Goals now:

- 581d lecture 1 —— survey of math software.
- 581b lecture 1 —— proof $\mathcal{O}_K$ is a ring

581b:

↙ central object of study in this class (so $\dim_{\mathbb{Q}} K < \infty$ and $K \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}$)

K = number field = finite algebraic extension of $\mathbb{Q}$ $\subseteq \mathbb{C}$ (fix)

|| (prim. elt thm) $\mathbb{Q}(z)$ ← You should know this from a Galois theory class — look up and read a proof!

for some root z of some poly $f(x) \in \mathbb{Q}[x]$.

$\mathcal{O}_K = \{ \alpha \in K : \alpha$ is a root of some monic polynomial in $\mathbb{Z}[x] \}$.

(monic: leading coef 1)

$\mathcal{O}_K$ is called the ring of integers of K.

Defn: Roots of monic polys in $\mathbb{Z}[x]$ are called "algebraic integers".

Theorem 1: $\mathcal{O}_K$ is a ring.

Rmk: It is not obvious that $\mathcal{O}_K$ is closed under addition or multiplication, so we prove it.

* **Fact from algebra**

A subgroup of a finitely generated abelian group is finitely generated. || **NOT obvious**

(we will come back to this later)

$R[\beta] \overset{\text{def}}{=}$ all poly expressions in β with coeff. in R.

(more conceptual criterion)

Lemma: (For $\alpha \in K$) $\alpha \in \mathcal{O}_K \iff \mathbb{Z}[\alpha]$ is a finitely generated $\mathbb{Z}$-module

Proof: ($\Rightarrow$) (easy) Say $f(\alpha) = 0$ with $f \in \mathbb{Z}[x]$ monic. Then $\mathbb{Z}[\alpha]$ gen by $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ where $d = \deg(f)$, since $\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0$.

($\Leftarrow$) Suppose $\mathbb{Z}[\alpha]$ f.g. by $f_1(\alpha), \ldots, f_n(\alpha)$ with $f_i(x) \in \mathbb{Z}[x]$.
Let $d = \max\{\deg(f_i) : i = 1, \ldots, n\} + 1$. Then $\alpha^d \in \mathbb{Z}[\alpha]$ so $\alpha^d = \sum a_i f_i(\alpha)$ some $a_i \in \mathbb{Z}$.
Then $g(\alpha) = 0$ where $g(x) = x^d + \sum a_i f_i(x) \in \mathbb{Z}[x]$ is monic and integral

Proof of Theorem 1:

Suppose $\alpha, \beta \in \mathcal{O}_K$, so α satisfies poly deg. m, β " n.

$\alpha+\beta \in \mathcal{O}_K$? $\alpha\beta \in \mathcal{O}_K$?

$\mathbb{Z}[\alpha,\beta]$ is generated by $\alpha^i \beta^j$ for $0 \le i < m$; $0 \le j < n$.

$\Rightarrow$ is finitely generated ab. group.

$\mathbb{Z}[\alpha\beta]$, $\mathbb{Z}[\alpha+\beta]$ both subgroups of f.g. $\mathbb{Z}[\alpha,\beta]$

$\Longrightarrow$ (by our fact above) $\mathbb{Z}[\alpha\beta]$ and $\mathbb{Z}[\alpha+\beta]$ both f.g.

$\xrightarrow{\text{lemma}}$ $\alpha\beta$, $\alpha+\beta \in \mathcal{O}_K$. $\square$

What about our fact?

Theorem: A subgroup (H) of a f.g. abelian group (G) is f.g.

Sketch of proof:

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{\varphi} & G \\ \cup & & \cup \\ W & \longrightarrow & H \end{array}$$

($\mathbb{Z}^n \twoheadrightarrow G$) since G is f.g.; ($W \twoheadrightarrow H$) just let $W = \varphi^{-1}(H)$

Note: W f.g. $\Rightarrow$ H is, since im of gens of W gen H.

Without loss, assume $G = \mathbb{Z}^n$.

Warm up: $n=1$. Then $H \subseteq \mathbb{Z}$ is an ideal in a PID (uses Euclid), so $H = (\alpha) = \langle \alpha \rangle$ is f.g. (by ≤ 1 elt!)

$n \ge 2$: $H = \langle (x_1,y_1), (x_2,y_2), (x_3,y_3), \ldots \rangle$ ← the gens.

$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \xrightarrow{\text{Hermite form}} \begin{pmatrix} \gcd(x_1,x_2) & a \\ 0 & b \end{pmatrix} \quad |a| < b.$$

(Hermite form: analogue of echelon but over $\mathbb{Z}$)

just keep adding new rows and consider HNF. If new row isn't in span of previous rows, HNF entries get smaller. Can't go on forever! $\blacksquare$