Orga: * Register on eCampus (to hand in exercises)

* All infos on webpage
* Do not record the lectures!

Aim of course: Study arithmetic of number fields
↕
finite field of $\mathbb{Q}$

Why? Can be used to study Diophantine equations, i.e. algebraic equations with integral coefficients, and their integral solutions

Example: Which primes p can be written as $p = x^2 + y^2$ for $x, y \in \mathbb{Z}$.

$2 = 1^2 + 1^2$

3 not

$5 = 2^2 + 1$

7 not

$\vdots$

$41 = 5^2 + 4^2$

$\vdots$

$285553 = ??$

Set $K = \mathbb{Q}(i) = \mathbb{Q}[T]/(T^2+1) \supseteq \mathcal{O}_K := \mathbb{Z}[i]$

Note $N_{K/\mathbb{Q}}(x+iy) = x^2 + y^2$, $x, y \in \mathbb{Q}$

$N_{K/\mathbb{Q}} : K \to \mathbb{Q}, \alpha \mapsto \alpha \cdot \bar{\alpha}$ multiplicati

Observation:

$$\varepsilon \in \mathcal{O}_K^\times \iff \varepsilon \in \mathcal{O}_K \text{ and } N_{K/\mathbb{Q}}(\varepsilon) = 1$$

$$\iff \varepsilon \in \{\pm 1, \pm i\}$$

Claim: $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$

$\iff$ $p \in \mathcal{O}_K$ not prime

(Recall: R int. domain

$r \in R \setminus \{0\}$ irreducible if $r = s \cdot t$ implies $s \in R^\times$ or $t \in R^\times$

$r \in R \setminus \{0\}$ prime if $r \mid s \cdot t$ implies $r \mid s$ or $r \mid t$.

non-unit

r prime $\Rightarrow$ r irreducible

$\Leftarrow$

if R is factorial, e.g. a principal ideal domain (PID))

"$\Rightarrow$" $p = (x+iy)(x-iy)$ in $\mathcal{O}_K = \mathbb{Z}[i]$

If $(x+iy) \in \mathcal{O}_K^* \Rightarrow (x-iy) \in \mathcal{O}_K^*$

$\Rightarrow p \in \mathcal{O}_K^* = \{\pm 1, \pm i\}$ ↯

$\Rightarrow$ p not irreducible $\Rightarrow$ p not prime

"$\Leftarrow$" $\mathcal{O}_K$ PID (Exercise)

$\Rightarrow \exists\, \pi_1, \pi_2 \in \mathcal{O}_K \setminus \mathcal{O}_K^*$ with

$\pi_1 \cdot \pi_2 \mid p$

$\Rightarrow N_{K/\mathbb{Q}}(\pi_1 \cdot \pi_2) \mid N_{K/\mathbb{Q}}(p) = p^2$

$\overset{!}{\Rightarrow}$ $N_{K/\mathbb{Q}}(\pi_1) = p$

as $N_{K/\mathbb{Q}}(\pi_i) \neq \pm 1$

Write $\pi_1 = x+iy \Rightarrow x^2+y^2 = N_{K/\mathbb{Q}}(\pi_1) = p$

Now, $(p) \subseteq \mathcal{O}_K$ prime

$\Leftrightarrow \mathcal{O}_K/(p) \cong \mathbb{Z}[T]/(p, T^2+1) \cong \mathbb{F}_p[T]/T^2+1$

integral domain

$\Leftrightarrow T^2+1 \in \mathbb{F}_p[T]$ irreducible

$\Leftrightarrow \exists \alpha \in \mathbb{F}_p^\times$, s.t. $\alpha^2 = -1 \in \mathbb{F}_p$

$\Leftrightarrow p$ odd and $4 \nmid \underbrace{|\mathbb{F}_p^\times|}_{p-1}$

$\mathbb{F}_p^\times$ cyclic

$\Leftrightarrow p \equiv 3 \ (4)$

Conclusion: $p = x^2+y^2$ with $x, y \in \mathbb{Z}$

iff $p=2$ or $p \equiv 1 \ (4)$

In part., $285553 = x^2+y^2$

We used knowledge of arithmetic properties of $K = \mathbb{Q}(i)$ resp. $\mathcal{O}_K = \mathbb{Z}[i]$ (descr. of units in $\mathcal{O}_K$, $\mathcal{O}_K$ PID, when $p \in \mathcal{O}_K$ prime?, ...)

Variant: $m \in \mathbb{Z}$. Which primes p can be written as $p = x^2 + my^2$ with $x, y \in \mathbb{Z}$?

=) need to develope arithmetic understanding of $K = \mathbb{Q}(\sqrt{-m})$, resp. $\mathbb{Z}[\sqrt{-m}]$

or more general number fields $K/\mathbb{Q}$.

1.1. Algebraic integers

Def: $A \subseteq B$ extension of rings

1) $x \in B$ is integral over A if exists monic polynomial

$f(T) \in A[T]$, $f(T) = T^n + a_1 T^{n-1} + \dots + a_n$
with $f(x) = 0$

2) B integral over A if every $x \in B$ is integral over A

Example: 1) $\mathbb{Z}[i] = \mathbb{Z}[T]/(T^2+1)$ integral over $\mathbb{Z}$

2) L/K ext. of fields $\Rightarrow$
L/K integral iff L/K algebraic

3) $A[T]$ not integral over A (if $A \neq 0$)

4) $n \geq 2 \Rightarrow \mathbb{Z}[\frac{1}{n}] \simeq \mathbb{Z}[T]/(nT-1)$
not integral over $\mathbb{Z}$

Prop. $A \subseteq B$ ext. of rings, $x \in B$
TFAE:

1) x integral over A

2) the subring $A[x] \subseteq B$ gen. by A, x, is a finitely gen. A-module

3) ex. subring $B' \subseteq B$, s.t. $x \in B'$ and B' is a fin. gen. A-module.

Proof: 1) $\Rightarrow$ 2) ✓, as

$$x^n \in A + Ax + \dots + Ax^{n-1}$$

for some $n \geq 1$.

2) $\Rightarrow$ 3) ✓

3) $\Rightarrow$ 1): Pick gen. $\alpha_1, \dots, \alpha_n \in B'$ as an A-module, w.log. $\alpha_1 = 1$

As $x \cdot B' \subseteq B'$ ex. $U \in Mat_{n \times n}(A)$, s.t. $\quad \{x b' \mid b' \in B'\}$

$x(\alpha_1, \dots, \alpha_n) = (\alpha_1, \dots, \alpha_n) \cdot U$, i.e.

$$x\alpha_j = \sum_i u_{ji} \alpha_j \quad \text{for } i, j = 1, \dots, n$$

$\uparrow$ A

$\Rightarrow (\alpha_1, \dots, \alpha_n)(x \cdot Id - U) = 0$

Set V as the cofactor matrix of $x \cdot Id - U$.

Then $(x Id - U) \cdot V = \det(x Id - U) \cdot Id$, and

$0 = (\alpha_1, \dots, \alpha_n)(x \cdot Id - U) \cdot V$

$= (\alpha_1, \dots, \alpha_n) \cdot \det(x Id - U) \cdot Id$

$\Rightarrow \det(x Id - U) \cdot \alpha_j = 0$, for all $j = 1, \dots n$

$\Rightarrow \det(x Id - U) = 0$

$\alpha_1 = 1$ ↑

monic polynomial in x with coeff. in A □

Corollary: $A \subseteq B$ ext. of rings

$\Rightarrow B' := \{x \in B \mid x \text{ integral over } A\} \subseteq B$ is a subring

Proof: $x, y \in B' \Rightarrow A[x,y]$ fin. gen. $/A$ $\overset{B}{\underset{U}{}}$

(by $x^i y^j$ for $i,j \leq n$, n suitably large)

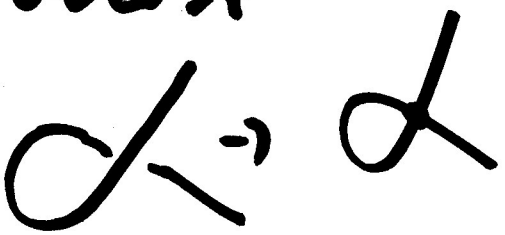
$\Rightarrow x \cdot y, x+y \in B'$ by prev. prop. □

Corollary: $A \subseteq B \subseteq C$ ext. of rings. Then

C integral over A

$\Leftrightarrow$ C integral over B and B integral over A

Proof: "$\Rightarrow$" ✓



"$\Leftarrow$" Pick $x \in C \Rightarrow$ ex. $b_i \in B$, s.t.

$$x^n + b_1 x^{n-1} + \dots + b_n = 0$$

Note $A[b_1, \dots, b_n]$ fin. gen. as an A-module

& $A[b_1, \dots, b_n, x]$ fin. gen. as $A[b_1, \dots, b_n]$

$\Rightarrow A[b_1, \dots, b_n, x]$ fin. gen. as an A-module

$\Rightarrow$ Conclude by last prop. □

Definition: $A \subseteq B$ ext. of rings

1) The integral closure of A in B is the subring of all $x \in B$ which are integral over A.
2) If the integral closure of A in B is A, then A is integrally closed in B.
3) If A int. domain, then A is called integrally closed (or normal) if it is integrally closed in its fraction field $\mathrm{Frac}(A)$.

Example: 1) $\mathbb{Z}$ is integrally closed.

Indeed, let $x = \frac{a}{b} \in \mathbb{Q}$ with $\gcd(a,b) = 1$.

Assume ex. $c_1, \dots, c_n \in \mathbb{Z}$, s.t.

$$x^n + c_1 x^{n-1} + \dots + c_n = 0$$

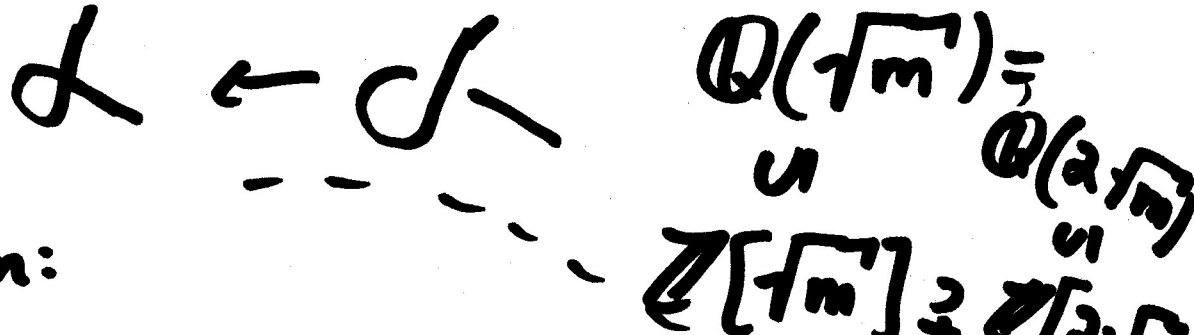
$$\Leftrightarrow a^n + c_1 a^{n-1} \cdot b + \dots + c_n \cdot b^n = 0$$

If $|b| > 1$, pick prime p with $p \mid b$

$\Rightarrow p \mid a \not\Rightarrow x \in \mathbb{Z}$

2) More generally, each factorial ring (e.g. each PID) is integrally closed

3) $\mathbb{Q}[X,Y]/(Y^2 - X^3 - X^2)$ not normal



Definition:

1) $x \in \mathbb{C}$ is an algebraic number (resp. an algebraic integer) - if x is integral over $\mathbb{Q}$ (resp. over $\mathbb{Z}$)

$\overline{\mathbb{Q}} = \{x \in \mathbb{C} \mid x \text{ algebraic numbers}\}$ is a (not countable) algebraically closed field.

2) A number field is a finite field extension of $\mathbb{Q}$

For $K/\mathbb{Q}$ a number field, we let $\mathcal{O}_K \subseteq K$ be the integral closure of $\mathbb{Z}$ in K, and call it the ring of integers of K

Example: $K = \mathbb{Q}(i) \Rightarrow \mathcal{O}_K = \mathbb{Z}[i]$
(as $\mathbb{Z}[i]$ is a PID)

Proposition: $x \in \mathbb{C}$ algebraic number, $f(T) = T^n + a_1 T^{n-1} + \dots + a_n \in \mathbb{Q}[T]$ its minimal poly. Then x algebraic integer $\Leftrightarrow f(T) \in \mathbb{Z}[T]$

Proof: "$\Leftarrow$" ✓ as $f(x) = 0$

"$\Rightarrow$" $\{x = x_1, \dots, x_n\}$ roots of f in $\mathbb{C}$

Then each x_i is an algebraic integer bec x is

Indeed, if $g(T) \in \mathbb{Z}[T]$ monic with $g(x) = 0$, then $g(x_i) = 0$

as exists $\iota : \mathbb{Q}(x) \hookrightarrow \mathbb{C}$, $\iota(x) = x_i$:

$$\mathbb{Q}(x) \cong \mathbb{Q}[T]/(f[T])$$

$$\left(\iota(g(x)) \underset{p}{=} g(\iota(x)) = g(x_i)\right)$$

$g \in \mathbb{Z}[T]$ (as a_i is a polynomial in $x_1, \dots, x_n$)

In part, each $a_i \in \mathbb{Q}$ is an algebraic integer

$\mathbb{Z}$ integrally closed $\Rightarrow a_i \in \mathbb{Z}$ ∎

Example: $K = \mathbb{Q}(\sqrt{D})$ with $D \in \mathbb{Z}$ squarefree

⚠

Then $\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega_D$

$$\omega_D = \begin{cases} \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \ (4) \\ \sqrt{D} & \text{if } D \equiv 2,3 \ (4) \end{cases}$$

Indeed,

$$\omega_D^2 - \omega_D + \frac{1-D}{4} = 0 \quad \text{if } D \equiv 1 \ (4)$$

$$\omega_D^2 - D = 0 \quad \text{if } D \equiv 2,3 \ (4)$$

Let $x = a + b\cdot\sqrt{D} \in \mathcal{O}_K$ with $a, b \in \mathbb{Q}$
$a, b \neq 0$

The min. poly. of x is

$$T^2 - 2aT + (a^2 - b^2 D)$$

$\Rightarrow$ (prev. prop.) $2a \in \mathbb{Z}$, $a^2 - b^2 D \in \mathbb{Z}$ $\quad \mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_K$

If $a \in \mathbb{Z}$, then $b \in \mathbb{Z}$ as D squarefree

If $a \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$, then $b \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$

(as $4b^2 \cdot D \in \mathbb{Z}$ with squarefree)

and $D \equiv 1 \ (4)$

(as $a = \frac{a'}{2}$, $b = \frac{b'}{2}$ with a', b' odd $\in \mathbb{Z}$

and $a'^2 \equiv b'^2 D \ (4)$

$\Rightarrow D \equiv \left(\frac{a'}{b'}\right)^2 \ (4)$

b' odd

$\Rightarrow D \equiv 1 \ (4)$

$\Rightarrow$ Can subtract a and b from x $\Rightarrow$ ✓