NOTES ON UNIQUE FACTORIZATION DOMAINS

Alfonso Gracia-Saz, MAT 347

Note: These notes summarize the approach I will take to Chapter 8. You are welcome to read Chapter 8 in the book instead, which simply uses a different order, and goes in slightly different depth at different points. If you read the book, notice that I will skip any references to *universal side divisors* and *Dedekind-Hasse norms*.

If you find any typos or mistakes, please let me know. These notes complement, but do not replace lectures.

Last updated on January 21, 2016.

Note 1. Through this paper, we will assume that all our rings are integral domains. R will always denote an integral domains, even if we don't say it each time.

Motivation: We know that every integer number is the product of prime numbers in a unique way. Sort of. We just believed our kindergarden teacher when she told us, and we omitted the fact that it needed to be proven. We want to prove that this is true, that something similar is true in the ring of polynomials over a field. More generally, in which domains is this true? In which domains does this fail?

1 Unique-factorization domains

In this section we want to define what it means that "every" element can be written as product of "primes" in a "unique" way (as we normally think of the integers), and we want to see some examples where this fails. It will take us a few definitions.

Definition 2. Let $a, b \in R$.

- We say that a is a *unit* when it has a multiplicative inverse. This is equivalent to $(a) = R$. The set of all units is denoted $R^\times$.
- We say that a divides b when there exists $c \in R$ such that $b = ac$. This is equivalent to $(b) \subseteq (a)$. When this happens, we write $a|b$.
- We say that a and b are associates when $a|b$ and $b|a$. This is equivalent to saying that there exists $u \in R^\times$ such that $b = ua$. This is equivalent to $(a) = (b)$.

Examples 3.

1. In the domain $\mathbb{Z}$, the units are 1 and -1. For every $a \in \mathbb{Z}$, the numbers a and $-a$ are associate.
2. The Gaussian integers are defined as the ring $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$. This ring has 4 units; what are they? Two out of the three numbers $2 + 3i, 3 - 2i, 3 + 2i$ are associate; which ones?
3. Let F be a field. The units of the ring of polynomials $F[x]$ are the polynomials of degree 0 (i.e., the "non-zero constant polynomials"). For example, in $\mathbb{Q}[x]$ the polynomials $2x + 1$ and $x + 1/2$ are associates.

Definition 4. Let $a \in R$. A *factorization* of a is a pair of numbers $b, c \in R$ such that $a = bc$. We say that the factorization is *trivial* when either b or c is a unit (equivalently, when either b or c is associate to a).

Lemma 5. Let $a \in R$ be an element which is not a unit and which is not zero. Then the following conditions are equivalent:

- Every factorization of a is trivial.
- The only divisors of a are associates and units.
- The ideal (a) is maximal in the poset $\{I \trianglelefteq R \mid (0) \neq I \neq (R), I \text{ is principal}\}$ with respect to inclusion.

When this conditions are true, we say that a is *irreducible*. Otherwise, we say that a is *reducible*.

Examples 6.

1. In $\mathbb{Z}$, the number 5 is irreducible because the only elements that divide it are its associates (5 and -5) and the units (1 and -1).
2. On the other hand, 5 is reducible in $\mathbb{Z}[i]$ because we can write it as $5 = (2 + i)(2 - i)$.
3. The polynomial $x^2 - 3$ is irreducible in $\mathbb{Q}[x]$, but it is reducible in $\mathbb{R}[x]$.

Definition 7. Let R be an integral domain. We say that R is a *unique factorization domain* or UFD when the following two conditions happen:

- Every $a \in R$ which is not zero and not a unit can be written as product of irreducibles.
- This decomposition is unique up to reordering and up to associates. More precisely, assume that $a = p_1 \cdots p_n = q_1 \cdots q_m$ and all p_i and q_j are irreducibles. Then $n = m$ and there exist a permutation $\sigma \in S_n$ such that p_i and $q_{\sigma(i)}$ are associates for all $i = 1, \ldots, n$.

Discussion 8. Notice that we can only require uniqueness of the decomposition up to reordering and associates. For example, in $\mathbb{Z}$, we can decompose 30 in various ways:

$$30 = 2 \cdot 3 \cdot 5 = 5 \cdot 3 \cdot 2 = (-2) \cdot 5 \cdot (-3) = \dots$$

The statement that you learned in grade-school about decomposition of integers as products of primes can be rewritten as "$\mathbb{Z}$ is a UFD". We are going to explore why this is true and we are going to try to prove that a few other domains are also UFDs. Even before that, we will see some examples of non-UFDs. Let's introduce an important family of examples.

Example 9 (Quadratic Rings)**.** Let $D \in \mathbb{Z}$ be a number that is not a square. We define

$$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}, \qquad \mathbb{Q}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}.$$

Notice that they are both subrings of $\mathbb{C}$, that $\mathbb{Q}[\sqrt{D}]$ is also a subfield of $\mathbb{C}$, and that $\mathbb{Q}[\sqrt{D}]$ is the field of fractions of $\mathbb{Z}[\sqrt{D}]$. $\mathbb{Z}[\sqrt{D}]$ is an interesting domain on which to study factorization.

Given $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$, we define $\overline{\alpha} := a - b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. Then we define the map $N : \mathbb{Z}[\sqrt{D}] \to \mathbb{Z}$ by

$$N(\alpha) := \alpha\overline{\alpha} = a^2 - Db^2.$$

Notice that the map $\alpha \in \mathbb{Z}[\sqrt{D}] \to \overline{\alpha} \in \mathbb{Z}[\sqrt{D}]$ is a ring homomorphism, which implies that $N(\alpha\beta) = N(\alpha)N(\beta)$ for every $\alpha, \beta \in \mathbb{Z}[\sqrt{D}]$. This map is a helpful tool to study factorization in $\mathbb{Z}[\sqrt{D}]$. We get the following three results:

1. $N(\alpha) = 0$ iff $\alpha = 0$.
2. Given $\alpha \in \mathbb{Z}[\sqrt{D}]$, α is a unit iff $N(\alpha) = \pm 1$. (Prove it.)
3. If $\alpha | \beta$ in $\mathbb{Z}[\sqrt{D}]$ then $N(\alpha) | N(\beta)$ in $\mathbb{Z}$. (Prove it.) The converse is not true.

Let's use this in two different cases.

Example 10 (Back to the Gaussian integers)**.** Let us consider $\mathbb{Z}[i]$, which is the quadratic ring with $D = -1$. In this case the map $N(x + iy) = x^2 + y^2$, which always takes positive values.

- An element $\alpha = x + iy$ is a unit iff $N(\alpha) = x^2 + y^2 = 1$. It is easy to prove this has only four solutions: $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.
- Claim: 3 is irreducible in $\mathbb{Z}[i]$. To prove it, assume that $3 = \alpha\beta$ is a non-trivial factorization in $\mathbb{Z}[i]$. Then $9 = N(3) = N(\alpha)N(\beta)$ must be a non-trivial decomposition in $\mathbb{Z}$. This means $N(\alpha) = 3$. If $\alpha = x + iy$, then $3 = x^2 + y^2$. We can directly check that this equation has no solutions.

- On the other hand, 5 is reducible because $5 = (2+i)(2-i)$.

We will prove later that $\mathbb{Z}[i]$ is a UFD.

Example 11. Let us now consider $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$. We claim that 6 can be written as a product of irreducibles in two different ways:

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

We need to prove that these four factors are, indeed, irreducible, and not associates.

Consider the norm $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ given by $N(\alpha) = x^2 + 5y^2$ for $\alpha = x + y\sqrt{5}i$. It is always positive.

- A direct calculation shows that the only elements with norm 1 are 1 and -1, which are the only units.
- A direct calculation shows that there are no elements with norm 2 or 3.
- $N(2) = 4$, $N(3) = 9$, $N(1 + \sqrt{5}i) = N(1 - \sqrt{5}i) = 6$, hence they are all irreducibles.

As a consequence, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD because it fails the *uniqueness* part of the definition. This should make you feel either a bit excited or a bit freaked out.

Example 12. Let S be the set of all formal functions $f : \mathbb{R} \to \mathbb{R}$ which are of the form

$$f(x) = a_0 + a_1 x^{q_1} + a_2 x^{q_2} + \ldots + a_m x^{q_m}$$

for some $m \in \mathbb{N}$; $a_0, \ldots, a_m \in \mathbb{R}$; $q_1, \ldots q_m \in \mathbb{Q}^+$; with the same conventions that we use when we define polynomials. Intuitively, S is the set of functions from $\mathbb{R}$ to $\mathbb{R}$ which are like polynomials, but the exponents of the variable are allowed to be any positive rational numbers.

The element $x \in S$ is not zero, is not a unit, is not irreducible, and cannot be written as product of irreducibles at all! (Try it: the factors you will come up with can always be further factored out). Hence, S is not a UFD because it fails the *existence* part of the definition. Try to actually prove this.

Exercises

1. Let $a, b \in R$ and assume they are associates.
   (a) Prove that a is irreducible if and only if b is irreducible.
   (b) Prove that a is reducible if and only if b is reducible.

(c) Prove that a is a unit if and only if b is a unit.

2. Let S be the set of polynomials with coefficients in $\mathbb{Z}$ that have no linear term (that is, the coefficient of x is 0). Show that S is a subring of $\mathbb{Z}[x]$. In fact, it is an integral domain. Prove that the element x^6 can be written as product of irreducibles in two different ways. Make sure to prove that the factors in your two decompositions are, indeed, irreducibles! This shows that S is not a UFD.

3. Prove that "being associates" is an equivalence relation in R. What is the equivalence class of 1? What is the equivalence class of 0?

2 Irreducible vs prime

In this section we try to see what is special about $\mathbb{Z}$ that makes it into a UFD. We start with the uniqueness of the decomposition as product of irreducibles. Irreducible number in the integers have an important property that is going to be fundamental in our quest.

Definition 13. Let $p \in R$ be an element which is not zero and is not a unit. We say that p is a *prime* when it satisfies the following property:

$$\text{If } p|ab \text{ with } a, b \in R, \text{ then } p|a \text{ or } p|b.$$

Lemma 14. Let p be a prime. If $p|a_1 \cdots a_n$ for some finite number n, then there exists $i = 1, \ldots, n$ such that $p|a_i$.

Proof. Use induction. □

Lemma 15. Let R be an integral domain. Every prime element is irreducible.

Proof. Let p be a prime element. I assume that p is reducible and I want to get a contradiction. This mean that we can write $p = ab$ where p is not associate to neither a, nor b.

I notice that $p|ab$. Since p is a prime, this means that $p|a$ or $p|b$. Without loss of generality I will assume that $p|a$. But now we have that $p|a$ and also $a|p$. This means p and a are associate. Contradiction. □

Example 16. The converse is not true in general. As an example, consider the ring $\mathbb{Z}[\sqrt{-5}]$ in Example 11. The element 2 is irreducible in R. However, $2|6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$, but 2 does not divide $1 + \sqrt{5}i$ and 2 does not divide $1 - \sqrt{5}i$. (How do we know that?) Hence, 2 is not a prime.

We have proven that in this domain R, the notions of irreducible and prime are different.

Lemma 17. In a UFD all irreducibles are prime.

Proof. Exercise. □

Theorem 18. Let R be a domain in which every irreducible element is prime. Then the decomposition of an element as product of irreducibles, if it exists, is unique.

(Notice that this is not enough to conclude that R is a UFD, since the decomposition as product of irreducibles may not exist.)

Proof. Let's assume that I have two different decompositions

$$p_1 \cdots p_n = q_1 \cdots q_m \tag{1}$$

where all p_i and q_j are irreducible. I want to prove that these two decompositions are the same, up to reordering and associates. I will proceed by induction on the maximum of n and m.

For the base case, if $n = m = 1$, we have $p_1 = q_1$ and we do not need to do anything.

Assume the result is true when $n \leq k$ and $m \leq k$ for some fixed $k \in \mathbb{Z}$. Now I assume I have two decompositions like in Equation (1) where $n \leq k+1$ and $m \leq k+1$. I notice that $p_1 | q_1 \cdots q_m$. Since p_1 is irreducible, it must be prime (by assumption in the statement of the theorem). Therefore, $p_1 | q_j$ for some j. Without loss of generality, I may assume that $j = 1$. I know now that $p_1 | q_1$. Since q_1 is irreducible, either p_1 is a unit (which is impossible since p_1 is irreducible) or p_1 and q_1 are associates. Let us write $p_1 = uq_1$ for some unit $u \in R$. Now Equation (1) becomes

$$p_1 \cdot p_2 \cdot p_3 \cdots p_n = u \cdot q_1 \cdot q_2 \cdot q_3 \cdots q_m$$

By the cancelation property in domains, this means

$$p_2 \cdot p_3 \cdots p_n = u \cdot q_2 \cdot q_3 \cdots q_m,$$

which I can rewrite as

$$p_2 \cdot p_3 \cdots p_n = (uq_2) \cdot q_3 \cdots q_m \tag{2}$$

Notice that uq_2 is a new irreducible. Finally, use the induction hypothesis on the two decompositions in (2) to complete the proof. □

> In $\mathbb{Z}$, being prime is the same as being irreducible. This is the essential property that allows us to prove that $\mathbb{Z}$ is a UFD. Hence, we will want to explore other domains with this same property. Of course, this raises the question: how do we prove in a particular domain that prime is the same as irreducible? The answer lies in greatest common divisors.

Exercises

4. Let R be an integral domain. Let $a, b \in R$ be two elements which are associate. Prove that a is prime if and only if b is prime.

5. Is 2 prime in $\mathbb{Z}$? Is 2 prime in $\mathbb{Z}[i]$?

6. Consider the domain S from Exercise 2. Find a polynomial which is irreducible in S but which is not prime in S.

7. Prove Lemma 17.

3 Greatest common divisors and Bézout domains

Our next step is going to be: how do we prove that prime and irreducible are the same thing in a particular domain? The answer will be that if have GCDs and they behave well, then we can prove it. We are going to need to start by defining what a gcd is in general.

Definition 19. Let $a, b \in R$. We say that $d \in R$ is *a greatest common divisor* (gcd) of a and b if the following two conditions are satisfied:

- $d|a$ and $d|b$.
- If $c \in R$ is another element such that $c|a$ and $c|b$, then $c|d$.

Note 20. Notice that based on the definition, the two elements a and b may in principle have one gcd, or various gcds, or none.

Lemma 21. Let R be an integral domain. Let $a, b \in R$. Assume that d is one gcd of a and b. Let $x \in R$ be another element. Then x is another gcd of a and b if and only if x and d are associates.

In other words, the gcd of two elements may or may not exist; if it exists, then it is defined only up to associates.

Examples 22.

1. Given two non-zero integer numbers $a, b \in \mathbb{Z}$, we know they have a greatest common divisor. (Well, in fact they have two: d and $-d$.) Moreover, we know that the gcd can be written as a linear combination of the two numbers; specifically, there exist $x, y \in \mathbb{Z}$ such that $d = xa + yb$.

2. Consider the domain $\mathbb{Z}[\sqrt{-5}]$ from Example 11. The elements 2 and $1+\sqrt{5}i$ have a greatest common divisor, which is 1. (To prove this, calculate their norms, and study what norms a common divisor may have.) However, it is impossible to find $x, y \in R$ such that $1 = 2x + (1+\sqrt{5}i)y$. (Why?)
   This is bad.

3. Consider the ring R from Example 11 again. Consider the elements $\alpha = 6$ and $\beta = 2(1+\sqrt{5}i)$. You can check directly that both 2 and $1+\sqrt{5}i$ are divisors of both α and β. Hence, if α and β had a gcd d, then d should be a multiple of both 2 and $1+\sqrt{5}i$. But no common multiple of 2 and $1+\sqrt{5}i$ is a divisor of both α and β. (To prove this, again look at the norm of elements.) Hence, the pair α and β do not have a gcd in R at all!
   This is even worse.

Definition 23. Let R be an integral domain. Consider the following two properties:

1. Given any non-zero elements $a, b \in R$, there exists a gcd d of a and b.
2. Moreover, d can be written as $d = xa + yb$ for some $x, y \in R$.

We say that R is a GCD-domain when it satisfies the first property. We say that R is a Bézout domain when it satisfies both properties.

Lemma 24. Every UFD is a GCD-domain.

Proof. Exercise. (Hint: think about how you compute the gcd of two elements in $\mathbb{Z}$ if you start from their decomposition as product of irreducibles.) □

Theorem 25. Let R be a Bézout domain. Then being prime is the same as being irreducible in R.

Notice that this is *not* the reciprocal of Lemma 24.

Proof. We already know that every prime is irreducible in every domain.

Let $p \in R$. Assume that p is irreducible and I want to show that p is prime. Assume that $p|ab$ with $a, b \in R$. I want to show that $p|a$ or that $p|b$. Let d be a gcd of p and a. Since $d|p$, d must be either a unit or associate to p.

- If d is associate to p, we have that $p|d$ and $d|a$, so that $p|a$ and we are done.
- Assume that d is a unit. In this case 1 is a gcd of p and a. Since R is a Bézout domain, we know there are $x, y \in R$ such that $1 = xa + yp$. Multiplying both sides by b, we get $b = x(ab) + ybp$. Since $p|ab$, this implies that $p|x(ab) + yb(p) = b$, and we are done.

□

If we put together Theorems 18 and 25, we have that in every Bézout domain, the decomposition of an element as product of irreducibles is unique. This is progress! The "only" thing left is how to prove that a certain domain is Bézout.

Exercises

8. Let $a, b \in R$ be non-zero elements. Assume that $a|b$. Find a gcd of a and b.
9. Prove Lemma 24.
10. Let R be a domain. Let $a, b, c, x \in R$ such that $a + bx = c$. Let $d \in R$. Prove that d is a gcd of a and b if and only if d is a gcd of b and c.
11. Consider the ring S of Exercise 2.
    (a) Prove that x^2 and x^3 have a gcd, but the gcd cannot be written as a linear combination of x^2 and x^3.
    (b) Prove that x^5 and x^6 do not have a gcd.

4 PIDs

In this section, we will write all the concepts from the previous section in terms of ideals. Then we will see the light! In particular, the proof that $\mathbb{Z}$ is a UFD will fall in our laps.

Lemma 26. Let $a, b \in R$. Let $d \in R$.

1. d is a common divisor of a and b iff $(a, b) = (a) + (b) \subseteq (d)$.
2. d is a gcd of a and b iff (d) is a minimum in the poset of principal ideals that contain (a, b) with respect to inclusion.

Proof.

1. We know that $d|a$ iff $(a) \subseteq (d)$. Similarly, $d|b$ iff $(b) \subseteq (d)$. Hence d is a common divisor of a and b iff (d) contains both (a) and (b). This is equivalent to $(a, b) = (a) + (b) \subseteq (d)$.

2. For d to be a gcd of a and b, it also needs to satisfy that every other common divisor of a and b divides d. This is the same as saying that if $(a,b) \subseteq (c)$ then $(d) \subseteq (c)$. Consider the poset

$$\mathcal{A} := \{(c) \trianglelefteq R \mid (a,b) \subseteq (c)\}$$

with respect to inclusion. We have proven that d is a gcd of a and b iff (d) is a minimum in the poset $\mathcal{A}$.

□

Discussion 27. Let's continue with the notation of Lemma 26 and its proof. One particularly easy case is when the ideal (a,b) is principal itself. That is, $(a,b) = (d)$ for some $d \in R$. Then (d) is guaranteed to be the minimum of the poset $\mathcal{A}$ and d is a gcd of the ideal (a,b). Since we already know that $(a,b) \subseteq (d)$ for a gcd d, the extra condition here is that $d \in (a,b)$. This is equivalent to saying that there exist $x, y \in R$ such that $d = xa + yb$. Notice that this is the second condition in the definition of Bézout domain! We have proven the following two results:

Lemma 28. Let $a, b \in R$. Assume the ideal (a,b) is principal. This means there exists $d \in R$ such that $(d) = (a,b)$. Then d is a gcd of a and b; moreover d is a linear combination of a and b.

Proposition 29. Let R be an integral domain. TFAE:

1. R is a Bézout domain.
2. For every $a, b \in R$, the ideal (a,b) is principal.
3. Every finitely-generated ideal in R is principal.

Definition 30. An integral domain R is a *principal-ideal domain* (abbreviated PID) when every ideal is principal. An integral domain R is a *Noetherian domain* when every ideal is finitely generated.

Theorem 31. R is a PID iff R is both a Bézout domain and a Noetherian domain.

Example 32. $\mathbb{Z}$ is a PID. $\mathbb{Z}[x]$ is not a PID.

Discussion 33. When we put together Theorem 18, 25, and 31, we see we have proven that in $\mathbb{Z}$ decomposition as product of irreducibles is unique. Yay! So the key was in looking at PIDs after all. To prove that $\mathbb{Z}$ is actually a UFD we also need to prove that the decomposition exists. This is very easy to do for $\mathbb{Z}$ directly. However, it would be nice to extend it to all PIDs so that we could have a theorem such as "every PID is a UFD". To do that, first we study what it means in terms of ideals for factorization as product of primes to always exists.

Lemma 34. Let R an integral domain. Assume that x contains an element that is not 0, not a unit, and cannot be written as product of irreducibles. Then there exists an infinite sequence $x_0, x_1, x_2, x_3, \ldots$ of elements in R such that

$$(x_0) \subset (x_1) \subset (x_2) \subset (x_3) \ldots$$

where all the inclusions are strict.

Proof. For elements in R, we know that x is a unit iff $(x) = R$. We know that x and y are associates iff $(x) = (y)$. Moreover, if we can factor $x = yz$ non-trivially (so that y and z are neither units, nor associates to x), then $(x) \subset (y)$ and $(x) \subset (z)$.

Pick an element $x \in R$ which is not zero, not a unit, and not the product of irreducibles. Call $x_0 := x$. Since x is not a product of irreducibles, in particular it is not irreducible, so we have a non-trivial factorization $x = yz$. At least one of y or z is also not a product of irreducibles. Whichever it is, call it x_1. Repeat. □

Theorem 35. If R is a Noetherian domain, then every non-zero, non-unit element is a product of irreducibles.

Proof. Assume not for contradiction. Then we have a sequence of elements $x_0, x_1, \ldots$ as in Lemma 34. For each n, let us call $I_n := (x_n) = (x_0, x_1, \ldots, x_n)$. We also define

$$I = (x_0, x_1, x_2, \ldots) = \bigcup_{n=0}^{\infty} I_n \trianglelefteq R$$

Since R is Noetherian, I must be finitely generated. Let $I = (a_1, \ldots, a_m)$. For each j, since $a_j \in I$ then exist n_j such that $a_j \in I_j$. Let $N := \max\{a_1, \ldots, a_m\}$. Then we can check that $(x_N) = (x_{N+1})$. Contradiction. □

Corollary 36. Every PID is a UFD!

Proof. This is just a matter of collection previous results: Theorems 18, 25, 31 and 35. □

So we are done! Well, not quite. Every PID is a UFD. It was easy to prove that $\mathbb{Z}$ was a PID directly (because we already knew what all the ideals of $\mathbb{Z}$ are). But it is not so easy to prove directly that any other domain is a PID. If we want to add a few more UFDs to our bag of example, we are going to need to introduce one more concept.

5 Euclidean domains

Discussion 37. We know that every PID is a UFD. We know that $\mathbb{Z}$ is a PID, and that is how we prove that it is a UFD. We want to extend this to other domains, so let us recall how we prove that $\mathbb{Z}$ is a PID, and then we will ask the question: in which other domains does the proof work?

Let $I \trianglelefteq \mathbb{Z}$. I want to show that I is principal. If $I = \{0\}$, then we are done. Otherwise, let a be a non-zero element of I of smallest absolute value. In other words, let us take $a \in I$ such that if $b \in I$ and $b \neq 0$ then $|a| \leq |b|$. We can always do this because the set $\mathbb{N}$ is well-ordered. I claim that then

$$\mathbb{Z}a = (a) = I,$$

which will complete the proof. It is clear that $(a) \subseteq I$, so we only need to prove that $I \subseteq (a)$.

Let $b \in I$. I want to show that $b \in (a)$. By the Euclidean algorithm (since $a \neq 0$) there exists $q, r \in \mathbb{Z}$ such that $b = qa + r$ and $|r| < |a|$. But then $r = b - qa \in I$ and hence $r = 0$ (by the minimality of $|a|$). Hence $a|b$ and $b \in (a)$. This completes the proof.

We see here that it all boils down to the Euclidean algorithm. This suggests the next definition.

Definition 38. Let R be an integral domain. A *Euclidean norm* in R is a map $N : R \setminus \{0\} \to \mathbb{N}$ satisfying the following. For every $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that:

- $a = qb + r$, and
- either $N(r) < N(b)$ or $r = 0$.

A *Euclidean domain* is an integral domain with a Euclidean norm.

Theorem 39. Every Euclidean domain is a PID.

Proof. Modify the proof in Discussion 37. Actually, you do not have to modify it that much at all. The same proof works. □

Corollary 40. Every Euclidean domain is a UFD.

Examples 41.

1. $\mathbb{Z}$ is a Euclidean domain with absolute value as norm. Notice that the quotient and remainder are not unique. For example, if we want to divide 5 into 37, we have two possible results:

$$37 = 7 * 5 + 2, \qquad \text{and} \qquad 37 = 8 * 5 + (-3).$$

2. Let F be a field. Then $F[X]$ is a Euclidean domain with degree as norm. Notice that in this case 0 does not have a norm. In this case, the Euclidean algorithm is what high-school teachers call long division.

3. $\mathbb{Z}[i]$ is a Euclidean domain. See Exercise 12 below.

Note 42. You know that in $\mathbb{Z}$, the Euclidean algorithm provides for a quick way to find the GCD of any two elements without having to factor them as product of irreducibles. The exact same algorithm works on any Euclidean domain. Hence

- In UFDs, we know GCDs are guaranteed to exist. The only way to compute them is through factorization (very slow).
- In Bézout domains, we know GCDs are guaranteed to exist and to satisfy the Bézout identity.
- In Euclidean domains, we know GCDs are guaranteed to exist and to satisfy the Bézout identity, and we have a fast way to compute them.

Exercises

12. Prove that $\mathbb{Z}[i]$ with the usual quadratic norm is a Euclidean domain.

    Hint: Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$. We want to "divide α into β with remainder". Operating in $\mathbb{C}$, write $\dfrac{\alpha}{\beta} = c + di$ with some $c, d \in \mathbb{Q}$. Take $\tilde{c}, \tilde{d} \in \mathbb{Z}$ such that $|c - \tilde{c}| \leq 1/2$ and $|d - \tilde{d}| \leq 1/2$. Let $\gamma := \tilde{c} + \tilde{d}i \in \mathbb{Z}[i]$. Show that we can take γ as the quotient of dividing α into β, with an appropriate choice for the remainder.

13. Which other quadratic rings are Euclidean domains with the usual quadratic norm?

14. Consider the polynomials $f(x) = x^5 - x^4 + x - 1$ and $g(x) = x^3 - x$ in $\mathbb{Q}[x]$.

    (a) Find a greatest common divisor $d(x)$ of $f(x)$ and $g(x)$ in $\mathbb{Q}[x]$.

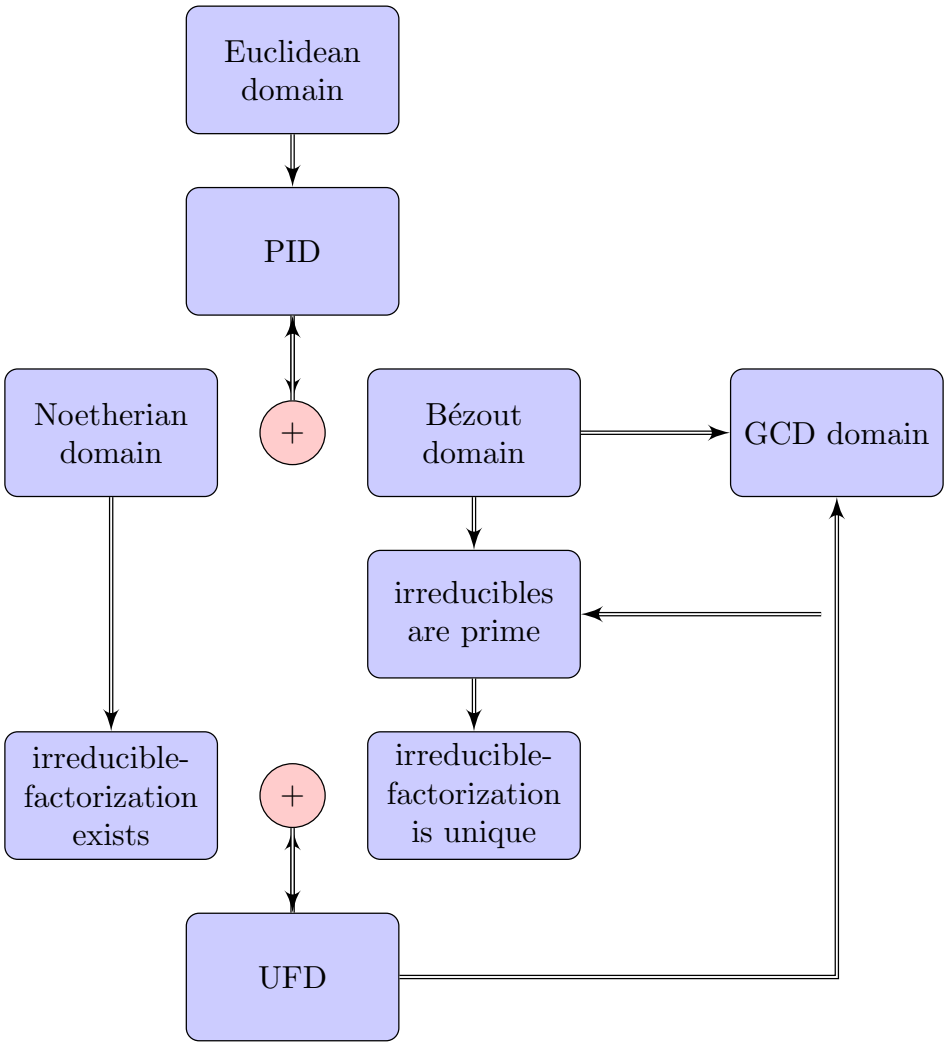
    (b) Find polynomials $a(x), b(x) \in \mathbb{Q}[x]$ such that $d(x) = a(x)f(x) + b(x)g(x)$.

15. **Partial-fraction decomposition.** In first-year calculus/analysis you learn a technique for integrating quotient of polynomials. The technique was presented to you as a recipe, but we never told you why it worked. Now, you know enough to show by yourself why it works!

    Let $a, b \in \mathbb{R}$ be two different real numbers. Let $f(x) \in \mathbb{R}[x]$. Prove that we can always find $A, B \in \mathbb{R}$ and $g(x) \in \mathbb{R}[x]$ such that

$$\frac{f(x)}{(x-a)(x-b)} = g(x) + \frac{A}{x-a} + \frac{B}{x-b}$$

6 Summary


Euclidean domain
PID
Noetherian domain
+
Bézout domain
GCD domain
irreducibles are prime
irreducible-factorization exists
+
irreducible-factorization is unique
UFD