# PROBLEM SESSION ON HEIGHTS

TA: JUANITA DUQUE-ROSERO

## About This Problem Set

The goal of these problems is to familiarize you with the concepts around Diophantine heights. We will study heights in projective space and elliptic curves. In each section, you will find a variety of problems; some of them get you to work with basic concepts with and some are meant to challenge you. The most advanced problems are marked with the symbol ✻. Please note that the list of problems is long, so I do not expect you to solve every single question during the AWS. **Please be kind to yourself and take things at your own pace!**

Most of these questions appeared in the problem sets for the Preliminary Arizona Winter School (PAWS) on Diophantine heights. The problems accompanied Padmavathi Srinivasan's lectures. You can find videos and notes from those lectures at the PAWS website. The problems for PAWS were compiled by Niven Achenjang, Juanita Duque-Rosero, Carlos Rivera, Padmavathi Srinivasan, and Marley Young.

## 1. Preliminaries: Projective Space, Morphisms, and Rational Maps

We make basic definitions in algebraic geometry related to projective varieties. If you are interested, a good place to learn more about these concepts is [5, Chapter 2].

**Definition 1.1.** The **projective $N$-space** over a field $K$, denoted by $\mathbb{P}^N$ or $\mathbb{P}^N(K)$, is the set of all $(N+1)$-tuples

$$(x_0, \dots, x_N) \in K^{N+1} \setminus \{(0, 0, \dots, 0)\}$$

modulo the equivalence relation

$$(x_0, \dots, x_N) \sim (y_0, \dots, y_N)$$

if there exists a $\lambda \in K \setminus \{0\}$ such that $x_i = \lambda y_i$ for all $i$. An equivalence class

$$\left\{(\lambda x_0, \dots, \lambda x_N) : \lambda \in K \setminus \{0\}\right\}$$

is denoted by $[x_0, \dots, x_N]$, and the $x_i$ are called *homogeneous coordinates* for the corresponding point in $\mathbb{P}^N$.

**Question 1.** Let's explore $\mathbb{P}^1(\mathbb{R})$. This is a space obtained from taking equivalence classes of elements in $\mathbb{R}^2$. Pick some points in $\mathbb{R}^2$ and draw all other elements that are equivalent to them. How does each equivalent class look like geometrically? Can you make sense of the "shape" of $\mathbb{P}^1(\mathbb{R})$?

**Question 2.** Show that for any $[x_0, \dots, x_N] \in \mathbb{P}^N(\mathbb{Q})$ we can choose homogeneous coordinates so $x_i \in \mathbb{Z}$ for all $i$ and $\gcd(x_0, \dots, x_N) = 1$.

**Definition 1.2.** A polynomial $f \in K[X_0, \dots, X_N]$ is *homogeneous of degree $d$* if

$$f(\lambda X_0, \dots, \lambda X_N) = \lambda^d f(X_0, \dots, X_N) \quad \text{for all } \lambda \in K.$$

**Question 3.** Prove that a polynomial is homogeneous of degree $d$ if and only if each of its monomials has degree $d$.

**Definition 1.3.** A *rational map of degree d* between projective spaces is a map

$$\begin{array}{cccc} \phi: & \mathbb{P}^N & \dashrightarrow & \mathbb{P}^M \\ & P & \mapsto & [f_0(P), \ldots, f_M(P)], \end{array}$$

where $f_0, \ldots, f_M \in K[X_0, \ldots, X_N]$ are homogeneous polynomials of degree $d$ with no common factors. The rational map $\phi$ is *defined at P* if at least one of the values $f_0(P), \ldots, f_M(P)$ is non-zero. The rational map $\phi$ is called a *morphism* if it is defined at every point of $\mathbb{P}^N(K)$. If the polynomials $f_0, \ldots, f_N$ have coefficients in a subfield $L$ of $K$, we say that $\phi$ is *defined over L*.

**Definition 1.4.** Let $f \in \bar{\mathbb{Q}}[X_0, \ldots, X_N]$ be a homogeneous polynomial. Then, we can define the *projective subvariety*

$$V(F) := \{P \in \mathbb{P}^N : f(P) = 0\}$$

cut out by $F$ (see Question 3). We sometimes write $C : F = G$ as shorthand to denote $C = V(F - G)$, e.g. $E : Y^2Z = X^3 - 432Z^3$ would mean $E := V(Y^2Z - (X^3 + 432Z^3))$.

**Question 4.** Let $f(T_0, T_1, \ldots, T_n)$ be a homogeneous polynomial. Given a point $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$, note that the expression $f(P) = f(x_0, \ldots, x_n)$ is not well-defined; that is, its value can depend on a choice of representative for $P$. Despite this, show that the if $f(x_0, \ldots, x_n) = 0$, then $f(y_0, \ldots, y_n) = 0$ for any other choice of $y_0, \ldots, y_n \in \bar{\mathbb{Q}}$ so that $P = [y_0, \ldots, y_n]$. Because of this, our notation

$$V(f) := \{P \in \mathbb{P}^n : f(P) = 0\} \subset \mathbb{P}^n,$$

from Definition 1 is justified.

Earlier, we defined rational maps and morphisms between projective spaces. One can similarly define rational maps and morphisms between projective varieties. The general definition is a bit involved, but for the purposes of this problem set, examples of the following form suffice.

**Definition 1.5.** Let $f(X_0, \ldots, X_N), g(X_0, \ldots, X_M)$ be homogeneous polynomials cutting out projective subvarieties $X = V(f) \subset \mathbb{P}^N$ and $Y = V(g) \subset \mathbb{P}^M$. Let $\phi_0, \ldots, \phi_M \in \bar{\mathbb{Q}}[T_0, \ldots, T_N]$ be homogeneous polynomials all of the same degree $d$, so they define a rational map

$$\phi := (\phi_0, \ldots, \phi_M) : \mathbb{P}^N \dashrightarrow \mathbb{P}^M.$$

If $\phi(P) \in Y(\bar{\mathbb{Q}})$ for all $P \in X(\bar{\mathbb{Q}})$ at which $\phi$ is defined, then the restriction $\phi|_X : X \dashrightarrow Y$ gives an example of a *rational function from X to Y*. This $\phi$ will be a *morphism from X to Y* if $\phi(P)$ is defined for all $P \in X(\bar{\mathbb{Q}})$ (even if $\phi(P)$ is not defined for all $P \in \mathbb{P}^N(\bar{\mathbb{Q}})$). If there exists a morphism $\psi : Y \to X$ so that $\phi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \phi = \mathrm{id}_X$, then we say that $\phi$ (and so also $\psi$) is an *isomorphism*.

In general, one can define rational functions $X \dashrightarrow Y$ which do not necessarily extend to rational functions $\mathbb{P}^N \dashrightarrow \mathbb{P}^M$, but we will not see those in this problem set.

**Question 5.** Show that the rational map $\phi : \mathbb{P}^2 \to \mathbb{P}^2$ given by

$$\phi([X, Y, Z]) = [X^2 - Y^2, XY - Z^2, Y^2 - Z^2]$$

is not a morphism.

**Question 6.** Show that the set

$$\left\{(a,b,c)\in\mathbb{Z}^3 \mid \gcd(a,b,c)=1, a^2+b^2=c^2, \text{ and } c\neq 0\right\}$$

of primitive Pythagorean triples is in bijection with the set

$$P := \left\{(u,v)\in\mathbb{Q}^2 : u^2+v^2=1\right\}$$

of rational points on the unit circle. Further show that there is a map

$$\begin{array}{rccc} f: & \mathbb{Q} & \longrightarrow & P \\ & t & \longmapsto & \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right) \end{array}$$

which is injective with image $P \setminus \{(-1,0)\}$.

**Question 7.** This question gives a projective interpretation of Question 6. We use the notation of that question.

(a) Convince yourself that we can view $\mathbb{Q}$ as a subset of $\mathbb{P}^1(\mathbb{Q})$ via $t \mapsto [t,1]$. Similarly, show that we can view $P$ as a subset of $\mathbb{P}^2(\mathbb{Q})$ via $(u,v)\mapsto[u,v,1]$ and show that this in fact gives a bijection $P \cong C(\mathbb{Q})$ onto the $\mathbb{Q}$-points of $C := V(X^2+Y^2=Z^2)$.

(b) Show that the map $f : \mathbb{Q}\to P$ extends to the rational map $\phi : \mathbb{P}^1 \to C$ given by

$$\phi([X,Y]) = [Y^2-X^2, 2XY, Y^2+X^2].$$

By '$\phi$ extends $f$' we mean that if $t\in\mathbb{Q}$, and $f(t)=(u,v)$, then $\phi([t,1])=[u,v,1]$.

(c) Show that $\phi$ is in fact an isomorphism. Hence, primitive Pythagorean triples are parameterized by $\mathbb{P}^1(\mathbb{Q})$ without caveats (the missing point $(-1,0)\in P$ from before now corresponds to the point $\infty := [1,0]\in\mathbb{P}^1(\mathbb{Q})$).

## 2. Preliminaries: Elliptic Curves

We now discuss elliptic curves. This topic is huge, and we are only presenting some basic properties of elliptic curves. For mere, see [2].

**Definition 2.1** ([2, p.42,§ III.I])**.** An **elliptic curve** $E$ over $\mathbb{Q}$ is a curve defined by an equation of the form

$$y^2 = x^3 + Ax + B,$$

where $A$ and $B$ are in $\mathbb{Q}$, and such that the number $\Delta := -16(4A^3+27B^2)$ is nonzero.

The equation $y^2 = x^3+Ax+B$ is called a **Weierstrass equation** for the elliptic curve $E$. The associated number $\Delta := -16(4A^3+27B^2)$ is called the **discriminant** of the Weierstrass equation. The discriminant is the analogue of the quantity $b^2-4ac$ for the quadratic polynomial $ax^2+bx+c$ – the quantity $-16(4A^3+27B^2)$ is zero precisely when the cubic $x^3+Ax+B$ has repeated roots. There is a wonderful online database of these curves in the LMFDB (L-functions and modular forms database) that I strongly encourage you all to explore as you familiarize yourself with these objects! The examples we consider here have links to their LMFDB pages.

**Question 8.** Consider the elliptic curve $E$ : $y^2 = x^3 - x$. Show that there is an isomorphism (of projective subvarieties) $\phi : E \to E$ given by $\phi(x,y) = (-x, iy)$.

**Question 9.** Say $\mathbb{P}^2$ is given homogeneous coordinates $[X : Y : Z]$. Consider the elliptic curves

$$V := V(X^3 + Y^3 = Z^3) \text{ and } W := V(Y^2 Z = X^3 - 432Z^3).$$

Show that $\phi = [12Z, 36(X - Y), X + Y] : V \to W$ is a morphism. For something a bit harder, show that $\phi$ is in fact an isomorphism.

The key property of elliptic curves is that, given points $P$ and $Q$ on an elliptic curve, then we can find another point on the elliptic curve $P + Q$. This is done in a very explicit way. You can look at [2, § III.2] for details or just ask me.

**Question 10.** Verify that $(1, 1)$ is a point of order 4 on the elliptic curve $E_1 : \; y^2 = x^3 - x^2 + x$, and that $(0, 2)$ is a point of order 3 on the elliptic curve $E_2 : \; y^2 = x^3 + 4$.

**Question 11.** Verify that the doubling map for the elliptic curve $y^2 = x^3 + 1$ is given by

$$P = (x, y) \mapsto 2P = \left( \frac{x^4 - 8x}{4x^3 + 4}, \frac{2x^6 + 40x^3}{8y^3} \right).$$

Note that we cannot plug in the point $(-1, 0)$ on the curve into the formula above – can you explain why?

The map $f(x) = \frac{x^4-8x}{4x^3+4}$ is an example of a *Lattès map*. A Lattès map is a rational function (i.e. a ratio of two polynomials) that describes the $x$-coordinate of the point $2P$ in terms of the $x$-coordinate of $P$ for some elliptic curve.

**Question 12.** This question deals with complex multiplication (CM) in elliptic curves, which will come up later in this set. Let $E$ be an elliptic curve over $\mathbb{C}$.

(a) Show that $\mathbb{Z} \subseteq \mathrm{End}(E)$, where $\mathrm{End}(E)$ denotes the ring of morphisms $E \to E$ that are also group homomorphisms.
(b) We say that $E$ has *complex multiplication* if $\mathbb{Z} \subsetneq \mathrm{End}(E)$. This is, $E$ possesses "additional symmetries". Show that the curve $E : \; y^2 = x^3 - x$ has complex multiplication over $\mathbb{C}$.
(c) Find a curve $E$ without complex multiplication. *Hint:* use the LMFDB!

**✻ Question 13.** Let $E : y^2 = x^3 + Ax + B$ and $E' : y^2 = x^3 + A'x + B'$ be two elliptic curves. We let the same letters $E, E'$ denote also the corresponding projective varieties

$$E : Y^2 Z = X^3 + AXZ^2 + BZ^3 \text{ and } E' : Y^2 Z = X^3 + A'XZ^2 + B'Z^3.$$

Let $\phi : E \to E'$ be an isomorphism such that $\phi([0 : 1 : 0]) = [0 : 1 : 0]$. Show that $\phi$ must be of the form

$$\phi([X, Y, Z]) = [\lambda^2 X : \lambda^3 Y : Z]$$

for some $\lambda \in \bar{\mathbb{Q}}$. Given that $\phi$ is of this form, write $A', B'$ in terms of $A, B, \lambda$.

**Question 14.** Try this exercise if you have access to one of the computing softwares Magma/Pari GP/SAGE. Open up the webpage of your favourite elliptic curve from this list of curves from the LMFDB of elliptic curves $E$ over $\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z}$. Using the "Show command" option on the top right of the webpage you opened up, learn how to enter the elliptic curve and a generator $P$ for the Mordell-Weil group into your chosen platform. Also compute the points $2P, 4P, 8P, 16P$ etc. using your chosen platform – what do you observe about the heights of the $x$-coordinates of these points? Repeat this experiment with a different elliptic curve from the list.

## 3. Heights in $\mathbb{Q}$

As a warm-up, we first define heights of rational numbers.

**Definition 3.1.** Let $x = p/q$ be a rational number written in lowest terms ($\gcd(p, q) = 1$). The height of $x$ is defined to be

$$H(x) = H(p/q) = \max\{|p|, |q|\}.$$

**Question 15.** Let $x_1, \dots, x_n \in \mathbb{Q}$. Prove the following basic properties of the height for rational numbers:

(a) $H(x_1 \cdots x_n) \leq H(x_1) \cdots H(x_n)$;
(b) $H(x_1 + \cdots + x_n) \leq nH(x_1) \cdots H(x_n)$.

One of the most important properties that we want to get when we define any height is the *Northcott property*.

**Definition 3.2.** The **Northcott property** for a height function $H : X \to K$ states that for any $N \geq 1$ there are only finitely many points of $X$ of bounded height.

**Question 16.** Show that the Northcott property holds for the height function of a rational number presented in Definition 3.1.

## 4. Heights in $\mathbb{P}^N(\mathbb{Q})$

We define the height in the case of $\mathbb{Q}$-*rational points* in $\mathbb{P}^N$ i.e. the set

$$\mathbb{P}^N(\mathbb{Q}) = \{[x_0, \dots, x_N] \in \mathbb{P}^N \mid x_i \in \mathbb{Q} \text{ for all } i\}.$$

**Definition 4.1.** Given a point $P = [x_0, \dots, x_N] \in \mathbb{P}^N(\mathbb{Q})$, we may assume that the homogeneous coordinates satisfy

$$x_0, \dots, x_N \in \mathbb{Z} \quad \text{and} \quad \gcd(x_0, \dots, x_N) = 1 \tag{4.2}$$

(see Question 2). Having done this, we define the **height** of $P$ to be

$$H(P) = \max\{|x_0|, \dots, |x_N|\},$$

and the **logarithmic height** of $P$ to be $h(P) = \log H(P)$.

**Question 17.** Prove the Northcott property for the height function in projective space. This is, show that for any $N \geq 1$ there are only finitely many points of $\mathbb{P}^n(\mathbb{Q})$ of bounded height.

**Question 18.** Let

$$\nu(B) = \#\{P \in \mathbb{P}^N(\mathbb{Q}) : H(P) \leq B\}. \tag{4.3}$$

Find positive constants $c_1$ and $c_2$ such that

$$c_1 B^{N+1} \leq \nu(B) \leq c_2 B^{N+1}$$

for all $B \geq 1$.

**✻ Question 19.** Let $\phi : \mathbb{P}^N \to \mathbb{P}^M$ be a rational map of degree $d$, defined over $\mathbb{Q}$. Prove that there exists a constant $C > 0$, depending only on $\phi$, such that

$$h(\phi(P)) \leq d\,h(P) + C$$

for all $P \in \mathbb{P}^N(\mathbb{Q})$ at which $\phi$ is defined.

In fact, if $\phi$ is a morphism, it is also possible to prove a lower bound of the form $h(\phi(P)) \geq dh(P) - C$, but we will not yet do so. For now, consider the following example. View the map $\phi$ from Question 7 (b) as a morphism $\phi\colon \mathbb{P}^1 \to \mathbb{P}^2$ of degree 2, and compute explicit constants $C_1, C_2 > 0$ such that

$$2h(P) - C_1 \leq h(\phi(P)) \leq 2h(P) + C_2$$

for all $P \in \mathbb{P}^1(\mathbb{Q})$.

**Question 20.** Consider the hyperplane

$$X := V(a_0x_0 + \ldots + a_{N+1}x_{N+1}) \subset \mathbb{P}^{N+1}$$

where $a_0, \ldots, a_{N+1} \in \mathbb{Q}$ are not all zero. Show that, for each integer $M \geq 1$,

$$\{P \in X(\mathbb{Q}) : H(P) \leq M\} \leq C(2M+1)^{(N+1)}$$

for some constant $C > 0$. *Hint:* Construct an isomorphism between $X$ and $\mathbb{P}^N$ and use Question 19.

**Question 21.** For $P = [x_0, \ldots, x_N] \in \mathbb{P}^N$ and $Q = [y_0, \ldots, y_M] \in \mathbb{P}^M$, define

$$P \star Q = [x_0y_0, x_0y_1, \ldots, x_iy_j, \ldots, x_Ny_M] \in \mathbb{P}^{MN+M+N}.$$

The map $(P, Q) \mapsto P \star Q$ is called the *Segre embedding* of $\mathbb{P}^N \times \mathbb{P}^M$ into $\mathbb{P}^{MN+M+N}$.

Prove that

$$H(P \star Q) = H(P)H(Q)$$

for any $P \in \mathbb{P}^N(\mathbb{Q})$ and $Q \in \mathbb{P}^M(\mathbb{Q})$.

**Question 22.** Let $M = \binom{N+d}{N} - 1$ and let $f_0, \ldots, f_M$ be the distinct monomials of degree $d$ in the $N+1$ variables $X_0, \ldots, X_N$. For any point $P = [x_0, \ldots, x_N] \in \mathbb{P}^N$, let

$$P^{(d)} = [f_0(P), \ldots, f_M(P)] \in \mathbb{P}^M.$$

The map $P \mapsto P^{(d)}$ is called the *$d$-uple embedding* of $\mathbb{P}^N$ into $\mathbb{P}^M$.

Prove that

$$H\left(P^{(d)}\right) = H(P)^d = H\left([x_0^d, \ldots, x_N^d]\right)$$

for all $P = [x_0, \ldots, x_N] \in \mathbb{P}^N(\mathbb{Q})$.

✻ **Question 23.** When $N = 1$, prove that

$$\lim_{B\to\infty} \frac{\nu(B)}{B^2} = \frac{12}{\pi^2}.$$

where $\nu$ is defined as in (4.3). More generally, prove that the limit

$$C(N) := \lim_{B\to\infty} \nu(B)/B^{N+1}$$

exists, and express it in terms of a value of the Riemann $\zeta$-function. Can you prove the more precise asymptotic behaviour

$$\nu(B) = \begin{cases} \frac{12}{\pi^2}B^2 + O(B\log B), & \text{if } N = 1; \\ C(N)B^{N+1} + O(B^N) & \text{if } N > 1, \end{cases}$$

as $B \to \infty$?

## 5. Preliminaries: Number Fields

Our goal will be to recall some of the theory of number fields, which we will need to define more general heights. This section might have some missing information, so you can look at [4, Chapter 13] or [3] for details.

**Definition 5.1.** 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 $K$.

**Question 24.** Let $i$ be the complex number such that $i^2 = -1$. Show that the subset $\{a+bi : a, b \in \mathbb{Q}\}$ of $\mathbb{C}$ is a number field of degree 2.

**Definition 5.2.** The **minimal polynomial** of an algebraic number $\alpha$ 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 algebraic numbers inside $\mathbb{C}$ is an **algebraic closure** $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

**Question 25.** Prove Gauss's 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 $\gcd(a_0, \ldots, a_n) = 1$.

**Question 26.** Prove that the minimal polynomial of an algebraic number is an irreducible element of $\mathbb{Z}[x]$.

**Question 27.** Suppose that the minimal polynomial $f \in \mathbb{Z}[x]$ of $\alpha$ 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

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

**Theorem 5.3** ([3, 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****.*

**Question 28.** Use Theorem 5.3 to show that every algebraic number field $K$ of degree $n$ admits precisely $n$ distinct embeddings $\sigma_1, \sigma_2, \ldots, \sigma_n : K \to \mathbb{C}$.

**Question 29.** This question will introduce you to splitting fields and get you more comfortable computing with number fields.

| Algebraic number | Minimal polynomial | Number field | Degree |
|---|---|---|---|
| $a/b \in \mathbb{Q}$<br>$\gcd(a, b) = 1,\ b > 0$ | $bx - a$ | $\mathbb{Q}$ | 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 |
| $\zeta_p$, a primitive $p$-th root of unity for a prime $p$ | $\phi_p(x) := \frac{x^p-1}{x-1}$<br>$p$-th cyclotomic polynomial | $\mathbb{Q}(\zeta_p) \cong \mathbb{Q}[x]/(\phi_p(x))$<br>$p$-th cyclotomic field | $p - 1$ |

(a) For each of the rows of the table, do the following.

- Find all of the roots of the minimal polynomial over the number field. How many roots do you find?
- Factor the minimal polynomial over the number field.

(c) Answer the same questions for the polynomial $f(x) := x^3 - 2$ over $S := \mathbb{Q}[x]/(x^6 - 108)$. You should only get linear factors. We call the number field $S$ the **splitting field** of $f(x)$: the smallest field extension of the base field over which $f(x)$ *splits* (decomposes into linear factors).

**Question 30.** Prove that any irreducible polynomial of degree $n$ in $\mathbb{Q}[x]$ has $n$ *distinct* roots in $\mathbb{C}$.

## 6. Heights of Algebraic Numbers

Now we have all of the necessary preliminaries to be able to define a height function for algebraic numbers!

**Definition 6.1.** Let $\alpha$ be an algebraic number in a number field $K$ of degree $n$ with minimal polynomial $a_0 x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the images of $\alpha$ under the $n$-embeddings of $K$ into $\mathbb{C}$ – these are called the $n$ conjugates of $\alpha$. Define the **Weil/absolute height**[1] $H(\alpha)$ of $\alpha$ by

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

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

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

**Question 31.** In this problem, you will show that $H(\alpha^{-1}) = H(\alpha)$.

(a) If $\alpha$ is a nonzero algebraic number with minimal polynomial $f(x) := a_0 x^n + a_1 x^{n-1} + \ldots + a_n$, then verify that $1/\alpha$ is also an algebraic number with minimal polynomial

$$f^{\text{rev}}(x) := x^n f(1/x) = a_0 + a_1 x + \ldots + a_n x^n$$

if $a_n > 0$, and minimal polynomial $-f^{\text{rev}}(x)$ if $a_n < 0$.

(b) Describe the roots of $f^{\text{rev}}(x)$ in terms of the roots of $f(x)$.

(b) Show that $H(\alpha^{-1}) = H(\alpha)$. *Hint: use Question 27.*

Let $\alpha$ be an algebraic number with minimal polynomial $a_0 x^n + \ldots + a_n$. We can view $\alpha$ as giving a point $[a_0 : a_1 : \cdots : a_n]$ in $\mathbb{P}^n(\mathbb{Q})$. Using Definition 4.1 of heights of points in $\mathbb{P}^n(\mathbb{Q})$, we can define

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

**Question 32.** Let $\alpha = \zeta_3$ be a primitive third root of unity. Compute $H(\alpha)$ and $H_2(\alpha)$. *Hint:* the minimal polynomial of $\alpha$ has degree 2.

✻ **Question 33.** There is also a third definition of a height function $H_3$, in terms of the *house* ⌂ and *denominator* den of an algebraic number $\alpha$ (See also [1][§ 3.4]):

[1] 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 [1][§ 3.3]

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

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 $\alpha$. Prove explicit inequalities relating $H(\alpha)$, $H_2(\alpha)$ and $H_3(\alpha)$.

**Question 34.** Fix $m \geq 1$. Consider the polynomial $g$ defined by

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

Show that $g(x) \in \mathbb{Z}[x]$ and that it is a power of the minimal polynomial of $\alpha^m$.

**Question 35.** Consider an algebraic number $\alpha$ with minimal polynomial $f(x) = a_0x^n + \ldots + a_n \in \mathbb{Z}[x]$, and conjuagtes $\alpha_1, \ldots, \alpha_n$. Let

$$\operatorname{Disc}(f) = \alpha_0^{2n-2} \prod_{i>j} (\alpha_i - \alpha_j)^2$$

be the discriminant of $f$. Show that

$$\frac{1}{n} \log |\operatorname{Disc}(f)| \leq \log n + (2n-2)h(\alpha).$$

**✻ Question 36.**

(a) Prove **Liouville's inequality**, namely that if $\alpha$ is an algebraic irrational number of degree $n \geq 2$, then there is a constant $C$ (depending on $\alpha$), such that for any rational number $a/b$ with $b > 0$, we have

$$\left|\alpha - \frac{a}{b}\right| \geq C/b^n.$$

(Hint: Let $f$ be the minimal polynomial of $\alpha$. Combine a lower bound on the nonzero rational number $f(a/b)$ and an upper bound for $|f(\alpha) - f(a/b)|/(\alpha - (a/b))$ using the Mean Value Theorem.)

(b) A **Liouville number** is a real number $x$ with the property that for any integer $n$, there is a rational number $a/b$ with $b > 1$ such that

$$0 < |x - (a/b)| < 1/b^n.$$

Prove that Liouville numbers are transcendental and that Liouville's constant

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

is a Liouville number.

## 7. Preliminaries: Rings of Integers

We will continue our study of algebraic integers, so you can think of this section as part II of section 5.

**Question 37.** Prove that for every algebraic number $\alpha$, there is a nonzero integer $m \in \mathbb{Z}$ such that $m\alpha$ is an algebraic integer.

**Question 38.**

(1) If $\alpha$ is an algebraic integer with minimal polynomial $f$ of degree $n$, prove that the discriminant of the power basis generated by $\alpha$ is precisely the discriminant of the polynomial $f$, and we have $\Delta(\alpha) := \Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\binom{n}{2}} \prod_{i=1}^{n} f'(\alpha_i)$. In particular, if $f(x) = x^2 + ax + b$, then the corresponding discriminant is $b^2 - 4a$ and if $f(x) = x^3 + ax + b$, then the corresponding discriminant is $-4a^3 - 27b^2$.

(2) Let $p$ be a prime and let $\phi_p$ be the $p$-th cyclotomic polynomial. That is

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Show that the discriminant of the power basis generated by a primitive $p$-th root of unity $\zeta_p$ is $(-1)^{\binom{p-1}{2}} p^{p-2}$. (Hint: Use the equality $\phi_p(x)(x-1) = x^p - 1$ and the product rule of differentiation to simplify $\phi'_p(\zeta_p)$.)

**Question 39.** Verify that $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are four mutually non-associate irreducible elements in the ring $\mathbb{Z}[\sqrt{-5}]$ that are not prime.

**Definition 7.1.** Let $K$ be a number field. An **algebraic integer** in $K$ is an element whose minimal polynomial $f(x) := a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{Z}[x]$ has $a_0 = 1$ (i.e. $f$ is a monic integral polynomial). The collection of all algebraic integers in $K$ is denoted $\mathcal{O}_K$ and is called the **ring of integers** of $K$.

**Question 40.** Let $K/\mathbb{Q}$ be a degree $n$ number field.

(a) Prove that if $I$ is a nonzero ideal of $\mathcal{O}_K$, then there is a nonzero integer $m$ in $I \cap \mathbb{Z}$.
(b) Show that every nonzero ideal $I$ is a sublattice of $\mathcal{O}_K$ of maximal rank, i.e. $I$ has finite index in $\mathcal{O}_K$, and is isomorphic to $\mathbb{Z}^n$ as an abelian group.

**Question 41.** Let $K = \mathbb{Q}\left(\sqrt{-23}\right)$.

(a) Find $\mathcal{O}_K$.
(b) Prove that the norm map $N : K \to \mathbb{Q}$ taking $\alpha \to \alpha\sigma(\alpha)$, where $\sigma$ is complex conjugation, takes values in $\mathbb{Z}$ when restricted to $\mathcal{O}_K$.
(c) Show that 2 is irreducible in $\mathcal{O}_K$ but not prime. Conclude that $\mathcal{O}_K$ is not a UFD.

**Definition 7.2.** Suppose that $\alpha$ is an algebraic number with irreducible polynomial $f$. Assume that $f$ factors in $\mathbb{R}[x]$ into $r$ linear factors and $s$ quadratic irreducible factors. Then $r + s = 2n$, and the $n$-embeddings of $K$ into $\mathbb{C}$ naturally split into $r$ real embeddings $\sigma_1, \sigma_2, \ldots, \sigma_r : K \to \mathbb{R}$ and $s$ pairs $(\tau_1, \overline{\tau_1}), (\tau_2, \overline{\tau_2}), \ldots, (\tau_s, \overline{\tau_s})$ of complex conjugate embeddings $K \to \mathbb{C}$. (Here for each $i$ between 1 and $s$, the embedding $\overline{\tau_i}$ is the one obtained by composing the embedding $\tau_i : K \to \mathbb{C}$ with complex conjugation.) The **Minkowski embedding** $K \to \mathbb{R}^n$ is given by

$$\begin{aligned} K &\to \mathbb{R}^r \times \mathbb{C}^s \cong \mathbb{R}^{r+2s} \\ \alpha &\mapsto (\sigma_1(\alpha), \dots, \sigma_r(\alpha), \mathrm{Re}(\tau_1(\alpha)), \mathrm{Im}(\tau_1(\alpha)), \dots, \mathrm{Re}(\tau_s(\alpha)), \mathrm{Im}(\tau_s(\alpha))), \end{aligned}$$

**Question 42.** Verify that $\sqrt{2}+1$ is a unit in the ring $\mathbb{Z}[\sqrt{2}]$. Use the Minkowski embedding to show that $\sqrt{2}+1$ has infinite order in the group of units of $\mathbb{Z}[\sqrt{2}]$.

$\ast$ **Question 43.** Show that the ring $\mathbb{Z}[\sqrt{-2}]$ is a UFD (Hint: it suffices to show that it is a Euclidean domain).

**Question 44.** Consider the elliptic curve $E : y^2 = x^3 - 2$. In this exercise, we will find all integer points on this curve. Fix any $x, y \in \mathbb{Z}$ satisfying $y^2 = x^3 - 2$.

(a) Show that $y$ is odd.

(b) Note that if we work in the ring $\mathbb{Z}[\sqrt{-2}]$, then we can write

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3.$$

Take for granted the fact that $\mathbb{Z}[\sqrt{-2}]$ is a UFD (see Question 43), and show that $y + \sqrt{-2}$ and $y - \sqrt{-2}$ are coprime.

(c) Show that there must exist some unit $u \in \mathbb{Z}[\sqrt{-2}]^\times$ and some $\alpha \in \mathbb{Z}[\sqrt{-2}]$ so that

$$y + \sqrt{-2} = u\alpha^3.$$

(d) Show that we can always take $u = 1$ above (Hint: if $\alpha \in \mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$, its complex norm $|\alpha|$ is an integer. Use this to compute $\mathbb{Z}[\sqrt{-2}]^\times$.)

(e) At this point, $y + \sqrt{-2}$ must be a cube in $\mathbb{Z}[\sqrt{-2}]$. Directly compute all (finitely many) possible values of $y$, and then use this to find all integral points of $E$ (See footnote for the end result[2]).

**Question 45.** Let $K = \mathbb{Q}\left(\sqrt{7}, \sqrt{-2}\right)$. Enlarge the finite index subgroup of $\mathcal{O}_K$ spanned by $1, \sqrt{7}, \sqrt{-2}, \sqrt{-14}$ to a $\mathbb{Z}$-basis for $\mathcal{O}_K$.

**Question 46.** Let $K$ be a number field of degree $n$ and $\beta_1, \dots, \beta_n$ be $\mathbb{Q}$-linearly independent algebraic integers in $K$. Show that the lattice $\Lambda$ spanned by the images of the $\beta_i$ has rank $n$ in $\mathbb{R}^n$ and that the fundamental domain of $\Lambda$ has volume $2^{-s}\sqrt{|\Delta(\beta_1, \beta_2, \dots, \beta_n)|}$, where $s$ is the number of pairs of complex embeddings of $K$.

**Definition 7.3.** A **Galois extension** $K/F$ is a field extension $F \subseteq K$ such that

(1) the extension is *finite*: the dimension of $K$ as a vector space over $F$, denoted by $[K : F]$, is finite.

(2) the extension is *algebraic*: for every $\alpha \in K$, there is a nonzero polynomial with coefficients in $F$ such that $\alpha$ is a root of this polynomial;

(3) the extension is *normal*: Every polynomial in $F[x]$ that has a root in $K$ has all roots in $K$;

(4) the extension is *separable*: For every $\alpha \in K$, its minimal polynomial is separable (does not have repeated roots).

[2]You should find that the only integer solutions to $y^2 = x^3 - 2$ are $(x, y) = (3, \pm 5)$

Equivalently, an extension $K/F$ is Galois if and only if $K$ is the splitting field of some separable polynomial over $F$. If $K/F$ is Galois, then we define $\mathrm{Gal}(K/F)$, the **Galois group** of $K/F$, to be the group $\mathrm{Aut}(K/F)$. This is, $\mathrm{Gal}(K/F)$ is the group of field automorphisms of $K$ that fix $F$. For details, see [4, Chapter 14].

**Question 47.** Consider the natural action of $S_n$ on $\mathbb{Z}[x_1, x_2, \dots, x_n]$, namely the permutation action on the indices of the variables. Let $r_D = \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ and let $D = r_D^2$.

(1) Let $\sigma \in S_n$. Show that $\sigma(D) = D$ for all $\sigma \in S_n$ and that $\sigma(r_D) = r_D$ if and only if $\sigma \in A_n$.
(2) Now let $p$ be an irreducible cubic polynomial in $\mathbb{Q}[x]$. Let $E$ be the splitting field of $p$ over $\mathbb{Q}$, let $\alpha_1, \alpha_2, \alpha_3$ be the roots of $p$ in $E$ and let $G := \mathrm{Gal}(E/\mathbb{Q})$. Show that $G$ is either $A_3$ or $S_3$.
(3) Let $G$ be as above. show that $G = A_3$ if and only if $r_D(\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Q}$. (In other words, the discriminant of the polynomial $p$ is a square in $\mathbb{Q}$ if and only if the splitting field of $p$ is a cubic Galois $A_3$ extension.) [3]

**Question 48.**

(1) Let $q(x) = x^3 - 21x - 7$. Show that $q$ is an irreducible polynomial in $\mathbb{Z}[x]$. (Caution: Remember that there is one extra step in going from being irreducible in $\mathbb{Q}[x]$ to being irreducible in $\mathbb{Z}[x]$). Graph the polynomial $q$ and show that all its roots are real.
(2) Compute the discriminant of the polynomial $q$ and show that the splitting field of $q$ is a cubic Galois $A_3$ extension of $\mathbb{Q}$. [4] (Hint: use Question 47).
(3) Show that if the splitting field of an irreducible cubic polynomial over $\mathbb{Q}$ is an $A_3$ extension, then all the roots of the cubic in $\mathbb{C}$ are real. (Remark: The converse is not necessarily true, but an explicit example does not come to mind. Let me know if you find one!)

**✻ Question 49.** Consider the affine elliptic curve with equation $y^2 - x^3 + x \in \mathbb{C}[x, y]$ and its associated affine coordinate ring $S := \mathbb{C}[x, y]/(y^2 - x^3 + x)$.

(1) Let $a$ be a complex number. Prove that if $a \notin \{-1, 0, 1\}$, then $S/(x - a)S$ has exactly two prime ideals, whose lifts $\mathfrak{p}_1, \mathfrak{p}_2$ to $S$ satisfy $(x-a)S = \mathfrak{p}_1\mathfrak{p}_2$ (the "**completely split**" case), and that if $a \in \{-1, 0, 1\}$, then $S/(x - a)S$ has a unique prime ideal $\mathfrak{p}$ and $(x - a)S = \mathfrak{p}^2$ (the "**ramified**" case).
(2) Show that every nonzero prime ideal of $S$ is of the form $(x - a, y - b)$ for some complex numbers $a$ and $b$. (Hint: Show that the intersection of a nonzero prime ideal of $S$ with $\mathbb{C}[x]$ is a *nonzero prime* ideal of $\mathbb{C}[x]$, and hence of the form $(x - a)$ for some complex number $a$.)

**✻ Question 50.** Let $p$ be a prime number, and let $K = \mathbb{Q}(\zeta_p)$, where $\zeta = \zeta_p$ is a primitive $p$th root of unity. In this problem, we want to compute the ring of integers $\mathcal{O}_K$. First, recall from Question 38 that $\mathbb{Z}[\zeta_p]$ has discriminant $\pm$(power of $p$). Recall also from lecture that

$$\Delta(\zeta_p) = [\mathcal{O}_K : \mathbb{Z}[\zeta_p]]^2 \Delta_K.$$

(1) Deduce that the index of $\mathbb{Z}[\zeta_p]$ in $\mathcal{O}_K$ is a power of $p$. Suppose that $(p\mathcal{O}_K \cap \mathbb{Z}[\zeta_p]) = p\mathbb{Z}[\zeta_p]$. Use this to show that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

[3] See sections 14.6 and 14.7 of Dummit and Foote for explicit solutions to cubic and quartic polynomials over $\mathbb{Q}$ by radicals. The explicit forms of the solutions can be used to give an alternate proof for the problem above.

[4] This is one of the extensions that shows up when you try to write down a primitive 7-th root of unity explicitly in terms of radicals.

(2) Note that the minimal polynomial of $\zeta - 1$ is

$$f(x) = \phi_p(x+1) = \frac{(x+1)^p - 1}{x}.$$

Show that $f(x)$ is $p$-Eisenstein[5]. Use this to show that $(\zeta - 1)^{p-1} \mid p$ in $\mathbb{Z}[\zeta]$.

(3) Show that $(p\mathcal{O}_K \cap \mathbb{Z}[\zeta_p]) = p\mathbb{Z}[\zeta_p]$ (Hint: $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$, so any $x \in p\mathcal{O}_K \cap \mathbb{Z}[\zeta_p]$ can be written as

$$x = c_0 + c_1(\zeta - 1) + \cdots + c_d(\zeta - 1)^d$$

where $d = [K : \mathbb{Q}] - 1 = p - 2$ and $c_i \in \mathbb{Z}$. Inductively show that $p \mid c_i$).

It turns out that for any number field $K$, the ring of integers $\mathcal{O}_K$ is **Dedekind domain**. This is, any ideal of $\mathcal{O}_K$ can be written uniquely as a product of prime ideals. In particular, let $p$ be a prime number, then the ideal $p\mathcal{O}_K$ can be factored as a product of prime ideals

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}.$$

**Definition 7.4.** The exponent $e_i$ of the prime ideal $\mathfrak{p}_i$ appearing in the factorization of $p\mathcal{O}_K$ is called the **ramification index** of $\mathfrak{p}_i$ over $p$, and is also denoted $e(\mathfrak{p}_i|p)$.

**Question 51.** Let $K = \mathbb{Q}(\alpha)$ be a number field. Let $f$ be the minimal polynomial of $\alpha$, and let $p$ be a prime that does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Suppose $f$ factors as

$$f(x) \equiv f_1(x)^{e_1} \dots f_r(x)^{e_r} \mod p,$$

where $f_i(x) \in \mathbb{Z}[x]$ such that $f_i(x) \mod p$ are pairwise distinct irreducible polynomials in $\mathbb{F}_p[x]$. Let $\mathfrak{p}_i := (p, f_i(\alpha))$ for each $i$. Verify that $\mathfrak{p}_i$ is a prime ideal.

**Question 52.** Let $K$ be a number field and $\mathcal{O}_K$ be its ring of integers.

(1) Show that if $I$ is a nonzero ideal of $\mathcal{O}_K$, then $I \cap \mathbb{Z}$ is a nonzero ideal of $\mathbb{Z}$. Use this to show that $I$ has finite index in $\mathcal{O}_K$.
(2) Show that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.
(3) Prove that every finite integral domain is a field. (Hint: To prove that a nonzero element $\alpha$ has a multiplicative inverse, consider the set $\{\alpha, \alpha^2, \dots\}$.)
(4) Combine the previous three parts to show that if $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_K$, then $\mathfrak{p}$ is in fact a maximal ideal. If $p$ is a generator for the ideal $\mathfrak{p} \cap \mathbb{Z}$, then $\mathcal{O}_K/\mathfrak{p}$ is a finite extension of the finite field $\mathbb{F}_p$.

**Definition 7.5.** Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. The inertia degree of $\mathfrak{p}$ is the degree of the extension

$$\mathcal{O}_K/\mathfrak{p}.$$

Note that this is well defined because of Question 52.

**Question 53.** Let $K$ be a number field and let $p$ be a prime number that does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. If $\mathfrak{p}_i$ is the prime ideal associated to the irreducible polynomial $f_i(x)$ appearing in the factorization of $f$ modulo $p$, show that the inertial degree of $\mathfrak{p}_i$ is the degree of the polynomial $f_i$.

**Question 54.** Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, where $K$ is a number field.

(1) Show that $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ for any integer $i$.

[5]i.e. $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ where $p \nmid a_0$, $p^2 \nmid a_n$, but $p \mid a_i$ for all $i > 0$ (including $i = n$)

(2) Let $\alpha \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$. Show that the map of $\mathcal{O}_K$-modules $\mathcal{O}_K/\mathfrak{p} \to \mathfrak{p}^i/\mathfrak{p}^{i+1}$ induced by sending 1 to $\alpha$ is an isomorphism.
(3) Verify that the dimension of $\mathcal{O}_K/\mathfrak{p}^r$ as a $\mathbb{F}_p$ vector space is $rf(\mathfrak{p}|p)$.

**Question 55.** Assume that $K$ is a number field.

(1) Show that every ideal of $\mathcal{O}_K$ is generated by at most two elements.
(2) Show that $\mathcal{O}_K$ is a PID if and only if it is a UFD.

## 8. Heights in $\mathbb{P}^N(K)$

In this section, we will use absolute values to define a height function on $\mathbb{P}^N(K)$.

**Definition 8.1.** An **absolute value** on a field $K$ is a function $|\cdot| \colon K \to \mathbb{R}$ such that for all $x, y \in K$, we have

(1) $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$. (**non-negativity** and **positive-definiteness**)
(2) $|xy| = |x| \cdot |y|$. (**multiplicativity**)
(3) $|x+y| \leq |x| + |y|$. (**triangle inequality**)

If an absolute value satifies the strong triangle inequality $|x+y| \leq \max(|x|, |y|)$ (which implies the weaker inequality 3), we say $|\cdot|$ is **non-Archimedean** (or ultrametric) absolute value. Otherwise, $|\cdot|$ is called **Archimedean**.

**Question 56.** This is a sanity check. Show that the usual absolute value on $\mathbb{C}$ is an absolute value. Can you prove that it is Archimedean?

**Question 57.** Let $\mathfrak{p}$ be a nonzero prime ideal in a number field $K$, with $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Show that the function $|\cdot|_{\mathfrak{p}}$ defined by

$$\begin{aligned} |\cdot|_{\mathfrak{p}} \colon K^* &\to \mathbb{R} \\ 0 &\mapsto 0 \\ x &\mapsto p^{-f(\mathfrak{p}|p)v_{\mathfrak{p}}(x)} \qquad \text{if } x \neq 0 \end{aligned}$$

is a non-Archimedean absolute value on $K$.

Note that every absolute value on a field $K$ gives $K$ the structure of a metric space where

$$d(x, y) = |x - y|.$$

This gives a topology on the field $K$.

**Definition 8.2.** We say that two absolute values are equivalent if they induce the same topology on $K$. A **place** of $K$ is an equivalence class of a nontrivial absolute value on $K$. The collection of all places of a field $K$ is denoted $M_K$. Archimedean places are also called **infinite places**, and non-Archimedean places are also called **finite places**. Moreover, MSpec($\mathcal{O}_K$) is the set of maximal ideals of $\mathcal{O}_K$.

**Question 58.** Show that the two different embeddings $K := \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{R}$ induce different topologies on $K$. (Hint: Can you construct a sequence of elements of $K$ that converges to 0 in one topology but does not converge in the other?)

✻ **Question 59.** Prove the product formula for number fields: for $x \in K^*$ we have

$$\left(\prod_{\mathfrak{p}\in \mathrm{MSpec}(\mathcal{O}_K)} |x|_{\mathfrak{p}}\right)\left(\prod_{i=1}^{r} |\sigma_i(x)|_{\mathbb{R}}\right)\left(\prod_{j=1}^{s} |\tau_j(x)|_{\mathbb{C}}^2\right) = 1.$$

(Hint: Let $x \in \mathcal{O}_K \setminus \{0\}$. Compute the size of $\mathcal{O}_K/x\mathcal{O}_K$ in two ways: (1) Show that it equals the product of the terms coming from the Archimedean places. (2) Show that if $x\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ and $\mathfrak{p}_i \cap \mathbb{Z} = p_i\mathbb{Z}$ with $p_i > 0$, then $\#\mathcal{O}_K/x\mathcal{O}_K = \prod p_i^{e_i f_i}$). This is analogous to the proof of the product formula over $\mathbb{Q}$.

**Definition 8.3.** Let $K$ be a number field. Define the height function $H : \mathbb{P}^n(K) \to \mathbb{R}$ as follows. Let $P \in \mathbb{P}^n(K)$ be a point with a representative $[x_0 : x_1 : \dots : x_n]$ with $x_i \in K$, not all zero (i.e. homogeneous coordinates for $P$). The **relative height of $P$ (relative to $K$)** $H_K(P)$ is defined to be the product

$$\prod_{\mathfrak{p}\in \mathrm{MSpec}(\mathcal{O}_K)} \max(|x_0|_{\mathfrak{p}}, \dots, |x_n|_{\mathfrak{p}})\left(\prod_{i=1}^{r} \max(|\sigma_i(x_0)|_{\mathbb{R}}, \dots, |\sigma_i(x_n)|_{\mathbb{R}})\right)\left(\prod_{j=1}^{s} \max(|\tau_j(x_0)|_{\mathbb{C}}^2, \dots, |\tau_j(x_n)|_{\mathbb{C}}^2)\right).$$

The **absolute height of $P$** is

$$H(P) := H_K(P)^{1/[K:\mathbb{Q}]}.$$

**Question 60.** Let $K = \mathbb{Q}\left(\sqrt{-1}\right)$. Compute the relative height $H_K$ of $P := [5, 6]$. Use this to compute $H(P)$.

**Question 61.** Prove that if $\alpha \in K$ for a number field $K$, then $H(\alpha) = H([\alpha : 1])$.

✻ **Question 62.** Prove that if $P \in \mathbb{P}^n(K)$ with homogeneous coordinates $[x_0 : x_1 : \dots : x_n]$, where $x_i \in K$ for $i \in \{0, \dots, n\}$ and one of the coordinates is equal to 1, then

$$H(P) \geq \left(\prod_{i=0}^{n} H(x_i)\right)^{1/n}.$$

**Question 63.** Let $K/\mathbb{Q}$ be a finite Galois extension (as in Definition 7.3). Show that if $\sigma$ is an automorphism of $K$ in $\mathrm{Gal}(K/\mathbb{Q})$ and $P = [x_0 : \dots : x_n] \in \mathbb{P}^n(K)$. Then,

$$H_K(\sigma(P)) = H_K(P),$$

where $\sigma(P) = [\sigma(x_0) : \dots : \sigma(x_n)]$.

✻ **Question 64** (Generalized Liouville's inequality)**.** Let $L/K$ be an extension of number fields and $S$ be a finite set of primes in $\mathcal{O}_L$. Let $\alpha, \beta$ be elements of $L$ with $\alpha \neq \beta$.

(a) Show that $H(\alpha - \beta) \leq 2H(\alpha)H(\beta)$.
(b) Show that $\prod_{\mathfrak{p}\in S} |\alpha|_{\mathfrak{p}} \leq H(\alpha)^n$.
(c) Show that

$$(2H(\alpha)H(\beta))^{-n} \leq \prod_{\mathfrak{p}\in S} |\alpha - \beta|_{\mathfrak{p}} \leq (2H(\alpha)H(\beta))^n.$$

[Hint: For the lower bound use that $H(\gamma) = H(1/\gamma)$ for any $\gamma \in \overline{\mathbb{Q}}$.]

## 9. Heights on Elliptic Curves

We are now ready to define heights on elliptic curves! This is not where the theory of heights ends, but will be the last topic we cover. If you are curious about other height functions or applications, please ask!

**Definition 9.1.** The **Weil height function** of an elliptic curve $E$ defined over a number field $K$ is the function

$$\begin{aligned} h_E : \ & E(\overline{\mathbb{Q}}) \to \mathbb{R} \\ & P \mapsto h(x(P)). \end{aligned}$$

**Definition 9.2** (Tate)**.** The **canonical** or **Néron-Tate** height on an elliptic curve $E$ over a number field $K$ is the function

$$\begin{aligned} \hat{h}_E : \ & E(\overline{\mathbb{Q}}) \to \mathbb{R} \\ & P \mapsto \lim_{N\to\infty} \frac{h_E(2^N P)}{2 \cdot 4^N} \end{aligned}$$

**Question 65.** Show that the canonical height function is well-defined. You can follow the proof of this fact in [2, Chapter 8, Proposition 9.1].

**Question 66.** Show that the canonical height function $\hat{h}_E : E(\overline{\mathbb{Q}}) \to \mathbb{R}$ satisfies the following properties:

(a) (**Northcott**) $|2\hat{h}_E - h_E|$ is a bounded function on $E(\overline{\mathbb{Q}})$. Hence, the set of points of $E(\overline{\mathbb{Q}})$ with bounded canonical height is finite.

(b) (**Parallelogram law**) Let $P, R \in E(\overline{\mathbb{Q}})$ be any two points of $E(\overline{\mathbb{Q}})$. Then, we have

$$\hat{h}_E(P+R) + \hat{h}_E(P-R) = 2\hat{h}_E(P) + 2\hat{h}_E(R).$$

In particular, for any positive integer $m$, we have

$$\hat{h}_E(mP) = m^2 \hat{h}_E(P) \quad \textbf{(canonicity)},$$

and

$$\hat{h}_E(P+R) \le 2\hat{h}_E(P) + 2\hat{h}_E(R).$$

(c) (**Uniqueness**) Any function $\hat{h}' : E(\overline{\mathbb{Q}}) \to \mathbb{R}$ satisfying Northcott and canonicity for any one integer $m \ge 2$ is equal to $\hat{h}_E$.

**Question 67.** Let $P \in E(\overline{\mathbb{Q}})$. Show that $\hat{h}_E(P) \ge 0$. Furthermore, show that $\hat{h}_E(P) = 0$ if and only if $P$ is a torsion point.

**Question 68.** Let $K$ be a number field, and let $E/K$ be an elliptic curve defined over $K$. Prove that the group $E(K)_{\mathrm{tors}}$ of torsion $K$-points is finite.

The next two questions ask you to adapt the construction of the canonical height function on an elliptic curve to a dynamical setting.

**Question 69.** Let $f : \mathbb{P}^n \to \mathbb{P}^n$ be a morphism of degree $d \ge 2$ defined over a number field $K$. Recall from lecture that $h(f(P)) = d\,h(P) + O(1)$ for any $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$, say

$$|h(f(P)) - d\,h(P)| \le C$$

for any $P \in \mathbb{P}^n(\overline{\mathbb{Q}})$. Use a telescoping sum argument to show that

$$\left|\frac{h(f^{\circ N}(P))}{d^N} - \frac{h(f^{\circ M}(P))}{d^M}\right| \leq \frac{C}{(d-1)d^M}$$

for all $N > M \geq 0$. Conclude from this that the function

$$\widehat{h}_f(P) := \lim_{N\to\infty} \frac{h(f^{\circ N}(P))}{d^N}$$

is well-defined, i.e. that the limit always converges.

**Question 70.** Let $E$ be an elliptic curve over a number field $K$. Consider the two statements.

(1) For all $P, Q \in E(\overline{\mathbb{Q}})$, we have

$$h_E(P+Q) + h_E(P-Q) = 2h_E(P) + 2h_E(Q) + O(1),$$

where the implied constants in $O(1)$ depend on $E$, but are independent of the pair of points $P, Q$.

(2) For any integer $m \in \mathbb{Z}$, we have

$$h_E(mP) = m^2 h_E(P) + O(1),$$

where the implied constants in the $O(1)$ notation depend only on $E$ and $m$ and not on the point $P$.

Show that 2 follows from 1.

✻ **Question 71.** Let $\alpha_1, \dots, \alpha_n$ be any $n$ algebraic numbers (not necessarily conjugate), and let

$$f(x) = (x-\alpha_1)\dots(x-\alpha_n) = x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \in \bar{\mathbb{Q}}[x].$$

Also set $a_0 = 1$. Show that

$$-n\log(2) + \sum_{i=1}^n h(\alpha_i) \leq h([1 : a_1 : \cdots : a_n]) \leq (n-1)\log 2 + \sum_{i=1}^n h(\alpha_i).$$

Hint: Fix a place $v$, and use induction on $n = \deg f$ to show that

$$c_v^{-n}\prod_{j=1}^n \max\{1, \left|\alpha_j\right|_v\} \leq \max_{0\leq i\leq n} \left|a_i\right|_v \leq c_v^{n-1}\prod_{j=1}^n \max\{1, \left|\alpha_j\right|_v\},$$

where $c_v = 1$ if $v$ is non-archimedean, but $c_v = 2$ if $v$ is real, and $c_v = 4$ if $v$ is complex. In the induction step, you'll want to write $f(x) = (x-\alpha_k)g(x)$ with $k$ chosen to maximize $\left|\alpha_k\right|_v$.

✻ **Question 72.** This problem will give you a way of computing $2\cdot E(K)$ to use the Descent method for $E(K)$. [6] Let $E$ be an elliptic curve defined over $K$. Consider the ring $R := K[x]/f(x)K[x]$. Define the map $\phi : E(K) \to R^\times/(R^\times)^2$ given by

$$\phi(P) = x(P) - x$$

Show the following

(1) $\phi$ is a homomorphism
(2) $\ker(\phi) = 2\cdot E(K)$

Use the map $\varphi$ to show that if $E : y^2 = f(x)$ and $f(x) \in \mathbb{Q}[x]$ has three rational roots, then $E(Q)/2E(Q)$ is finite.

[6] This problem comes from Section 7 of this REU paper

$\ast$ **Question 73.** Let $G$ be an abelian group. Show that $G$ is finitely generated if and only if

(1) $G$ admits a norm (as an abelian group). This is, there is a map $|\cdot| : G \to \mathbb{R}_{\geq 0}$ such that
  (i) $| mp |=| m || p |$ for all $g \in G$ and $m \in \mathbb{Z}$,
  (ii) $| h + g |\leq |h| + |g|$ for all $h, g \in G$,
  (iii) for each $c \in \mathbb{R}$ the set $Gc := \{g \in G \mid |p| \leq c\}$ is finite.

(2) $G/mG$ is finite for some integer $m > 1$.

Does your proof determine explicitly a set of generators? Note that this is analogous to the descent method used in the lectures to show that $E(K)$ is finitely generated, where $E$ is an elliptic curve defined over a number field $K$.

**Question 74.** Let $y^2 = x^3 + Ax + B$ be the defining equation for an elliptic curve $E$, where $A$, $B$ are constants in $K$ such that $4A^3 + 27B^2 \neq 0$. Assume that $P$ and $Q$ are points on $E$ such that $x(P) = [x_1 : 1], x(Q) = [x_2 : 1], x(P + Q) = [x_3 : 1]$ and $x(P - Q) = [x_4 : 1]$ (where $x_i = \infty$ if the corresponding point is infinity on $\mathbb{P}^1$). Show that the following identities hold.

(a) $x_3 + x_4 = \dfrac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2}$.

(b) $x_3x_4 = \dfrac{(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1x_2}$.

**Question 75.** Let $A$ and $B$ be elements of $K$ such that $4A^3 + 27B^2 \neq 0$. Let $g_0, g_1, g_2$ in $K[t, u, v]$ be defined as follows:

$$g_0(t, u, v) := u^2 - 4tv,$$
$$g_1(t, u, v) := 2u(At + v) + 4Bt^2,$$
$$g_2(t, u, v) := (v - At)^2 - 4Btu.$$

(a) Show that if $t = 0$, then $u = v = 0$.
(b) Assume $t \neq 0$. Define $z := u/2t$. Using $g_0 = 0$, show that $z^2 = v/t$.
(c) Define $\psi(z) := 4z(A+z^2)+4B$ and $\phi(z) := (z^2-A)^2-8Bz$. Show that $g_1(t, u, v) = t^2\psi(z)$ and $g_2(t, u, v) = t^2\phi(z)$.
(d) Verify that $(12z^2 + 16A)\phi(z) - (3z^3 - 5Az - 27B)\psi(z) = 4(4A^3 + 27B^2)$.
(e) Conclude that $\psi$ and $\phi$ cannot simultaneously vanish, and hence $g_0, g_1, g_2$ have no common zero with $t \neq 0$.

Conclude that if $(t, u, v)$ is a common zero of $g_0, g_1$ and $g_2$, then $t = u = v = 0$.

**Question 76.** Let $K$ be a number field, and let $E/K$ be an elliptic curve with canonical height $\widehat{h}_E : E(\overline{\mathbb{Q}}) \to \mathbb{R}$. Consider the pairing

$$\langle P, Q\rangle := \frac{1}{2}\left[\widehat{h}_E(P + Q) - \widehat{h}_E(P) - \widehat{h}_E(Q)\right]$$

on $E(\overline{\mathbb{Q}}) \times E(\overline{\mathbb{Q}})$.

(1) Show that $\langle P, Q\rangle$ is symmetric, bilinear, and satisfies $\langle P, P\rangle = \widehat{h}_E(P)$. The is sometimes called the **height pairing** on $E$.
  Hint: first show that $\widehat{h}_E$ satisfies an exact parallelogram law.
(2) If you know about tensor products, then show that $\langle -, -\rangle$ extends to a positive definite inner product on the real vector space $E(\overline{\mathbb{Q}}) \otimes_{\mathbb{Z}} \mathbb{R}$.

We will see an application of (a generalization of this) in Question 80.

**Question 77.** The Hilbert's Nullstellensatz is an essential theorem in algebraicc geometry. The most common version of this theorem is given as follows. Let $k$ be an algebraically closed field and consider an ideal $J \subseteq k[X_0, \dots, X_n]$. Define

$$V(J) := \{x \in k^{n+1} \;:\; f(x) = 0 \text{ for all } f \in J\}.$$

The Hilbert Nullstellensatz states that if $f \in k[X_0, \dots, X_n]$ is a polynomial such that $f(x) = 0$ for all $x \in V(J)$, then there must be $e \in \mathbb{Z}_{\geq 0}$ such that $f^e \in J$.

Suppose $F : \mathbb{P}^N \to \mathbb{P}^M$ is a morphism of degree $d$ over a number field $K$, i.e.

$$F(P) = [f_0(P) : \;\dots\; : f_M(P)],$$

where the $f_i$ are homogeneous polynomials of degree $d$ in $N+1$ variables with coefficients in $K$. Assume that the $f_i$ have no common zeros in $\overline{\mathbb{Q}}^{N+1} \setminus (0, 0, \dots, 0)$. Use Hilbert's Nullstellensatz to show that if $[X_0, \dots, X_N]$ are coordinates for $\mathbb{P}^N$, then there is an exponent $e \in \mathbb{Z}_{\geq 0}$ and there are polynomials $g_{ij} \in K[x_0, \dots, x_N]$ for $i \in \{0, \dots, N\}$ and $j \in \{0, \dots, M\}$ such that for every $i \in \{0, \dots, N\}$, we have

$$x_i^e = \sum_{j=0}^{M} g_{ij} f_j.$$

**Definition 9.3.** For $K$ a number field, $v$ a place of $K$, and $g \in K[x_0, \dots, x_n]$ a polynomial, we let $|g|_v$ denote the maximal absolute value of any of its coefficients, i.e. if $g = \sum_I a_I x^I$ with $I$ ranging over all multi-indices $(c_0, \dots, c_n) \in \mathbb{Z}_{\geq 0}^{n+1}$ with $c_0 + \cdots + c_n \leq \deg g$,[7] then $|g|_v = \max_I \left|a_I\right|_v$.

**Question 78.** In this problem, we will show that for a morphism $F = [f_0, \dots, f_M] : \mathbb{P}^N \to \mathbb{P}^M$ of degree $d$ over a number field $K$, one has

$$h(F(P)) = d\,h(P) + O(1)$$

if the polynomials $f_i \in K[x_0, \dots, x_N]$ have no common zero other than $(x_0, \dots, x_N) = (0, \dots, 0)$.

(1) Let $g \in K[x_0, \dots, x_N]$ be homogeneous of degree $d$, and let $v$ be a place of $K$. If $v$ is archimedean, show that

$$|g(P)|_v \leq \binom{N+d}{d} |g|_v \max_{0 \leq i \leq N} \left|x_i\right|_v^d \text{ for all } P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathbb{Q}}).$$

If $v$ is non-archimedean, show that

$$|g(P)|_v \leq |g|_v \max_{0 \leq i \leq N} \left|x_i\right|_v^d \text{ for all } P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathbb{Q}}).$$

Use this to conclude that

$$h(F(P)) \leq d\,h(P) + C_2 \text{ for all } P = [x_0, \dots, x_N] \in \mathbb{P}^N(\overline{\mathbb{Q}}),$$

where $C_2 = [K : \mathbb{Q}] \log \binom{N+d}{d} + h(F)$, where $|F|_v := \max_{0 \leq j \leq M} \left|f_j\right|_v$ and $h(F) := \sum_v \log |F|_v$.[8]

[7] Here, $x^I := x_0^{c_0} x_1^{c_1} \dots x_n^{c_n}$ and $a_I \in K$ is just some choice of coefficient associated with $I$.

[8] This $h(F)$ is the height of the projective point whose coordinates are given by the collection of coefficients of the $f_j$'s

(2) Hilbert's Nullstellsatz (See Question 77) guarantees the existence of an exponent $e$ and polynomials $g_{ij} \in K[x_0, \dots, x_N]$ such that for every $i \in \{0, \dots, N\}$, we have

$$x_i^e = \sum_{j=0}^{M} g_{ij} f_j.$$

For a place $v$, let $|G|_v := \max_{i,j} \left|g_{ij}\right|_v$. To avoid breaking into archimedean and non-archimedean cases, we now introduce

$$\epsilon_v := \begin{cases} 1 & \text{if } v \text{ archimedean} \\ 0 & \text{otherwise.} \end{cases}$$

To ease notation even further, for a point $P = [x_0, \dots, x_N]$ in projective space, we define $|P|_v := \max_{0 \le i \le N} \left|x_i\right|_v$. Now, arguing as in (1), show that

$$|P|_v^e \le (M+1)^{\epsilon_v} \left( \max_{i,j} \left|g_{ij}(P)\right|_v \right) |F(P)|_v \le C' \, |F(P)|_v \, |P|_v^{e-d} \text{ for any } P \in \mathbb{P}^N(\overline{\mathbb{Q}}),$$

where $C' := (M+1)^{\epsilon_v} \binom{N+e-d}{N}^{\epsilon_v} |G|_v$. Use this to conclude that

$$dh(P) + C_1 \le h(F(P)) \text{ for all } P \in \mathbb{P}^N(\overline{\mathbb{Q}}),$$

where $C_1 = [K : \mathbb{Q}] \left( \log(M+1) + \log \binom{N+e-d}{N} \right) + h(G)$, where $h(G) := \sum_v \log |G|_v$.

**Question 79.** Consider the degree 2 rational map

$$\begin{array}{cccc} F: & \mathbb{P}^2 & \longrightarrow & \mathbb{P}^2 \\ & [x, y, z] & \longmapsto & [x^2, xy, z^2]. \end{array}$$

Note that $F$ above is not a morphism, so Question 78 does not apply to it. Show in fact there are infinitely many points $P \in \mathbb{P}^2(\mathbb{Q})$ such that $h(F(P)) = h(P)$.

✻ **Question 80.** This question will assume some familiarity with algebraic curves and their jacobians. In addition to the Mordell-Weil Theorem (that the group of rational points on an elliptic curve is finitely generated), another celebrated application of heights is in Vojta's proof of the **Mordell Conjecture**[9]. This conjecture states that any curve of genus $g \ge 2$ defined over a number field $K$ has finitely many $K$-points. After assuming some hard facts about heights on curves and their jacobians, we will ask you to prove this statement.

Let $K$ be a number field, let $C/K$ be a curve of genus $g \ge 2$, and let $J = \mathrm{Jac}(C)$ be its jacobian. Assume that $C(K) \ne \emptyset$, so we may define an Abel-Jacobi embedding $j : C \hookrightarrow J$. We take for granted the following facts.

(1) There exists a height function $\widehat{h} : J(\overline{\mathbb{Q}}) \to \mathbb{R}$ which satisfies both the Northcott property and that $\widehat{h}(mx) = m^2 \widehat{h}(x)$ for any $m \in \mathbb{Z}$ and $x \in J(\overline{\mathbb{Q}})$. [10]

[9] This conjecture was originally proved by Faltings.

[10] For those more familiar with the Weil height machinery, on $J$, there is a so-called theta divisor $\Theta := \underbrace{j(C) + \cdots + j(C)}_{(g-1) \text{ summands}} \subset J$. The function $\widehat{h}$ alluded to here is a canonical version of the height function associated to the divisor $\Theta + [-1]^*\Theta$, where $[-1] : J \to J$ is negation in $J$'s group law.

In particular, the points of height 0 are exactly the torsion points of $J$. Furthermore, the map $\langle -, - \rangle : J(\overline{\mathbb{Q}}) \times J(\overline{\mathbb{Q}}) \to \mathbb{R}$ defined by

$$\langle x, y \rangle := \frac{1}{2}\left[\widehat{h}(x+y) - \widehat{h}(x) - \widehat{h}(y)\right]$$

is a symmetric, bilinear pairing satisfying $\langle x, x \rangle = \widehat{h}(x)$. Inspired by this, we introduce the notation

$$\|x\| := \sqrt{\langle x, x \rangle} = \sqrt{\widehat{h}(x)}$$

for $x \in J(\overline{\mathbb{Q}})$.

(2) The group $J(K) \subset J(\overline{\mathbb{Q}})$ of $K$-points on the jacobian is finitely generated, and the pairing $\langle -, - \rangle$ considered above gives a positive definite inner product on the finite dimensional vector space $V := J(K) \otimes_{\mathbb{Z}} \mathbb{R}$.

(3) For any $\epsilon > 0$, there exists constants $B > 0$ and $\kappa \geq 1$ such that for any distinct $P, Q \in C(\overline{\mathbb{Q}})$ satisfying both[11]

$$\|j(P)\| \geq \|j(Q)\| > B \text{ and } \frac{\langle j(P), j(Q) \rangle}{\|j(P)\| \|j(Q)\|} \geq \frac{3}{4} + \epsilon,$$

one has

$$\|j(P)\| \leq \kappa \|j(Q)\|.$$

This is called **Vojta's inequality**.

Use the above 3 facts in order to prove that $C(K)$ is finite. Hint: look at the image of $C(K)$ in $V$, and split $V$ into (finitely many!) cones s.t. any two points in a given cone have a small angle between them.

## References


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

[2] Joseph H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[3] Matt Baker, *Algebraic Number Theory Course Notes*. https://drive.google.com/file/d/1WzKMLX5rb9INEYkSiaNHXjw6TZYHwWEV/view. 2022.

[4] David S. Dummit and Richard M. Foote, *Abstract algebra*. Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004.

[5] Klaus Hulek, *Elementary algebraic geometry*. Translated from the 2000 German original by Helena Verrill. Student Mathematical Library, 20. American Mathematical Society, Providence, RI, 2003.


[11] The constant $3/4$ appearing below can actually be replaced with $\sqrt{g}/g$. For an elliptic curve, we have $g = 1$, and so the statement of Vojta's inequality would be useless in that case. This is good because there exists elliptic curves with infinitely many rational points.