Algebraic Number Theory

Lecture 2, 15th October 2021

Recall: ⌜ **Thm 1.3**: If $p \geq 3$ is a prime then

$$\begin{array}{c} a,b \in \mathbb{Z} \\ p = a^2+b^2 \end{array} \iff p \equiv 1 \mod 4 \text{ ⌟}$$

proof: today

$$\begin{array}{c} \| \\ (a+bi)(a-bi) \end{array} \quad \text{in } \mathbb{Z}[i]$$

$\rightsquigarrow$ Rings, domain, units, field:
- commutative
- $R^\times = R \setminus \{0\}$
- $1 \neq 0$

irreducible, prime

Number field	$\mathbb{Q}$	$\mathbb{Q}(i)$
	$\cup$	$\cup$
ring of integers	$\mathbb{Z}$	$\mathbb{Z}[i]$
Units	± 1	$\pm i, \pm 1$
primes (up to ass)	prime numbers	Today
UFD	✓	

Definition 1.9 An integral domain R is called a <u>unique factorization domain</u> (UFD) or <u>factorial ring</u>, if

i) any non-zero element $a \in R \setminus \{0\}$ can be written as

$$a = u\, p_1 \cdot \ldots \cdot p_n \qquad (*)$$

where $p_1, \ldots, p_n \in R$ are irreducible and $u \in R^\times$.

ii) the representation $(*)$ is unique in the sense that whenever

$$a = u'\, p_1' \cdot \ldots \cdot p_{n'}',$$

with p_j' irreducible and $u' \in R^\times$, then $n' = n$ and there exist a permutation $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ with

$$p_i = \varepsilon_i\, p'_{\sigma(i)} \quad \text{for some } \varepsilon_i \in R^\times.$$

We want to show that $\mathbb{Z}[i]$ is factorial, by showing that it is euclidean.

Definition 1.10 A domain R is called an Eucledian domain/ring if there exists a function $N: R\setminus\{0\} \to \mathbb{Z}_{\geq 0}$, such that for any $a, b \in R$ with $b \neq 0$ there exist $q, r \in R$ such that

$$a = q \cdot b + r$$

"division by b with rest r"
$11 = 2 \cdot 5 + 1$
$= 3 \cdot 5 - 4$

with either $N(r) < N(b)$ or $r = 0$.

Proposition 1.11 Euclidean rings are factorial.

proof: HW1

Example 1.12 i) $R = \mathbb{Z}$, $N: x \mapsto |x|$

ii) If K is a field then $R = K[x]$ is an eucledian ring with $N(f) = \deg(f)$.

Proposition 1.13 $\mathbb{Z}[i]$ is euclidean.

Proof: We consider the <u>norm</u>

$$N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_{\geq 0}$$
$$\alpha \longmapsto |\alpha|^2$$

For $a, b \in \mathbb{Z}[i]$ with $b \neq 0$ we want to find $q, r \in \mathbb{Z}[i]$ with $|r|^2 < |b|^2$, s.th

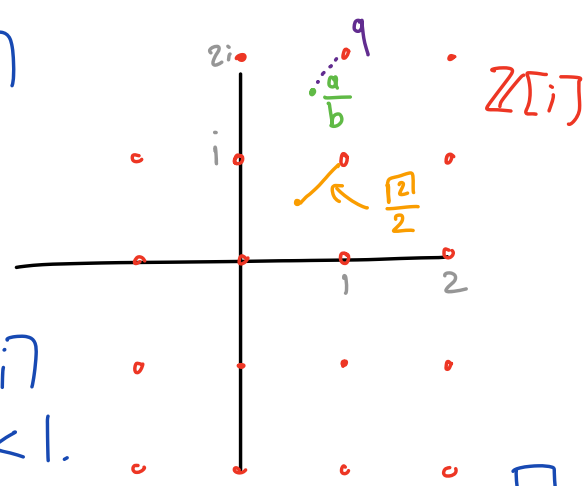
$$a = b \cdot q + r.$$

Therefore we want to find a $q \in \mathbb{Z}[i]$ with

$$\left| \frac{a}{b} - q \right| < 1. \qquad (*)$$

(then $r := \alpha - bq$ satisfies $|r|^2 < |b|^2$)

We can visualize $\mathbb{Z}[i]$ as a lattice in $\mathbb{C}$.



The distance of the complex number $\frac{a}{b}$ to the nearest point q in $\mathbb{Z}[i]$ can not be larger than $\frac{\sqrt{2}}{2} < 1$. This q then satisfies $(*)$. $\square$

Lemma 1.14 (Wilson's theorem)

For any prime p we have $(p-1)! \equiv -1 \mod p$.

Proof: HW

Now we can finally prove Theorem 1.3.

Proof (of Thm. 1.3) (only need to show "$\Leftarrow$")

Let p be prime with $p = 4n+1$.

Set $x = 2n!$ and use Lemma 1.15 to get

$$-1 \equiv (p-1)! \equiv 1 \cdot 2 \cdot \ldots \cdot 2n \cdot (p-2n) \cdot (p-2n-1) \cdot \ldots (p-2)(p-1)$$

$$\equiv (2n)!(-1)^{2n}(2n)!$$

$$\equiv x^2 \mod p$$

Therefore $p \mid x^2+1 = (x+i)(x-i)$, but $p \nmid (x+i)$ and $p \nmid (x-i)$ since $\frac{x}{p} \pm \frac{i}{p} \notin \mathbb{Z}[i]$.

$\Rightarrow$ p is not prime $\underset{\uparrow}{\Rightarrow}$ p is not irreducible.

$\mathbb{Z}[i]$ is factorial (prime $\Leftrightarrow$ irred)

Since $\mathbb{Z}[i]$ is factorial we can write

$$p = \alpha \cdot \beta \quad \text{with } \alpha, \beta \notin \mathbb{Z}[i]^\times.$$

Now since $\underset{\substack{\| \\ p^2}}{N(p)} = N(\alpha\beta) \underset{\substack{\uparrow \\ \text{check!}}}{=} N(\alpha)N(\beta) \in \mathbb{Z}$

we have that $N(\alpha) = p$, since by HW1 $N(\alpha) = 1 \iff \alpha \in \mathbb{Z}[i]^\times$.

And if $\alpha = a + ib$ for some $a, b \in \mathbb{Z}$

we get $N(\alpha) = a^2 + b^2 = p$. $\square$

In particular, we see that a prime $p \equiv 1 \mod 4$ is not prime any more in $\mathbb{Z}[i]$.

Q: What are the prime elements in $\mathbb{Z}[i]$?

When trying to find all prime or irreducible elements of a ring one usually just considers equivalence classes of associated elements.

Definition 1.15 Two elements $a, b \in R$ are called <u>associated</u>, if there exists a unit $\varepsilon - R^\times$ with $a = \varepsilon b$. Notation: $a \sim b$.

Lemma 1.16: If $a \in R$ is prime (resp. irreducible) then all elements $b \in R$ with $a \sim b$ are also prime (resp. irreducible).

Proof: Easy to check by using that $R^\times$ is a group. $\square$

Theorem 1.17 The prime elements π of $\mathbb{Z}[i]$ are, up to associated elements, given by

(i) $\pi = 1 + i$

(ii) $\pi = a + bi$ with $a^2 + b^2 = p$ prime
and $p \equiv 1 \mod 4$
$a > |b| > 0$

(iii) $\pi = p$, p prime with $p \equiv 3 \mod 4$.

Proof: • The elements in (i) and (ii) are prime since if $\pi = \alpha\beta$ for some $\alpha, \beta \in R$ we get $p = N(\pi) = N(\alpha)N(\beta)$ for a prime p. Therefore $N(\alpha)=1$ or $N(\beta)=1$, i.e. α or β is a unit.

$\Rightarrow \pi$ irreducible $\overset{\mathbb{Z}[i] \text{ factorial}}{\Longrightarrow} \pi$ prime.

• If $\pi = p$ for $p \equiv 3 \mod 4$ then $p = \alpha\beta$ with non-units α, β would imply

$$N(\alpha) = p \underset{\substack{\uparrow \\ \alpha = a+bi}}{=} a^2+b^2,$$

which is not possible due to Theorem 1.3.

• It remains to show that any prime element is associated to one of the ones in (i), (ii) or (iii).

Let $\pi = a+bi$ be prime, then in $\mathbb{Z}$ we have

$$N(\pi) = \pi \cdot \underset{(a-bi)}{\overline{\pi}} = p_1 \cdot \ldots \cdot p_r$$

for rational primes $p_1, \ldots, p_r$.

Since π is prime we get $\pi \mid p$ for some rational prime p.

$$\Rightarrow \quad N(\pi) \mid N(p) = p^2$$

From this we get $N(\pi) = p$ or $N(\pi) = p^2$.

If $N(\pi) = p$ we have $p = a^2 + b^2$, i.e π is associated to (i) or (ii).
$(p=2)$

If $N(\pi) = p^2$ then $\pi \sim p$

because $\frac{p}{\pi} \in \mathbb{Z}[i]$ satisfies $N(\frac{p}{\pi}) = 1$

i.e $\underbrace{\frac{p}{\pi}}_{=\varepsilon} \in \mathbb{Z}^\times$ and thus $\pi\varepsilon = p$.

But then we need to have $p \equiv 3 \mod 4$

i.e. π is associated to an element in (iii)

$\square$

Proposition 1.18 The elements in $\mathbb{Z}[i]$ are exactly those in $\mathbb{Q}(i)$, which are a solution of

$$X^2 + aX + b = 0 \quad (\star)$$

$$\overset{\shortparallel}{(X-(c+di))(X-(c-di))}$$

for some $a, b \in \mathbb{Z}$.

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

Proof:

The element $c + di \in \mathbb{Z}[i]$ is the solution of $(\star)$ for $a = -2c \in \mathbb{Z}$, $b = c^2 + d^2$

Conversely assume that for given $a, b \in \mathbb{Z}$ $c + di \in \mathbb{Q}(i)$ is a solution to $(\star)$.

Then $2c \in \mathbb{Z}$ and if we write $d = \frac{p}{q}$ with $\gcd(p,q) = 1$ then

$$\underset{\in\mathbb{Z}}{4b} = \underset{\in\mathbb{Z}}{(2c)^2} + \overbrace{\left(\frac{2p}{q}\right)}^{2d}{}^2$$

$$\Rightarrow \frac{4p^2}{q^2} \in \mathbb{Z} \Rightarrow q^2 \mid 4 \underset{q=1 \text{ or } 2}{\Rightarrow} 2d \in \mathbb{Z}$$

But $4b = (2c)^2 + (2d)^2 \equiv 0 \mod 4$ can just have a solution if $2c$ and $2d$ are even i.e. we get $c, d \in \mathbb{Z}$.

$\square$

Summary

Field	$\mathbb{Q}$	$\mathbb{Q}(i)$	K
ring of Integers	$\mathbb{Z}$	$\mathbb{Z}[i]$	$\mathcal{O}_K$
Units	± 1	$\pm i, \pm 1$	Dirichlet Unit theorem
primes (up to ass)	Prime numbers	Thm, 1.17	$\rightsquigarrow$ ideals
UFD	✓	✓	