Algebraic Number Theory

Aidan [redacted] **Mentor:** Dylan Costa

Thursday 11th December, 2025

University of Connecticut

Introduction

Primary Text:

- Keith Conrad
  Extended Lecture Notes on Algebraic Number Theory
  November 2024.

Background Knowledge:

- finite extensions of fields
- prime & maximal ideals
- modules
- (some) Linear Algebra

Table of Contents

Algebraic Integers

Definition (Number Field)

A ***Number Field*** is a finite extension of $\mathbb{Q}$

Examples

$\mathbb{Q}(i)$ $\quad$ $\mathbb{Q}(i, \sqrt{2})$

$\mathbb{Q}(\sqrt[3]{2})$ $\quad$ $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p})$

Definition (Algebraic Integer)

An element α of a field extension of $\mathbb{Q}$ is called an ***Algebraic Integer*** if it is the root of a monic polynomial in $\mathbb{Z}[X]$

Examples

$\sqrt{2}$ is the root of the monic polynomial $X^2 - 2$. Likewise, i is the root of the monic polynomial $X^2 + 1$. They are both algebraic integers.

Proposition

Let K be a number field and α be an element of K. If α is an algebraic integer, then the minimal polynomial of α over $\mathbb{Q}$ is in $\mathbb{Z}[X]$.

Proof.

Suppose K number field and $\alpha \in K$ is an algebraic integer. Let $p(X) \in \mathbb{Z}[X]$ be the monic polynomial with $p(\alpha) = 0$ such that $p(X)$ is of minimal degree. Suppose $p(X)$ was reducible in $\mathbb{Q}[X]$. By Gauss' lemma, a polynomial is irreducible in $\mathbb{Q}[X]$ iff it is irreducible in $\mathbb{Z}[X]$. As such, $p(X)$ would be reducible in $\mathbb{Z}[X]$ into $p(X) = f(X)g(X)$. But $0 = f(\alpha)g(\alpha)$ would imply that α is a root of one of $f(X)$ or $g(X)$, contradicting that $p(X)$ is minimal. ■

Example

$1/\sqrt{2}$ has the minimal polynomial $X^2 - \frac{1}{2} \notin \mathbb{Z}[X]$ and is therefore not an algebraic integer.

Definition (Ring of Integers)

The ***Ring of Integers*** of a number field K is the ring of all algebraic integers contained in K, denoted $\mathcal{O}_K$.

Examples

Trivially, we have $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

For a more interesting example, we have that

$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}\left[\sqrt{-5}\right] \qquad \mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$$

Theorem

For a number field K and $\alpha \in K$, α is in $\mathcal{O}_K$ if and only if its minimal polynomial over $\mathbb{Q}$ is in $\mathbb{Z}[X]$.

Lets show the second claim, that $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$:

Proof.

First, note that $i \in \mathcal{O}_{\mathbb{Q}(i)}$ so $\mathbb{Z}[i] \subseteq \mathcal{O}_{\mathbb{Q}(i)}$. Now, let $\alpha = p + qi \in \mathcal{O}_{\mathbb{Q}(i)}$. WLOG suppose $q \neq 0$. The minimal polynomial of α over $\mathbb{Q}$ is

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - 2pX + p^2 + q^2$$

By the previous theorem, $2p \in \mathbb{Z}$ and $p^2 + q^2 \in \mathbb{Z}$. We have two cases: either $2p$ is even or odd. If $2p$ is even then $p \in \mathbb{Z}$ so $q^2 \in \mathbb{Z}$. Since integers only have integral or irrational roots, $q \in \mathbb{Z}$. If $2p$ is odd, then $p = \frac{p'}{2}$ for some odd p'. Let $m = p^2 + q^2 \in \mathbb{Z}$. Then $4m = p'^2 + 4q^2 = p'^2 + (2q)^2$ Therefore $(2q)^2 \in \mathbb{Z}$. Reducing modulo 4 gives us $3p'^2 \equiv (2q)^2 \bmod 4$. As every odd squares to $1 \bmod 4$, we have that $3 \equiv (2q)^2 \bmod 4$. But, 3 is not a square $\bmod 4$. Therefore $2p$ must be even and so $p, q \in \mathbb{Z}$. As such, $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$. ■

With a proof very similar to the one before, we may find the ring of integers for any quadratic field.

Theorem

For $d \in \mathbb{Z} - \{0, 1\}$ squarefree, the ring of integers of $\mathbb{Q}(\sqrt{d})$ is

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \not\equiv 1 \bmod 4 \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \bmod 4 \end{cases}$$

The Gaussian Integers

The ring of integers $\mathbb{Z}[i]$ is referred to as the ***Gaussian Integers*** and is of special importance to us.

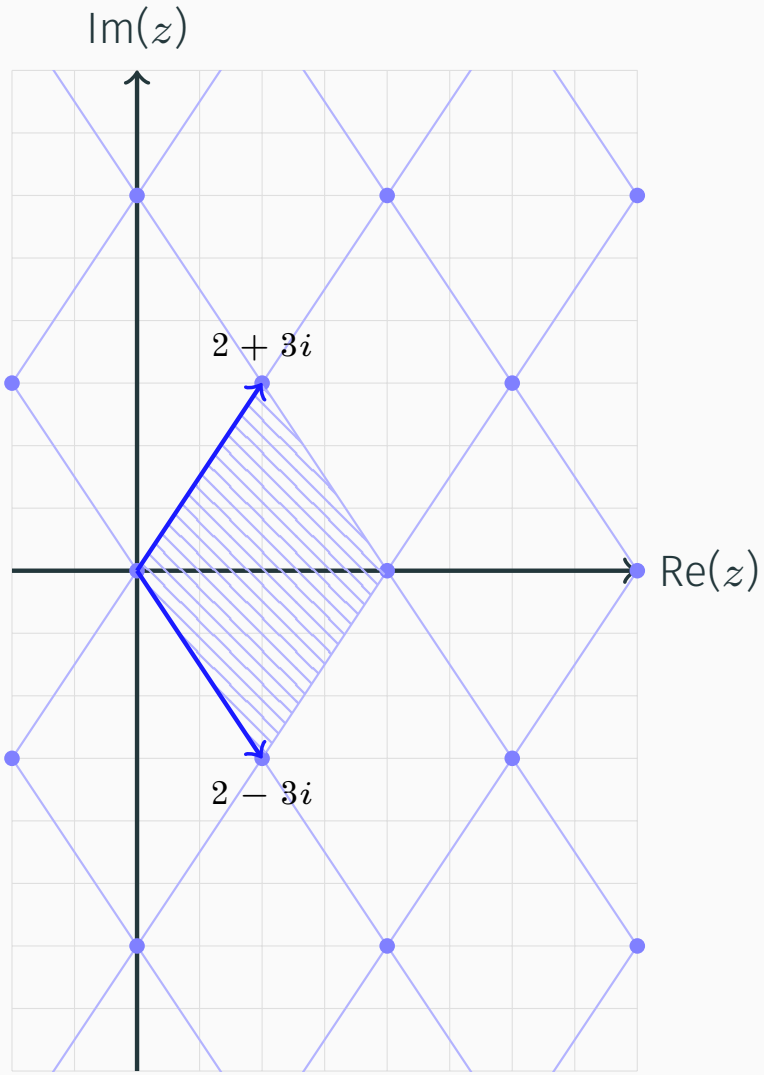
In UFDs like $\mathbb{Z}[i]$ we have unique factorizations into irreducible. But, a prime lifted from $\mathbb{Z}$ into $\mathbb{Z}[i]$ does not necessarily remain irreducible.

Examples

$$2 = (1+i)(1-i) \qquad 13 = (3+2i)(3-2i)$$

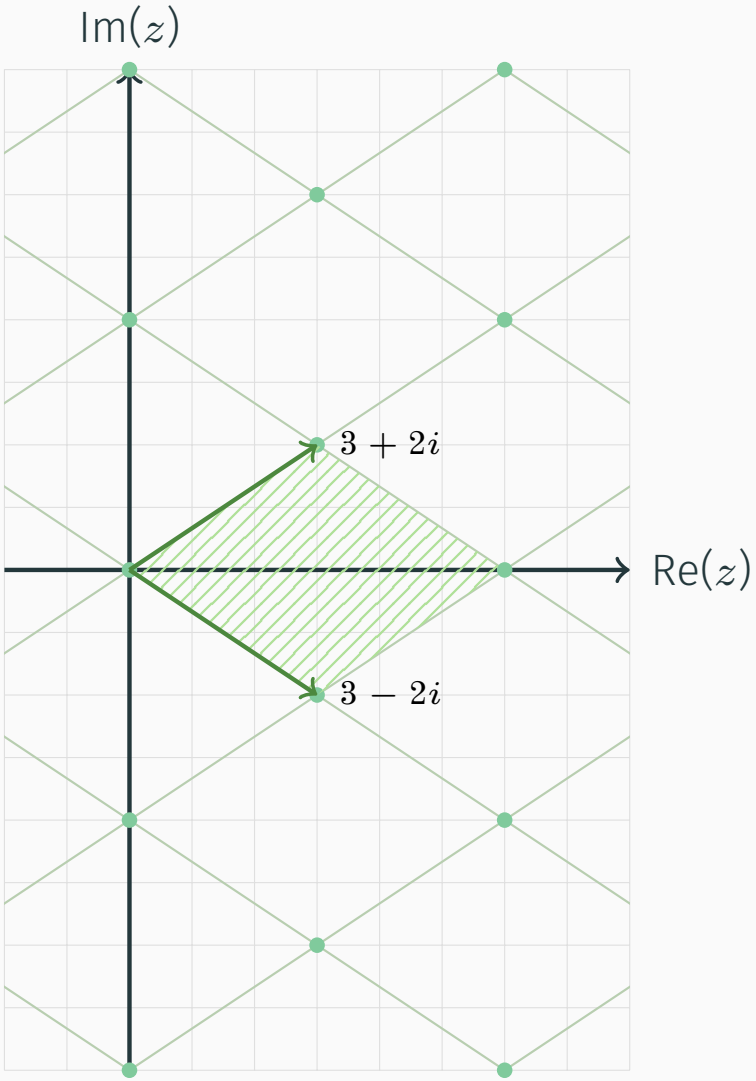
So, while the $26 = 2 \cdot 13$ is a prime factorization in $\mathbb{Z}$, in $\mathbb{Z}[i]$ it becomes

$$26 = (1+i)(1-i)(3+2i)(3-2i).$$



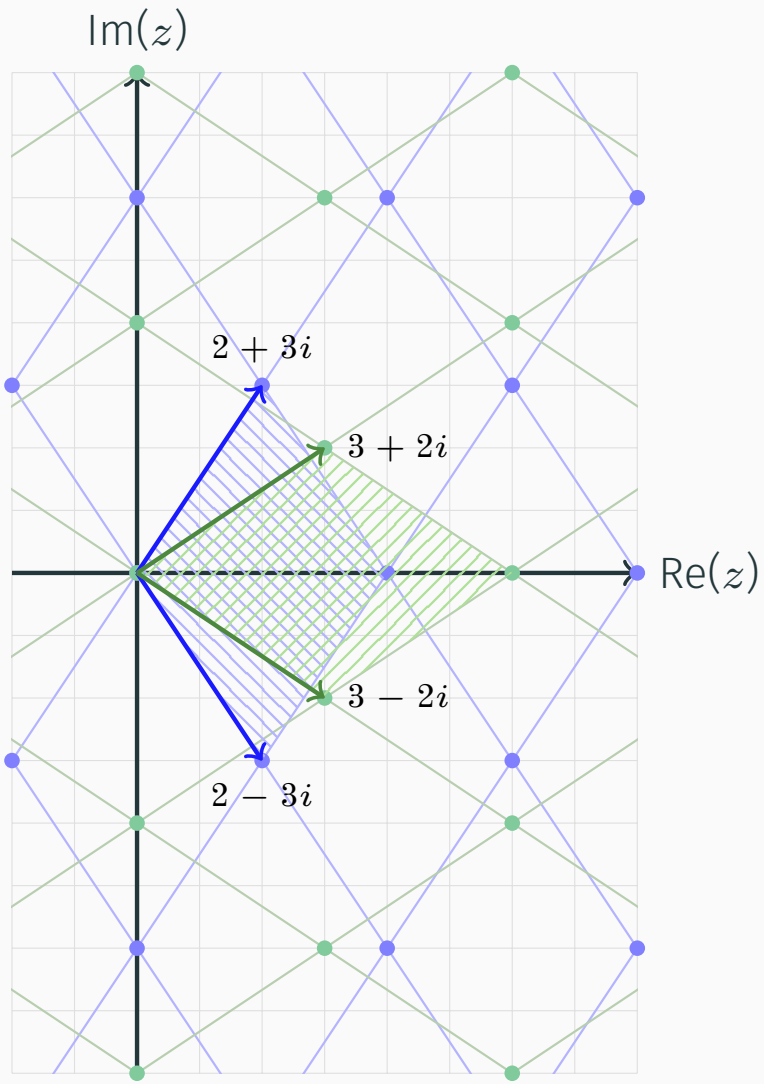
One factorization into irreducibles is:

$$13 = (2 + 3i)(2 - 3i)$$



Another factorization into irreducibles is:

$$13 = (3 + 2i)(3 - 2i)$$



Their areas are equal with

$$\begin{aligned} 13 &= (3-2i)(3+2i) \\ &= (2+3i)(2-3i) \end{aligned}$$

As the lattice bases differ by only a unit,

$$\begin{aligned} 3-2i &= -i(2+3i) \\ 3+2i &= i(2-3i) \end{aligned}$$

this does not violate the unique factorization.

Primes vs. Prime Ideals

Again, when we lift elements into larger rings, we might not only lose primes, but also the uniqueness of prime factorization entirely.

Example

In $\mathbb{Z}[\sqrt{-5}]$, the element 6 has a two distinct factorizations:

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

Note: $2, 3, 1 + \sqrt{-5},$ *and* $1 - \sqrt{-5}$ *are all irreducible in* $\mathbb{Z}[\sqrt{-5}]$.

While $\mathcal{O}_K$ may or may not be a UFD, we always have a unique factorization of nonzero ideals as a product of prime ideals. In $\mathbb{Z}[\sqrt{-5}]$, the following is true of ideals:

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

These two factorizations of ideals *are* identical because

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

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

which are prime ideals.

Thank you!