UNIQUE FACTORIZATION IN DOMAINS

JIHONG CAI AND PARTH DESHMUKH

1. Introduction

Unique factorization, often first encountered in the realm of integers, holds deep significance across vast areas of mathematics. Historically, the ancient Greeks laid some of the earliest foundations recognizing the significance of prime numbers. Euclid's monumental work, the "Elements", which dates back to around 300 BC, contained seminal ideas about numbers and their divisibility. Although the Greeks worked extensively with numbers, the explicit statement and appreciation of unique factorization as a fundamental theorem of arithmetic were not fully crystallized until Gauss's treatment in the 19th century.

The beauty and utility of unique factorization go beyond mere historical appreciation. It offers a structured way to decompose elements, aiding in simplifying mathematical expressions, solving intricate Diophantine equations, understanding number-theoretic functions, and probing deep results in analytic number theory. The predictability it provides is an essential tool for mathematicians.

Generalizing to broader algebraic contexts, the concept finds its place in ring theory. Unique Factorization Domains (UFDs) extend the property to certain commutative rings. Yet, not all rings enjoy this unique factorization privilege. This realization led to further classifications, with Principal Ideal Domains (PIDs) and Euclidean Domains standing out as generalizations where unique factorization still holds.

Some cornerstone theorems are intimately tied with this property. Gauss's Lemma, for instance, bridges the world of integers and rationals, ensuring that irreducibility in one implies irreducibility in the other. The Fundamental Theorem of Algebra, promising a root for every non-constant polynomial, combined with factorization properties, assures a unique breakdown for such polynomials into linear factors. Then there's Dirichlet's Theorem on Arithmetic Progressions, a deep result in number theory, guaranteeing infinite primes in arithmetic progressions, a proof of which leans heavily on unique factorization.

In the grand tapestry of mathematics, unique factorization, whether in the integers or its generalizations in ring theory, remains one of the fundamental threads weaving through centuries of mathematical thought, tying together seemingly disparate areas into a cohesive whole.

2. Fundamental Theorem of Arithmetic

The concept of prime numbers has ancient origins, with civilizations such as the ancient Egyptians and Greeks recognizing their significance. However, it was the Greeks who laid the foundational work for modern number theory.

This note is for the MATRIX event on 10/12/2023.

Euclid's "Elements," a masterpiece from around 300 BC, dedicates an entire book (Book IX) to number theory, with propositions related to prime numbers. Among his many contributions, Proposition 20 of Book IX offers a procedure (resembling the modern-day Euclidean Algorithm) to find the greatest common divisor of two numbers. His proof in Proposition 20 indirectly affirms that numbers have unique prime factorizations, although this wasn't explicitly stated as the Fundamental Theorem of Arithmetic at the time.

The explicit understanding and articulation of the Fundamental Theorem of Arithmetic took many centuries to mature. It wasn't until the 19th century that Carl Friedrich Gauss, one of the greatest mathematicians of all time, coined the term "Fundamental Theorem of Arithmetic" in his groundbreaking work "Disquisitiones Arithmeticae" in 1801. Gauss's work was pivotal not just for the articulation of the theorem but also for setting the tone for rigorous mathematical proofs in number theory.

In between Euclid and Gauss, many mathematicians undoubtedly recognized the importance of prime factorization, but it's Gauss's treatment that remains most influential and marks the theorem's modern formulation.

For every integer $n > 1$, there exist prime numbers $p_1, p_2, \ldots, p_k$ (not necessarily distinct) and positive integers $e_1, e_2, \ldots, e_k$ such that:

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

Moreover, this representation is unique, up to the order of the factors. In other words, if there is another set of primes $q_1, q_2, \ldots, q_m$ and integers $f_1, f_2, \ldots, f_m$ such that:

$$n = q_1^{f_1} q_2^{f_2} \ldots q_m^{f_m}$$

then $k = m$, and after rearranging if necessary, $p_i = q_i$ and $e_i = f_i$ for all i.

3. Algebraic Properties of the Integers $\mathbb{Z}$

To understand how factorization works in integer-like algebraic structures, we need to first understand what properties does integers have. These properties are summarized as what is called rings.

Definition. *A **ring** R is a set with two binary operations addition $+$ and multiplication $\cdot$ such that*

(A1). *associativity of addition: $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$*
(A2). *additive identity: $0 \in R$ such that $a + 0 = a = 0 + a$ for all $a \in R$*
(A3). *additive inverse: for all $a \in R$, there exists $-a \in R$ such that $a+(-a) = 0 = (-a)+a$.*
(A4). *commutativity of addition: $(a + b = b + a)$ for all $a, b \in R$*
(M1). *associativity of multiplication: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.*
(M2). *multiplicative identity: $1 \in R$ such that $a \cdot 1 = a = 1 \cdot a$*
(DL). *distributive law: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.*

Note that there we always assume the ring is unital. There are textbooks that do not require R to contain multiplicative identity.

In particular, one may realize two more properties of integers: multiplication is commutative and there is no zero-divisors.

Definition. *An element $r \in R$ is called a **zero-divisor** if there is another element $s \neq 0 \in R$ such that $rs = 0$ or $sr = 0$.*

Example. Consider $\mathbb{Z}/6\mathbb{Z} = \{[m] : m = 0, 1, 2, 3, 4, 5\}$ be the collection of equivalence class modulo 6. 2 is a zero-divisor since $2 \cdot 3 = 6 \equiv 0 \mod 6$.

Now, let's give a more complete description of the algebraic properties of the integer $\mathbb{Z}$.

Definition. *An **integral domain** (or **domain** for short) is a commutative ring which does not contain any zero-divisor. That means, in addition to the ring axioms, integral domain also satisfies*

(M3). *commutativity of multiplication: $a \cdot b = b \cdot a$ for all $a, b \in R$*
(M4). *no zero-divisor: for all $a \in R$, no non-zero element $b \neq 0 \in R$ exists such that $ab = 0$ or $ba = 0$.*

Note that if we require, in addition, that every element has an multiplicative inverse, then the commutative ring becomes a field. One way we can add multiplicative inverses in is via ring of fraction. This construction will be useful in the study of commutative algebra and algebraic geometry.

To generalize the notion of factorization, we need to introduce a key concepts that turn our usual description of factorization in terms of numbers in the general ring language.

Definition. *An **ideal** of R is a subset $I \subseteq R$ such that I is an additive subgroup of R and for any $x \in I$ and $a \in R$, $ax \in I$. That means*

$$I = \left\{ \sum a_i x_i : a_i \in R, x_i \in I \right\}$$

Example. Consider the ring of integers $\mathbb{Z}$. All multiples of 2 form an ideal. That is, $(2) = \{0, \pm 2, \pm 4, \pm 6, \ldots\}$. In fact, pick any number $n \in \mathbb{Z}$, $(n) = \{0, \pm n, \pm 2n, \pm 3n, \ldots\} = \{an : a \in \mathbb{Z}\}$. All ideals in $\mathbb{Z}$ are of this form.

Definition. *Given a set of elements $a_1, \ldots, a_n \in R$, we call $I = (a_1, \ldots, a_n)$ the **ideal generated by** $a_1, \ldots, a_n$ if*

$$I = \left\{ \sum a_i x_i : x_i \in R \right\}.$$

This means, we have a different description of factorization in $\mathbb{Z}$. Namely, instead of asking how to factorize 6, we can ask how to factorize the entire ideal generated by 6. That is, instead of $6 = 2 \cdot 3$, we can write $(6) = (2)(3)$.

We can also multiply two ideals.

Definition. *Given two ideals $I, J \subseteq R$, we can define their product as*

$$I \cdot J = \left\{ \sum a_i b_i : a_i \in I, b_i \in J \right\}.$$

It is clear that this multiplication of ideals is commutative and associative, hence we can explicitly write that if $I = (a_1, \ldots, a_n)$ and $J = (b_1, \ldots, b_m)$, then $IJ = (a_i b_j)$ where $i = 1, \ldots, n$ and $j = 1, \ldots, m$.

This is a handy tool when we want to generalize factorization to ideals.

4. Creating New Rings

The ring of integers $\mathbb{Z}$ is too nice to be interesting for mathematicians. (I know, it sounds ridiculous, but mathematicians are mathematicians.) So we want to build new rings on the existing ones we have. There are a few ways to do so, such as a subring or quotient ring. In this talk, we are particularly interested in adjoining new elements to our ring. The difference is, we are taking smaller structures by doing subring and quotient, but we get bigger (and perhaps more ugly) structures by doing adjoining.

To create new ring from R, we can adjoin an element $\alpha \notin R$. We define

$$R[\alpha] = \left\{ \sum_{0}^{n} r_i a^i : r_i \in R \right\}.$$

Of course, take $\alpha \in R$, $R[\alpha] = R$. Please verify this so that this definition makes sense.

Example. Let $R = \mathbb{Z}$ and $\alpha = i$ the imaginary unit.

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Example. Let $R = \mathbb{Z}$ and $\alpha = \sqrt{2}$ the imaginary unit.

$$\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}.$$

Example. Let $R = \mathbb{Z}$ and $\alpha = \sqrt{-5}$ the imaginary unit.

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

Spoiler: we will see this $\mathbb{Z}[\sqrt{-5}]$ is our trouble-maker in unique factorization.

Note. If you want more math, we can consider all these adjoin actions as taking quotient of polynomial ring. That is

$$\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[x]/(x^2 - 2)$$

where $(x^2 - 2)$ is the ideal generated by $x^2 - 2$. Another example if the Gaussian integers.

$$\mathbb{Z}[i] = \mathbb{Z}[x]/(x^2 + 1).$$

Nowever, there is no way to write, say, $\mathbb{Z}[\pi]$ in this form because π is not an algebraic integer.

5. Factorization in Rings and Domains

To do factorization, let's first observe what ingredients we need. For example

$$21 = 3 \cdot 7.$$

Here, we factor the number into product of 3 and 7 and both of these numbers are primes. In addition, consider

$$12 = 2 \cdot 6 = 2^2 \cdot 3.$$

We want to factorize this number completely into the smallest components possible. This corresponds to the notion of irreducible element in R. Further, note that

$$15 = 3 \cdot 5 = -3 \cdot -5.$$

We usually dismiss the case by multiplying -1 on both sides and require factors to be positive. We want to identify exactly what these elements, called units, are. Hence, we introduce the following definitions:

Definition. *Let $u \in R$. We call u a* ***unit*** *if it has multiplicative inverse. That means, there exists $r \in R$ such that $ur = ru = 1$.*

Definition. *Let $r, s \in R$. We say they are* ***associates*** *of each other if there exists a unit u such that $r = us$.*

Example. In $\mathbb{Z}$, 2 and -2 are associates because -1 is a unit (that is a multiplicative inverse of itself) and $-2 = 2 \cdot (-1)$.

We we think about what it means to be a prime, the intuitive answer might be it cannot be further factorized. That means the only divisor of it is 1 and itself. This is what we called irreducible in ring theory.

Definition. *Give an element $r \in R$. It is **reducible** if there exists $a, b \in R$ that is not a unit such that $r = ab$. An element is called **irreducible** if it is not reducible.*

Another way to see prime in $\mathbb{Z}$ is to say that if p divides ab, then it divides either a or b. Let's formulate that into a definition.

Definition. *Suppose $p|ab$. Then p is **prime** if and only if $p|a$ or $p|b$. $p|a$ means there exists $r \in R$ such that $a = rp$.*

Note that in domains, prime elements are irreducible. The converse if not true. For example, in $\mathbb{Z}[\sqrt{-5}]$, 3 is irreducible but not a prime. However, the following is true:

Theorem. *Prime and irreducible are equivalent in unique factorization domains (UFDs).*

This is the object that we are most interested in in today's talk. We want to explore when domains are UFDs and when they are not. This also justifies the fact that why there are two equivalent way of defining primes in $\mathbb{Z}$.

6. Pythagorean Triples and Gaussian Integers

Here we want to provide a tangible example for why studying unique factorization is useful: characterizing all Pythagorean triples.

Given a Pythagorean triple (a, b, c), we have:

$$a^2 + b^2 = c^2$$

From this relation, the hypotenuse c can be expressed as:

$$c = \sqrt{a^2 + b^2}$$

Consider the Gaussian integer $z = a + bi$. The norm $N(z)$ is given by:

$$N(z) = z \cdot \overline{z} = (a + bi)(a - bi) = a^2 + b^2 = c^2$$

The ring of Gaussian integers, $\mathbb{Z}[i]$, possesses unique factorization, akin to the integers $\mathbb{Z}$. Any non-zero, non-unit Gaussian integer can be uniquely represented as a product of Gaussian primes (up to ordering and units). The units in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

For our Gaussian integer $z = a + bi$, where neither a nor b are both even (otherwise, the triple is not primitive), we have $N(z) = c^2$.

If z is a Gaussian prime, its norm $N(z)$ must also be a prime in $\mathbb{Z}$. However, this is a contradiction since c^2 isn't prime. Therefore, z is not a Gaussian prime.

Now, factor z as $z = p \cdot q$, where neither p nor q are units.

Given the unique factorization in $\mathbb{Z}[i]$:

$$N(z) = N(p)N(q)$$

or

$$c^2 = N(p)N(q)$$

If $N(p) = c$ and $N(q) = c$, one possibility is that p and q are associates, i.e., one is a unit times the other.

Without loss of generality, let $q = up$, where u is a unit in $\mathbb{Z}[i]$. For $z = p \cdot up$, and $u = \pm i$, numbers p and q are of the form $m \pm ni$, where $m, n \in \mathbb{Z}$.

Expanding $p \cdot q$:

$$(m + ni)(m - ni) = m^2 + n^2$$

gives the parameterization:

$$a = m^2 - n^2$$

$$b = 2mn$$

$$c = m^2 + n^2$$

Thus, through the properties of Gaussian integers, we have derived the characterization of primitive Pythagorean triples.

7. Unique Factorization Domain: Definition and Examples

Definition. *A **unique factorization domain (UFD)** is a domain such that every non-zero non-unit element $r \in R$ satisfies*

1. *$r = p_1 p_2 \dots p_n$ for some irreducibles $p_1, \dots, p_n \in R$ where $n \geq 1$ and*
2. *the decomposition is unique up to associates: if $r = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$, then $n = m$ and $p_i = u_j q_j$ for all $i = 1, \dots, n$.*

There are a dozen equivalent statements about UFD. If you are interested, it is listed on Wikipedia, though it will require more advanced tools in commutative algebra.

There are also more than enough facts about UFD to fill a full course but those are too powerful for the discussion today.

Now let's see some examples of UFD. One of the first goals is to classify some important classes of UFDs so that when I am doing research, I do not need to check every single time if I am working with a UFD. The discovery of UFD is attributed to Ernst Eduard Kummer who mistakenly assume $\mathbb{Z}[\sqrt{-5}]$ is a UFD and observed some ridiculous results.

In the 19th century, Ernst Eduard Kummer was studying higher reciprocity laws and Fermat's Last Theorem for specific prime exponents. He initially believed that certain rings of algebraic integers in cyclotomic fields were UFDs. However, he discovered that this assumption was wrong when he encountered problems with the ring $\mathbb{Z}[\sqrt{-5}]$, realizing that there were "ideal numbers" or "ideals" that behaved as if they factored uniquely, even if the numbers themselves did not.

Kummer's discovery of the failure of unique factorization in some number rings led him to introduce the concept of "ideals" in rings, which eventually became a foundational part of modern algebraic number theory. While the mistake led to this important advancement, it's worth noting that Kummer himself was not "confused" for a long time; rather, the discovery of the non-UFD nature of certain rings was an integral step in his development of the theory of ideals.

The take away of the story is: if you find your abstract algebra class on ring theory too hard, Kummer is the one to blame.

So let's explore some examples where there is unique factorization first.

Example. The most familiar example is the ring of integers $\mathbb{Z}$. Its unique factorization is guaranteed by the fundamental theorem of arithmetic.

Example. The Gaussian integers $\mathbb{Z}[i]$ is a UFD. Why? Take all primes in $\mathbb{Z}$ and write it in terms of irredicibles in $\mathbb{Z}[i]$. There are three cases:

(1) $2 = (1+i)(1-i) = -i(1-i)^2$.
(2) $3 = 3$
(3) $5 = (1+2i)(1-2i)$

Example. The polynomial ring over a field $k[x]$ is a UFD. This is why you can do your homework on factorizing polynomials (or at least it's possible to do, not sure if you actually did it or not).

Example. Consider the rings of the form $\mathbb{Z}[\sqrt{d}]$, where $d \in \mathbb{N}$ some positive square-free integers. $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{3}]$, $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[\sqrt{7}]$, $\mathbb{Z}[\sqrt{11}]$ are all UFDs.

Example. Now consider the rings of the form $\mathbb{Z}[\sqrt{-d}]$, where $d \in \mathbb{N}$ some positive square-free integers. We have a very satisfying result classifying all UFDs of this form.

Theorem (Stark–Heegner Theorem)**.** *There are exactly nine Heegner number. They are 1, 2, 3, 7, 11, 19, 43, 67, and 163.*

Corollary. *Given the ring $\mathbb{Z}[\sqrt{-d}]$ for some square-free natural number $d \in \mathbb{N}$. Only $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-7}]$, $\mathbb{Z}[\sqrt{-11}]$, $\mathbb{Z}[\sqrt{-19}]$, $\mathbb{Z}[\sqrt{-43}]$, $\mathbb{Z}[\sqrt{-67}]$, and $\mathbb{Z}[\sqrt{-163}]$ are the only unique factorization domains.*

This is a very satisfying result for mathematicians. We usually will get something ambiguous such as anything that satisfies these three conditions will have some shared properties, rather than having an explicit characterization of all possible cases.

8. How Un-unique is Factorization in Non-UFD

We want to take a close look at non-UFDs in this section. In particular, $\mathbb{Z}[\sqrt{-5}]$.

Imagine factorizing 6 in $\mathbb{Z}[\sqrt{-5}]$.

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

We can check that $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ are all irreducible. However, none of them are primes. That means they do not give a good enough factorization in $\mathbb{Z}[\sqrt{-5}]$.

Now consider the factorization in the ideal.

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

This does not look like a complete factorization, so we can make it better. But how?

The answer is to make the ideal bigger.

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

by citing that $(2, 1-\sqrt{-5}) = (2, 1+\sqrt{-5})$. Verify this. We can check that $(2, 1-\sqrt{-5}), (3, 1-\sqrt{-5}), (3, 1-\sqrt{-5})$ are prime ideals (surprise, surprise!). Now we want to generalize this idea and count how many ways we can factorize a number in ring theoretical sense. We will introduce the ideal class group.

9. Failure of Unique Factorization: Ideal Class Groups

We have introduced the notion of ideals. But we need to understand how they differ from each other. As always, before investigating on how strucutres are different, we need to know what does it mean to be "the same".

Definition. *Let $I, J \subseteq R$ be two ideals of R. We say I and J are **similar**, denoted by $I \sim J$, if there exists some $\lambda \in F$ such that $\lambda I = J$, where F is the number field we are working in.*

The definition of number field is abstract. If you are interested, here it is:

Definition. *A **number field** is a subfield in $\mathbb{C}$ that is finite-dimensional as a vector space over $\mathbb{Q}$.*

Essentially, this means that given, for example, $\mathbb{Z}[\sqrt{2}]$, the number field is just $\mathbb{Q}[\sqrt{2}]$. That is, changing integer coefficients to rational coefficients.

More generally, it is the smallest field that contains R.

Example. The number field for Gaussian integer is $\mathbb{Z}[i] \subseteq \mathbb{Q}[i]$.

Example. The number field for the ring $\mathbb{Z}[\zeta] \subseteq \mathbb{Q}[\zeta]$ where ζ is the roots of unity.

Proposition. *If $I \sim I'$, then $IJ \sim I'J$.*

We write $I \sim J$ because it is in fact an equivalence relation. (If you know what that is, verify it.) Now we can collect these equivalence classes, together with ideal multiplication, forms an abelian group. This is because $I\vec{I} = (1)$ is principal, so the inverse of ideal is well-defined. This group is what we called the ideal class group (the group formed by collecting ideal classes).

Theorem. *The ideal class group $\mathrm{Cl}(F)$ is finite.*

Example. Consider $R = \mathbb{Z}[\sqrt{-5}]$, the class group is $\mathbb{Z}/2\mathbb{Z}$. The only ideals up to similarity are (1) and $(2, 1+\sqrt{5})$.

Theorem. *Let R is a domain with F as its number field. If R is an UFD, then $\mathrm{Cl}(F)$ is trivial. That means, it is a trivial group, singling the unique way of factorization.*

Example. Let $F = \mathbb{Q}[\sqrt{15}]$ be the number field. $\mathrm{Cl}(F) = \mathrm{Cl}(\mathbb{Q}[\sqrt{15}]) = C_2$, the cyclic group of order 2.

Example. For the number field with roots of unity, $\mathrm{Cl}(\mathbb{Q}[\zeta_{17}]) = 1$

Example. For the number field with roots of unity, $\mathrm{Cl}(\mathbb{Q}[\zeta_{23}]) = 3$

Example. For the number field with roots of unity, $\mathrm{Cl}(\mathbb{Q}[\zeta_{31}]) = 9$

Example. For the number field with roots of unity, $\mathrm{Cl}(\mathbb{Q}[\zeta_{43}]) = 211$

Example. For the number field with roots of unity, $\mathrm{Cl}(\mathbb{Q}[\zeta_{53}]) = 4886$

Example. For the number field with roots of unity, $\mathrm{Cl}(\mathbb{Q}[\zeta_{67}]) = 853513$

Example. For the number field with roots of unity, $\mathrm{Cl}(\mathbb{Q}[\zeta_{163}]) = 10834138978768308207500526544$

These examples are just an illustration how how crazy things can get even with gradual increase of power. And this is among the most understood area of unique factorization.

To fully understand this, it is up to you to build a complete picture. That means, we do not know (by we, I mean mathematicians not just me). The best attempt is something called Iwasawa theory, which takes a few hundred pages to prove by itself, involving some very hard math, such as Galois theory, representation theory, category theory, module theory, and much more.

If you are interested in solving this puzzle for the community of number theory, I can provide some more references (including the book proving Iwasawa theory).

Email address: `jihongc2@illinois.edu`
Email address: `parthd2@illinois.edu`

Mathematical Advancement Through Research Idea eXchange (MATRIX)

Department of Mathematics, University of Illinois Urbana-Champaign