Lecture Notes on Algebraic Number Theory

Shiyue Li

Mathcamp 2018

Acknowledgment: Over the course of Algebraic Number Theory class (Week 1) in Canada/USA Mathcamp 2018, these notes are improved and completed via conversations with Mira, Kevin, J-Lo, students in the class, and other Mathcamp staff.

Contents

1 Rendez-vous with rings

> For the schooling of one's powers of thought only the practice of thinking is really useful. The independent solving of challenging problems will aid the reader far more than aphorisms.
>
> Pólya and Szegö

The goal of the Day 1 of our class is to understand the following concepts.

- Definition of rings and ideals;
- Integral Domains;
- Unique Factorization Domains;
- Principal Ideal Domains.

1.1 Integers and Unique Factorization

Here is one theorem that you are probably famailar with.

Theorem 1.1. *Every integer greater than* 1 *can be uniquely factored into products of primes.*

In an effort to study the integral solutions to equations in the form $x^2 + ay^2$, mathematicians factor the form into $(x - \sqrt{-a}y)(x + \sqrt{-a}y)$. Hence it was natural to study the set

$$\mathbb{Z}[\sqrt{-a}] = \{x + \sqrt{-a}y : x, y \in \mathbb{Z}\}.$$

But for example in $\mathbb{Z}[\sqrt{-3}]$, we see that $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ and this is a failure of unique factorization.

When people are studying Diophantine equations, different number systems come up, and just like above, they do not always have unique factorization.

In 1847, Gabriel Lamé provided a proof for Fermat's Last Theorem, but it was relying on a false fact that a particular number system $\mathbb{Z}[\zeta_n]$ (ζ_n is the root of unity) had this unique factorization property. To trace their path, let us think about where UF can fail? Rearranging the factors might be one, so we allow the number system to be **commutative**: $ab = ba$ for all a and b in the system.

Moreover, all these number systems that number theorists are interested belong to a family of algebraic structures called rings.

1.2 Rings and ideals

Definition 1.2. A **ring** R is a set R together with two operations, $+$ and $\times$, such that the following holds:

(1) R with $+$ satisfies:

- $+$ is assotiative: $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$;
- $+$ is commutative: $a+b = b+a$ for all $a, b \in R$;
- R has an identity element 0 with respect to $+$: $0 + a = a$ for all $a \in R$;
- The additive inverses live in R: there exists $-a \in R$ such that $a + (-a) = 0$.

(2) R with $\times$ satisfies the following things:

- $\times$ is assotiative; $a(bc) = (ab)c$.
- R has an identity element 1 with respect to $\times$: $1 \times a = a \times 1 = a$ for all $a \in R$.
- $ab = ba$ for all $a, b \in R$.

(3) Distributive laws hold. $(a+b) \times c = a \times c + b \times c$ for all $a, b, c \in R$;

Remark 1.3. A ring with a multiplicative identity "1" is often called unital. A ring without one is called "rng" (pronunced as "rung" or "wrong").

Example 1.4. (a) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all rings.

(b) $\mathbb{Z}_n =$ integers mod n.

(c) $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ are all rings.

(d) $\mathbb{Z}[x^2, x^3]$.

(e) $\mathbb{Q}[x, y]$, the set of polynomials in two variables with rational coefficients.

Definition 1.5. A subset I of a ring R is called an ideal of R if

- I is an additive subgroup of R;
- For all $r \in R$, and $x \in I$, $rx \in I$.

So now let us see what the ideals in $\mathbb{Z}$ are.

Definition 1.6. Given a set $x_1, x_2, \ldots, x_n \in R$,

$$(x_1, \ldots, x_n) = \{r_1 x_1 + r_2 x_2 + \cdots r_n x_n | r_i \in R\}.$$

Note that this is an ideal. We call this the ideal **generated by** $x_1, x_2, \ldots, x_n$.

Question 1.7. Using this language, how would you describe the set of all multiples of an integer n?

Example 1.8.

(a) What is (0)?

(b) What is (1)?

(c) What is $(2, 5)$?

(d) What is $(4, 6)$? What is $(2, 4, 7)$?

(e) What is the pattern here?

Proposition 1.9. *I is an ideal in $\mathbb{Z}$ if and only if $I = (x)$ for some $x \in \mathbb{Z}$.*

Let's work out the proof together.

Proof. Let I be an ideal in $\mathbb{Z}$ and x be the smallest positive element of I.

□

1.3 Life forms in a commutative ring

Definition 1.10. An element $a \in R$ is called a **unit** if there exists some $b \in R$ such that $ab = 1$.

Example 1.11. In the following rings, let us describe the units.

(i) $\mathbb{Z}$.

(ii) $\mathbb{Z}[\sqrt{5}]$.

(iii) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(iv) $\mathbb{Z}_4$.

Example 1.12. In $\mathbb{Z}$, when you multiply two nonzero integers you always get some nonzero integers.

Example 1.13. In $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$, $2 \cdot 3 = 0$.

Definition 1.14. R is called a **integral domain** or **domain** if R is nonzero and does not have any zero divisors; that is, there is no nonzero elements a such that there exists some nonzero b such that $ab = 0$.

Integral domains have many subcategories of rings that we are interested in.

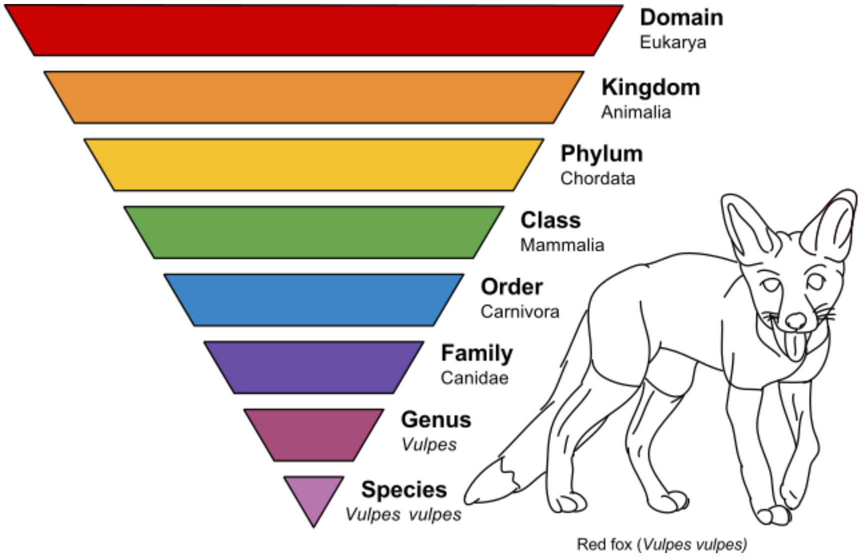

Figure 1: Taxonomic rank for describing all life forms on Earth. Source: `https://en.wikipedia.org/wiki/Taxonomic_rank`

In real life and for nomenclatural purposes, we categorize organisms based on their features (See Figure 1.) At the highest rank all of these are grouped together with all other organisms possessing cell nuclei in the domain Eukarya. Similarly, we start out with all of the algebraic structures that satisfies ring axioms. In the next level, we look at whether they have zero-divisors or not (integral domains). Then moreover, within the realm of all integral domains, we can categorize these integral domains by what types of elements they possess or do not possess. Hence we need to know more features like “being a zero divisor”.

1.4 Unique Factorization Domains

Definition 1.15. Two elements $a, b \in R$ are called **associates** if there exists a unit $u \in R$ such that $au = b$.

Example 1.16. In $\mathbb{Z}$, $6 = 2 \cdot 3 = (-2) \cdot (-3)$. Associates play the same role in factorization.

To explain more why associates like 2 and -2 are the same in factorization, we need something called norm map. The norm map measures roughly the “size” of a number.

For $\mathbb{Z}[\sqrt{-5}]$, we have the norm $N(a+b\sqrt{-5}) = a^2+5b^2$. In the complex plane, this is precisely the length of the line segment from $a+b\sqrt{-5}i$ to 0. We can show that this norm is multiplicative, and that an element has norm 1 if and only if it is a unit (Exercise).

In general, we have

Definition 1.17. Let R be an integral domain. A **norm map** $N : R \to \mathbb{N}$ satisfies the following axioms:

- $N(ab) = N(a)N(b)$ for all $a, b \in R$;
- $N(a) = 1$ if and only if a is a unit.

Definition 1.18. $a \in R$ is **irreducible** if $a = bc$ implies that b or c is a unit.

Definition 1.19. If $p \in R$ that is nonzero and non-unit is called a **prime** if $p|ab$ implies that $p|a$ or $p|b$.

Question 1.20. What is the difference between irreducibles and primes? When are situations when irreducibles are not primes?

Example 1.21. But in $\mathbb{Z}[\sqrt{-5}]$, is this the case? You see that $1+\sqrt{-5}|6 = 2 \cdot 3$ but $1+\sqrt{-5}$ does not divide 2 or 3 (Exercise) . So $1+\sqrt{-5}$ is not a “prime” but it is an irreducible. This is why:

Proposition 1.22. *In any domain R, primes are irreducible.*

Proof. Suppose $p \in R$ is a prime and say $p = ab$.

□

Definition 1.23. A **unique factorization domain (UFD)** is an integral domain in which every non-zero non-unit element can be written as a product of prime elements (or irreducible elements), uniquely up to order and units

Proposition 1.24. *If R is a UFD, then irreducibles are primes.*

Proof. Exercise. □

1.5 Principal Ideal Domains

In particular, this

Definition 1.25. An ideal $I \subseteq R$ is called a **principal ideal** if it can be generated by only one element in R. That is, I can be written as (x) for some $x \in R$. In other words, every element in I can be written in the form of $rx = xr$ for some $r \in R$.

Definition 1.26. If R is an integral domain where every ideal is a principal ideal, R is a principal ideal domain, or PID.

Example 1.27. We showed in Example 1.9 that $\mathbb{Z}$ is a PID.

Example 1.28.

- What about $\mathbb{Q}$?
- $\mathbb{Z}[x, y]$ is not a PID. Why?
- $\mathbb{Z}[\sqrt{-5}]$ is not a PID. Why? Find an ideal that is not generated by one element. (You can prove by brute force or prove by the next theorem.)

Theorem 1.29. *Every principal ideal domain R is a unique factorization domain.*

Proof.

- Use contradiction to show that that every element in a PID can be factored into a product of irreducibles.

  Assume for contradiction that there exists some elements in R that cannot be written as a product of irreducibles. Denote the set of such element be Σ, and Σ is not empty. Take some element x in Σ: x is not irreducible so $x = a_1 b_1$ for non-units, non-irreducible $a, b \in R$ where at least one of a, b is in Σ (why?) WLOG, $a \in \Sigma$. Then $(x) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$. Consider the union of all ideals appeared in this ascending chain and use the fact that R is a PID:

- Show that in a PID, if x is irreducible, then (x) is a **maximal ideal**. That is, if $I \supseteq (x)$, $I = (x)$ or $I = R$. (Exercise)
- Show that in PID, if (x) is maximal, then x is prime.

- Complete the proof by showing uniqueness of the factorization into irreducibles that we obtained in first step.

□

1.6 Euclidean Domains

Definition 1.30. An integral domain R is Euclidean if it comes with a valuation:

$$v : R \to \mathbb{Z}_{\geq 0}$$

such that

- $v(xy) \geq v(x)$ for all nonzero $x, y \in R$.
- For any $a, b \in R$ with $b \neq 0$, there exists $q, r \in R$ such that $a = bq + r$ and $v(r) < v(b)$.

Remark 1.31. The function v might not necessarily multiplicative. We do not assume that the pair (q, r) is unique.

Example 1.32. Suppose $R = \mathbb{Z}$. We can define $v(x) = |x|$ for all $x \in \mathbb{Z}$.

Example 1.33. Suppose $R = \mathbb{Q}[x]$. We can define $v(f) = \deg(f) =$ biggest exponent of the monomials of f. In exercise, you will show using this valuation on $\mathbb{Q}[x]$ to show that if F is a field, then $F[x]$ is an Euclidean domain.

Theorem 1.34. *Every Euclidean Domain (ED) is a Principle Ideal Domain.*

Proof. [1] □

Proposition 1.35. *The Gaussian inetegers $\mathbb{Z}[i]$ is ED.*

Proof. Consider the valuation $v(a + bi) := N(a + bi) = a^2 + b^2$ on $\mathbb{Z}[i]$. □

[1] deal in a ED R endowed with a norm map N. Since R is an ED, there exists an element m with minimal norm under N.

1.7 Exercises for Day 1

Exercise 1.36. Prove Bézout's Lemma: for any integers $a, b \in \mathbb{Z}$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

Exercise 1.37. Show that the norm defined in Example 1.1.6 on $\mathbb{Z}[\sqrt{-5}]$ is multiplicative and that an element $a + b\sqrt{-5}$ is a unit if and only if $a + b\sqrt{-5}$ has norm 1. In other words, it satisfies the criteria for a norm map given in the definition.

Exercise 1.38. Show that in integral domains, all primes are irreducible.

Exercise 1.39. We did Example 1.21 at the end of the class very quickly. Review and prove it yourself. Make sure you understand how norm map works in this case.

Exercise 1.40. Read up to Definition 1.25 and prove that: If R is a UFD, then irreducibles are primes.

Exercise 1.41. The Question 2 on Qualifying Quiz was secretly about ideals. Can you see how?

1.8 Exercises for Day 2

Exercise 1.42 (Polynomials over a Field)**.** Show that if F is a field, $F[x]$ the set of polynomials with a single variable x with coefficients in F, is also an ED. (You have seen in last homework that this is a ring. If you haven't yet, convince yourself that it is indeed an integral domain first.)

Exercise 1.43. Later in the exercise you will see that $\mathbb{Z}[\sqrt{2}]$ is UFD. But.... Show that in $\mathbb{Z}[\sqrt{2}]$, $5 + \sqrt{2} = (1 + \sqrt{2})(-3 + 4\sqrt{2}) = (7 + 5\sqrt{2})(-25 + 18\sqrt{2})$. Is this unique factorization?

Exercise 1.44. For any domain R, if $(a) = (b)$ then $a \sim b$ ("$a \sim b$ means a b are associates).

Exercise 1.45. In any PID R, if x is irreducible, then (x) is a **maximal ideal** of R; that is, if any ideal I contains (x), either $I = (x)$ or $I = R$. [6]

Exercise 1.46. You may have been wondering, we defined $\mathbb{Z}[x]$ as polynomials in x, but we defined $\mathbb{Z}[\sqrt{-5}]$ as linear combinations of 1 and $\sqrt{-5}$. Are these two definitions fundamentally the same? Why?

Exercise 1.47. Read up to Example 1.33, and prove 1.34.

Exercise 1.48. How would you arrange the following objects by their containment relations: integral domains, principal ideal domains, euclidean domains, fields, and unique factorization domains?

[6] Hint: Let $I = (y)$ (R is PID) be an ideal that contain (x). Then $(x) \subseteq (y)$. Expess x in terms of y and use the fact that x is irreducible.

Exercise 1.49. Show that every field F (every nonzero element is a unit) is a Euclidean Domain.

Exercise 1.50 (Challenge)**.** Show that $\mathbb{Z}[i]$ is UFD. (Show that it is ED).

Exercise 1.51. Show that $\mathbb{Z}[\sqrt{\pm 2}]$ is UFD.

Exercise 1.52 (Challenge: Integral Domain and Prime Ideals)**.** Let A be a ring and $\mathfrak{p}$ be an ideal of A. Show that $A/\mathfrak{p}$ is an integral domain if and only if $\mathfrak{p}$ is a prime ideal.

Exercise 1.53 (Challenge: Field and Maximal Ideals)**.** Let A be a ring and $\mathfrak{m}$ be an ideal of A. Show that $A/\mathfrak{m}$ is a field if and only if $\mathfrak{m}$ is a maximal ideal.

Exercise 1.54 (Challenge: Turn Non-UFD into UFD)**.** Show that $\mathbb{Z}[\sqrt{-3}]$ is not a ED but $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is. Further, show that $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is UFD.

2 Beyond $\mathbb{Z}$ and $\mathbb{Q}$

2.1 Algebraic Number Fields

Definition 2.1. An **algebraic number** is a complex number $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$ for some polynomial $f \in \mathbb{Q}[x]$.

Example 2.2.

- Are integers and rationals algebraic numbers?
- Is i an algebraic number?
- Is $\frac{\sqrt[3]{3}}{2}$ an algebraic number?
- What about the **Golden Ratio** $:= \frac{1+\sqrt{5}}{2}$?
- What about π?

Definition 2.3. An subfield $K \subseteq \mathbb{C}$ is **algbraic number field** if $K = \mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_n]$ where $\alpha_1, \alpha_2, \ldots, a_n$ are all algebraic numbers.

Example 2.4. Familiar-looking objects like $\mathbb{Q}, \mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{-5}]$ are all algebraic number fields.

Question 2.5. We only knew that $\mathbb{Q}[\sqrt{5}], \mathbb{Q}[\sqrt{-5}]$ are rings. Are they really fields?

Black Box 2.6. Let α be an algebraic number. Then $\mathbb{Q}[\alpha] := \{f(\alpha) : f \in \mathbb{Q}[x]\}$ is a field. Then we can write $\mathbb{Q}(\alpha)$ to emphasize its field-ness.

Black Box 2.7. For any given algebraic number field $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, there exists an algebraic number $\alpha \in \mathbb{C}$ such that $K = \mathbb{Q}(\alpha)$. Check out **Primitive Root Theorem**

In homework, you will see examples that demonstrate the truthfulness of the black-boxes. For proofs of the black-boxes, you can talk to me in TAU or go to **Viv's class on Galois Theory** in Week 3!

Question 2.8. How do we obtain these algebraic number fields from our old friends $(\mathbb{Z}[i], \mathbb{Z}[\sqrt{5}], \mathbb{Z}[\sqrt{-5}])$?

Definition 2.9. Let R be an integral domain. Then the field of fractions $K(R)$ is the set of elements

$$\{\frac{a}{b} : a \in R, b \neq 0 \in R\}$$

with the natural addition and multiplication. Note that as in rational numbers, $\frac{a}{b} = \frac{c}{d}$ if $ad = cb$.

Example 2.10.

- The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.
- What is the field of fractions of $\mathbb{Z}[\sqrt{5}], \mathbb{Z}[\sqrt{-5}]$?

2.2 "Integers" in Algebraic Number Fields

Question 2.11. We know that we can invert things in $\mathbb{Z}[\alpha]$ to get an algebraic number field $\mathbb{Q}(\alpha)$. Given an algebraic number field, how do we recover the set $\mathbb{Z}[\alpha]$? More importantly, what makes this $\mathbb{Z}[\alpha]$ special?

Example 2.12. In $\mathbb{Z}[i]$, what is a polynomial with integer coefficients that $a + bi$ is a root for?

Example 2.13. In $\mathbb{Z}[\sqrt{-5}]$, what is the polynomial with integer coefficients that $a + b\sqrt{-5} = a + \sqrt{5}bi$ is a root for?

Question 2.14. What do you notice about these polynomials?

Question 2.15. Take any element in $\mathbb{Q}[\sqrt{-5}]$, but not in $\mathbb{Z}[\sqrt{-5}]$, does it satisfy your answer to the above question?

Definition 2.16. An **algebraic integer** is an element α of a number field K such that $f(\alpha) = 0$ for some *monic* $f \in \mathbb{Z}[x]$ (i.e., the leading coefficient is 1).

Definition 2.17. Let K be an algebraic number field. The **ring of integers** of K, denoted by $\mathcal{O}_K$, is the set of all algebraic integers contained in K.

Black Box 2.18. $\mathcal{O}_K$ is in fact, a ring. The most general proof requires the concepts of integrality and working with modules, a generization of vector space over a ring R where we can talk about ring actions. Talk to Lara about her **Intro to Ring Theory (Week 2)** course to find out. You can surely talk to me at TAU about it.

2.3 Integrality

Now let us talk about integrality.

Example 2.19. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. This is a consequence of the Rational Root Theorem that states: If $\alpha = \frac{m}{n} \in \mathbb{Q}$ satisfies a polynomial

$$f(X) = a_d X^d + \cdots + a_0 \in \mathbb{Z}[x],$$

then $m | a_0$ and $n | a_d$. Since $a_d = 1$, $n = 1$ and $\alpha \in \mathbb{Z}$.

Definition 2.20. Let R be an integral domain in its field of fractions F and let $\alpha \in F$. We say that α is **integral over** R if there exists a monic polynomial $f(x)$ with R coefficients such that $f(\alpha) = \alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. R is **integrally closed** if every element in the field of fractions $K(R)$ of R is in R.

Fact 2.21. For any algebraic number field K, $\mathcal{O}_K$ is integrally closed.

Definition 2.22. The set of elements of that are integral over R is called the integral closure of R in K. It is a subring of K containing R.

Example 2.23. In Day 2's Homework, you have seen that $\mathbb{Z}[\sqrt{-3}]$ is not an ED, but $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ is, hence also a UFD. In fact, $\frac{1+\sqrt{-3}}{2}$ is an algebraic integer (what polynomial does it satisfy?), so it's an element in the ring of integers. You can check that $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$. We say that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{-3})$ is $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$.

Example 2.24. In Day 2's Homework, you see that $\mathbb{Z}[i]$ is UFD. In fact, $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. We say that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$ and that $\mathbb{Z}[i]$ is integrally closed.

Example 2.25. In Day 2's Homework, you see that $\mathbb{Z}[\sqrt{2}]$ is UFD. In fact, $\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}]$. We say that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$ is $\mathbb{Z}[\sqrt{2}]$ and that $\mathbb{Z}[\sqrt{2}]$ is integrally closed.

We have just seen several examples of UFDs that turned out to be integrally closed. This is not a coincidence!

Theorem 2.26. *UFDs are integrally closed.*

Proof. Suppose R is a UFD, and that $\frac{a}{b} \in K(R)$ is integral over R; thus $c_0 + c_1 \left(\frac{a}{b}\right) + \ldots + \left(\frac{a}{b}\right)^n = 0$ for some $c_0, \ldots, c_{n-1} \in R$. Note that we can assume a and b have no common factors (other than units) by cancelling. Multiplying by b^n, we get $a^n = -bc_{n-1}a^{n-1} - \cdots - b^n c_0$. The right-hand side is divisible by b. Since we assumed a and b had no common factors, and since R is a UFD, a^n and b have no common factors. Thus b is a unit in R, so $\frac{a}{b}$ is actually in R. Thus R contains all elements that are integral over it. □

Unfortunately, integral closure isn't enough to guarantee something is a UFD. For example, $\mathbb{Z}[\sqrt{-5}]$ is integrally closed (Exercise), but it's not a UFD!

2.4 Factorization in the "Ideal" World

Fact 2.27. Every ring of integers is a Dedekind domain.

Definition 2.28. A **Dedekind domain** is a domain R satisfying the following properties:

- R is integrally closed in $K(R)$.
- Prime ideals are maximal ideals. In other words, there are no ideals strictly containing a prime ideal other than the entire ring;
- R is Noetherian. In other words, there are no infinite sequences of ideals in which each is a strict subset of the next.

Remark 2.29.

- The first condition makes sure that the ring of integers possesses the integral elements in K.
- The second and third conditions parallel the requirement we originally set to ensure a ring is a UFD: the second condition is similar to saying that irreducibles and primes are the same thing.

  > Recall $\mathfrak{p}$ is a prime ideal if and only if $ab \in \mathfrak{p}$ implies that $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. After knowing the multiplication of ideals, the above definition can be translated into the thoughts that (Exercise):
  >
  > – $\mathfrak{p}$ is a prime ideal if $\mathfrak{p}$ divides $(a)(b)$ implies $\mathfrak{p}$ divides (a) or $\mathfrak{p}$ divides (b).
  >
  > – $\mathfrak{p}$ is a prime ideal if $\mathfrak{p} \supseteq (a)(b)$ then $\mathfrak{p} \supseteq (a)$ or $\mathfrak{p} \supseteq (b)$.
  >
  > In other words: **To divide is to contain! To contain is to divide!**

  Now since prime ideals are maximal ideals. Every nontrivial nonzero ideal has to be contained in prime ideals, and hence prime ideals divide nontrivial nonzero ideals, functioning as irreducibles in the non-ideal world.
- The third condition is similar to saying that repeated factoring halts.

Fact 2.30. In a Dedekind domain, every ideal factors uniquely into prime ideals.

In particular, this means that even when the integral closure of $\mathbb{Z}$ in some algebraic number field doesn't have unique factorization (e.g. $\mathbb{Z}[\sqrt{-5}]$), its ideals will!

Theorem 2.31. *A Dedekind domain R is a UFD if and only if it is a PID.*

Proof. We prove two implications.

$(\Longleftarrow)$ Since PID is UFD, we are done.

($\Longrightarrow$) If a dedekind domain R is a UFD, then we only need to show that prime ideal is principal because every nonzero ideal can be factored into prime ideals (Exercise).

Let $\mathfrak{p}$ be any prime ideal and $\alpha \in \mathfrak{p}$. Since R is a UFD,

$$\alpha = q_1 q_2 \cdots q_n$$

where all q_i's are irreducibles. On Day 2, we showed that in UFD, irreducibles are primes. Thus q_i's are primes and (q_i)'s are all prime ideals. The equation above further implies that

$$(\alpha) = (q_1)(q_2)\cdots(q_3).$$

Since $\mathfrak{p}$ divides (α) by "To Contain is To Divide!", $\mathfrak{p}|(q_1)(q_2)\cdots(q_n)$, and then $\mathfrak{p}|(q_i)$ for some i by being a prime ideal. Since "To Divide is to Contain!" $\mathfrak{p} \supseteq (q_i)$. But since (q_i) is also a prime ideal, hence maximal and $\mathfrak{p} \neq R$ by definition (prime ideals have to be proper), $\mathfrak{p} = (q_i)$. Therefore, every prime ideal in R is principal.

□

In Day 3's Homework, you have seen that $\mathbb{Z}[\sqrt{-5}]$ is the ring of integer of $\mathbb{Q}(\sqrt{-5})$. Then it is a Dedekind Domain and its ideals factor uniquely into products of prime ideals. (We know from homework that $\mathbb{Z}[\sqrt{-5}]$ is integrally closed. We should believe that it is Noetherian (Exercise). We take it for granted that every prime ideal in $\mathbb{Z}[\sqrt{-5}]$ is maximal.) In homework you have seen the ideal operations. It turns out even though as an element 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, the ideal (2) can actually be written as a product of two ideals! In fact,

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

So no matter how you factor, we get

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

and these ideals are all prime. So even though numbers don't factor uniquely, the ideals do.

The idea of Dedekind domain is useful when we need to consider unique factorization of ideals as product of prime ideals in the ideal world.

For example, algebraic number theorists use a measurement called the **class number** of a Dedekind domain, which in some sense counts how many ways an ideal can fail to be principal (a Dedekind domain is a PID iff its class number is 1). It turns out there are ways of computing the class number of a ring of integers using the geometry of lattices.

You see that the four prime ideals we see in the prime ideal factorization of (6) in $\mathbb{Z}[\sqrt{-5}]$ are all generated by 2 elements and they are all not principal. In fact, these non-principal prime ideals are all the same; they all belong to the same **ideal class**, and the principal ideals belong to one ideal class. Then it is not hard to believe that the class number of $\mathbb{Z}[\sqrt{-5}]$ is 2!

2.5 Exercises for Day 3

Exercise 2.32. Non-"algebraic integer" algebraic number certainly exists! For example, consider $\frac{\sqrt{2}}{3}$. It is a root of the polynomial $p(x) = 9x^2 - 2$. Show that $\frac{\sqrt{2}}{3}$ is not an algebraic integer. [6]

Exercise 2.33. Show that the set of algebraic numbers is countable. Since $\mathbb{C}$ is uncountable, deduce that there are uncountably many transcendental (non-algebraic) numbers.

Exercise 2.34. Show that $\mathbb{Q}[\sqrt{5}]$ is a field. Hence we can write $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}[\sqrt{5}]$.

Exercise 2.35. Show that there exists $\theta \in \mathbb{C}$ such that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\theta)$. (Hint: Start by writing out elements in $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, which is the same as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Be careful about what each element looks like!)

Exercise 2.36. Show that $\mathbb{Z}[\sqrt{-5}]$ is integrally closed.

Exercise 2.37. It's fairly tricky to prove that every commutative domain has an integral closure in its field of fractions. We can handle a special case: let's find the integral closure of $\mathbb{Z}[\sqrt{d}]$ for any squarefree integer d. In other words, we need to find which elements of the field of fractions are integral over $\mathbb{Z}[\sqrt{d}]$.

(i) In class, we assume without proving that the field of fraction of $\mathbb{Z}[\sqrt{d}]$ is $\mathbb{Q}(\sqrt{d})$. Prove that $\mathbb{Q}[\sqrt{d}]$, the set $\{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$, is the field of fractions of $\mathbb{Z}[\sqrt{d}]$.

(ii) Let $a + b\sqrt{d}$ be an arbitrary element of $\mathbb{Q}[\sqrt{d}]$. Find a polynomial in $\mathbb{Q}[x]$ which has this as a root.

(iii) To be integral over $\mathbb{Z}[\sqrt{d}]$, the polynomial must be monic and all coefficients be in $\mathbb{Z}[\sqrt{d}]$. Since the coefficients of the polynomial you found in part (ii) are in $\mathbb{Q}$, this just requires them to be in $\mathbb{Z}$. For any given d, find values of a, b that will make these coefficients integers.

(iv) For some values of d, you will have found that $\mathbb{Z}[\sqrt{d}]$ is actually integrally closed. For others, you will have found extra points that are integral over it. If you add in the extra points you found, is the result still a ring? Is it integrally closed? (Be careful with definitions!)

Exercise 2.38 (Operations on Ideals)**.** Let R be a ring, and I, J be ideals in R. Then we define the sum and product of ideals as

$$I + J := \{a + b : a \in I, b \in J\},$$

[6] Hint: Start by assuming for contradiction that it is a root for some monic polynomial over $\mathbb{Z}$.

and

$$IJ := \{a_1b_1 + a_2b_2 + \cdots + a_nb_n : a_i \in I, b_i \in J \text{ for all } 1 \leq i \leq n\}.$$

Prove these equalities by computing the products on the right-hand side.

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

Therefore, $(6) = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$ is uniquely factored into prime ideals (we haven't show that each of the factor ideal is prime yet and we don't know if this is actually unique).

Exercise 2.39. Show that the ring $\mathbb{Z}[x^2, x^3]$ does not factor into unique prime ideals. (Use the fact that (x^2, x^3) is a prime ideal.)

2.6 Exercises for Day 4

Exercise 2.40. Contemplate on the reason why a ring of integer $\mathcal{O}_{\mathbb{Z}[\sqrt{d}]}$ is Noetherian, for a given number field $\mathbb{Q}(\sqrt{d})$ and square-free d. Talk to Shiyue or J-Lo about the intuition about it.

Exercise 2.41. Show that if every prime ideal is principal in a Dedekind domain, then every nonzero ideal is principal.

Exercise 2.42. Let R be a Dedekind domain, and let $I \subseteq R$ be an ideal. Show that $I \subseteq P$ for prime ideal P if and only if P is a factor in the prime factorzation of I.

Exercise 2.43. Let P and Q be distinct prime ideals of the Dedekind domain D. Show that $PQ = P \cap Q$.

Exercise 2.44 (Chinese Remainder Theorem)**.** Let R be an arbitrary ring and let $I, J \subseteq R$ be ideals. We say that I and J are **coprime** if $I + J = R$. Prove that I, J are coprime ideals in R, then

$$R/(I \cap J) \cong R/I \times R/J.$$

[2]

[2] Hint: Map $R/I \cap J$ to $R/I \times R/J$ by $r + (I \cap J) \mapsto (r + I, r + J)$. Map $R/I \times R/J \to R/(I \cap J)$ as follows.

3 Why is $x^2 + x + 41$ prime for $|x| < 40$?

What do you get when you plug in a number with absolute value smaller that 40 in to the polynomial $x^2 + x + 41$?

Here is the result for the first few terms:

```
x =  -1 ; x^2 + x + 41 =  41
x =  0 ; x^2 + x + 41 =  41
x =  1 ; x^2 + x + 41 =  43
x =  2 ; x^2 + x + 41 =  47
x =  3 ; x^2 + x + 41 =  53
x =  4 ; x^2 + x + 41 =  61
x =  5 ; x^2 + x + 41 =  71
x =  6 ; x^2 + x + 41 =  83
x =  7 ; x^2 + x + 41 =  97
x =  8 ; x^2 + x + 41 =  113
x =  9 ; x^2 + x + 41 =  131
x =  10 ; x^2 + x + 41 =  151
x =  11 ; x^2 + x + 41 =  173
x =  12 ; x^2 + x + 41 =  197
x =  13 ; x^2 + x + 41 =  223
x =  14 ; x^2 + x + 41 =  251
x =  15 ; x^2 + x + 41 =  281
x =  16 ; x^2 + x + 41 =  313
x =  17 ; x^2 + x + 41 =  347
x =  18 ; x^2 + x + 41 =  383
x =  19 ; x^2 + x + 41 =  421
x =  20 ; x^2 + x + 41 =  461
x =  21 ; x^2 + x + 41 =  503
x =  22 ; x^2 + x + 41 =  547
x =  23 ; x^2 + x + 41 =  593
x =  24 ; x^2 + x + 41 =  641
x =  25 ; x^2 + x + 41 =  691
x =  26 ; x^2 + x + 41 =  743
x =  27 ; x^2 + x + 41 =  797
x =  28 ; x^2 + x + 41 =  853
x =  29 ; x^2 + x + 41 =  911
x =  30 ; x^2 + x + 41 =  971
x =  31 ; x^2 + x + 41 =  1033
x =  32 ; x^2 + x + 41 =  1097
x =  33 ; x^2 + x + 41 =  1163
x =  34 ; x^2 + x + 41 =  1231
x =  35 ; x^2 + x + 41 =  1301
```

```
x =  36 ; x^2 + x + 41 =  1373
x =  37 ; x^2 + x + 41 =  1447
x =  38 ; x^2 + x + 41 =  1523
x =  39 ; x^2 + x + 41 =  1601
```

What do you notice about all the numbers? They are all primes! Why???

3.1 Let's see why

Fact 3.1. Let $p(x) = x^2 + x + 41$. Then $p(n)$ is prime for all $|n| < 40$.

How do we justify this theoretically and hopefully extend the proof for some other polynomials? Our strategy is the following:

Strategy:

- Step 1: To show that $n^2 + n + 41$ is a prime for $|n| < 40$, we need to show that it does not have prime factors less than $\sqrt{n^2 + n + 41} < \sqrt{39^2 + 39 + 41} = \sqrt{1601} < 41$.
- Step 2: Completing the square, we observe that

$$\begin{aligned} n^2 + n + 41 &= n^2 + n + \frac{1}{4} + \left(41 - \frac{1}{4}\right) \\ &= \left(n + \frac{1}{2}\right)^2 + \left(\frac{\sqrt{163}}{2}\right)^2 \\ &= \left(n + \frac{1}{2} + \frac{\sqrt{-163}}{2}\right)\left(n + \frac{1}{2} - \frac{\sqrt{-163}}{2}\right) \\ &= N\left(n + \frac{1 + \sqrt{-163}}{2}\right) \end{aligned}$$

  where N is the norm of the ring of integer $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$.

- Step 3: Let $\frac{1+\sqrt{-163}}{2}$ be α. Summarizing what we have done, the goal becomes **to show that** $N(n + \alpha)$ **has no prime factor smaller than** 41**.**
- Step 4: Put all these amazing thoughts into action!

Justification. Since $N(n + \alpha) \in \mathbb{Z}_{\geq 0}$, it suffices to show that $N(n + \alpha)$ does not have prime divisors in $\mathbb{Z}$. Suppose on the contrary that there exists a prime $p \in \mathbb{Z}$, $p < 41$ such that p divides $N(n + \alpha) = (n + \alpha)(n + \overline{\alpha})$.

Strategy

- If p is is not a prime in $\mathbb{Z}[\alpha]$, then this problem is hard.
- If p is a prime in $\mathbb{Z}[\alpha]$, then....

If p is a prime, then p divides $(n+\alpha)(n+\overline{\alpha})$ implies that p divides $n+\alpha$ or $n+\overline{\alpha}$ in $\mathbb{Z}[\alpha]$. If p divides $n+\alpha$, then there exists $k+\ell\alpha \in \mathbb{Z}[\alpha]$ such that

$$n+\alpha = (k+\ell\alpha)p = kp + \ell p\alpha$$

where $k, \ell \in \mathbb{Z}$. Since ℓ, p are integers, it is impossible for ℓp to be ± 1. Similarly for the case when p divides $n+\overline{\alpha}$.

Question

- Can p be prime in $\mathbb{Z}[\alpha]$?

Answer

- If p is irreducible in $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\alpha]$ is UFD, then p is prime.
- If p is not irreducible in $\mathbb{Z}[\alpha]$ or $\mathbb{Z}[\alpha]$ is not UFD, then this question is hard.

Assume $\mathbb{Z}[\alpha]$ is a UFD, let us show that $p < 41$ is irreducible in $\mathbb{Z}[\alpha]$. Suppose on the contrary $p = ab$ for some non-units a, b in $\mathbb{Z}[\alpha]$. Since p is prime in $\mathbb{Z}$, a, b cannot be integers. Then a, b have to be in $\mathbb{Z}[\alpha] \setminus \mathbb{Z}$. Observe that

$$N(p) = N(a)N(b) < 41^2.$$

Let c be in $\mathbb{Z}[\alpha] \setminus \mathbb{Z}$.

- If $N(c) > 41$, then we have reached a contradiction.
- If not, then this question is hard.

Now we want to show that for any $c \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}$, $N(c) > 41$. Let $c = r + s\alpha$ where $s \neq 0$, $s, r \in \mathbb{Z}$. Then let us analyze the norm of c.

$$\begin{aligned} N(c) &= r^2 + rs + 41s^2 \\ &= \left(r + \frac{s}{2}\right)^2 + 41s^2 - \left(\frac{s}{2}\right)^2 \\ &= \left(r + \frac{s}{2}\right)^2 + \left(\frac{163}{4}\right) s^2 \end{aligned}$$

If $|s| = 1$, then

$$N(c) = \left(r + \frac{s}{2}\right)^2 + \left(\frac{163}{4}\right) s^2 = \left(r + \frac{1}{2}\right)^2 + \frac{163}{4} \geq \frac{1}{4} + \frac{163}{4} = 41.$$

If $|s| \geq 2$, then

$$\begin{aligned} N(c) &= r^2 + rs + 41s^2 \\ &\geq (r+1)^2 + 163 > 41. \end{aligned}$$

Therefore, $N(p) = N(a)N(b) \geq 41^2$, a contradiction. p is an irreducible in $\mathbb{Z}[\alpha]$.

Crucial Fact

- $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ is UFD.

Thus p is a prime in $\mathbb{Z}[\alpha]$ and p divides $n + \alpha$ or $n + \overline{\alpha}$, which as we saw is impossible in $\mathbb{Z}[\alpha]$. □

To summarize:

- We saw that we can rewrite $p(x) = x^2 + x + 41$ as $f(n) = N(n + \alpha)$ in $\mathbb{Z}[\alpha]$, where $\alpha = \frac{1+\sqrt{-163}}{2}$.
- Then we s howed that $N(n + \alpha)$ has no prime divisors less than 41.
- Therefore, if $p(n) = N(n + \alpha)$ has at least two prime factors, it must be at least 41^2 in absolute value.
- But $|n^2 + n + 41| < 41^2$ when $|n| < 40$. Therefore, $p(n)$ must be a prime number for all these consecutive n values!

3.2 What is special about 41 and 163?

We have seen in our exploration that $163 = 4 \cdot 41 - 1$.

Question

- Is true that for every integer n, $x^2 + x + n$ gives us primes for $|x| < n - 2$?

No. Counterexamples abound.

Remember in our justification of the Fact 3.1, we used the crucial fact that $\mathbb{Z}[\frac{1+\sqrt{-163}}{2}]$ is UFD.

Astonishing Fact: There are only **NINE** square-free positive number d such that the ring of integer of $\mathbb{Q}(\sqrt{-d})$ is UFD. They are $1, 2, 3, 7, 11, 19, 43, 67, 163$. They are called **Heegner numbers**.

The Heegner numbers have lots of amazing properties. For example:

- The value of the function $e^{\pi\sqrt{x}}$ at Heegner numbers > 19 are extremely close to integers. For example:

$$\begin{aligned} e^{\pi\sqrt{19}} &\approx 96^3 + 744 - 0.22 \\ e^{\pi\sqrt{43}} &\approx 960^3 + 744 - 0.000\,22 \\ e^{\pi\sqrt{67}} &\approx 5\,280^3 + 744 - 0.000\,0013 \\ e^{\pi\sqrt{163}} &\approx 640\,320^3 + 744 - 0.000\,000\,000\,000\,75 \end{aligned}$$

  In particular, $e^{\pi\sqrt{163}} \approx 640\,320^3 + 744$ is called Ramanujan's constant.