Lecture 13

11 March 2024 14:09

Last time:

- In the rng $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ we characterised all units and zero-divisors.
- In a domain (commutative ring with identity) R, $a, b \in R$ are associates if $a = b \cdot u$ for u a unit of R.

This is an equivalence relation, the equivalence classes are called associate classes.

Example:

Consider the rng of Gaussian integers

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

This is an integral domain (it has no zero-divisors) as this a subring of $\mathbb{C}$ (which is a field therfore an integral domain).

- What are the units of $\mathbb{Z}[i]$?

Some units: $1, -1, i, -i$.

Claim: These are the only units of $\mathbb{Z}[i]$:

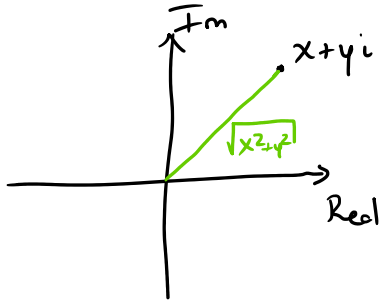
Proof: Suppose $a + bi \in \mathbb{Z}[i]$ is a unit.

This means, there exists $c + di \in \mathbb{Z}[i]$ such that

$$(a+bi)(c+di) = 1.$$

Recall: Every complex number has a "norm" or "modulus squared"

$$|x+yi|^2 = x^2+y^2$$

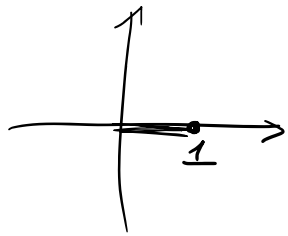


This is multiplicative!

$$|(x+yi)(z+wi)|^2 = |x+yi|^2 \cdot |z+wi|^2$$

(Do this as an exercise!)

We can apply modulus squared on both sides of the equation:



$$|(a+bi)(c+di)|^2 = |1|^2 = 1$$

$$|a+bi|^2 \cdot |c+di|^2 = 1$$

$$(a^2+b^2)\cdot(c^2+d^2) = 1$$ ← this is an equation in $\mathbb{Z}$.

As a^2+b^2 and c^2+d^2 are both nonnegative integers, we must have

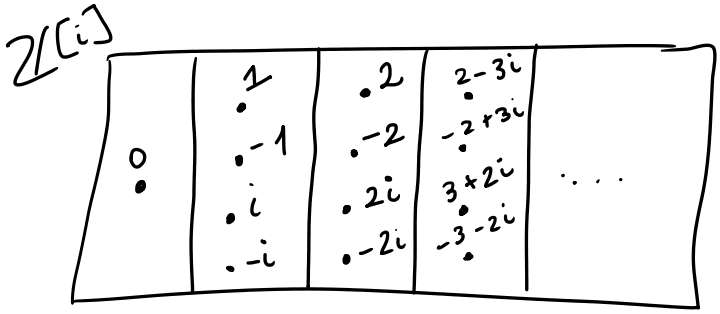
$$a^2+b^2 = 1 \quad \text{and} \quad c^2+d^2 = 1.$$

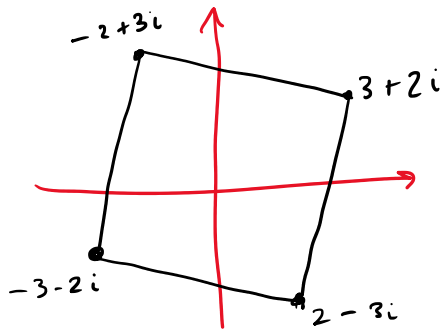
Therefore $a = \pm 1$ and $b = 0$

or $a = 0$ and $b = \pm 1$

This means $a+bi = 1, -1, i, -i$.

The partition of $\mathbb{Z}[i]$ into associate classes is:





Irreducibles and factorisation:

Definition: Let R be an integral domain.

An element $r \in R$ is called **irreducible**

if
- $r \neq 0$ and r is not a unit
- whenever $r = a \cdot b$ then either a or b is a unit.

Example:

- The irreducible elements of $\mathbb{Z}$ are the prime numbers and minus the prime numbers.

Definition: An integral domain R is called

Definition: An integral domain R is called a **unique factorisation domain** if every nonzero element r of R which is not a unit can be factored as a product of irreducible elements, and this factorisation is "unique up to associates", that is:

(a) For every $r \in R$ $r \neq 0$ r not a unit, there exist $p_1, p_2, \dots, p_n$ irreducible elements of R such that

$$r = p_1 \cdot p_2 \cdot p_3 \cdots p_n$$

(b) If $p_1, \dots, p_n$ and $q_1, \dots, q_m$ are irreducible elements of r such that

$$p_1 \cdot p_2 \cdots p_n = q_1 \cdots q_m$$

then, after reordering the elements, $n = m$ and p_i and q_i are associates for all i.

Example: $R = \mathbb{Z}$

$r = 2 \cdot 2 \cdot 2 \cdot 5$

$$60 = \underbrace{3 \cdot 2 \cdot 2 \cdot 5}_{\text{irreducible elements}}$$

$$= \underbrace{-2 \cdot 3 \cdot -5 \cdot 2}_{\text{irreducible elements}}$$

some factorisation up to reordering and associates.

Example: $\mathbb{Z}$ is a unique factorisation domain (UFD), because any integer can be factored "uniquely" as a product of irreducible elements.

Example: Any field is a UFD because there are no nonzero elements that are not a unit.

Gauss' Lemma:

If R is a UFD (unique factorisation domain) then $R[x]$ is also a UFD.

- In particular, $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ UFD

- In particular, $\mathbb{Z}[x]$, [illegible] are UFD

$a^3+b^3=(a+b)(a^2-ab+b^2)$

Examples. $R = \mathbb{R}[x]$

units of $\mathbb{R}[x]$ are the nonzero constants.

$$f = x^3+1 = (x+1)(x^2-x+1)$$

Are these factors irreducible?

- $x+1$ is irreducible because it has degree one, so a factorisation $(x+1) = a \cdot b$ would involve a constant polynomial, which must be a unit.
- x^2-x+1 is irreducible because its roots are $\frac{1 \pm \sqrt{1-4}}{2} = \frac{1}{2} \pm \frac{\sqrt{3}}{2} i$

So we need complex coefficients to factor it: $x^2-x+1 = \left(x-\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\right)\left(x-\left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\right)$

Example: $R = \mathbb{C}[x]$

$$f = x^3+1 = (x+1)\left(x-\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)\right)\left(x-\left(\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\right)$$

is the unique factorisation of f into irreducible elements.

- In $R = \mathbb{C}[x]$, the irreducible elements are linear polynomials, since every polynomial of degree ≥ 2 can be factored (uniquely) into linear factors (by Fundamental Theorem of Algebra).
- In $R = \mathbb{R}[x]$, the irreducible elements are linear polynomials, and quadratic polynomials without real roots.