Chapter 1

Introduction

- Course website
- Zulip

Chapter 2

Gaussian and Eisenstein integers

- URL to video
- $\overline{\mathbb{Q}}$: roots of monic polynomials over $\mathbb{Q}$
- $\overline{\mathbb{Q}}$: roots of monic polynomials over $\mathbb{Z}$
- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$: is a ring.
- $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$: is a field.

Proposition 1. The ring $\mathbb{Z}[i]$ is a Euclidean domain: For $a, b \in \mathbb{Z}[i]$ with $b \neq 0$ we can write $a = qb + r$ where $|r| < |b|$ where $|\cdot|$ is the complex absolute value.

Proof. Consider a/b. We have $a/b = q + r/b$. We want $|r/b| < 1$. Round to the nearest gaussian integer, call it $\texttt{round}(a/b)$. When we're on $Z[i]$, we're trying to bound the distance to the nearest gaussian integer. So we're sitting on a unit square, and we are asking "what is the distance from our point to nearest lattice point"? The worst case is when our point is at the center of the square, or the distance is $\sqrt{(2)}/2$.

The distance from a/b to the nearest gaussian integer is $1/\sqrt{2} < 1$. we write $a/b = q + r/b$. This means that $r/b \leq 1/\sqrt{2} < 1$. So when we write $a = qb + r$, we have that $|r| < |b|$.

Perhaps slightly more intuitively, we are on a 2D plane, and we are running the Euclidean algorithm on 2D vectors.

Also, for any constant c, there are only finitely many possible absolute values of Gaussian integers less than $\mathbb{C}$.

Even though we infact have finitely many Gaussian integers themselves, and not just absolute values, because this will come in handy later. For example, when considering polynomials over $\mathbb{C}$, if we are considering the polynomial $(x - a)$, we have infinitely many constant polynomials with degree less than 1 (equal to 0), but there is a finite number of absolute values (ie degrees)less than 1.a