(x)) = \deg(f(x))$.*
3. *If $f(x) = ag(x)$ with $g(x)$ primitive, then $c(f) \sim a$.*

Proposition 4.5.2 [Gauss' Lemma] *Let D be a UFD, $0 \neq f(x), g(x) \in D[x]$. If $f(x)$ and $g(x)$ are primitive, then $f(x)g(x)$ is primitive.*

Proof. (By contradiction) Assume $f(x)$ and $g(x)$ are primitive, and $f(x)g(x)$ is not primitive. Write

$$\begin{aligned} f(x) &= a_0 + a_1 x + \cdots + a_n x^n \\ g(x) &= b_0 + b_1 x + \cdots + b_m x^m \\ f(x)g(x) &= c_0 + c_1 x + \cdots + c_{n+m} x^{n+m} \end{aligned}$$

so that $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. Since $f(x)g(x)$ is not primitive, $d = c(f(x)g(x)) =$ g.c.d.$\{c_0, \dots, c_{n+m}\}$ is not a unit, and there is $p \in D$ irreducible such that $p|d$. If follows that $p|c_k$ for every $k = 0, \dots, n+m$. On the other hand, since $f(x)$ and $g(x)$ are primitive, there are a_j and b_l such that $p \not| a_j$ and $p \not| b_l$. Choose j and l smallest, so that $p|a_0, \dots, a_{j-1}, b_0, bl-1$. Then, since

$$c_{j+l} = \sum_{i=0}^{j+l} a_i b_{j+l-i} = \left(\sum_{i=0}^{j-l} a_i b_{j+l-i} \right) + a_j b_l + \left(\sum_{i=j+1}^{j+l} a_i b_{j+l-i} \right)$$

we get that p divides $a_j b_l$. Since p is prime, this forces $p|a_j$ or $p|b_l$, a contradiction. ■

Corollary 4.5.3 *Let D be a UFD, $0 \neq f(x), g(x) \in D[x]$.*

$$c(fg) \sim c(f) \cdot c(g).$$

Proof. Let $\widehat{f}(x), \widehat{g}(x) \in D$ be primitive such that $f(x) = c(f)\widehat{f}(x)$ and $g = c(g)\widehat{g}(x)$. Then $f(x)g(x) = c(f)c(g)\widehat{f}(x)\widehat{g}(x)$. By Gauss's lemma $\widehat{f}(x)\widehat{g}(x)$ is primitive, so by Lemma 4.5.1 we get $c(fg) \sim c(f) \cdot c(g)$, as desired. ■

The converse of Gauss' lemma follows from this corollary and Lemma 4.4.2.

02/04/19

Corollary 4.5.4 *Let D be a UFD, $0 \neq f(x), g(x) \in D[x]$. $f(x)g(x)$ is primitive iff $f(x)$ and $g(x)$ are primitive.*

Lemma 4.5.5 *Let D be a UFD, $f(x) \in D[x]$ with $\deg(f(x)) \geq 1$. If $f(x)$ is irreducible then it is primitive.*

Proof. Let $\widehat{f}(x) \in D[x]$ be primitive such that $f(x) = c(f) \cdot \widehat{f}(x)$. Since $f(x)$ is irreducible, one of $c(f)$ and $f\hat{(x)}$ is a unit. But $\deg(\widehat{f}(x)) = \deg(f(x)) \geq 1$, so $\widehat{f}(x)$ is not a unit, so $c(f)$ is a unit, i.e. $c(f) \sim 1$, and $f(x)$ is primitive. ■

Recall that when R is a subring of S, the polynomial ring $R[x]$ is a subring of $S[x]$. The next proposition relates three rings, a UFD D, its ring of polynomials $D[x]$, and the ring of polynomials of its field of quotients. It connects the concept of irreducible in these three rings.

Proposition 4.5.6 *Let D be a UFD, and Q its field of fractions. Let $p \in D$ and $f(x) \in D[x]$ with $\deg(f(x)) \geq 1$, and $g(x) \in Q[x]$.*

1. *p is irreducible in D iff it is irreducible in $D[x]$.*
2. *There are $a, b \in D$ and a primitive $\widehat{g}(x) \in D[x]$ such that $g(x) = \dfrac{a}{b}\widehat{g}(x)$.*
3. *If $f(x)$ is irreducible in $D[x]$ then it is irreducible in $Q[x]$.*
4. *If $f(x)$ is primitive and irreducible in $Q[x]$, then it is irreducible in $D[x]$.*

Proof. (1) Since $p \in D$ has degree 0, the only way to write p as a product of two polynomials is by both factors being constant. Since D and $D[x]$ have the same units, the result follows at once.
(2) Note first that the coefficients of any $g(x) \in Q[x]$ are fractions of elements of D. Each of those fractions can be taken to be "*reduced*", meaning that the g.c.d. of numerator and denominator is a unit. If we let b be the l.c.m. of the denominators of the coefficients of $g(x)$, then $bg(x) \in D[x]$. Let $a = c(bg(x))$, and $\widehat{g}(x) \in D[x]$ primitive, such that $bg(x) = a\widehat{g}(x)$. Thus, we have $g(x) = \dfrac{a}{b}\widehat{g}(x)$
(3) By contradiction. Assume $f(x)$ is irreducible in $D[x]$ but reducible in $Q[x]$ and write $f(x) = g(x)h(x)$ with $g(x), h(x) \in Q[x]$ nznu, i.e. non-constant. Let $a, b, c, d \in D$ and $\widehat{g}(x), \widehat{h}(x) \in D[x]$ primitive such that $g(x) = \dfrac{a}{b}\ \widehat{g}(x)$ and $h(x) = \dfrac{c}{d}\ \widehat{h}(x)$. We get $f(x) = \dfrac{ac}{bd}\ \widehat{g}(x)\widehat{h}(x)$, i.e. $bd\ f(x) = ac\ \widehat{g}(x)\widehat{h}(x)$. By Gauss's Lemma $\widehat{g}(x)\widehat{h}(x)$ is primitive. By Lemma 4.5.5, $f(x)$ is primitive. Taking content of both sides, we get $ac \sim bd$, and $u = \dfrac{ac}{bd} \in D$ is a unit. We have $f(x) = u\ \widehat{g}(x)\widehat{h}(x)$, and $\widehat{g}(x)$, $\widehat{h}(x)$ are non-constant. This contradicts the irreducibility of $f(x)$ in $D[x]$.
(4) Suppose $f(x) = g(x)h(x)$ with $g(x), h(x) \in D[x]$, nznu. By Corollary 4.5.4, $g(x)$ and $h(x)$ are primitive, but being non-units, they must be non-constant, contradicting the irreducibility of $f(x)$ in $Q[x]$. ■

Note 4.5.1. Note that the condition in Proposition 4.5.6.4 of $f(x)$ being primitive is necessary. For example, the polynomial $f(x) = 2x + 2$ is irreducible in $\mathbb{Q}[x]$, but it is not irreducible in $\mathbb{Z}[x]$.

Scholium 4.5.7 *If $f(x)$ is reducible in $Q[x]$, then it factors as a product of non-constant polynomials of lower degree in $D[x]$.*

Using Proposition 4.5.6.3 we obtain another corollary to Gauss Lemma.

Corollary 4.5.8 *Let D be a UFD, and Q its field of quotients. Let $f(x) \in D[x]$ and $g(x) \in Q[x]$. If $f(x)$ is primitive and $f(x)g(x) \in D[x]$, then $g(x) \in D[x]$.*

Proof. Let $a, b \in D$ and $\widehat{g}(x) \in D[x]$ primitive, such that $g(x) = \dfrac{a}{b}\widehat{g}(x)$. Let $h(x) = f(x)g(x)$. Then $bh(x) = af(x)\widehat{g}(x)$ in $D[x]$. By Corollary 4.5.3 and the fact that both $f(x)$ and $\widehat{g}(x)$ are primitive, we get

$$b \cdot c(h(x)) \sim a,$$

so $b \mid a$ and $\dfrac{a}{b} \in D$. ■

We can combine Lemma 4.5.5 with Proposition 4.5.6.3,4 and obtain the following proposition.

Proposition 4.5.9 *Let D be a UFD, Q its field of fractions, and $f(x) \in D[x]$ non-constant polynomial. $f(x)$ is irreducible in $D[x]$ iff it is primitive and irreducible in $Q[x]$.*

We now have all the ingredients needed to prove Theorem 4.4.5.

Theorem 4.5.5 *f D is a UFD, then the ring $D[x]$ of polynomials over D is a UFD.*

Proof. Let $f(x) \in D[x]$ be nznu. We want to show that $f(x)$ can be factored as a product of irreducibles in a unique way, up to order and associates.
Existence: By induction on $\deg(f(x))$.
Base case. If $\deg(f(x)) = 0$, then $f(x)$ is a constant polynomial, $f(x) = a \in D$. Since D is a UFD, we can factor a as a product of irreducibles in D.

By Proposition 4.5.6.1, all these irreducibles in D are irreducible in $D[x]$
Inductive step. If $\deg(f(x) > 1$, write $f(x) = c(f)\ \widehat{f}(x)$ with $\widehat{f}(x)$ primitive. Write $c(f)$ as a product of irreducibles in D, which are also irreducible in $D[x]$. Now, if $\widehat{f}(x)$ is irreducible, we are done. Otherwise, write $\widehat{f}(x) = g(x)h(x)$ with $g(x), h(x) \in D[x]$ nznu. By Corollary 4.5.4 $g(x)$ and $h(x)$ are primitive, so neither one is a constant, and therefore $\deg(g(x)), \deg(h(x)) < \deg(f(x))$, and by induction hypothesis, each of $g(x)$ and $h(x)$ can be factored as a product of irreducibles.

Uniqueness: Assume $f(x) = p_1(x)\cdots p_r(x) = q_1(x)\cdots q_s(x)$ with each $p_i(x)$ and each $q_j(x)$ irreducible in $D[x]$. Rearrange, if needed, so that 02/05/19

$p_1(x), \ldots, p_k(x)$	are non-constant	and	$p_{k+1}, \ldots, p_r$	are constant
$q_1(x), \ldots, q_l(x)$	are non-constant	and	$q_{l+1}, \ldots, q_s$	are constant

By Lemma 4.5.5 and 4.5.2, $p_1(x)\cdots p_k(x)$ and $q_1(x)\cdots q_l(x)$ are primitive, and therefore by Lemma 4.5.1.3, we get $c(f) \sim p_{k+1}\cdots p_r \sim q_{l+1}\ldots q_s$. We can replace some p_i with an associate and some q_j with an associate, such that $p_{k+1}\cdots p_r = q_{l+1}\ldots q_s \in D$, so $p_1(x)\cdots p_k(x) = q_1(x)\cdots q_l(x) \in D[x]$. By Proposition 4.5.6.3 we have $p_1(x), \ldots, p_k(x), q_1(x), \ldots, q_l(x)$ are irreducible in $Q[x]$, where Q is the field of fractions of D. But we know that $Q[x]$ is a UFD, so we must have $k = l$ and after some possible rearrangements $p_i(x) \sim q_i(x)$ (associates in $Q[x]$) for $i = 1, \ldots k$. Since the units in $Q[x]$ are all non-zero constants, there must be $a_i, b_i \in D$ such that $p_i(x) = \dfrac{a_i}{b_i} q_i(x)$. This means that in $D[x]$, $b_i p_i(x) = a_i q_i(x)$, and taking the content, we get

$$b_i \sim c(b_i p_i(x)) \sim c(a_i q_i(x)) \sim a_i.$$

There is a unit $u_i \in D$ such that $b_i = u_i a_i$, so $q_i(x) = u_i p_i(x)$, and $p_i(x) \sim q_i(x)$ (associates in $D[x]$). Now consider $k < i$. We have $p_{k+1}\cdots p_r = q_{k+1}\ldots q_s \in D$, and since D is a UFD, we must have $r = s$ and $p_i \sim q_i$ in D for $i = k+1, \ldots, r$. ■

4.6 Irreducibility Criteria

We now establish some additional irreducibility criteria. Recall that Proposition 4.3.2 gives us some irreducibility criteria for polynomials in $F[x]$, where

F is a field. These additional criteria consider polynomials over a UFD, and relates them to polynomials over the its field of fractions.

Proposition 4.6.1 [Gallian 17.3] *Let D be a UFD, and Q its field of fractions. Let S an ID, and $\varphi : D \to S$ a ring homomorphism. Let*

$$\begin{array}{rccl} \overline{\varphi}: & D[x] & \to & S[x] \\ & r & \mapsto & \varphi(r) \qquad \text{for } r \in R \\ & x & \mapsto & x \end{array}$$

be the induced homomorphism on polynomials. Let $f(x) \in D[x]$ be non-constant and let $\overline{f}(x) = \overline{\varphi}(f(x))$. If the leading coefficient of $f(x)$ is not in the kernel of φ, and $\overline{f(x)}$ is irreducible in $S[x]$, then $f(x)$ is irreducible in $Q[x]$. Moreover, if $f(x)$ is primitive, then it is also irreducible in $D[x]$.

02/06/19

Proof. Assume $f(x)$ is reducible in $Q[x]$. By Scholium 4.5.7 there are non-constant $g(x), h(x) \in D[x]$, such that $f(x) = g(x)h(x)$. Since the leading coefficient of $f(x)$ is not in $\ker(\varphi)$, neither are the leading coefficients of $g(x)$ and $h(x)$. Thus, we have $\overline{f}(x) = \overline{g}(x)\overline{h}(x)$ with $\overline{g}(x), \overline{h}(x)$ non-constant, showing that $\overline{f}(x)$ is reducible in $S[x]$. The moreover part follows from Proposition 4.5.6.4. ■

Example 4.6.1. Let $f(x) = x^4 + 2x^2 + 2x - x + 1 \in \mathbb{Z}[x]$. Reducing the coefficients $\pmod 2$, we get $\overline{f}(x) = x^4 + x + 1 \in \mathbb{Z}_2[x]$. We claim this polynomial is irreducible. First, it has no root in $\mathbb{Z}_2$, so, by Corollary 4.1.4, it has no linear factors. To factor it as a product of two quadratic polynomials, it would take the form

$$x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1),$$

but looking at the coefficients of x and x^3 we get $1 = a + b = 0$, a contradiction. Now, using Proposition 4.6.1, $f(x)$ is irreducible in $\mathbb{Q}[x]$. Since $f(x)$ is also primitive, it is irreducible in $\mathbb{Z}[x]$.

Proposition 4.6.2 *[Eisenstein's Criterion] Let D be an integral domain, P a prime ideal of D and $f(x) \in D[x]$ primitive. Write*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

If $a_0, \ldots, a_{n-1} \in P$, $a_n \notin P$ and $a_0 \notin P^2$, then $f(x)$ is irreducible in $D[x]$.

Proof. If we had $f(x)$ reducible in $D[x]$, with the use of Proposition 4.5.6.4 and Scholium 4.5.7, it would factor as a product of two non-constant polynomials of lower degree, say $f(x) = g(x)h(x)$ where

$$\begin{aligned} g(x) &= b_0 + b_1 x + \cdots + b_k x^k, \\ h(x) &= c_0 + c_1 x + \cdots + c_{n-k} x^{n-k}, \end{aligned}$$

and $1 \leq k < n$. We have $a_0 = b_0 c_0$, so one and only one of b_0, c_0 is in P. WLOG, let's say $b_0 \in P$ and $c_0 \notin P$. Now, $a_n = b_k c_{n-k} \notin P$, so $b_k \notin P$. Let $t \in \mathbb{N}$ be smallest such that $b_t \notin P$. Consider the coefficient

$$a_t = b_0 c_t + b_1 c_{t-1} + \cdots b_t c_0.$$

Since P is a prime ideal, the last summand on the right hand side, $b_t c_0 \notin P$. By the choice of t all other summand in the right hand side are in P. And, since $t \leq k < n$ we have $a_t \in P$, a contradiction. ■

We state the special case when $D = \mathbb{Z}$.

Corollary 4.6.3 [Eisenstein's Criterion for $\mathbb{Z}$, Gallian 17.4] *Let*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$$

be primitive, and $p \in Z$ a prime number such that $p | a_0, \ldots, a_{n-1}$, $p \not| a_n$ and $p^2 \not| a_0$. Then $f(x)$ is irreducible.

Examples 4.6.2.

1. The polynomial $x^4 + 10x + 5 \in \mathbb{Z}[x]$ is irreducible. Apply Eisenstein's criterion with $p = 5$.

2. If $1 \neq a \in \mathbb{Z}$ is divisible by a prime number p, but not by p^2, then $x^n - a$ is irreducible in $\mathbb{Z}[x]$.

3. For a prime number p, the cyclotomic polynomial

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$$

is irreducible. To see this, observe that

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}, \quad \text{so} \quad \Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{i=1}^{p} \binom{p}{i} x^{i-1},$$

so $\Phi_p(x+1)$ is irreducible, by Eisenstein's criterion. It follows that $\Phi_p(x)$ is also irreducible.

4. A similar argument to that of previous example, shows that $x^4 + 1 \in \mathbb{Z}[x]$ is irreducible.

The only remaining piece of Theorem 4.0.1 is an example of a PID that is not an ED.

Exercise 4.6.1. Let $\gamma = \dfrac{1 + \sqrt{-19}}{2}$ and consider the subring of $\mathbb{C}$ given by:

$$R = \{a + b\gamma \mid a, b \in \mathbb{Z}\}$$

Prove that R is a PID but not an ED. A detailed proof can be found in [3]. The readers is encourage to prove as much as possible before looking up the reference.

02/08/19 Problem Set 01 presentations

Part III

Vector Spaces