Heights of algebraic numbers

Padmavathi Srinivasan

Week 2

Last time we defined the height function $H \colon \mathbb{Q} \to \mathbb{R}$, which sends a rational number a/b written in lowest form to $H(a/b) := \max(|a|, |b|)$. The main goal of today's lecture is to define heights for a larger class of numbers called "algebraic numbers". Matt Baker's course notes on Algebraic number theory offers a friendly introduction to the subject, with many explicit Diophantine problems that explain the concrete origins of the subject. We refer the interested reader to his text for supplementing these lecture notes with proofs of various facts that we will simply state in these notes. We will give many examples of all the new ideas, and enough tools to help the reader work through concrete computations on their own.

1 An introduction to Algebraic number theory

Definition 1. A number field is a field K which is a finite extension of $\mathbb{Q}$. The degree $[K : \mathbb{Q}]$ of a number field K is the dimension of K as a $\mathbb{Q}$-vector space. An algebraic number is an element of a number field K.

Example 2. Let i be the complex number such that $i^2 = -1$. The subset $\{a + bi \colon a, b \in \mathbb{Q}\}$ of $\mathbb{C}$ is an example of a number field of degree 2.

Observe that if α is an element of a number field K, then the powers of α are also elements of K and the set

$$\{\alpha, \alpha^2, \alpha^3, \alpha^4, \ldots\}$$

is an *infinite* collection of vectors in the *finite* dimensional $\mathbb{Q}$ vector space K. This means there has to be a nontrivial linear dependence relation between the various powers of α, or in other words, there are elements $a_0, a_1, \ldots, a_n$ in $\mathbb{Q}$, not all zero, such that

$$a_o\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0.$$

We can scale any such relation by the least common multiple of the denominators of the a_i and further assume that the a_i are integers, and such that the $\gcd(a_0, a_1, \ldots, a_n) = 1$.

Definition 3. The minimal polynomial of an algebraic number α is a polynomial $f(x) \in \mathbb{Z}[x]$ of *lowest degree* such that $f(\alpha) = 0$ and such that the leading coefficient of f is positive and the greatest common divisor of all its coefficients is 1. The union of all number fields inside $\mathbb{C}$ is an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Suggested exercises 4. Prove Gauss' lemma: a polynomial $f := a_0x^n + a_1x^{n-1} + \ldots + a_n$ in $\mathbb{Z}[x]$ is irreducible if and only if it is irreducible in $\mathbb{Q}[x]$ and $\gcd(a_0, \ldots, a_n) = 1$.

Suggested exercises 5. Prove that the minimal polynomial of an algebraic number is an irreducible element of $\mathbb{Z}[x]$.

Suggested exercises 6. If α is a nonzero algebraic number with minimal polynomial $f(x) := a_0x^n + a_1x^{n-1} + \ldots + a_n$, then verify that $1/\alpha$ is also an algebraic number with minimal polynomial $f^{\text{rev}}(x) := x^n f(1/x) = a_0 + a_1x + \ldots + a_nx^n$ if $a_n > 0$, and minimal polynomial $-f^{\text{rev}}(x)$ if $a_n < 0$.

An element of $\mathbb{C}$ that is not an algebraic number is called a transcendental number. The collection of all algebraic numbers $\overline{\mathbb{Q}}$ is a *countable* subfield of the *uncountable* field $\mathbb{C}$. This means there are uncountably many transcendental numbers out there, although it is really difficult to prove that any given number is actually transcendental! The most famous examples of transcendental numbers are e and π.[1] Another class of examples of transcendental numbers are the Liouville numbers – these are numbers that are *too well* approximated by rational numbers to be algebraic. For example, Liouville's constant defined to be the number

$$\sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0.110001000000000000000001...$$

is a transcendental number. See your homework to learn more about Liouville numbers!

Back to algebraic numbers – how do we build number fields? One way is to start with an irreducible polynomial f in $\mathbb{Q}[x]$, observe that it generates a maximal ideal of the polynomial ring $\mathbb{Q}[x]$ and take the quotient $K := \mathbb{Q}[x]/(f(x))$ – this is a field! Using the polynomial f to iteratively rewrite the higher powers of x as a linear combination of the monomials $1, x, x^2, \ldots, x^{n-1}$, one can directly check that a basis for K as a $\mathbb{Q}$ vector space is given by the classes of $1, x, x^2, \ldots, x^{n-1}$ modulo the ideal $(f(x))$. In other words, the field K is a number field of degree n. Note that this larger field K now has a root of the previously irreducible polynomial $f(x) \in \mathbb{Q}[x]$ – namely the class of x modulo the ideal (f) is a root of the polynomial f in the field K! Here are some examples of algebraic numbers and their minimal polynomials.

Algebraic number	**Minimal polynomial**	**Number field**	**Degree**
$a/b \in \mathbb{Q}$ $\gcd(a,b) = 1,\ b > 0$	$bx - a$	$\mathbb{Q}$	1
i	$x^2 + 1$	$\mathbb{Q}(i) \cong \mathbb{Q}[x]/(x^2+1)$	2
$\sqrt{2} + 1$	$(x-1)^2 - 2$	$\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2)$	2
$\sqrt[3]{2}$	$x^3 - 2$	$\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}[x]/(x^3-2)$	3
ζ_p, a primitive p-th root of unity for a prime p	$\varphi_p(x) := \frac{x^p-1}{x-1}$ p-th cyclotomic polynomial	$\mathbb{Q}(\zeta_p) \cong \mathbb{Q}[x]/(\varphi_p(x))$ p-th cyclotomic field	$p - 1$

It is natural to ask if every number field arises from the construction above. The answer is yes, and this is known as the primitive element theorem.

[1] See this Numberphile video for Hermite's proof that e is transcendental.

Fact 1. [Bak22, Theorem A.6] *Every number field K is of the form $\mathbb{Q}[x]/(f(x))$ for some irreducible polynomial $f(x) \in \mathbb{Q}[x]$. A root of the polynomial f in K is called a primitive element.*

Example 7. The intersection of all the subfields of $\mathbb{R}$ containing the two quadratic (i.e. degree 2) subfields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ is a number field called a "biquadratic field". This number field can be written as $\mathbb{Q}[x]/(f(x))$ for $f(x) = x^4 - 10x^2 + 1$ – the polynomial $f(x)$ is the minimal polynomial of the algebraic number $\sqrt{2} + \sqrt{3}$.

To define the height of an algebraic number, we need a measure of its size. One way to achieve this is to view our algebraic number as a complex number, and use the usual complex absolute value to measure size. It turns out if an algebraic number α has minimal polynomial of degree n, then there are precisely n different ways to view it as a complex number. More precisely,

Lemma 8. *Every algebraic number field K of degree n admits precisely n distinct embeddings $\sigma_1, \sigma_2, \ldots, \sigma_n \colon K \to \mathbb{C}$.*

Proof. Use Fact 1 to write K as $\mathbb{Q}[x]/(f(x))$. Any embedding $K \hookrightarrow \mathbb{C}$ is completely determined by where x goes, and x must be sent to a root of the polynomial f in $\mathbb{C}$. Since any irreducible polynomial of degree n in $\mathbb{Q}[x]$ has n *distinct* roots in $\mathbb{C}$, the result follows. □

Suggested exercises 9. Prove the claim that any irreducible polynomial of degree n in $\mathbb{Q}[x]$ has n *distinct* roots in $\mathbb{C}$.

Armed with these embeddings, we are now ready to extend our previous definition of height function from $\mathbb{Q}$ to arbitrary algebraic numbers.

2 The height of an algebraic number

Definition 10. Let α be an algebraic number in a number field K of degree n with minimal polynomial $a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the images of α under the n-embeddings of K into $\mathbb{C}$ – these are called the n conjugates of α. Define the Weil/absolute height[2] $H(\alpha)$ of α by

$$H(\alpha) := \left(|a_0| \prod_i \max(1, |\alpha_i|) \right)^{1/n},$$

and the Weil/absolute logarithmic height $h(\alpha)$ of α by

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

[2] The quantity $H(\alpha)^n := |a_0| \prod_i \max(1, |\alpha_i|)$ is called the Mahler measure of the polynomial f. One can more generally talk about the Mahler measure for any polynomial in $\mathbb{C}[x]$ and there is a formula for it as a contour integral on the unit circle in $\mathbb{C}$. See [Wal00][§ 3.3]

Algebraic number α	**Minimal polynomial**	**Conjugates of α**	**Absolute height**
$a/b \in \mathbb{Q}$ $\gcd(a,b)=1,\ b>0$	$bx-a$	a/b	$\lvert b\rvert \max(1, \lvert a/b\rvert)$ $= \max(\lvert a\rvert, \lvert b\rvert)$
i	x^2+1	$i, -i$	1
$\sqrt{2}+1$	$(x-1)^2-2$	$1+\sqrt{2}, 1-\sqrt{2}$	$\sqrt{\sqrt{2}+1}$
$\sqrt[3]{2}$	x^3-2	$\sqrt[3]{2}, \sqrt[3]{2}\zeta_3, \sqrt[3]{2}\zeta_3^2$	$\sqrt[3]{2}$
$1/\sqrt[3]{2}$	$2x^3-1$	$1/\sqrt[3]{2}, 1/\sqrt[3]{2}\zeta_3, 1/\sqrt[3]{2}\zeta_3^2$	$\sqrt[3]{2}$
$\sqrt{2}+\sqrt{3}$	x^4-10x^2+1	$\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3},$ $\sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3}$	$\sqrt{(\sqrt{2}+\sqrt{3})}$
ζ_p, p prime	$\varphi_p(x) := \frac{x^p-1}{x-1}$	$\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1}$	1

Suggested exercises 11. Suppose that the minimal polynomial $f \in \mathbb{Z}[x]$ of α factors as

$$f(x) = a_0x^n + \ldots + a_n = a_0(x-\alpha_1)\cdots(x-\alpha_n)$$

over $\mathbb{C}$. Then prove that for every i between 0 and n, we have

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

We now record some properties of the height function. Part d below, the Northcott property is the most important of them all, and explains why the definition above is a good definition for the height of an algebraic number. When we work with algebraic numbers of arbitrary degree, it is important to upgrade the earlier statement of Northcott property for rational numbers from looking at numbers of bounded height to looking at algebraic numbers of bounded height *and bounded degree*. A reason for this is the collection of all roots of unity is an infinite set of algebraic numbers all of which have height 1. We say that two algebraic numbers α and α' are conjugate if they have the same minimal polynomial.

Proposition 12.

(a) *If α and α' are conjugate, then $H(\alpha) = H(\alpha')$.*

(b) *$H(\alpha) \geq 1$ for every algebraic number α.*

(c) *(canonical height property) For every $m \in \mathbb{Z}$ and nonzero algebraic number α, we have $H(\alpha^m) = H(\alpha)^{|m|}$.*

(d) *(Northcott property) There are only finitely many algebraic numbers of bounded height and bounded degree.*

Proof. Part a is clear from the definition of H. Part b is immediate since the height is defined to be a root of a product of numbers, each of which is greater than or equal to 1.

Factor the minimal polynomial $f \in \mathbb{Z}[x]$ of α as

$$f(x) = a_0x^n + \ldots + a_n = a_0(x-\alpha_1)\cdots(x-\alpha_n),$$

where $\alpha_1, \alpha_2, \dots, \alpha_n$ are the conjugates of α in $\mathbb{C}$. By exercise 11, we have $a_n/a_0 = \prod_i \alpha_i$. Combining this with the definition of the height function and exercise 6, shows $H(\alpha^{-1}) = H(\alpha)$. (Prove this!) So it suffices to prove part c when $m \geq 1$. Fix $m \geq 1$. Consider the polynomial g defined by

$$g(x) := a_0^m(x - \alpha_1^m) \cdots (x - \alpha_n^m).$$

One can show $g(x) \in \mathbb{Z}[x]$ and that it is a power of the minimal polynomial of α^m. Combining this with the definition of height function once again, we get that $H(\alpha^m) = H(\alpha)^m$. This proves part c.

Fix a degree $n \geq 1$ and a bound $N \geq 1$. We will show that there are finitely many degree n algebraic numbers of height at most N. Let $f(x) := a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$ be the minimal polynomial of such a number. We will show that there are only finitely many possibilities for f by proving an upper bound on $|a_i|$ depending only on n and N. Exercise 11 gives us the bound

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

Combining this inequality with the bounds

$$|a_0| \leq H(\alpha)^n, \qquad \text{and} \qquad \max_{j=1}^{n} |\alpha_j| \leq H(\alpha)^n,$$

we get

$$|a_i| \leq \binom{n}{i} H(\alpha)^{n(i+1)} \leq 2^n N^{n(n+1)}. \qquad \square$$

In fact, the proof above suggests another equally good definition of a height of an algebraic number α. View the coefficients of the minimal polynomial $a_0x^n + \ldots + a_n$ as giving a point $[a_0 : a_1 : \cdots : a_n]$ in $\mathbb{P}^n(\mathbb{Q})$. Using the definition of heights of points in $\mathbb{P}^n(\mathbb{Q})$ from last time, we can define

$$H_2(\alpha) := H([a_0 : a_1 : \cdots : a_n]).$$

Note that the Northcott property for the height function H_2 (the statement in Lemma 12 d) is true, and actually even easier to prove than the statement for H! Our proof above implicitly compares the two height functions H and H_2.

Suggested exercises 13. There is also a third definition of a height function H_3, in terms of the *house* ⌂ and *denominator* den of an algebraic number α (See also [Wal00][§ 3.4]):

$$\begin{aligned} \text{⌂}(\alpha) &:= \overline{|\alpha|} = \max_{j=1}^{n} |\alpha_j| \\ \operatorname{den}(\alpha) &:= \min\{D \in \mathbb{Z} :\ D > 0,\ D\alpha \text{ has a monic minimal polynomial in } \mathbb{Z}[x]\} \\ H_3(\alpha) &:= \operatorname{den}(\alpha) \max(1, \text{⌂}(\alpha)). \end{aligned}$$

Prove that $\operatorname{den}(\alpha)$ is well-defined and divides the leading coefficient a_0 of the minimal polynomial $a_0x^n + \ldots + a_n$ of α. Prove explicit inequalities relating $H(\alpha), H_2(\alpha)$ and $H_3(\alpha)$.

Theorem 14 (Kronecker)**.** *Let α be a nonzero algebraic number. Then* $H(\alpha) = 1$ (*equivalently* $h(\alpha) = 0$) *if and only if α is a root of unity.*

Proof. If α is a root of unity, then its minimal polynomial has leading coefficient 1 and all the conjugates of α lie on the unit circle. It follows that $H(\alpha) = 1$.

Suppose $H(\alpha) = 1$. Then $H(\alpha^n) = H(\alpha)^n = 1$ for all $n \geq 1$ by Lemma 12 c. If α belongs to a number field K, so do all powers of α, and it follows that all powers of α have degree bounded by degree of K. Therefore, the collection of algebraic numbers

$$S := \{\alpha, \alpha^2, \alpha^3, \alpha^4, \dots\}$$

has bounded height (by 1) and bounded degree (by $[K : \mathbb{Q}]$). By the Northcott property (Lemma 12 d), it follows that S is finite. This means there are two integers $n > m$ such that $\alpha^n = \alpha^m$. Since $\alpha \neq 0$ this is equivalent to $\alpha^{n-m} = 1$. □

Remark 15. The roots of unity are exactly the collection of all torsion points for multiplication in the group $\mathbb{C}^*$. Kronecker's theorem admits a generalization to elliptic curves. We will prove that the set of points on an elliptic curve of logarithmic canonical height 0 are precisely the torsion points. The argument is identical, once we know that the analogous canonical height property $\hat{h}_E(mP) = m^2\hat{h}_E(P)$ and the Northcott property holds for canonical heights for points on elliptic curves.

It is an open problem (called "Lehmer's problem") whether $H(\alpha)^n$ can get arbitrarily close to 1 for α an algebraic number of degree n that is not a root of unity. We can immediately see using our earlier table of examples with $\alpha = 2^{1/n}$ that $H(\alpha)^n = 2$. (This example also explains why it is $H(\alpha)^n$ that appears in the formulation of this problem, and not $H(\alpha)$ itself, since $2^{1/n} \to 1$ as $n \to \infty$.) The current record for the smallest value for $H(\alpha)^n$ found by Lehmer in 1933 is

$$H(\alpha)^{10} = 1.176280818\dots$$

and this was for any root of the polynomial (called Lehmer's polynomial)

$$L(z) = z^{10} + z^9 - z^7 - z^6 - z^5 - z^4 - z^3 + z + 1.$$

In 1965, Schinzel and Zassenhaus proposed a closely related conjecture to Lehmer's problem. Recall the definitions of house and denominator of an algebraic number from exercise 13. Let α be a nonzero algebraic number of degree $n \geq 2$ and denominator 1 that is not a root of unity. The Schinzel-Zassenhaus conjecture predicts that there is an absolute constant c such that

$$\text{⌂}(\alpha) = \overline{|\alpha|} > 1 + \frac{c}{n}$$

for every number α as above. This conjecture was very recently proved by Dimitrov in 2019, who showed that for any such α

$$\text{⌂}(\alpha) = \overline{|\alpha|} \geq 2^{1/4n} \sim 1 + \frac{\log(2)}{4n}.$$

3 Revisiting heights on projective spaces

Recall that we defined the height of a point $P = [x_0 : x_1 : \ldots : x_n]$ of $\mathbb{P}^n(\mathbb{Q})$ by first saying that every point of $\mathbb{P}^n(\mathbb{Q})$ has a representative where the x_i are in $\mathbb{Z}$ and $\gcd(x_0, x_1, \ldots, x_n) = 1$, and defined $H(P) = \max(|x_0|, |x_1|, \ldots, |x_n|)$. To extend this definition to points of $\mathbb{P}^n(K)$ for a number field K, we first need an analogue of the integers inside a general number K. Defining the ring of algebraic integers $\mathcal{O}_K$ of K will be the starting point of our next lecture.

References

[Bak22] Matt Baker, *Algebraic Number Theory Course Notes* (2022). ↑3

[Wal00] Michel Waldschmidt, *Diophantine approximation on linear algebraic groups*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 326, Springer-Verlag, Berlin, 2000. Transcendence properties of the exponential function in several variables. MR1756786 ↑3, 5