Prime ideals, places, and heights on projective spaces

Padmavathi Srinivasan

Week 4

Last time we defined the ring of algebraic integers $\mathcal{O}_K$ inside a number field K. We saw that unique factorization can fail in these more general number rings. For example, we showed that the element 6 in the ring of integers $\mathbb{Z}[\sqrt{-5}]$ of $\mathbb{Q}(\sqrt{-5})$ admits two different factorizations into irreducible elements. However, we have Kummer's theorem [Bak22, Chapter 1, Theorem 1.25, Theorem 1.27] that tells us every nonzero *ideal* factors uniquely into a product of *prime ideals*. We say that $\mathcal{O}_K$ admits unique factorization of ideals. In today's lecture, we will learn to explicitly write down prime ideals of $\mathcal{O}_K$, and learn how to use them to define a height function for points on $\mathbb{P}^n(K)$.

1 Prime ideals in the ring of integers

Let p be a prime number. Our first goal is to explicitly describe the prime factorization $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ of the ideal $p\mathcal{O}_K$.

Definition 1. 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 $e(\mathfrak{p}_i|p)$.

Fact 1. [Bak22, Chapter 2, Corollary 2.20] *The only prime numbers p such that they have a prime ideal $\mathfrak{p}$ appearing in the factorization of $p\mathcal{O}_K$ with $e(p|p) > 1$ (also known as the collection of ramified primes in the extension K) are the primes p dividing the discriminant Δ_K of K.*

Fact 2. [Bak22, Chapter 3, Corollary 3.14]*[Minkowski] For any number field $K \neq \mathbb{Q}$, we have $|\Delta_K| > 1$. In particular, if $K \neq \mathbb{Q}$, the collection of ramified primes in K is nonempty and finite.*

Let K be a number field. Suppose α is an algebraic integer that is a primitive element of the number field K. Let f be the minimal polynomial of α, 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.

Suggested exercises 2. Let $\mathfrak{p}_i := (p, f_i(\alpha))$ for each i. Verify that $\mathfrak{p}_i$ is a prime ideal.

Theorem 3. [Bak22, Theorem 2.16]*[Kummer's factorization theorem] Let $\mathfrak{p}_i := (p, f_i(\alpha))$ for each i. Then $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ with ramification index e_i, and we have the factorization*

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

In particular, Kummer's factorization theorem applies to all primes p if $\mathcal{O}_K = \mathbb{Z}[\alpha]$. However, there are examples where it does not suffice. For example, we stated (without proof) last time that 3 divides the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ for any algebraic integer α in the ring of integers of the biquadratic field $\mathbb{Q}(\sqrt{7}, \sqrt{10})$. Nevertheless, it applies to most primes in any given number field. For example, when $K = \mathbb{Q}(\sqrt{-5})$, then $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$, and $x^2 + 5 \equiv (x+1)^2 \mod 2$, and $x^2 + 5 \equiv (x+1)(x-1) \mod 3$, explaining where the prime ideal factorizations

$$2\mathcal{O}_K = (2, \sqrt{-5}+1)^2 \qquad 3\mathcal{O}_K = (3, \sqrt{-5}+1)(3, \sqrt{-5}-1)$$

come from.

Example 4. Let $K = \mathbb{Q}(\sqrt{d})$ for d a squarefree integer, and p be a prime number. Assume further that p is odd if $d \equiv 1 \mod 4$. From our lecture last time, we know that the index $[\mathcal{O}_K : \mathbb{Z}[\sqrt{d}]]$ is 1 or 2, depending on whether $d \equiv 2, 3 \mod 4$ or $d \equiv 1 \mod 4$. In particular, Kummer's factorization theorem with $\alpha = \sqrt{d}$ applies to any odd prime p, and also applies to the prime 2 if $d \equiv 2, 3 \mod 4$.

If p divides d, since $x^2 - d \equiv x^2 \mod p$, Kummer's factorization theorem then tells us that $p\mathcal{O}_K = \mathfrak{p}^2$ for the prime ideal $\mathfrak{p} := (p, \alpha)$ of $\mathcal{O}_K$.

If $p \nmid d$ and $d \equiv a^2 \mod p$ for some integer a, then $x^2 - d \equiv (x-a)(x+a) \mod p$, and correspondingly, we have that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for two distinct prime ideals defined by $\mathfrak{p}_1 := (p, \sqrt{d} - a)$ and $\mathfrak{p}_2 := (p, \sqrt{d} + a)$.

If d is not a square modulo p, then $p\mathcal{O}_K$ is itself a prime ideal.

It is not too hard to test if d is a square modulo p by computing the corresponding Legendre symbol $\left(\frac{d}{p}\right)$. For a given d, one can list the collection of split primes p (those that split into 2 linear factors) and the collection of inert primes p (those that generate a prime ideal of $\mathcal{O}_K$) by using quadratic reciprocity to relate the Legendre symbol $\left(\frac{d}{p}\right)$ to $\left(\frac{p}{d}\right)$. The next example carries this out for $d = -1$.

Example 5. Let $K = \mathbb{Q}(\sqrt{-1})$. Then $\mathcal{O}_K = \mathbb{Z}[i]$. This is a special case of the previous example and Kummer's factorization theorem applies to all primes p. We know that -1 is a square modulo p if and only if $p \equiv 1 \mod 4$, so this tells us that

$$p\mathcal{O}_K = \begin{cases} (1+i)^2 & \text{if } p = 2 \\ \mathfrak{p}_1\mathfrak{p}_2 & \text{if } p \equiv 1 \mod 4 \\ \text{is prime} & \text{if } p \equiv 3 \mod 4. \end{cases}$$

Given Kummer's factorization theorem, it is now natural to ask if every prime ideal of $\mathcal{O}_K$ appears in the factorization of the principal ideal $p\mathcal{O}_K$ for some prime number p. The answer is yes, and for proving this we will need to combine a few more consequences of unique factorization of ideals. We now state the necessary results. Recall that in a degree n number field, the ring of integers $\mathcal{O}_K$ is isomorphic to $\mathbb{Z}^n$ as an abelian group.

Suggested exercises 6.

(a) 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 $\mathcal{O}_K$.

(b) Show that if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, then $\mathfrak{p} \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$.

(c) Prove that every finite integral domain is a field. (Hint: To prove that a nonzero element α has a multiplicative inverse, consider the set $\{\alpha, \alpha^2, \ldots\}$.)

(d) 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 $\mathbb{F}_p$.

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_K$, and let p be a generator for the ideal $\mathfrak{p} \cap \mathbb{Z}$. One of the consequences of having unique factorization of ideals is the following very useful result (stated here without proof). It is often summarized as "to contain is to divide".

Fact 3. [Bak22, Lemma 1.39] *If I and J are two ideals of $\mathcal{O}_K$, then $I \subset J$ if and only if J divides I, i.e. there exists another ideal I' such that $I'J = I$.*

If $\mathfrak{p}$ is a nonzero prime ideal, then Exercise 6 4 tells us that $\mathfrak{p} \cap \mathbb{Z}$ is a nonzero prime ideal, say generated by the prime number p. Then $p\mathcal{O}_K \subset \mathfrak{p}$, and by applying Fact 3we get

Lemma 7. *Every nonzero prime ideal appears in the factorization of $p\mathcal{O}_K$ for some prime number p.*

Let $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Exercise 6 tells us that if $\mathfrak{p}$ is a prime ideal, then $\mathcal{O}_K/\mathfrak{p}$ is a finite field that is an extension of the field $\mathbb{Z}/p\mathbb{Z}$.

Definition 8. The degree of the finite field extension $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}$ is called the inertial degree or the residue degree of $\mathfrak{p}$ over p, and is denoted $f(\mathfrak{p}|p)$.

Definition 9. A prime p of $\mathbb{Z}$ is said to completely split in K if $e(\mathfrak{p}|p) = f(\mathfrak{p}|p) = 1$ for every $\mathfrak{p}$ above p.

Suggested exercises 10. For a prime p where Kummer's factorization theorem 3 applies, and $\mathfrak{p}_i$ is the prime ideal associated to the monic irreducible polynomial $f_i(x) \mod p$ appearing in the factorization of f modulo p, then one can show that $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p[x]/(\overline{f_i(x)})$, so the inertial degree is simply the degree of the polynomial f_i.

Example 11. Let $K = \mathbb{Q}(\sqrt[3]{2})$. Then we showed last time that $\mathcal{O}_K = \mathbb{Z}[\sqrt[3]{2}]$. Since $x^3 - 2 \cong (x-3)(x^2+3x-1) \mod 5$, using Exercise 10 it follows that $5\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, with $\mathfrak{p}_1 = (5, \sqrt[3]{2} - 3), \mathfrak{p}_2 = (5, (\sqrt[3]{2}^2 + 3\sqrt[3]{2} - 1)), e(\mathfrak{p}_1|5) = e(\mathfrak{p}_2|5) = 1$, $f(\mathfrak{p}_1|5) = 1$ and $f(\mathfrak{p}_2|5) = 2$.

Suggested exercises 12. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. Show $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ for any integer i. 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 α is an isomorphism. Verify that the dimension of $\mathcal{O}_K/\mathfrak{p}^r$ as a $\mathbb{F}_p$ vector space is $rf(\mathfrak{p}|p)$.

Since any two distinct maximal ideals generate the unit ideal, by combining the factorization $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ with Exercise 6 4, we get

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathcal{O}_K/\mathfrak{p}_1^{e_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_r^{e_r}.$$

Combining this decomposition with Exercise 12 and comparing the dimensions of the two sides as $\mathbb{F}_p$ vector spaces, we get the following useful numerical constraint:

Lemma 13.

$$\sum_{\mathfrak{p}|p\mathcal{O}_K} e(\mathfrak{p}|p)f(\mathfrak{p}|p) = [K:\mathbb{Q}].$$

One can also prove the following results using unique factorization of ideals, and I encourage you to try these exercises with your TAs!

Suggested exercises 14.

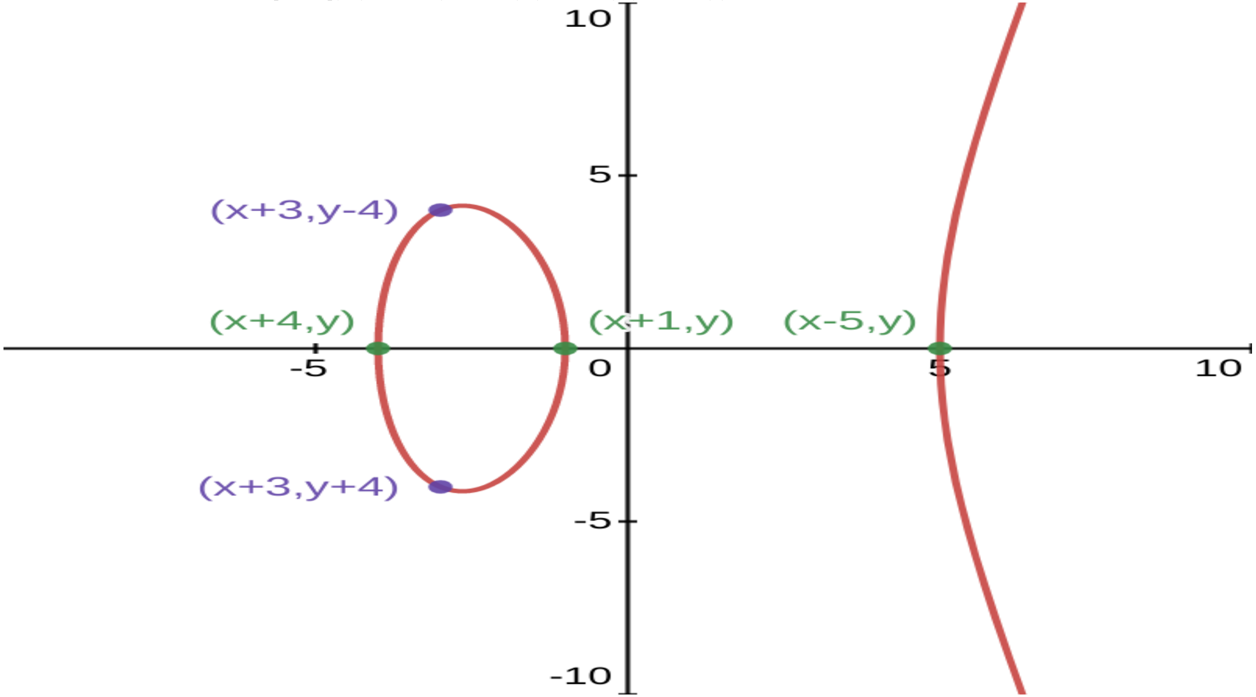
(a) Show that every ideal of $\mathcal{O}_K$ is generated by at most two elements.

(b) Show that $\mathcal{O}_K$ is a PID if and only if it is a UFD.

A useful analogy

There is a beautiful geometric "function field" analogue of the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_K$, where the base PID $\mathbb{Z}$ is replaced by the polynomial ring $K[x]$ over a field K (the "ring of functions on the affine line"). For example, the inclusion $K[x] \to K[x,y]/(y^2 - f(x))$ for a squarefree polynomial $f(x)$ in $K[x]$ behaves in many ways like $\mathbb{Z} \to \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[y]/(y^2-d)$ for a squarefree integer d. See [Poo, Section 2.6] for a table of the corresponding objects on the two sides.

Some prime ideals in the coordinate ring
$S := \mathbb{C}[x,y]/(y^2 - (x+1)(x+4)(x-5))$ of an affine elliptic curve



For example, if $K = \mathbb{C}$, and $f(x) = (x+4)(x+1)(x-5) \in \mathbb{C}[x]$, the nonzero prime ideals of the ring $S := \mathbb{C}[x,y]/(y^2 - f(x))$ are maximal, and their intersection with $\mathbb{C}[x]$ is a nonzero prime ideal of $\mathbb{C}[x]$, namely an ideal of the form $(x-a)$ for some complex number

a. If $a \in \{-4,-1,5\}$, then $(x-a)S = (y, x-a)^2$ and the ideal $(x-a)$ ramifies in S. In this case, the maximal ideal appearing in the factorization of $(x-a)$ corresponding to the unique point $x = a, y = 0$ on the elliptic curve with equation $y^2 = f(x)$ lying above the point $x = a$ in $\mathbb{C}$. If $a \notin \{-4,-1,5)$, then $(x-a)S = (x-a, y-b)(x-a, y+b)$, where $(y+b)(y-b) = y^2 - f(a)$, so the ideal $(x-a)$ completely splits in S. In this case, the two distinct maximal ideals in the factorization of $(x-a)S$ when $a \notin \{-4,-1,5\}$ correspond precisely to the two distinct points in $\mathbb{C}^2$ on the curve $y^2 = f(x)$ with $x = a$.

Structure theorems for the ring of integers

Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}_k$. Given $x \in \mathcal{O}_K \setminus \{0\}$, let $\nu_{\mathfrak{p}}(x)$ denote the exponent of $\mathfrak{p}$ in the factorization of the ideal $x\mathcal{O}_K$. Then $\nu_{\mathfrak{p}}$ extends uniquely to a group homomorphism $K^* \to \mathbb{Z}$ (Verify this!), and is called the $\mathfrak{p}$-adic valuation on K.

Example 15. Let a/b be a nonzero rational number written in lowest form, so that $\gcd(a,b) = 1$. Write down the prime factorizations of a and b as $a = p_1^{l_1} \dots p_r^{l_r}, b = q_1^{m_1} \dots q_s^{m_s}$ for some collection of pairwise distinct prime numbers $\{p_1, \dots, p_r, q_1, \dots, q_s\}$ and exponents $l_1, \dots, l_r, m_1, \dots, m_s$ in $\mathbb{Z}_{\geq 0}$. Let p be an arbitrary prime number. Then

$$\nu_p(a/b) = \begin{cases} l_i & \text{if } p = p_i \text{ for some i } \in \{1,2,\dots,r\} \\ -m_i & \text{if } p = q_i \text{ for some i } \in \{1,2,\dots,s\} \\ 0 & \text{otherwise.} \end{cases}$$

Suggested exercises 16. Verify that $\nu_{\mathfrak{p}}$ extends to a group homomorphism $K^* \to \mathbb{Z}$. Show that if $x \in K^*$, then $\nu_{\mathfrak{p}}(x) = 0$ for almost all nonzero prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$.

We now collect the $\nu_{\mathfrak{p}}$ for each of the nonzero prime ideals $\mathfrak{p}$ into one homomorphism. Let $\oplus_{\mathfrak{p}}\mathbb{Z}$ be the free abelian group on the collection of nonzero prime ideals. We have a group homomorphism

$$\begin{aligned} \iota \colon K^* &\to \oplus_{\mathfrak{p}}\mathbb{Z} \\ x &\mapsto (\nu_{\mathfrak{p}}(x))_{\mathfrak{p}} \end{aligned}$$

The kernel of ι is precisely the group of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$, and the cokernel of ι (i.e. the quotient $\oplus_{\mathfrak{p}}\mathbb{Z}/(\text{im } (\iota)))$ is an important invariant of the number field called the class group $\mathrm{Cl}(\mathcal{O}_K)$. Since $\mathrm{Cl}(\mathcal{O}_K)$ is trivial exactly when all ideals of $\mathcal{O}_K$ are principal, and since being a UFD and being a PID are equivalent for $\mathcal{O}_K$ (Exercise 14), the class group measures the failure of unique factorization in $\mathcal{O}_K$. The two main theorems about number fields that one usually learns in a first course in Algebraic Number Theory are the following. These can both be proved using Geometry of Numbers techniques.

Fact 4.

(a) [Bak22, Chapter 3, Theorem 3.19] *(Dirichlet's Unit Theorem) The group $\mathcal{O}_K^*$ of units of $\mathcal{O}_K$ is a finitely generated abelian group of rank $r + s - 1$ where r, s are the number of real and pairs of complex conjugate embeddings of the number field K.*

(b) [Bak22, Chapter 1, Theorem 1.62] *The class group of a number field K is finite.*

2 Absolute values on number fields

We will need one more ingredient before defining $H : \mathbb{P}^n(K) \to \mathbb{R}$ for K a number field, which is the classification of absolute values on K.

Definition 17. 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

(a) $|x| \geq 0$, and $|x| = 0$ if and only if $x = 0$. (non-negativity and positive-definiteness)

(b) $|xy| = |x| \cdot |y|$. (multiplicativity)

(c) $|x + y| \leq |x| + |y|$. (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.

Multiplicativity and positive definiteness of the absolute value imply that $|1| = 1$. The name non-Archimedean comes from the observation that if $|\cdot|$ satisfies the strong triangle inequality and $n \geq 1$ an integer, then

$$|n| = |1 + 1 + \ldots + 1| \leq \max(|1|, |1|, \ldots, |1|) = 1.$$

Example 18. The *trivial* absolute value on a field K is the absolute value such that $|x| = 1$ for all $x \neq 0$, and $|0| = 0$.

Example 19. The usual complex absolute value function $a + bi \mapsto \sqrt{a^2 + b^2} = |a + bi|_{\mathbb{C}}$ is an absolute value on $\mathbb{C}$. Let $\sigma_i\colon K \to \mathbb{C}$ be an embedding of a number field K into $\mathbb{C}$. Then $x \mapsto |\sigma_i(x)|$ is an Archimedean absolute value on the number field K.

Example 20. Let $\mathfrak{p}$ be a nonzero prime ideal in a number field K, with $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$. Then the function $|\cdot|_{\mathfrak{p}}|$ defined by

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

is a non-Archimedean absolute value on K, called the normalized $\mathfrak{p}$-adic absolute value on K. Non-negativity, positive-definiteness and multiplicativity are immediate from the definition. Using the "to contain is to divide" principle 3, we see that $x \in \mathfrak{p}^{\nu_{\mathfrak{p}}(x)}, y \in \mathfrak{p}^{\nu_{\mathfrak{p}}(y)}$ and so $x + y \in \mathfrak{p}^{\min(\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y))}$, and the strong triangle inequality follows.

The following lemma is immediate from Example 15 and Example 20.

Lemma 21. *[Product formula] If $x \in \mathbb{Q}^*$, then $|x|_{\mathbb{R}} \prod_{\text{primes } p} |x|_p = 1$.*

Every absolute value on a field K gives K the structure of a metric space where

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

Example 22. The trivial absolute value on K (Example 18) induces the discrete topology on K.

Analogous of the construction of the real numbers from the rational numbers by adding limits of all Cauchy sequences, one can analogously construct new fields $K_{\mathfrak{p}}$ from a number field K and a nonzero prime ideal $\mathfrak{p}$ called the completion of K with respect to the associated $\mathfrak{p}$-adic absolute value. These new fields have very different topology from the real numbers. For example, one can show that they are totally disconnected, i.e., the only connected proper subsets are singletons! If you are interested in learning more about the p-adic numbers $\mathbb{Q}_p$, see Renee Bell's lectures from last year's PAWS (we will not use them).

Definition 23. 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.

Suggested exercises 24. Show that the two different embeddings $K := \mathbb{Q}(\sqrt{2}) \to \mathbb{R}$ 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?)

If $s > 0$ is a real number and $|\cdot|$ is an absolute value, then $|\cdot|^s$ is an equivalent absolute value. We have the following classification theorem for all places of a number field K that essentially says the only places are the examples we have already constructed. It was proved for $\mathbb{Q}$ by Ostrowski in 1916.

Theorem 25. [Bak22, Chapter 5, Theorem 5.23]

- *Every Archimedean absolute value on K is equivalent to the restriction to K of the usual absolute value on $\mathbb{C}$ for some embedding of K into $\mathbb{C}$.*
- *Every nontrivial non-Archimedean absolute value on K is equivalent to the $\mathfrak{p}$-adic absolute value for some nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.*

More precisely, there are bijections.

$$\begin{aligned}\{\text{non-Archimedean places of } K\} \leftrightarrow &\{\text{nonzero prime ideals of } \mathcal{O}_K\}\\ \{\text{Archimedean places of } K\} \leftrightarrow &\{\text{real embeddings } K \to \mathbb{R}\}\\ &\cup \{\text{conjugate pairs of complex embeddings } K \to \mathbb{C}\}.\end{aligned}$$

Let $\operatorname{MSpec}(\mathcal{O}_K)$ denote the collection of nonzero prime ideals of $\mathcal{O}_K$ (the notation MSpec stands for maximal spectrum, the collection of maximal ideals). Let $\sigma_1, \ldots, \sigma_r \colon K \to \mathbb{R}$ be the collection of real embeddings of $\mathcal{O}_K$, and let $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$ be the collection of pairs of complex conjugate embeddings.

Lemma 26. *[Product formula for number fields] Let $x \in K^*$. Then*

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

Suggested exercises 27. Prove Lemma 26. (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 Lemma 13.)

3 Heights on projective spaces

Definition 28. Let K be a number field. Define the height function $H\colon \mathbb{P}^n(K) \to \mathbb{R}$ 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

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

Proposition 29. [Sil09, Proposition 5.4] *Let K be a number field, and $P \in \mathbb{P}^n(K)$ a point.*

(a) *The height $H_K(P)$ is well-defined, independent of the choice of homogeneous coordinates for P.*

(b) *$H_K(P) \geq 1$.*

(c) *Let L/K be a finite extension of number fields. Then*

$$H_L(P) = H_K(P)^{[L:K]}.$$

In particular, $H(P)$ is independent of the choice of number field K such that $P \in \mathbb{P}^n(K)$.

Proof. The seemingly infinite product in the definition is actually a finite product, since almost all the terms in the product are 1. (See Exercise 16.) Part a follows from the product formula for number fields 26, because if we scale all coordinates of a chosen representative by a nonzero scalar x in K, then the resulting expression changes by the left hand side of the product formula. Since the right hand side of the product formula is 1, the resulting expression is unchanged. Part b follows because we can change representatives for the point P by suitably scaling the chosen representative to make one of the homogeneous coordinates equal to 1. Then each of the factors in the product defining $H_K(P)$ is at least 1, so their product $H_K(P)$ and in turn $H(P)$ are also at least 1. We skip the proof of Part c, and refer the interested reader to [Sil09, Proposition 5.4]. □

Suggested exercises 30. Prove that if $\alpha \in K$, then $H(\alpha) = H([\alpha\colon 1])$.

Suggested exercises 31. Prove that the definition above agrees with the previous definition for heights of points in $\mathbb{P}^n(\mathbb{Q})$.

Suggested exercises 32. Prove that if $P \in \mathbb{P}^n(K)$ with homogeneous coordinates $[x_0 : x_1 : \ldots : x_n]$ with all the x_i in K and one of the coordinates equal to 1, then

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

Theorem 33. [Sil09, Theorem 5.11] *(Northcott property) There are only finitely many points P of $\mathbb{P}^n(\overline{\mathbb{Q}})$ of bounded absolute height and bounded degree.*

Proof. This follows from Exercise 32 and the Northcott property for algebraic numbers, namely that there are finitely many algebraic numbers of bounded height and bounded degree. □

This definition illustrates the second main feature common to various height functions that are used in Diophantine Geometry, namely that

"Height functions come with local decompositions".

(Here local indicates that there is one term for each place of the number field.) The main feature that we look for in height functions is that they have a Northcott property, namely that there are finitely many points of bounded height and bounded degree. Next lecture we will learn how height functions on projective spaces are used in the proof of the Mordell-Weil theorem.

References

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 ↑8, 9

[Bak22] Matt Baker, *Algebraic Number Theory Course Notes* (2022). ↑1, 2, 3, 5, 7

[Poo] Bjorn Poonen, *Lectures on rational points on curves.* ↑4