Lecture 3 - Height functions

Algebraic Integers

Recap: So far we have defined height functions

$$H: \mathbb{P}^n(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}$$

$$H: K \longrightarrow \mathbb{R}, \quad K \text{ \# field}$$

Next goal: $H: \mathbb{P}^n(K) \longrightarrow \mathbb{R}$

K # field.

Recall: $H: \mathbb{P}^n(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}$

For eg: $H\left[\frac{6}{11} : \frac{8}{11} : \frac{10}{11}\right]$

$$= H\left[\begin{array}{c} 3 : 4 : 5 \\ \uparrow \nearrow \nearrow \end{array}\right] = 5$$

$\gcd(3, 4, 5) = 1$

Question:

1) What's the analogue of the nice subring $\mathbb{Z} \hookrightarrow \mathbb{Q}$ for a general #field? $\;??? \hookrightarrow K$

2) Is this subring of K a unique factorization domain?

§1 Algebraic Integers

Defn: Let K be a # field.
An algebraic number $\alpha \in K$ is an algebraic integer if the minimal polynomial

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Z}[x]$$

satisfies $a_0 = 1$, i.e. f is a monic integral polynomial.

$\mathcal{O}_K :=$ Collection of all algebraic integers of K.

Examples We will try to compute $K = \mathbb{Q}, \mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt[3]{2})$

$\mathbb{Q}(\zeta_p), \mathbb{Q}(\sqrt{7}, \sqrt{10})$

Ex 1 $K = \mathbb{Q}$

$\frac{a}{b} \in \mathbb{Q}$ $\rightsquigarrow$ Minimal polynomial

$\gcd(a,b) = 1$

$b > 0$

$f(x) = bx - a$

$\frac{a}{b}$ is an alg. integer

$\Leftrightarrow bx - a$ is monic, i.e. $b = 1$

$\Leftrightarrow \frac{a}{b}$ is an integer.

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}.$$

[Ex 2] $K = \mathbb{Q}(\sqrt{d})$ d: squarefree integer.

$\alpha = \sqrt{d} \rightsquigarrow$ Min. poly $x^2 - d = f(x)$

This is a monic integral poly

- $\sqrt{d}$ is an algebraic integer.
- $\frac{\sqrt{d}}{2}$ is NOT an algebraic integ

Minimal polynomial $4x^2 - d$. → NOT monic

Let's try to understand when

Q: $\alpha = \frac{1+\sqrt{d}}{2}$ is an alg. integer?

Recall: If $\alpha_1, \ldots \alpha_n \in \mathbb{C}$ are conjugates of α in $\mathbb{C}$, then the minimal polynomial $f_\alpha(x)$ is a multiple of $g(x) = (x-\alpha_1)\cdots(x-\alpha_n)$, $g(x) \in \mathbb{Q}(x)$

$\mathbb{Q}(x) \xrightarrow{\sigma_1, \sigma_2} \mathbb{C}$

$\frac{\mathbb{Q}(x)}{x^2 - d}$

$\sigma_1(x) = \sqrt{d}$

$\sigma_2(x) = -\sqrt{d}$

$$\alpha_1 = \frac{1+\sqrt{d}}{2}, \quad \alpha_2 = \frac{1-\sqrt{d}}{2}$$

$$g(x) = (x-\alpha_1)(x-\alpha_2)$$

$$= \left(x - \left(\frac{1+\sqrt{d}}{2}\right)\right)\left(x - \left(\frac{1-\sqrt{d}}{2}\right)\right)$$

$$= x^2 - x + \left(\frac{1-d}{4}\right).$$

$f_\alpha(x)$ is a multiple of $g(x)$

$$f_\alpha(x) = \begin{cases} 1 \cdot x^2 - x + \frac{1-d}{4} & \text{when } d \equiv 1 \bmod 4 \\ 2x^2 - 2x + \frac{1-d}{2} & \text{when } d \equiv 3 \bmod 4 \\ 4x^2 - 4x + 1 - d & \text{when } d \equiv 2 \bmod 4 \end{cases}$$

$\frac{1+\sqrt{d}}{2}$ is an algebraic integer if and only if $d \equiv 1 \bmod 4$.

Take away: Can check if any given algebraic # is an algebraic integer.

Fact 1 (Corollary 1.11, ANT)

$\mathcal{O}_K$ is a subring of K.

For eg: $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$, we know $\alpha = \sqrt{7}$, $\beta = \sqrt{10}$ are algebraic integers.

$\Rightarrow$ $\alpha+\beta = \sqrt{7}+\sqrt{10}$

Fact $(\alpha+\beta)^2 = (\sqrt{7}+\sqrt{10})^2$ } are also algebraic integers

The abelian group generated by $\{1, (\sqrt{7}+\sqrt{10}), (\sqrt{7}+\sqrt{10})^2, (\sqrt{7}+\sqrt{10})^3\}$ is contained in $\mathcal{O}_K$.

Fact 2: As an abelian group, $\mathcal{O}_K \cong \mathbb{Z}^n$, where $n = [K:\mathbb{Q}]$

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathbb{Q} \\ \downarrow & & \downarrow \\ \mathbb{Z}^n \cong \mathcal{O}_K & \hookrightarrow & K \cong \mathbb{Q}^n \end{array}$$

Defn: A basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module is an integral basis

---

Ex: We will show that

$d \equiv 2,3 \bmod 4$, $\{1, \sqrt{d}\}$ is an integral basis

$d \equiv 1 \bmod 4$, $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is an integral basis

---

Minkowski's geometry of numbers

View $\mathcal{O}_K$ as an n-dim'l lattice in $\mathbb{R}^n$ -- How?

$K = \dfrac{\mathbb{Q}[x]}{(f(x))}$ f irreducible poly $\in \mathbb{Q}[x]$ degree n.

Factor $f(x)$ over $\mathbb{R}[x]$.

$$f(x) = \underbrace{(x-\alpha_1)\cdots(x-\alpha_r)}_{r \text{ linear factors}}\underbrace{(x^2+\cdots x+\cdots)}_{s \text{ quadratic factors}}$$

Note $r + 2s = n$

The n embeddings $K \hookrightarrow \mathbb{C}$

r real embeddings: $K \hookrightarrow \mathbb{R}$, $x \longmapsto \alpha_i$

s pairs of complex conjugate embeddings: $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$

$\sigma_1, \sigma_2, \dots \sigma_r$ $\quad \tau_i : K \hookrightarrow \mathbb{C}$

$x \mapsto$ root of an irr-quadratic factor of $f(x) \in \mathbb{R}[x]$

$\overline{\tau_i} =$ Complex conjugation $\circ \tau_i$

Defn: The Minkowski embedding

$$i : K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s \simeq \mathbb{R}^n.$$

$$\alpha \mapsto (\sigma_1(\alpha), \dots \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \dots \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha)))$$

Fact 3 (ANT, Propn 3-1)

The image of $\mathcal{O}_K$ is a rank n lattice in $\mathbb{R}^n$.

Example (a) $K = \frac{\mathbb{Q}[X]}{X^2+1} = \mathbb{Q}(i)$

$f(X) = X^2+1$ is irreducible in $\mathbb{R}[X]$

$n = r+2s$ $\quad s=1$

$2 = 0+2\cdot 1$ $\quad \tau_1 : K \hookrightarrow \mathbb{C}$, $X \mapsto i$

The Minkowski embedding:

$$i : K \hookrightarrow \mathbb{C}^1$$

$$X \mapsto (\mathrm{Re}(i), \mathrm{Im}(i)) = (0,1)$$

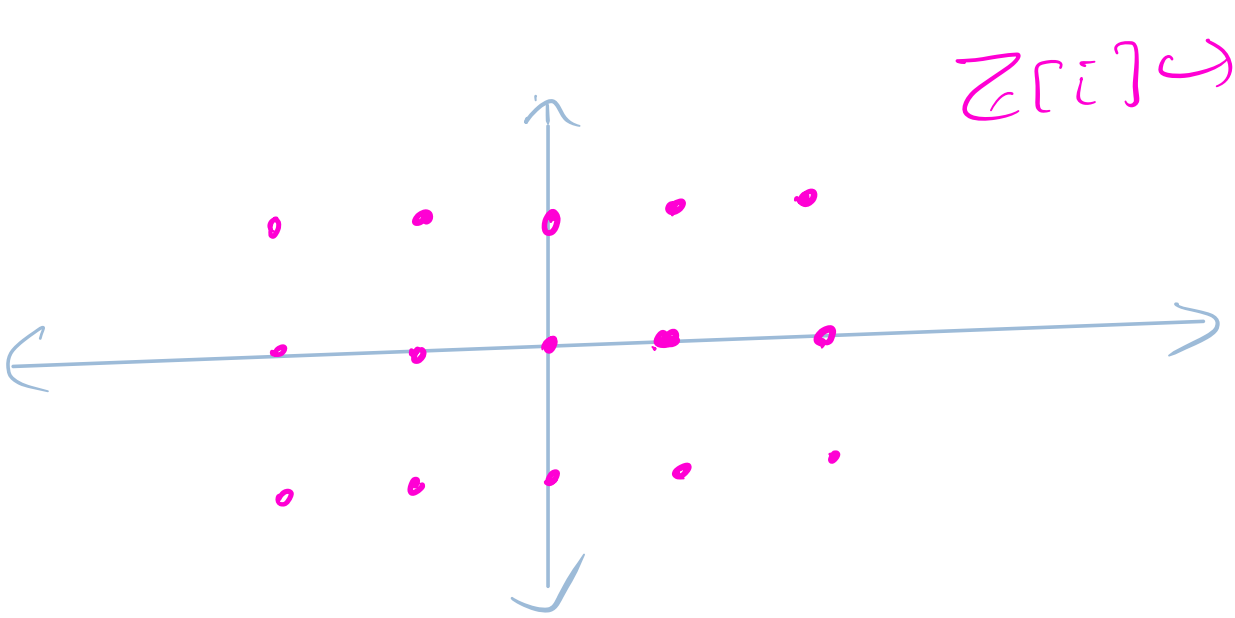
$$1 \mapsto (\mathrm{Re}(1), \mathrm{Im}(1)) = (1,0)$$

We will show $\mathcal{O}_K = \mathbb{Z}[i]$

$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}i \hookrightarrow \mathbb{C} \cong \mathbb{R}^2$

$1 \longmapsto (1,0)$

$i \longmapsto (0,1)$



Eg. b) $\mathbb{Q}(\sqrt{2})$ $n = 2$

$f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}) / \mathbb{R}(x$

$r = 2$ $\quad \sigma_1 : K \hookrightarrow \mathbb{R}$

$s = 0$ $\quad \sigma_2 : K \hookrightarrow \mathbb{R}$

$$K \hookrightarrow \mathbb{R} \times \mathbb{R}$$

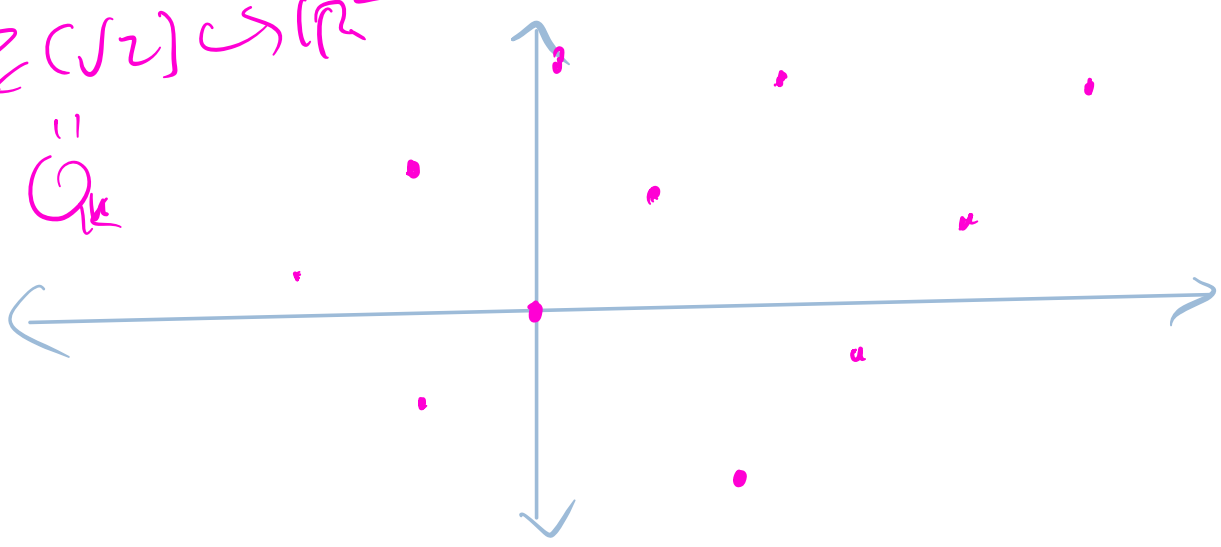
$$\sqrt{2} \longmapsto (\sqrt{2}, -\sqrt{2})$$

$$1 \longmapsto (1, 1)$$

We will show that $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}[\sqrt{2}]$

$\mathbb{Z}[\sqrt{2}] \hookrightarrow \mathbb{R}^2$

$\mathcal{O}_K$



Question: How to find an integral basis for K?

Q Is there a primitive element theorem for $\mathcal{O}_K$, ie, is there an algebraic integer α s.t $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_K$?

"power basis"

A: NO! For $K = \mathbb{Q}(\sqrt{7+\sqrt{10}})$

$\alpha = \sqrt{7}+\sqrt{10}$, $\mathbb{Q}(\alpha) = K$

But $\mathbb{Z}$-span of $1, \alpha, \alpha^2, \alpha^3$

$\mathbb{Z}[\alpha] = \dfrac{\mathbb{Z}[x]}{(f_\alpha(x))}$ has index

divisible by 3 in $\mathcal{O}_K$.

For <u>any</u> algebraic integer α

$\mathbb{Z}[\alpha]$ has index divisible by

3 in $\mathcal{O}_K$.

<u>Proof:</u> Uses "ramification theory"

Defn: If $\mathcal{O}_K$ has a power basis we say K is **monogenic**.

§ Computational tools for $\mathcal{O}_K$

Exercise: For any primitive element $\alpha \in K$, there is some integer $m \in \mathbb{Z}$ (nonzero) s.t. $m\alpha \in \mathcal{O}_K$.

↓ Also a primitive element for K.

$\rightsquigarrow$ Powers of $m\alpha$ generate a rank n free abelian

Subgroup of $\mathcal{O}_K$, in particular $\mathbb{Z}[m\alpha]$ has finite index in $\mathcal{O}_K$.

From now on, assume $K = \frac{\mathbb{Q}[X]}{f(x)}$,

$f(x)$ is a monic integral poly in $\mathbb{Z}[x]$

Root α. alg. integer.

STEP 1 Index bounds for $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$:

TOOL: Discriminant.

Fix embeddings $\sigma_1 \dots \sigma_n : K \hookrightarrow \mathbb{C}$

Defn: Given n alg. integers $\beta_1, \dots, \beta_n$ in $\mathcal{O}_K$,

define the discriminant

$$\Delta(\beta_1, \dots \beta_n) := \det \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_n(\beta_1) \\ \sigma_1(\beta_2) & \cdots & \sigma_n(\beta_2) \\ \vdots & & \sigma_n(\beta_n) \end{pmatrix}^2$$

$n \times n$ matrix

Example $K = \mathbb{Q}(\sqrt{d})$

$$\Delta(1, \sqrt{d}) = \det \begin{pmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{pmatrix}^2$$

$$= [-\sqrt{d} - \sqrt{d}]^2$$

$$= 4d$$

Fact:

(1) The discriminant of an algebraic integer is an integer in $\mathbb{Z}$.

(2) Any two integral bases have the same discriminant.

↙

Defn: Discriminant attached to an integral basis is called Δ_K "discriminant of K".

Fact: Volume of a "fundamental

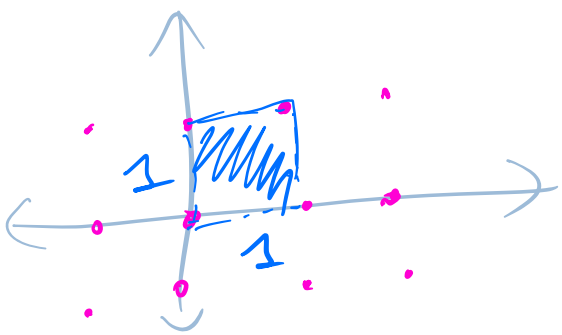
"domain" for the lattice

(image of O_K) $\mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_n$

is $2^{-s}\sqrt{|\Delta(\alpha_1, \ldots, \alpha_n)|}$

For eg. $\mathbb{Z} + \mathbb{Z}i = \mathbb{Z}[i] = \frac{\mathbb{Z}[X]}{X^2+1}$

$-1 \equiv 3 \bmod 4$



Area of fundamental domain = 1

$s = 1, r = 0$

$r + 2s = n = 2$

$\Delta(1, i) = 4(-1) = -4$

$X^2 - (-1)$

$$\text{Area} = 1 = 2^{-1}\sqrt{|-4|}$$

$$= 2^{-1} \cdot 2 = 1$$

Tool 1 If $\beta_1 \dots, \beta_n$ generate an index m subgroup of $\mathcal{O}_K$

$$\underbrace{\Delta(\beta_1 \dots \beta_n)}_{\in \mathbb{Z}} = m^2 \underbrace{\Delta_K}_{\in \mathbb{Z}}$$

In particular, if $\Delta(\beta_1 \dots \beta_n)$ is squarefree, then $m = 1$, i.e.

$$\mathcal{O}_K = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 + \dots + \mathbb{Z}\beta_n.$$

In general, get bounds on index.

Example 2 $f(x) = x^2 - d$

$\Delta(1, \sqrt{d}) = 4d = m^2 \Delta_K$

$\uparrow$ squarefree integer.

$\Rightarrow m = 1$ or 2

$\Rightarrow$ If $d \equiv 1 \bmod 4$, then

$\mathbb{Z}[\sqrt{d}] \subsetneq \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] \subseteq \mathcal{O}_K$

index 2

index $= 1$ or 2

$\Rightarrow \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \mathcal{O}_K$

when $d \equiv 1 \bmod 4$,

i.e $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ is a

power basis for $\mathcal{O}_K$.

Exercise: (a) If $f(x) = x^2+bx+c \in \mathbb{Z}[x]$

root alg. integer α

$\Delta(1, \alpha) = b^2 - 4c$

(b) If $f(x) = x^3 + ax + b \in \mathbb{Z}[x]$

root alg. integer α, then

$$\Delta(1, \alpha, \alpha^2) = -4a^3 - 27b^2.$$

Example 3 $f(x) = x^3 - 2x + 3$

$$\Delta(1, \alpha, \alpha^2) = -4(-2)^3 - 27(3^2)$$

$$= -211 \leftarrow \text{prime!}$$

$$= m^2 \Delta_K$$

$$\Rightarrow m = 1 \Rightarrow \mathbb{Z}[\alpha] = \mathcal{O}_K.$$

Example 4 $f(x) = x^3 - 2$

$$\Delta(1, \alpha, \alpha^2) = -27(-2)^2 = -108$$

$$= -2^2 3^3 = m^2 \Delta_K$$

$\Rightarrow m = 1, 2, 3, 6.$

Examples] $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$

(Exercise): $\Delta(1, \alpha, \ldots \alpha^{p-1}) = p^{p-1}$

p odd prime $= m^2 \underbrace{\Delta_K}_{\in \mathbb{Z}}$

$m = 1, p, p^2, \ldots p^{\frac{p-1}{2}}.$

STEP 2] Ruling out prime divisors of index m.

TOOL 2] [ANT, Propn. 2.9]

If $f(x)$ is Eisenstein $\mathbb{Q}$, root α

$$\left[\text{i.e. } f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, \text{ then } p \mid a_i \text{ & } p^2 \nmid a_n\right],$$

then $p \nmid m$ = Index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$

Examples continued.

$f(x) = x^{p-1} + \cdots + 1$, root ζ_p

Look @ $g(x) = f(x+1)$, min. polynomial of $\beta = \zeta_p - 1$

$g(x)$ is Eisenstein @ p

$\Rightarrow p \nmid$ index of $\mathbb{Z}[\beta]$ in $\mathbb{Z}[\alpha]$

$$\mathbb{Z}[\zeta_p - 1] = \mathbb{Z}[\zeta_p]$$

But we already showed using discriminants, the only possibilities for index m is ~~$1, p, p^2, \ldots, p^{\frac{p-1}{2}}$~~ $\Rightarrow m = 1$

$$\mathbb{Z}[\zeta_p] = \mathcal{O}_{\mathbb{Q}(\zeta_p)}.$$

Ex 4 ctd $f(x) = x^3 - 2$

Eisenstein @ 2

$\Rightarrow 2 \times [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2}]]$

$\downarrow$

One of ~~1~~, ~~2~~, 3, ~~6~~.

$g(x) = f(x+2) \rightarrow$ Eisenstein @ 2 & 3

$3 \times [\mathcal{O}_K : \mathbb{Z}[\sqrt[3]{2} - 2]]$

$\Rightarrow m = 1$

Rules out $m=3$

$\mathcal{O}_{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{Z}[\sqrt[3]{2}]$

STEP 3] Enlarging the subgroup

Tool: If $\alpha_1, \ldots, \alpha_n$ generate an index m subgroup, & $m \neq 1$, then one of the $m^n - 1$ algebraic numbers

$$\left\{ m_1 \frac{\alpha_1}{m} + \cdots + m_n \frac{\alpha_n}{m} : \begin{array}{l} 0 \leq m_i \leq m-1 \\ \text{not all } m_i = 0 \end{array} \right\}$$

is an algebraic integer.

Ex: If $K = \mathbb{Q}(\sqrt{d})$

$d = 2, 3 \bmod 4$

d squarefree

Suppose the index of $\mathbb{Z}[\sqrt{d}]$ in $\mathcal{O}_K$ is 2. Then one of the three alg numbers

$\{\frac{1}{2}, \frac{\sqrt{d}}{2}, \frac{1+\sqrt{d}}{2}\}$ MUST

be an algebraic integer.

This means $m \neq 2$, $m = 3$,

i.e. $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$

when $d \equiv 2, 3 \bmod 4$.

STEP 1 & (STEP 2) & (STEP 3)

$\Rightarrow$ Algorithm for computing $\mathcal{O}_K$.

---

§2 Unique factorization?

$\mathcal{O}_K$ is NOT always a U.F.D. ☹

Example $K = \mathbb{Q}(\sqrt{-5})$

$-5 \equiv 3 \bmod 4$

$\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ NOT a U.F.D.

$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ irreducible, not associate.

Thm (Kummer, ANT 3-27)

Every ideal factors uniquely into a product of prime ideals $\rightsquigarrow$ Enough for defining heights.

$$\mathfrak{p}_1 = (2, 1+\sqrt{-5}) \qquad \mathfrak{p}_3 = (3, 1+\sqrt{-5})$$

$$\mathfrak{p}_2 = (2, 1-\sqrt{-5}) \qquad \mathfrak{p}_4 = (3, 1-\sqrt{-5})$$

$$(6) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4)$$

$$= (2)(3) \qquad = (1+\sqrt{-5})(1-\sqrt{-5})$$