Math 538, Lecture 3 17/1/2024

Last time: Trying to use unique factorization in $\mathbb{Z}[\zeta_p]$ to solve $x^p - y^p = z^p$.

Today: # fields, alg integers

Recall: $K/\mathbb{Q}$ is an extension, call $\alpha \in K$ an algebraic integer if $\exists$ monic $p \in \mathbb{Z}[x]$ s.t. $p(\alpha) = 0$

Saw: true iff min poly in $\mathbb{Z}[x]$

Saw: $\alpha \in \mathbb{Q}$ is integral iff $\alpha \in \mathbb{Z}$

§

Notation: $\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ is an alg. integer}\}$

$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, saw $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$

Lemma: $\beta \in \mathcal{O}_K$ iff $\mathbb{Z}[\beta]$ is a finitely generated $\mathbb{Z}$-module, iff $\exists$ f.g. $\mathbb{Z}$-module $\{0\} \neq M \subset K$ s.t. $\beta M \subset M$

Cor: $\mathcal{O}_K = \bigcup \{\text{f.g. } \mathbb{Z}\text{-submodules } M \subset K \text{ s.t. } 1 \cdot M \subset M\}$

Pf: If $\beta \in \mathcal{O}_k$, $p(\beta)=0$ p monic, deg n, then $\mathbb{Z}[\beta] = \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}$.

RHS contained in $\mathbb{Z}[\beta]$, contains $\mathbb{Z}$, closed under mult by β: $\beta \cdot \beta^i = \beta^{i+1}$, $\beta \cdot \beta^{n-1} = \beta^n$

$$\beta^n = \beta^n - p(\beta) \in \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}$$

Conversely let $M \subset k$ be gen by $\{w_i\}_{i=1}^n$, Then $\beta \cdot w_j = \sum_i a_{ij} w_i$ ($\beta w_j \in M$)

for some $a_{ij} \in \mathbb{Z}$. Let p_A = char poly of $A = (a_{ij})_{i,j=1}^n$

Cayley-Hamilton: $p_A(\beta)$ is the zero endo. of M

But k is a field and $M \neq \{0\}$ so $p_A(\beta) = 0$ in k so $\beta \in \mathcal{O}_k$ ∎

Theorem: Let $\alpha, \beta \in \mathcal{O}_k$. Then $\alpha \pm \beta, \alpha\beta \in \mathcal{O}_k$

Pf: Suppose $\alpha M \subset M$, $\beta N \subset N$ where $M, N \neq \{0\}$

$M = \text{span}_{\mathbb{Z}}\{x_i\}_{i=1}^m$, $N = \text{span}_{\mathbb{Z}}\{y_j\}_{j=1}^n$,

Then $M_N = \mathrm{Span}\{x_i y_j\}_{i,j} \subset K$ is f.g.
and $\alpha(M_N), \beta(M_N) \subset M_N$

So M_N is stable by $\mathbb{Z}[\alpha,\beta]$, $M_N \neq \{0\}$. ∎

Cor: $\mathcal{O}_K \subset K$ is a subring (the ring of integers)
(1) Every Galois conjugate of $\alpha \in \mathcal{O}_K$ is an integer.
(2) The min poly of $\alpha \in \mathcal{O}_K$ is in $\mathbb{Z}[x]$
(3) $\mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha)$, $N_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Z}$
(4) $\alpha \in \mathcal{O}_K^{\times}$ if $N_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Z}^{\times} \in \{\pm 1\}$

PF: Let L/K be the normal closure over $\mathbb{Q}$.
Then $\mathcal{O}_K = \mathcal{O}_L \cap K$, all conjugates of $\alpha \in \mathcal{O}_K$ lie in L, satisfy same $\mathbb{Z}[x]$-poly as α That's (1)

(2) Then min poly of α is:

$$\prod_{\mu \in \mathrm{Hom}(\mathbb{Q}(\alpha), \overline{\mathbb{Q}})} (x - \mu(\alpha)) = \prod_{\mu \in \mathrm{Hom}(\mathbb{Q}(\alpha), L)} (x - \mu(\alpha)) \in \mathcal{O}_L[x] \cap \mathbb{Q}[x] = \mathbb{Z}[x]$$

since $\mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$

$$\mathcal{O}_{\overline{\mathbb{Q}}}[x] \cap \mathbb{Q}[x] = \mathbb{Z}[x]$$

since $\mathcal{O}_{\overline{\mathbb{Q}}} \cap \mathbb{Q} = \mathbb{Z}$

(3) $\mathrm{Tr}_{\mathbb{Q}(\alpha)}^{\mathbb{Q}}\alpha$, $N_{\mathbb{Q}(\alpha)}^{\mathbb{Q}}\alpha$ are coeff of min poly,

$$\mathrm{Tr}_{\mathbb{Q}}^{K}\alpha = [K:\mathbb{Q}(\alpha)]\cdot \mathrm{Tr}_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}\alpha$$

$$N_{\mathbb{Q}}^{K}\alpha = \left(N_{\mathbb{Q}}^{\mathbb{Q}(\alpha)}\alpha\right)^{[K:\mathbb{Q}(\alpha)]}$$

Cor: Tr, N are poly in Galois conjugates so lie in $\mathcal{O}_L$, in $\mathbb{Q}$ so in $\mathbb{Z}$

(4) Exercise

Claim: $[K:\mathbb{Q}]=n$, then $\mathcal{O}_K$ = free $\mathbb{Z}$-module on $\mathbb{Q}$-basis of K

$\Rightarrow$ max'l subring of $\mathcal{O}_K$ which is a f.g. $\mathbb{Z}$-module

order in K

Also call $\mathcal{O}_K$ the maximal order

Lemma: Let $\alpha\in K$. then $\exists m\in\mathbb{Z}_{\geq 1}$ s.t. $m\alpha\in\mathcal{O}_K$

Pf: Let $f=\sum_{i=0}^{d} a_i x^i \in \mathbb{Q}[x]$ be the min poly of α.

then $\sum_{i=0}^{d} a_i m^{d-i} (m\alpha)^i = m^d f(\alpha) = 0$

choose m large enough s.t. $a_i m \in \mathbb{Z}$ for all $0 \le i \le d-1$

$\Rightarrow$ $a_i m^{d-i} = a_i m \cdot m^{d-i-1} \in \mathbb{Z}$. ∎

Cor: $\exists$ $\mathbb{Q}$-basis of K consisting of integers

Lemma: The quadratic form $(x,y) = \mathrm{Tr}_{\mathbb{Q}}^{K}(xy)$ is non-degenerate.

Pf: If $x \neq 0$ then $\mathrm{Tr}_{\mathbb{Q}}^{K}(x \cdot x^{-1}) = n \neq 0$

Prop: $\exists$ $\mathbb{Q}$-basis $\{w_i^*\}_{i=1}^n$ of K s.t. $\mathcal{O}_K \subset \bigoplus_{i=1}^n \mathbb{Z} w_i^*$.

Pf: Say $\{w_i\}_{i=1}^n \subset K$ is a $\mathbb{Q}$-basis s.t. $\bigoplus_{i=1}^n \mathbb{Z} w_i \subset \mathcal{O}_K$

dualise wrt Tr.

Let $\{w_i^*\}$ be the dual basis: $\mathrm{Tr}_{\mathbb{Q}}^{K}(w_i w_j^*) = \delta_{ij}$.

Let $\alpha \in \mathcal{O}_K$, then $a_i := \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha w_i) \in \mathbb{Z}$

$\Rightarrow$ $\alpha = \sum_j a_j w_j^* \in \bigoplus_j \mathbb{Z} w_j^*$.

(Cor: the dual of $\mathcal{O}_K$ wrt $(\cdot,\cdot)$ contains $\mathcal{O}_K$
it's called the different of K)

Observe: the ab gp $(\mathcal{O}_K, +)$
contains $\mathbb{Z}^n$, embeds in $\mathbb{R}^n$.

Thm: $\mathcal{O}_K \cong \mathbb{Z}^n$ as a f.g. ab gp.

(clear: $\mathbb{Z}$-basis of $\mathcal{O}_K$ is a $\mathbb{Q}$-basis of K)

Examples

$$\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right] \subset \mathbb{Q}(w)$$

$\uparrow w$

two orders in $\mathbb{Q}(w)$;
max'l order is $\mathbb{Z}[w]$.

smaller orders exist eg. $\mathbb{Z}[2\sqrt{-3}]$

Example (HW)
in $K = \mathbb{Q}(\zeta_n)$, $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$

Unique factorization

Fix $K/\mathbb{Q}$, degree n

Lemma-

Defn Let $I, J \lhd R$. Then $IJ = \{\sum_{i=1}^{k} a_i b_i \mid \begin{matrix} a_i \in I \\ b_i \in J \end{matrix}\}$ is the ideal of R gen by products $\{ab \mid \begin{matrix} a \in I \\ b \in J \end{matrix}\}$

Ex: $(IJ)K = I(JK)$, $IJ = JI$, $R \cdot I = I$.

Convention: For this section, "ideal" excludes (0), includes $\mathcal{O}_K$. A "prime" of $\mathcal{O}_K$ means a prime ideal, "rational prime" means prime $p \in \mathbb{Z}$

Prop: Let $\mathfrak{a} \lhd \mathcal{O}_K$ be a proper ideal

(1) $\mathfrak{a} \cap \mathbb{Z} \lhd \mathbb{Z}$ is a proper ideal.

(2) $[\mathcal{O}_K : \mathfrak{a}] < \infty$.

(3) $\mathfrak{a}$ is f.g. in fact $\operatorname{rank}_{\mathbb{Z}} \mathfrak{a} = n$

(4) If $\mathfrak{a}$ is prime, $\mathfrak{a} \cap \mathbb{Z} = (p)$ for a rational prime p

say $\mathfrak{a}$ lies above (p)

Pf: Ex.

Defn: The norm of $\mathfrak{a} \lhd \mathcal{O}_K$ is $N\mathfrak{a} \overset{\text{def}}{=} [\mathcal{O}_K : \mathfrak{a}]$

Remark: Let p be a rational prime, then $p\mathcal{O}_K$ is a proper ideal, so contained in some max'l ideal (say $\mathfrak{P}$). Then

$$p\mathbb{Z} = p\mathcal{O}_K \cap \mathbb{Z} \subseteq \mathfrak{P} \cap \mathbb{Z} \subsetneq \mathbb{Z}$$

But $p\mathbb{Z}$ is max'l so $\mathfrak{P} \cap \mathbb{Z} \cap \mathbb{Z} = p\mathbb{Z}$: all primes of $\mathbb{Z}$ extend to primes of $\mathcal{O}_K$.

Observation: If L/K extension of #fields, $\mathfrak{P}$ prime of $\mathcal{O}_L$, must have $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ is a prime of $\mathcal{O}_K$ below $\mathfrak{P}$.

But showing $\exists$ primes of L above $\mathfrak{p} \triangleleft \mathcal{O}_K$ is less obvious: need to show $\mathfrak{p}\cdot\mathcal{O}_L \neq \mathcal{O}_L$.

Goal: Show every ideal of $\mathcal{O}_K$ has a unique factorization as product of prime ideals (Thm of Kummer; pf here due to Dedekind)

Recall proof that every $a \in \mathbb{Z}_{\geq 1}$ is a pdt of irreducibles: Let a be minimal s.t. a is not such a pdt; then $a \geq 2$, let $p = \min\{b \geq 2 \mid b \mid a\}$

Then p is irred. Now $\frac{a}{p} \in \mathbb{Z}$, smaller than a, so $\frac{a}{p}$ is a pdt of irred, $\Rightarrow$ same for $a = p \cdot \frac{a}{p}$.

Replace a with $\mathfrak{a} \lhd \mathcal{O}_K$, p with a max'l ideal $\mathfrak{p} \lhd \mathcal{O}_K$, $\mathfrak{p} \supseteq \mathfrak{a}$. (1) Need to construct $\mathfrak{p}^{-1}$, $\mathfrak{p}(\mathfrak{p}^{-1}\mathfrak{a}) = \mathfrak{a}$

(2) difficulty: show $\mathfrak{p}^{-1}\mathfrak{a}$ is "smaller"

Def: An $\mathcal{O}_K$-submodule $\mathfrak{a} \subset K$ is a **fractional ideal** if $\exists\, \alpha \in K^*$ s.t. $\alpha \cdot \mathfrak{a} \subset \mathcal{O}_K$.

$\Leftrightarrow$ {fractional ideals} $= \{ \alpha \cdot \mathfrak{b} : \alpha \in K^*, \mathfrak{b} \lhd \mathcal{O}_K \}$

Example: $\alpha\mathbb{Z}$, $\alpha \in \mathbb{Q}^*$. (e.g. $\frac{1}{2}\mathbb{Z}$)

If $\mathfrak{a}, \mathfrak{b}$ are fractional ideals let

$$\mathfrak{a}\mathfrak{b} = \left\{ \sum_{i=1}^{k} \alpha_i \beta_i \;\middle|\; \begin{matrix} \alpha_i \in \mathfrak{a} \\ \beta_i \in \mathfrak{b} \end{matrix} \right\}$$

again $\mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a}$, $(\mathfrak{a}\mathfrak{b})\mathfrak{c} = \mathfrak{a}(\mathfrak{b}\mathfrak{c})$, $(1) = \mathcal{O}_K$ has $\mathfrak{a} \cdot (1) = \mathfrak{a}$.

Def: Call $\mathfrak{a}$ **invertible** if have $\bar{\mathfrak{a}}$ st $\mathfrak{a}\bar{\mathfrak{a}} = (1)$

Lemma: Every proper ideal of $\mathcal{O}_K$ contains a product of primes

Pf: Let $\mathfrak{a}$ be a maximal counterexample. If $\mathfrak{a}$ is not itself prime, have $x, y \in \mathcal{O}_K$, $x, y \notin \mathfrak{a}$ s.t. $xy \in \mathfrak{a}$

Then $(\mathfrak{a}, x) \cdot (\mathfrak{a}, y) = \mathfrak{a}$

But $(\mathfrak{a}, x), (\mathfrak{a}, y) \supsetneq \mathfrak{a}$, so each contains a product of primes $\Rightarrow \Leftarrow$

Q: Using C-H over rings:

Say R ring, M f.g. R-module.

$M = \langle m_1, \dots, m_n \rangle$. Say $T \in \mathrm{End}_R(M)$

Then have $a_{ij} \in R$ s.t. $T m_j = \sum_i a_{ij} m_i$

Let $A = (a_{ij})$, $p_A(x) = \det(x I_n - A) \in R[x]$

Thm (Cayley-Hamilton) $p_A(A) = 0$.

(originally, thm is when R is a field, but actually it's an identity in $\mathbb{Z}[(x_{ij})_{i,j=1}^n]$)

Apply $p_A(T)$ to M.

Ex: $T^k \cdot m_j = \sum_{i=1}^n (A^k)_{ij} m_i$

$\Rightarrow p_A(T) \cdot m_j = \sum_{i=1}^n (p_A(A))_{ij} m_i = 0$

$\Rightarrow p_A(T) \cdot m_j = 0$, so $p_A(T) = 0$ in $\mathrm{End}_R(M)$.

Say K field, $M \subset K$ f.g. $\mathbb{Z}$-module, $\neq 0$

$\beta \in K$ has $\beta M \subset M$. Then mult'n β is an endo. of M, so $\subset$. If above set

$p_A \in \mathbb{Z}[x]$ s.t. $p_A(\beta) = 0$ in $\mathrm{End}_{\mathbb{Z}}(M)$

if $x \in M$ is non-zero, $p_A(\beta) \cdot x = 0$

so $p_A(\beta) = 0$ in K

so $\beta \in \mathcal{O}_K$

More on duality

If V fdsp / F have dual V^*, pairing

$$(V^*, V) \to F \quad \text{(evaluation)}$$

If have any bilinear form $W \times V \to F$ any $w \in W$ defines a linear functional by $(w, \cdot)$

Case: $W = V$, $\dim_F V = n < \infty$

Call $(\cdot,\cdot) : V \times V \to F$ non-degenerate

if $\forall_{x \neq 0} x \in V \; \exists y, z \in V$ s.t. $(x, y) \neq 0$, $(z, x) \neq 0$

i.e. map $V \to V^*$ $x \mapsto (x, \cdot)$
is injective $\Rightarrow$ isom

Galois theory: if char $K \neq 0$, $[L:K] = n$

then $L \times L \to K$: $(x,y) \mapsto \mathrm{Tr}_K^L(xy)$

is a non-degen pairing: $\mathrm{Tr}_K^L(x \cdot x^{-1}) = [L:K] \neq 0$

$\Rightarrow$ identified L^* (dual as K-vsp) with L

---

if $U \xrightarrow{f} V$ set dual

$f^*: V^* \to U^*$ (composition with f)

if $f: U \to V$ is an inclusion

get f^* is a quotient map

$\{x_i\} \subset V$ basis, $\{\varphi_j\} \subset V^\vee$ dual basis

when $\varphi_j(x_i) = \delta_{ij}$

if identify $V, V^\vee$ can't pairing the dual basis means

$$\langle x_j^\vee, x_i \rangle = \delta_{ij}$$

(cf. $\mathrm{Tr}_k^L(\omega_i^\vee \omega_j) = \delta_{ij}$

Can also have duality for free $\mathbb{Z}$-modules

M free $\mathbb{Z}$-module, $M^\vee = \mathrm{Hom}(M; \mathbb{Z})$

spanned by dual basis: if $M = \bigoplus_i \mathbb{Z} m_i$

have $\varphi_j : M \to \mathbb{Z}$ def. by $\varphi_j(m_i) = \delta_{ij}$

if φ any map $\varphi = \sum_{j=1}^{n} \varphi(m_j) \cdot \varphi_j$

M^* also free $\mathbb{Z}$-module

Say M free $\mathbb{Z}$-module, $M_{\mathbb{Q}} = M \otimes_{\mathbb{Z}} \mathbb{Q}$ get $\mathbb{Q}$-vsp
on same basis

$$M^* = \{ \varphi \in M_{\mathbb{Q}}^* \mid \varphi(M) \subset \mathbb{Z} \}$$

(in general, if $V = \mathbb{Q}$-vsp, $M \subset V$ additive sp,
map $V^* \to M^*$ by restriction.)

If M spanning, restriction injective
then
$$M^* = \{ \varphi \in V^* \mid \varphi(M) \subseteq \mathbb{Z} \}$$

if have pairing $V \times V \to \mathbb{Q}$ (non-degen)

identifies M^* with subset of V.

We had $M = \mathcal{O}_K$, $V = K$, $F = \mathbb{Q}$.
pairing : trace pairing.

$$\bigoplus_{i=1}^{n} \mathbb{Z} w_i \subset \mathcal{O}_K$$

$$\downarrow$$

$$\left(\bigoplus_{i=1}^{n} \mathbb{Z} w_i\right)^{\vee} \subset \mathcal{O}_K^{\vee}$$

apply identification using trace form.

$$\left(\bigoplus_{i=1}^{n} \mathbb{Z} w_i\right)^{\vee} \cong \bigoplus_{i=1}^{n} \mathbb{Z} w_i^{\vee}$$

$w_i^{\vee}$ = dual basis

<u>checked</u>: $\mathcal{O}_K^{\vee} \supset \mathcal{O}_K$

(if $\alpha \in \mathcal{O}_K$, $(\alpha, \cdot) : \mathcal{O}_K \to \mathbb{Z}$

so get injection $\mathcal{O}_K \hookrightarrow \mathcal{O}_K^{\vee}$)

$$\Rightarrow \bigoplus_{i=1}^{n} \mathbb{Z} w_i \subset \mathcal{O}_K \subset \mathcal{O}_K^{\vee} \subset \bigoplus_{i=1}^{n} \mathbb{Z} w_i^{\vee}.$$

if $M \subset N$

$\operatorname{Hom}_{\mathbb{Z}}(N, \mathbb{Z}) \subset \operatorname{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$