Heights of algebraic numbers

Last time:

We defined $H: \mathbb{Q} \to \mathbb{R}$

$$\frac{a}{b} \longmapsto \max(|a|, |b|)$$

$\gcd(a,b) = 1$

Today's goal: Define $H: \overline{\mathbb{Q}} \to \mathbb{R}$

Collection of all "algebraic numbers"

§1 Intro to algebraic # thy

Defn 1: A number field is a field K is a finite extension of $\mathbb{Q}$.

The degree of a # field K is its dimension a $\mathbb{Q}$-vector space $[K:\mathbb{Q}]$.

Example:

$\{a+bi : a, b \in \mathbb{Q}\}$ is a field. It's a degree 2 # field. $\{1, i\}$ basis as a $\mathbb{Q}$-vector space.

Defn: An algebraic # is an element of a number field.

Observe: If α alg # in a # field K

$\{\alpha, \alpha^2, \alpha^3, \ldots\}$ is an <u>infinite</u> collection of vectors inside a <u>finite</u> dim $\mathbb{Q}$-vector space.

$\Rightarrow$ There is a <u>non-trivial</u> linear dependence relation

$$a_0 \alpha^n + a_1 \alpha^{n-1} + \cdots + a_0 = 0$$

for some $a_i \in \mathbb{Q}$, <u>not all zero</u>

<u>Example</u>: The algebraic # i satisfies $1 \cdot i^2 + 1 = 0$

$$1 \cdot i^3 - 1 \cdot i = 0$$

Basis for $\{a+bi : a, b \in \mathbb{Q}\} = \{1, i\}$

$$\frac{\mathbb{Q}[x]}{(x^2+1)}$$

Defn: The **minimal polynomial** of an alg # α is the polynomial $f(x) \in \mathbb{Z}[x]$ of lowest degree such that - $f(\alpha) = 0$

- $\gcd(a_0, a_1, \ldots, a_n) = 1$

- $a_0 > 0$

$f(x) = a_0 x^n + \ldots + a_n$

Ex: Check that the min. polynomial is irreducible in $\mathbb{Z}[x]$.

Q: How to build a number field K?

A: Pick $f(x) \in \mathbb{Q}[x]$ irreducible, degree n.

$(f(x)) \subset \mathbb{Q}[x]$ maximal ideal.

$$\Rightarrow \frac{\mathbb{Q}[x]}{(f(x))} \text{ is a field!}$$

$$\begin{array}{c} \frac{\mathbb{Q}[x]}{(f(x))} \\ \cup \\ \mathbb{Q} \end{array}$$

CHECK: $K := \frac{\mathbb{Q}[x]}{f(x)}$ is a # field of degree n.

Explicit basis: $\{1, x, x^2, \ldots, x^{n-1}\}$

__Observe:__ $\overline{X} \bmod f$ is a root of the polynomial f in $K = \frac{\mathbb{Q}[x]}{(f(x))}$

Ex: x^2+1 is irreducible

But in $K = \frac{\mathbb{Q}[t]}{t^2+1}$

$$x^2+1 = (x+t)(x-t)$$

__Examples__

Alg #	Min. poly.	# field	degree
a/b $\gcd(a,b)=1$	$bx-a$	$\mathbb{Q}$	1

$b>0$			
i	x^2+1	$\frac{\mathbb{Q}[x]}{(x^2+1)} = \mathbb{Q}(i)$	2
$\sqrt{2}+1$	$(x-1)^2-2$	$\mathbb{Q}(\sqrt{2}) = \frac{\mathbb{Q}[x]}{x^2-2}$	2
$\sqrt[3]{2}$	x^3-2	$\mathbb{Q}(\sqrt[3]{2}) := \frac{\mathbb{Q}[x]}{x^3-2}$	3
ζ_p primitive p^{th} root of unity p prime	$\Phi_p(x) = \frac{x^p-1}{x-1}$ p^{th} cyclotomic polynomial $= x^{p-1} + \dots + 1$	$\frac{\mathbb{Q}[x]}{\Phi_p(x)} = \mathbb{Q}(\zeta_p)$ p^{th} cyclotomic field.	$p-1$

Defn: The collection of all algebraic numbers inside $\mathbb{C}$ is a subfield - denoted $\overline{\mathbb{Q}}$

-- an "algebraic closure" of $\mathbb{Q}$.

Primitive Element Theorem

Every number field K is of the form $\frac{\mathbb{Q}[x]}{f(x)}$ for some irreducible polynomial $f(x) \in \mathbb{Q}[x]$.

A root of f in K is called a **primitive element**.

Ex:

$\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} : a,b,c,d\in\mathbb{Q}\}$

degree 4 number field

$$\simeq \frac{\mathbb{Q}[x]}{(f(x))} \simeq \frac{\mathbb{Q}[x]}{x^4-10x^2+1}$$

minimal polynomial of $\sqrt{2}+\sqrt{3}$

Proof: Omitted.

We want to define $H : \overline{\mathbb{Q}} \to \mathbb{R}$

We have complex absolute value

$$|a+bi| = \sqrt{a^2+b^2}$$

<u>Lemma:</u> An alg # field $K = \dfrac{\mathbb{Q}[x]}{f(x)}$ of degree n

has n <u>distinct</u> embeddings

$\sigma_1, \sigma_2, \ldots, \sigma_n : K \hookrightarrow \mathbb{C}$

<u>Proof:</u> $\mathbb{Q}[x] \to \dfrac{\mathbb{Q}[x]}{f(x)} \hookrightarrow \mathbb{C}$

$$1 \longmapsto 1$$

$$f(x) \longmapsto 0$$

$$x \longmapsto \underbrace{\text{Root of } f \text{ in } \mathbb{C}}$$

n distinct roots of f in $\mathbb{C}$

Ex: $K = \dfrac{\mathbb{Q}[x]}{x^2+1} \hookrightarrow \mathbb{C}$

$$x \overset{\sigma_1}{\longmapsto} i$$

$$x \overset{\sigma_2}{\longmapsto} -i$$

$x^2+1 = (x+i)(x-i)$

§2: Heights

Defn: α algebraic #

$f = a_0 x^n + \cdots + a_n$ minimal polynomial of α

degree n.

$\alpha_i := \sigma_i(\alpha)$ "conjugates of α in $\mathbb{C}$"

Weil/absolute height of α

$$H(\alpha) = \left[|a_0| \prod_{j=1}^{n} \max(1, |\alpha_j|) \right]^{\frac{1}{n}}$$

logarithmic height $h(\alpha) := \log H(\alpha)$.

Example:

1) $\alpha = \dfrac{a}{b} \in K = \mathbb{Q} \xhookrightarrow{\sigma_1} \mathbb{C}$

$\gcd(a,b) = 1,\ b > 0$

Minimal polynomial: $bX - a$

Only conjugate of α is $\frac{a}{b}$.

$$H(\alpha) = \left[|b| \max\left(1, \left|\frac{a}{b}\right|\right)\right]^{\frac{1}{1}}$$

$$= \begin{cases} |b|\, 1 & \text{if } 1 \geq \left|\frac{a}{b}\right| \\ |b| \left|\frac{a}{b}\right| & \text{if } 1 \leq \left|\frac{a}{b}\right| \end{cases}$$

$$= \begin{cases} |b| & \text{if } |b| \geq |a| \\ |a| & \text{if } |b| \leq |a| \end{cases}$$

$$= \max(|a|, |b|)$$

2) $\alpha = i$

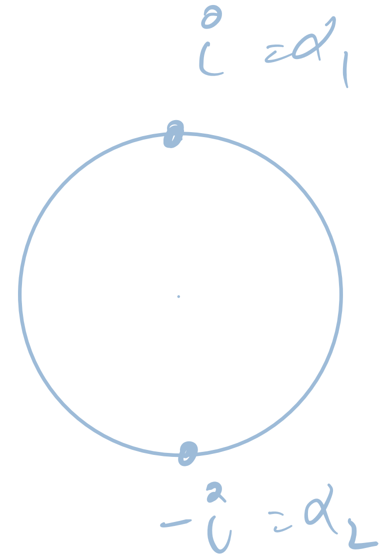
$f(x) = x^2 + 1$ Minimal polynomial

Leading coefficient : 1

$$K = \frac{\mathbb{Q}(x)}{x^2+1} \begin{array}{l} \xrightarrow{\sigma_1} \mathbb{C} \\ \xrightarrow{\sigma_2} \mathbb{C} \end{array}$$

$$x \longmapsto i$$
$$x \longmapsto -i$$

$$\alpha_1 = \sigma_1(\alpha) = i$$
$$\alpha_2 = \sigma_2(\alpha) = -i$$



Unit circle

$$H(\alpha) = \left[1 \cdot \max(1, |i|) \cdot \max(1, |-i|)\right]^{\frac{1}{2}}$$

$$= \left[1 \cdot 1 \cdot 1\right]^{\frac{1}{2}} = 1$$

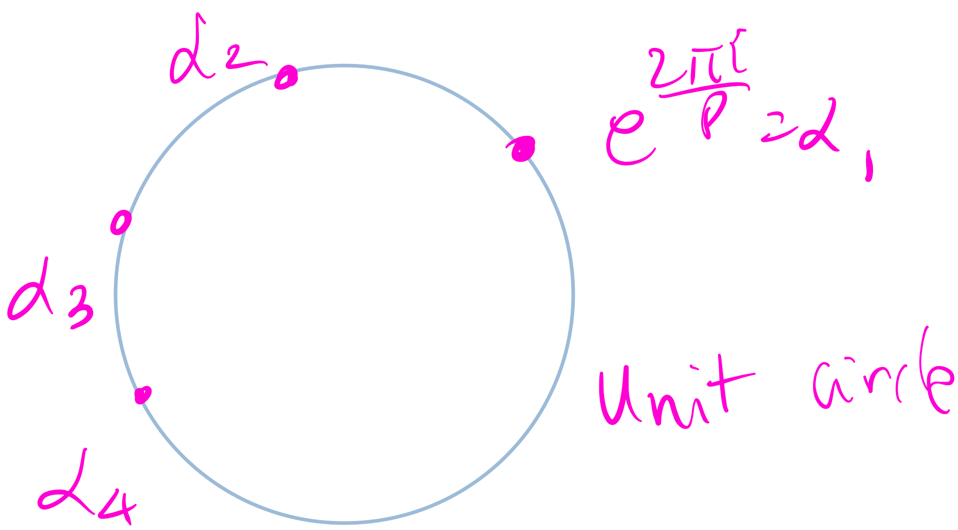
3) $\alpha = \zeta_p$ primitive p^{th} root of unity

Min. poly. $\Phi_p(x) = \dfrac{x^p - 1}{x - 1}$

$= 1 \cdot x^{p-1} + \cdots + 1$

Conjugates of α

$= \{ e^{\frac{2\pi i}{p}}, e^{\frac{2\pi i \cdot 2}{p}}, \ldots \}$



$\rightsquigarrow$) Check: $H(\zeta_p) = (\underbrace{1 \cdot 1 \cdot 1 \cdots 1}_{})^{\frac{1}{p-1}}$

$= 1$

4) $\alpha = \sqrt{2} + 1$

$\beta = (\sqrt{2}+1)^2$

Min. poly: $f(x) = (x-1)^2 - 2$

$= 1 \cdot x^2 + \cdots$

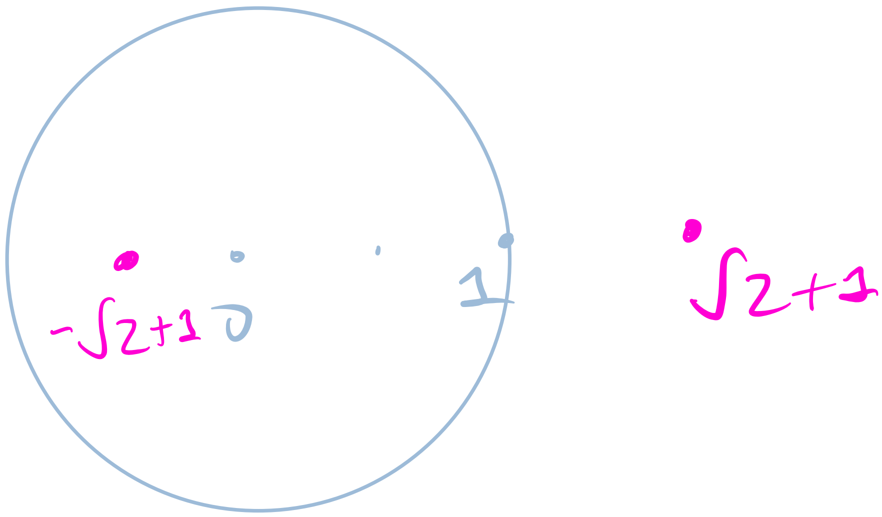
$K = \dfrac{\mathbb{Q}[x]}{x^2-2} \longrightarrow \mathbb{C}$

$x \xmapsto{\sigma_1} \sqrt{2}$

$x \xmapsto{\sigma_2} -\sqrt{2}$

$$\alpha_1 = \sigma_1(\alpha) = \sqrt{2}+1$$

$$\alpha_2 = \sigma_2(\alpha) = -\sqrt{2}+1$$



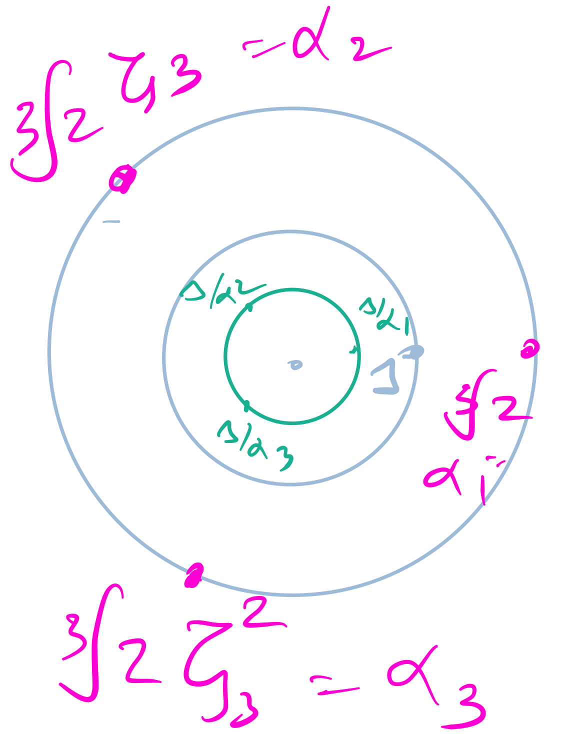
$$H(\alpha) = \left[1 \cdot \max\left(1, |\sqrt{2}+1|\right) \cdot \max\left(1, \underbrace{|-\sqrt{2}+1|}_{= \sqrt{2}-1}\right)\right]^{\frac{1}{2}}$$

$$= \left(1 \cdot (\sqrt{2}+1) \cdot 1\right)^{\frac{1}{2}}$$

$= \sqrt{\sqrt{2} + 1}$, $H(\beta) = \sqrt{2}+1 = H(\alpha)^2$

5) $\alpha = \sqrt[3]{2}$

$f(x) = 1 \cdot x^3 - 2$



$H(\alpha) =$

$\left[1 \cdot |\sqrt[3]{2}| \cdot |\sqrt[3]{2}\,\zeta_3| \cdot |\sqrt[3]{2}\,\zeta_3^2|\right]^{\frac{1}{3}}$

$= \sqrt[3]{2}$

6) $\alpha = \frac{1}{\sqrt[3]{2}}$

Min. poly of $\frac{1}{\sqrt[3]{2}} = - f^{rev}(x)$

$$= 2x^3 - 1$$

$$H(\alpha) = \left[|2| \max\left(1, \left|\frac{1}{\sqrt[3]{2}}\right|\right) \max\left(1, \left|\frac{\zeta_3}{\sqrt[3]{2}}\right|\right) \max\left(1, \left|\frac{\zeta_3^2}{\sqrt[3]{2}}\right|\right) \right]^{\frac{1}{3}}$$

$$= (2 \cdot 1 \cdot 1 \cdot 1)^{\frac{1}{3}} = \sqrt[3]{2}$$

Properties of Heights

(a) If α & α' have same min. poly., then $H(\alpha) = H(\alpha')$.

(b) $H(\alpha) \geq 1$

(c) If $\alpha \neq 0$, $H(\alpha^{-1}) = H(\alpha)^{1}$

Check

$$H(\alpha^{m}) = H(\alpha)^{|m|}$$

(d) Northcott property

There are only finitely many alg #s

of bounded heights &

bounded degree.

Proof sketch

(a) Fix degree n

Fix bound $N \geq 1$

Will show only fin. many

alg #s of degree n, $ht \leq N$

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

min. poly of α

Will show $\boxed{|a_i| \le 2^n N^{n(n+1)}}$

$\rightsquigarrow$ finitely many such f

$\rightsquigarrow$ finitely many such alg #s

$$f(x) = a_0 x^n + \cdots a_i x^{n-i} + a_n$$

$$= a_0 (x - \alpha_1) \cdots (x - \alpha_n) \in \mathbb{C}[x]$$

Check:

$$a_i = a_0 \Big(\sum_{1 \le s_1 < s_2 \cdots < s_i \le n} (-1)^i \alpha_{s_1} \cdots \alpha_{s_i} \Big)$$

$$|a_i| \le |a_0| \left(\sum |(-1)^i \alpha_{s_1} \cdots \alpha_{s_i}| \right)$$

Triangle inequality

$$\le |a_0| \binom{n}{i} \left(\max_{j=1}^{n} |\alpha_j| \right)^i$$

$$\le H(\alpha)^n \underline{\binom{n}{i}} \left[H(\alpha)^n \right]^i$$

$$\le H(\alpha)^{n+n\cdot n} \quad 2^n$$

$$\le N^{n^2+n} \cdot 2^n \quad \boxtimes$$

Kronecker's theorem $\alpha \neq 0$

$H(\alpha) = 1$ if and only if

α is a root of unity.

$\Leftarrow$ ✓

Proof: $\Rightarrow$). Suppose $H(\alpha) = 1$

$m \geq 1$

$$H(\alpha^m) \underset{(c)}{=} H(\alpha)^m = 1$$

- degree $(\alpha^m) \leq n$

$\alpha^m \in K$ # field, deg $\underline{n}$.

$\cdot \{\alpha, \alpha^2, \alpha^3, \ldots \} = S$

bounded height (≤ 1)?

bounded degree ($\leq n$)

$\Rightarrow$ S is finite!

Northcott's

$\Rightarrow \exists\, n > m$

$$\alpha^n = \alpha^m$$

$$\Rightarrow \alpha^{n-m} = 1$$

$\alpha \neq 0$

<u>Next time:</u> Heights on $\mathbb{P}^n(K)$

for K # field.

$\mathbb{Z} \hookrightarrow \mathbb{Q}$ :: ??? $\hookrightarrow K$

Define algebraic integers of K