Lecture 2: Algebraic Integers

Last time: $\mathbb{Z}[i] \subseteq \mathbb{Q}(i)$

[Consider delaying or skipping the proof.]

Prop: $\mathbb{Z}[i] = \{\alpha \in \mathbb{Q}(i) \mid \exists\, a, b \in \mathbb{Z}$ so that α is a root of $x^2 + ax + b = 0\}$

Pf: If $\alpha = c + \underbrace{d}_{\neq 0} i \in \mathbb{Q}(i)$ is a root of $f(x) = x^2 + ax + b = 0$ where $a, b \in \mathbb{Q}$, then $f(x) = (x - \alpha)(x - \bar{\alpha}) \Rightarrow a = -2c,\ b = c^2 + d^2$.

So if $\alpha \in \mathbb{Z}[i]$ then $a, b \in \mathbb{Z}$. Conversely, if $c, d \in \mathbb{Z}$, then $2c$ and $2d \in \mathbb{Z}$ as $(2c)^2 + (2d)^2 = 4b$

Moreover, $(2c)^2$ and $(2d)^2$ must be $0 \bmod 4$ by $\uparrow$ and thus $c, d \in \mathbb{Z}$. $\blacksquare$

Def: $\alpha \in \overline{\mathbb{Q}}$ is an <u>algebraic integer</u> if it is the root of a <u>monic</u> poly in $\mathbb{Z}[x]$.

$\uparrow$ lead coeff 1.

Alg. ints: $3,\ i,\ \sqrt{2},\ \frac{1+\sqrt{5}}{2}$

Non ints: $\frac{1}{2},\ \frac{1+i}{2},\ \frac{1+\sqrt{5}}{4}$ $\longleftarrow$ are still roots of int polys, e.g. $2x - 1 = 0$.

Notation: $K/\mathbb{Q}$ then $\mathcal{O}_K$ = all alg. ints in K.

Ex: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, $\mathcal{O}_{\mathbb{Q}(\sqrt{5})} = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$.

<u>Gauss's Lemma</u>: $f \in \mathbb{Z}[x]$ factors in $\mathbb{Q}[x] \Rightarrow$ factors in $\mathbb{Z}[x]$.

<u>Cor</u>: $\mathcal{O}_K$ is a subring $\left[A = \mathcal{O}_{\overline{\mathbb{Q}}}\right.$ is a subring of $\left.\overline{\mathbb{Q}}\right]$

<u>Thm</u>: T.F.A.E. for $\alpha \in \overline{\mathbb{Q}}$:

1) α is an alg. int
2) The additive group of $\mathbb{Z}[\alpha]$ is finitely generated.
3) $\alpha \in A$, a subring with f.g. additive group.
4) $\alpha A \subseteq A$ for a finitely gen additive subgroup of $\overline{\mathbb{Q}}$.

<u>Contrast</u>: $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ with
$\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^b} \mid a,b \in \mathbb{Z}\}$ which isn't finitely gen as an additive group.

<u>Pf of Cor</u>: α, β are alg. ints $\Rightarrow$ $\mathbb{Z}[\alpha]$ is gen under $+$ by $\alpha_1, \ldots, \alpha_n$ and $\mathbb{Z}[\beta]$ by $\beta_1, \ldots, \beta_m$. Then $\mathbb{Z}[\alpha, \beta]$ is additively gen by $\{\alpha_i \beta_j\}$ finite.
$\Rightarrow$ by (3) that $\alpha\beta$ and $\alpha + \beta$ are alg. integers.

<u>Pf of Thm</u>: (1) $\Rightarrow$ (2): If $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0 = 0$ where $a_i \in \mathbb{Z}$, then $(\mathbb{Z}[\alpha], +)$ is gen by $1, \alpha, \ldots, \alpha^{n-1}$

(2) $\Rightarrow$ (3) $\Rightarrow$ (4): clear.

(4) $\Rightarrow$ (1) Suppose $a_1, \ldots, a_n$ generate A.

Consider $\vec{v} = (a_1, \ldots, a_n) \in \overline{\mathbb{Q}}^n$. As $\alpha a_i \in A$, there is an *integer* matrix M so that $\alpha \vec{v} = M\vec{v}$.

Then α is a root of $\mathrm{char}(M) = \det(xI - M)$, a *monic* polynomial in $\mathbb{Z}[x]$. So α is an alg. int. $\blacksquare$

[The rings $\mathcal{O}_K$ will be the central objects of this course. Typically more complicated than $\mathbb{Z}[i]$; e.g. unique factorization fails.]

L/K - field extension. Given $\alpha \in L$, consider

$$T_\alpha : L \to L, \quad x \mapsto \alpha x$$

as a linear transformation of K-vector spaces. Then

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{tr}(T_\alpha) \quad \text{(trace)}$$

$$\mathcal{N}_{L/K}(\alpha) = \det(T_\alpha) \quad \text{(norm)}$$

Here $\underbrace{\mathrm{Tr}_{L/K} : L \to K}_{\text{under} +}$ and $\mathcal{N}_{L/K} : L^\times \to K^\times$ are homomorphisms.

<u>Ex</u>: $\mathbb{Q}(i)/\mathbb{Q}$ $\quad \alpha = a + bi \quad$ basis $= \{1, i\}$ $\quad T_\alpha = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

$$\mathrm{tr}(\alpha) = 2a \qquad \mathcal{N}(\alpha) = a^2 + b^2 \leftarrow \text{from last time.}$$

$$= \alpha + \bar{\alpha} \qquad = \alpha\bar{\alpha}$$

Prop: L/K seperable (e.g. char $=0$). Let $\sigma_1, \dots, \sigma_d : L \to \overline{K}$ be the $d = [L:K]$ distinct embeddings which are the id on K. Then

$$tr_{L/K}(\alpha) = \sum \sigma_i(\alpha) \quad \text{and} \quad \mathcal{N}_{L/K}(\alpha) = \prod \sigma_i(\alpha)$$

Pf when $L = K(\alpha)$: Notice that if $f(x) \in K(x)$, then $f(\alpha) = 0 \iff f(T_\alpha) = 0$. Thus

$$\text{min poly } \alpha = \text{char poly of } T_\alpha$$

$$\text{min poly } \alpha = \prod (x - \sigma_i(\alpha)) = x^d - \left(\sum \sigma_i(\alpha)\right)x^{d-1} + \cdots + (-1)^d \prod \sigma_i(\alpha)$$

$$\text{char poly of } T_\alpha = \det(xI - T_\alpha) = x^d - tr(T_\alpha)x^{d-1} + \cdots + (-1)^d \det T_\alpha$$

[or calculate w.r.t. the basis $\{1, \alpha, \dots, \alpha^{d-1}\}$.] ∎

Basic Props:

$$\begin{array}{c} M \ni \alpha \\ | \\ L \\ | \\ K \end{array} \qquad tr_{M/K} = Tr_{L/K} \circ Tr_{M/L} \qquad \mathcal{N}_{M/K} = \mathcal{N}_{L/K} \circ \mathcal{N}_{M/L}$$

Ex:

$$\begin{array}{c} M = \mathbb{Q}(i, \sqrt{2}) \\ | \\ L = \mathbb{Q}(i) \\ | \\ \mathbb{Q} \end{array}$$

$$tr_{M/\mathbb{Q}}(i + \sqrt{2}) = i + \sqrt{2} + (-i + \sqrt{2}) + (i - \sqrt{2}) + (-i - \sqrt{2}) = 0$$

$$tr_{M/L}(i + \sqrt{2}) = 2i$$