Math 538, lecture 5, 13/1/2024

Last time: $K/\mathbb{Q}$ algebraic,

def **ring of integers** $\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ integral over } \mathbb{Z}\}$

saw: ① this is a ring, if $\dim_{\mathbb{Q}} K = n$,

② $\mathcal{O}_K = \bigoplus_{i=1}^{n} \mathbb{Z}\omega_i$, $\{\omega_i\}_{i=1}^{n} \subset K$ a $\mathbb{Q}$-basis

③ If $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ proper (exclude (0)), then

- (i) $\mathfrak{a} \cap \mathbb{Z} \trianglelefteq \mathbb{Z}$ proper
- (ii) $N\mathfrak{a} \overset{\text{def}}{=} [\mathcal{O}_K : \mathfrak{a}] < \infty$ "**norm**" of $\mathfrak{a}$
- (iii) $\operatorname{rk}_{\mathbb{Z}} \mathfrak{a} = n$
- (iv) $\mathfrak{a}$ prime $\Rightarrow$ $\mathfrak{a}$ maximal, $\mathfrak{a} \cap \mathbb{Z} = (p)$ prime in $\mathbb{Z}$.

④ A **fractional ideal** in K is a subset of the form $\alpha\mathfrak{a}$: $\mathfrak{a} \trianglelefteq \mathcal{O}_K$, $\alpha \in K^\times$
$\Leftrightarrow$ f.g. $\mathcal{O}_K$-submodule of K.

Lemma: Every ideal of $\mathcal{O}_K$ contains ($=$divides) a product of primes.

Def If I, J are fractional ideals then so is $IJ = \langle ij \mid \substack{i \in I \\ j \in J} \rangle$, this gives a monoid structure.

<u>Today</u>: Fractional ideals form a group, free on primes (= unique factorization)

<u>Prop</u>: Let $\mathfrak{p} < \mathcal{O}_K$ be prime.

Then $\mathfrak{p}^{-1} = \{x \in \mathcal{O}_K \mid x\mathfrak{p} \subset \mathcal{O}_K\}$ is a fractional ideal properly containing $\mathcal{O}_K \Rightarrow \mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}_K$.

<u>Pf</u>: Let $x, y \in \mathfrak{p}^{-1}$, $\alpha \in \mathcal{O}_K$. Then

$$(\alpha x + y)\mathfrak{p} \subseteq x\alpha\mathfrak{p} + y\mathfrak{p} \subseteq \mathcal{O}_K + \mathcal{O}_K = \mathcal{O}_K.$$

[Aside: clearly $(\alpha\mathcal{O}_K)^{-1} = \alpha^{-1}\mathcal{O}_K$ for all $\alpha \in K^\times$]
[if $\mathfrak{a} \subset \mathfrak{b}$ then $\mathfrak{a}^{-1} \supset \mathfrak{b}^{-1}$]

Know (for any $\mathfrak{a}$) $\mathfrak{a} \cap \mathbb{Z} = (m)$ for $m > 1$.

$\Rightarrow m\mathcal{O}_K \subset \mathfrak{a} \subset \mathcal{O}_K$

$\Rightarrow \mathcal{O}_K \subset \mathfrak{a}^{-1} \subset m^{-1}\mathcal{O}_K$ $\Rightarrow m\mathfrak{a}^{-1} \subset \mathcal{O}_K$

$\Rightarrow \mathrm{rk}_{\mathbb{Z}}\, \mathfrak{a}^{-1} = n$ $(\mathrm{rk}_{\mathbb{Z}}\, \mathcal{O}_K, \mathrm{rk}_{\mathbb{Z}}\, m^{-1}\mathcal{O}_K = n$

Conclusion: For any $\mathfrak{a} \triangleleft \mathcal{O}_K$, $\mathfrak{a}^{-1}$ is a fractional ideal. $\Rightarrow$ same true for all fractional ideals

Return to prime $\mathfrak{p} \supset p\mathcal{O}_K$, $p \in \mathbb{Z}$ prime

Clear that $\mathfrak{p} \subset \mathfrak{p}^{-1}\mathfrak{p} \subset \mathcal{O}_K$, $\mathfrak{p}^{-1} \supset \mathcal{O}_K$

construction $\quad$ $\mathfrak{p}$ ideal

Since $\mathfrak{p}$ is maximal, two possibilities:

(1) $\mathfrak{p}^{-1}\mathfrak{p} = \mathfrak{p}$ $\Rightarrow$ $\mathfrak{p}^{-1} = \mathcal{O}_K$ (Cayley-Hamilton argument)

(2) $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$ $\Rightarrow$ $\mathfrak{p}^{-1} \supsetneq \mathcal{O}_K$ $(\mathcal{O}_K\mathfrak{p} = \mathfrak{p})$.

To see $\mathfrak{p}^{-1} \neq \mathcal{O}_K$, consider $(p) = p\mathcal{O}_K$.
St contains a product of primes:

$\mathfrak{p} \supset p\mathcal{O}_K \supset \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r.$

If $\mathfrak{p} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ have $\mathfrak{p} \supset \mathfrak{p}_i$ for some i.

By maximality of primes, $\mathfrak{p} = \mathfrak{p}_1$ wlog.

Wlog choose r minimal then than have some

$$\alpha \in \mathfrak{p}_2 \mathfrak{p}_3 \cdots \mathfrak{p}_r \setminus p\mathcal{O}_K$$

Then $\alpha \mathfrak{p} = \alpha \mathfrak{p}_1 \in \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \subset p\mathcal{O}_K$

$$\Rightarrow \frac{\alpha}{p} \in \mathcal{O}_K \quad , \quad \frac{\alpha}{p}\mathfrak{p} \subset \mathcal{O}_K$$

$$\Rightarrow \frac{\alpha}{p} \in \mathfrak{p}^{-1}, \quad \mathfrak{p}^{-1} \not\subset \mathcal{O}_K, \; \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K. \quad \blacksquare$$

Theorem: All ideals in $\mathcal{O}_K$ are invertible; every ideal has a unique representation of the form

$$\prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_i$ prime, $e_i \in \mathbb{Z}_{\geq 1}$.
Finally, $\mathfrak{a} \mid \mathfrak{b}$ in the monoid of ideals iff $\mathfrak{b} \subset \mathfrak{a}$.

Pf: let $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ be an ideal, $\mathfrak{p}$ a max'l ideal containing $\mathfrak{a}$. Then

$$\mathfrak{p}^{-1}\mathfrak{a} \subset \mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}_K$$

Also $\mathfrak{p}^{-1}\mathfrak{a} \supsetneq \mathfrak{a}$ (C-H argument)

Now let $\mathfrak{a} \trianglelefteq \mathcal{O}_K$ be max'l among ideals lack a representation as above, $\mathfrak{p}$ a prime containing it. Then $\mathfrak{p}^{-1}\mathfrak{a} \supsetneq \mathfrak{a}$ so $\mathfrak{p}^{-1}\mathfrak{a}$ has a representation $\Rightarrow\Leftarrow$.

$$\Rightarrow \text{all } \mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i \quad \text{then} \quad \left(\prod_{i=1}^{r} \mathfrak{p}_i^{-1}\right)\mathfrak{a} = (1)$$

so all ideals are invertible.

Suppose now $\prod_{i=1}^{r} \mathfrak{p}_i = \prod_{j=1}^{s} \mathfrak{q}_j$

for some primes $\{\mathfrak{p}_i\}$, $\{\mathfrak{q}_j\}$, suppose $r \geq s$ minimal s.t. $r \neq s$ or $\{\mathfrak{q}_j\}$ not permutation of $\{\mathfrak{p}_i\}$

must have $r, s \geq 1$ (any non-trivial prod of primes isn't $\mathcal{O}_K$)

Then $\mathfrak{p}_r \supseteq \prod_j \mathfrak{q}_j$ so $\mathfrak{p}_r \supset \mathfrak{q}_j$ for some j

(wlog $j=s$) so $\mathfrak{p}_r = \mathfrak{q}_s$.

Multiply by $\mathfrak{p}_r^{-1}$, get

$$\prod_{i=1}^{r-1} \mathfrak{p}_i = \prod_{j=1}^{s-1} \mathfrak{q}_j.$$

By minimality of $r+s$, have $r-1=s-1$ and $\{\mathfrak{p}_i\}_{i=1}^{r-1}$ is a permutation of $\{\mathfrak{q}_j\}_{j=1}^{s-1}$

$\Rightarrow \Leftarrow$

Finally, if $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ then $\mathfrak{b} = \mathfrak{a}\mathfrak{c} \subset \mathfrak{a}\mathcal{O}_K = \mathfrak{a}$.

if $\mathfrak{b} \subset \mathfrak{a}$ then $\mathfrak{a}^{-1}\mathfrak{b} \subset \mathfrak{a}^{-1}\mathfrak{a} = \mathcal{O}_K$

so $\mathfrak{a}^{-1}\mathfrak{b}$ is an ideal, s.t. $\mathfrak{a}\cdot(\mathfrak{a}^{-1}\mathfrak{b}) = \mathfrak{b}$. ∎

<u>Cor:</u> Every fractional ideal is invertible, (so fractional ideals form a group), Every element in the group has a unique representation

$\prod_{\mathfrak{p} \text{ primes}} \mathfrak{p}^{e_\mathfrak{p}}$, $e_\mathfrak{p} \in \mathbb{Z}$ all but finitely many are zero

Also $\mathfrak{a} \supset \mathfrak{b}$ iff $\mathfrak{a}^{-1}\mathfrak{b}$ is an ideal of $\mathcal{O}_K$

Pf: if $\mathfrak{a} \trianglelefteq \mathcal{O}_K$, $\alpha \in K$, $\mathfrak{a}\alpha \cdot (\alpha^{-1}\mathfrak{a}^{-1}) = \mathcal{O}_K$
rest as usual

Remark: in $\mathbb{Z}[\sqrt{-5}]$ $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$
all irred.

in $\mathbb{Z}[\sqrt{-3}]$: $2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

In first case, $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z}[\sqrt{-5}]$ is not a PID

In second case, $\mathcal{O}_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}[\omega] \supsetneq \mathbb{Z}[\sqrt{-3}]$

$\omega = \frac{-1+\sqrt{-3}}{2}$.

$\mathbb{Z}[\omega]$ is a PID

Failure of $\mathcal{O}_K$ to be a UFD $\Leftrightarrow$ PID:

Def: (Dedekind): Call a fractional ideal
principal if it is of the form $\alpha\mathcal{O}_K$.

Clear: $\{\text{principal fractional ideals}\} < \{\text{all fractional ideals}\}$

is subgroup. Call elements of quotient

ideal classes, quotient group the class group

$Cl(K)$.

Observe: ideals surject onto class group

Thm: The class group is finite

Def: The class number of K is $h_K = \# Cl(K)$

In fact ("Dirichlet-type thm") primes surject on $Cl(K)$. Further (Hilbert classfield + Chebotarev density theorem)

$$\frac{\#\{\mathfrak{p} \triangleleft \mathcal{O}_K \text{ prime} \mid N\mathfrak{p} \le x,\ \mathfrak{p} \in \text{fixed class}\}}{\#\{\mathfrak{p} \triangleleft \mathcal{O}_K \text{, prime} \mid N\mathfrak{p} \le x\}} \xrightarrow[x \to \infty]{} \frac{1}{h_K}.$$

(also $\#\{\mathfrak{p} \mid N\mathfrak{p} \le x\} \sim Li(x)$

better: $\displaystyle\sum_{N\mathfrak{p} \le x} \log N\mathfrak{p} \sim x.$)

Cohen-Lenstra Heuristics

Ex: $\mathcal{A}$ = set of isom classes of FAG.

$$\frac{1}{Z} = \sum_{A \in \mathcal{A}} \frac{1}{\# \mathrm{Aut}(A)} < \infty$$

So define $p(A) = \frac{Z}{\# \mathrm{Aut}(A)}$ get

prob measure on $\mathcal{A}$

Conj: As $d \to \infty$ along square free #,

$\{ Cl(\mathbb{Q}(\sqrt{d})) \}_d$ is equidistributed in $\mathcal{A}$

(As $-d \to -\infty$ through negatives of squarefree negatives, $h_{\mathbb{Q}(\sqrt{d})} \to \infty$)

Ex: In $\mathbb{Q}(\sqrt{d})$, have bijection

$\{$ ideal classes $\}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ $\leftrightarrow$ $\{$ classes of binary integral quadratic form of discr. discr $\mathbb{Q}(\sqrt{d})$ $\}$

$\mathfrak{a} \lhd \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ ideal, $\mathfrak{a} \cong \mathbb{Z}^2$ as ab gp

$N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ is a quad form

$(\mathfrak{a}, N|_{\mathfrak{a}})$ is a quadratic form

Back to $\mathbb{Z}[\sqrt{-3}] \subseteq \mathbb{Z}[\omega]$, $\omega = \frac{-1+\sqrt{-3}}{2}$.

have $\omega \cdot \bar{\omega} = 1$ so $(2\omega) \cdot (2\bar{\omega}) = 4 = 2 \cdot 2$

failure of unique factorization in $\mathbb{Z}[\sqrt{-3}]$

But $\mathbb{Z}[\omega]$ is a PID

$$N(a+b\omega) = a^2 + b^2 - ab$$

$$N\left(\left(a - \tfrac{1}{2}b\right) + \tfrac{1}{2}b\sqrt{-3}\right) \geq \frac{b^2}{4}$$

If $N = 2$, $\frac{b^2}{4} \leq 2$ so $b^2 \leq 8$

so $b \in \{0, \pm 1, \pm 2\}$

R ring, $1 \in S \subset R$ closed under $\cdot$

$$R[S^{-1}] = \left\{ \frac{a}{s} \,\middle|\, \begin{matrix} a \in R \\ s \in S \end{matrix} \right\}$$

If $\mathfrak{p} \lhd R$ prime, $S = R \setminus \mathfrak{p}$

Get $R_{\mathfrak{p}} = R[(R \setminus \mathfrak{p})^{-1}]$.

Then $\mathfrak{p}$ unique maximal ideal.

<u>Facts</u> for all rational primes $p \neq 2$,

$$\mathbb{Z}[\sqrt{-3}][\{l \neq p\}^{-1}] \cong \mathbb{Z}[\omega][\{l \neq p\}^{-1}]$$

Suppose $K = \mathbb{Q}(\alpha)$, $p(\alpha) = 0$ p monic, irred.

$$\mathbb{Z}[x]/(p) \subset K = \mathbb{Q}[x]/(p)$$

is an order not necc. max'l

(e.g. $\mathbb{Q}(\sqrt{-3})$ $p = x^2 + 3$)