Something about ...

Roberto Gualdi

Contents

Something about...

This text contains the general lines of the introductory talks given during the DAGA seminar at the University of Barcelona, starting from December 2016 (see `www.math.u-bordeaux.fr/~robgualdi/DAGA.html`). The priority of the expositions was to let the audience of graduate students understand the main concepts and ideas appearing in the progress of their colleagues' theses. No claim of new results is made. A talk was considered to be successful whenever the audience could say to *have learnt something about* their colleagues expertise field, which justifies the title of the present text.
The talks being aimed to graduate students with an algebraic background, the classically taught notions in algebra and geometry are assumed as prerequisite; anyway, any useful and non-basic definition is recalled and explained. As a result, the text should be readable and fully understandable at an advanced bachelor level.
The author of the talk is responsible for the notations, definitions and results appearing in it.

1

...heights

by Roberto GUALDI

Motivation

Given f a polynomial with integer coefficients in an arbitrary number of variables, a classical question in number theory is to know the number of its solutions living in $\mathbb{Q}$ or, more generally, in a fixed number field K, which is by definition a finite field extension of $\mathbb{Q}$. The correct way to attack the problem (or at least a way that has proved to be fruitful) is to consider the solutions of f over K as the set of K-rational points of a suitable compactification of the variety $Z(f) = \{f = 0\}$. The first non-trivial case is the one of a polynomial in two variables, which defines, after homogenization, a curve in the projective plane. It is then interesting to be able to answer the following more general question.

Question 1. *Let C be a geometrically irreducible[1] smooth projective curve over a number field K. How many K-rational points does C have?*

An apparently very different question, but surprisingly deeply related to the previous one, is the following.

Question 2. *Which is naively simpler,* 1 *or* $^{2016}/_{2017}$*?*

Genus of curves. Recall that the **genus** of a geometrically irreducible smooth projective curve is defined as the dimension of the space of globally defined 1-forms on C, that is the space of global sections of the canonical line bundle Ω^1_C

[1] A scheme X over a field k is said to enjoy *geometrically* a certain property if its base change $X_{\overline{k}}$ over the algebraic closure of k does.

of C, which is the dual of the tangent line bundle. The genus of a smooth projective curve C is one of the main ingredients of Riemann-Roch theorem: for any line bundle $\mathcal{L}$ on C, one has that

$$g(C) = \deg(\mathcal{L}) + 1 - \chi(\mathcal{L})$$

where $\chi(\mathcal{L})$ is the Euler characteristic of $\mathcal{L}$, defined in general as

$$\chi(\mathcal{F}) = \sum_{j=0}^{\dim X} (-1)^j \dim_k H^j(X, \mathcal{F})$$

for a sheaf $\mathcal{F}$ on a scheme X over k. In particular, $\deg\left(\Omega^1_C\right) = 2g(C) - 2$.

Remark. When C is a smooth curve in $\mathbb{P}^2$, defined by the homogeneous polynomial f, the genus of C is related to the degree d of f by the formula

$$g(C) = \frac{(d-1)(d-2)}{2} = \binom{d-1}{2}.$$

Geometry and arithmetic of curves. It is nowadays clear that the answer to Question 1 lies on a beautiful interplay between the geometrical and the arithmetical properties of the curve C. It turned out that the genus of the curve determines the number of rational points it has. In details:

- when $g(C) = 0$: the curve has either no K-rational points (for example, the curve $x_0^2 + x_1^2 + x_2^2 = 0$) or infinitely many of them
- when $g(C) = 1$: the situation is more delicate. It can happen that C has no K-rational points. When it has at least one, C is an elliptic curve over K: *Mordell-Weil theorem* (1922) implies then that the set of K-rational points of C is a finitely generated abelian group, which can even be finite (for example, in the case of the elliptic curve $x_0x_2^2 - x_1^3 + px_0^2x_1 = 0$, with p congruent to 7 or 11 modulo 16). The problem of determining the rank of this group (in particular whether C has finitely or infinitely many rational points over K) is highly non-trivial and it is the main statement of the *Birch and Swinnerton-Dyer conjecture*, nowadays far from being solved
- when $g(C) \geq 2$: *Faltings's theorem* (1983/1984) asserts that C has finitely many K-rational points, as conjectured by Mordell in 1922.

Remark. As an application of Faltings's theorem and the recalled genus-degree formula, one easily sees that the n-Fermat curve $x_1^n + x_2^n = x_0^n$ only has finitely many K-rational points for $n \geq 4$. In particular, the equation $x^n + y^n = z^n$, with $n \geq 4$ has finitely many solutions living in $\mathbb{Q}$. This is *almost* Fermat last theorem (an elementary proof of it for the case $n = 3$ was already known to Euler).

Complexity of numbers. Regarding Question 2, it seems clear that 1 is a naively much simpler number than the other one, even if their absolute values are close. In order to justify this intuitive answer, one needs to formally define a notion of *complexity* of algebraic numbers. The theory of heights perfectly answers this need; moreover, it proves to be a powerful and ubiquitous tool in number theory, representing, for instance, one of the main instruments for the proof of Faltings's theorem.

Adelic fields

The natural setting in which to develop a theory of heights is the one of an adelic field, which is a field together with a collection of absolute values and certain additional data.

Absolute values. Fix a field K throughout the whole subsection. An **absolute value** over K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying the following three axioms:

(i) $|x| = 0$ if and only if $x = 0_K$

(ii) $|x \cdot y| = |x| \cdot |y|$

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

Whenever $|\cdot|$ satisfies, instead of (iii), the stronger inequality

$$|x + y| \leq \max\{|x|, |y|\}$$

for every $x, y \in K$, one says that $|\cdot|$ is a **non-archimedean** absolute value. Otherwise, $|\cdot|$ is said to be **archimedean**.

Example. Over every field K there is a non-archimedean absolute value, the *trivial absolute value* $|\cdot|_{\mathrm{tr}}$, defined as

$$|x|_{\mathrm{tr}} = \begin{cases} 0 & x = 0_K \\ 1 & \text{otherwise} \end{cases}.$$

Example. Over the fields $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ the usual ("Euclidean") absolute value, the modulus of a number, is an archimedean absolute value, which we will denote by $|\cdot|_\infty$.

Example. Let p be a prime number and consider $x \in \mathbb{Q}$. After writing $x = p^{l \cdot a/b}$ with a and b both coprime with p and $l \in \mathbb{Z}$, set $|x|_p := p^{-l}$. The function $|\cdot|_p$ defines a non-archimedean absolute value over $\mathbb{Q}$, which is called the *p-adic absolute value*.

Places. Every absolute value $|\cdot|$ over K induces a distance, by $d(x,y) := |x-y|$, hence a topology. Two absolute values are called *equivalent* if they induce the same topology on K. A class of equivalent absolute values is called a **place**. Some elementary computations prove that two absolute values $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if there exists $\lambda \in \mathbb{R}_{>0}$ such that

$$|x|_1 = |x|_2^{\lambda}$$

for every $x \in K$. In particular, the archimedean and non-archimedean properties are stable under equivalence of absolute values and it is then meaningful to speak about *archimedean places* and *non-archimedean places*.

Remark. The relation between two equivalent absolute values is a useful tool to produce absolute values which are equivalent to a given one. Anyway, one should be careful while performing this operation. Whilst in the case of $|\cdot|$ being non-archimedean $|\cdot|^{\lambda}$ is an absolute value for any $\lambda \in \mathbb{R}_{>0}$, this is no longer true in the archimedean case. Indeed, when $|\cdot|$ is archimedean, $|\cdot|^{\lambda}$ is an absolute value for any $\lambda \in (0,1]$, but the triangular inequality could fail for $\lambda > 1$.

A classical result by Ostrowski describes all the places over the field of rational numbers.

Theorem 1 (Ostrowski)**.** *The only absolute values over $\mathbb{Q}$ are, up to equivalence: the trivial absolute value, the usual Euclidean absolute value and the p-adic absolute values, with p running in the set of prime numbers.*

Adelic fields. Having reviewed the basic definitions and examples related to absolute values, we can now define the notion of adelic field.

Definition 1. An **adelic field** is the datum $(K, \{|\cdot|_v, n_v\}_{v\in\mathfrak{M}})$ of a field K, together with a collection of places $\mathfrak{M}$ over K and the choice, for each place $v \in \mathfrak{M}$, of an absolute values $|\cdot|_v$ in v and of a positive real number n_v, satisfying the following two axioms:

(i) if v is a non-trivial non-archimedean place, then

$$\{\log|x|_v : x \in K^{\times}\} \simeq \mathbb{Z}$$

as a group (that is, v is associated to a discrete valuation)

(ii) for every $x \in K^{\times}$, $|x|_v = 1$ for all but finitely many $v \in \mathfrak{M}$.

The number n_v is often referred to as the *weight* of the place v. A property that is often required to hold for adelic fields in the theory of heights is the following.

Definition 2. An adelic field $(K, \{|\cdot|_v, n_v\}_{v\in\mathfrak{M}})$ is said to satisfy the **product formula** if for every $x \in K^{\times}$ one has

$$\prod_{v\in\mathfrak{M}} |x|_v^{n_v} = 1.$$

The identity in the previous definition is meaningful since, by the definition of adelic field, the quantity $|x|_v$ equals 1 for almost all $v \in \mathfrak{M}$. Hence, the infinite product reduces to a finite one. Obviously, the product formula can be written in the equivalent logarithmic version

$$\sum_{v \in \mathfrak{M}} n_v \cdot \log |x|_v = 0.$$

Proposition 1. *Denote by $\mathfrak{M}_{\mathbb{Q}}$ the collection of all places over $\mathbb{Q}$. Then, the datum $\left(\mathbb{Q}, \{|\cdot|_v, 1\}_{v \in \mathfrak{M}_{\mathbb{Q}}}\right)$ is an adelic field satisfying the product formula, where $|\cdot|_v$ are normalized as in the examples of the previous section.*

Proof. It is immediate to verify that $\left(\mathbb{Q}, \{|\cdot|_v, 1\}_{v \in \mathfrak{M}_{\mathbb{Q}}}\right)$ is an adelic field. In order to check that the product formula holds, notice that it is enough to verify it for prime numbers. Then, for a prime number p, one has

$$\prod_{v \in \mathfrak{M}_{\mathbb{Q}}} |p|_v = |p|_{\text{tr}} \cdot |p|_p \cdot |p|_\infty = p^{-1} \cdot p = 1,$$

which concludes the proof. □

Another classical example is the one of *function fields*, as follows.

Example. Let C be a smooth projective curve over a field k. Let $K := k(C)$ be the function field of the curve, $\mathfrak{M}_C$ the collection of closed points of C. For every $v \in \mathfrak{M}_C$, consider the absolute value

$$|\cdot|_v := c_k^{-\operatorname{ord}_v(\cdot)},$$

where ord_v is the order of vanishing of a rational function over C at the closed point v and c_k is a constant depending on the base field k (in details, c_k is the cardinality of k if k is finite, $c_k = e$ otherwise). One shows that, with such choices, $(K, \{|\cdot|_v, |k(v) : k|\}_{v \in \mathfrak{M}_C})$ is an adelic field satisfying the product formula.

At last, we investigate the relation between adelic field structures and finite field extensions. Suppose L/K is a finite field extension. Consider a place w over L. An absolute value in this equivalence class restricts to an absolute value over K and then defines a place v over K. Easily, v does not depend on the choice of the absolute value in w. Moreover, archimedean and non-archimedean places of L restrict to archimedean and non-archimedean places of K, respectively. If w restricts to v, one says[2] that w **divides** v and writes $w|v$.

Proposition 2. *Let $(K, \{|\cdot|_v, n_v\}_{v \in \mathfrak{M}})$ be an adelic field satisfying the product formula. Let L/K be a finite field extension. Then, there exists a canonical adelic field structure on L, $(L, \{|\cdot|_w, n_w\}_{w \in \mathfrak{N}})$ which satisfies the following properties:*

1. *$\mathfrak{N}$ is the set of places of L which restrict on K to a place in $\mathfrak{M}$*

[2]This suggestive name has a classical number theoretical explanation.

2. *whenever $w|v$, the restriction of $|\cdot|_w$ to K coincides with $|\cdot|_v$*
3. $\sum_{w|v} n_w = n_v$
4. $(L, \{|\cdot|_w, n_w\}_{w\in\mathfrak{N}})$ *satisfies the product formula.*

Remark. The construction in Proposition 2 is quite explicit. For instance, it allows to define a canonical structure of an adelic field with product formula on any number field, starting from the adelic field structure of $\mathbb{Q}$ given in Proposition 1. In details, let K be a number field. The adelic field structure given by Proposition 2 is $(K, \{|\cdot|_w, n_w\}_{w\in\mathfrak{N}})$, where $\mathfrak{N}$ is the collection of all places over K (for a more specific result, see the discussion about a generalized Ostrowski theorem here), and for every $w \in \mathfrak{N}$:

$$|\cdot|_w := |N_{K_w/\mathbb{Q}_v}(\cdot)|_v^{\frac{1}{[K_w:\mathbb{Q}_v]}}$$

(here the norm of a field extension appears, and the extension $K_w/\mathbb{Q}_v$ is finite since $K_w/\mathbb{Q}_v$ is) and

$$n_w := \frac{|K_w : \mathbb{Q}_v|}{|K : \mathbb{Q}|}.$$

Canonical height on $\mathbb{P}^1$

We now come to the main object of the talk. In order to keep the exposition as basic as possible, we restrict here to the case of the simplest possible height, which is the canonical height on $\mathbb{P}^1$, also known as the *Weil height* on $\mathbb{P}^1$. This baby example is anyway already interesting enough: it enjoys useful property, thought posing non-trivial open problems. We start by giving a general definition of canonical height over any base adelic field. We will then restrict to the case of the projective line over $\mathbb{Q}$.

The general case. For a base field K and a finite field extension L of K, the L-rational points of $\mathbb{P}^1_K$ will be expressed in homogeneous coordinates as $[x_0 : x_1]$ with $x_0, x_1 \in L$.

Definition 3. Let $(L, \{|\cdot|_w, n_w\}_{w\in\mathfrak{N}})$ be an adelic field satisfying the product formula. Let $P = [x_0, x_1]$ be a L-rational point of $\mathbb{P}^1_L$. The **canonical height** (also, the **Weil height**) **of** P **over** L is defined as

$$h_L(P) := \sum_{w\in\mathfrak{N}} n_w \log \max\{|x_0|_w, |x_1|_w\}.$$

Remark. The product formula assures that the previous definition does not depend on the choice of the homogeneous coordinates of P. Indeed, the computation for $[x_0, x_1]$ and $[\lambda x_0, \lambda x_1]$ for any $\lambda \in L^\times$ yields the same value of the sum defining $h_L(P)$.

Consider now an adelic field $(K, \{|\cdot|_v, n_v\}_{v\in\mathfrak{M}})$ satisfying the product formula and fix an algebraic closure $\overline{K}$ of K. Consider $P \in \mathbb{P}^1_K\left(\overline{K}\right)$; this means that there exists a finite field extension L of K such that $P \in \mathbb{P}^1_K(L)$. Definition 3 allows to define the height of P over L, endowed with the canonical adelic structure given by Proposition 2. The value of this height does not depend on the choice of the field L. To check this claim, write $P = [x_0, x_1]$, with $x_0, x_1 \in \overline{K}$. Let L be any finite field extension of K such that $P \in \mathbb{P}^1_K(L)$; then $L \supseteq K[x_0, x_1]$. The canonical adelic structures induced by K on L and $K[x_0, x_1]$ are compatible in the sense that $(L, \{|\cdot|_w, n_w\}_{w\in\mathfrak{N}})$ and $(K[x_0, x_1], \{|\cdot|_v, n_v\}_{v\in\mathfrak{M}})$ satisfy the first three properties of the statement of Proposition 2. Then:

$$\begin{aligned} h_L(P) &= \sum_{w\in\mathfrak{N}} n_w \log\max\{|x_0|_w, |x_1|_w\} = \sum_{v\in\mathfrak{M}} \sum_{\substack{w\in\mathfrak{N}\\ w|v}} n_w \log\max\{|x_0|_w, |x_1|_w\} \\ &= \sum_{v\in\mathfrak{M}} \left(\sum_{w|v} n_w\right) \log\max\{|x_0|_v, |x_1|_v\} = \sum_{v\in\mathfrak{M}} n_v \log\max\{|x_0|_v, |x_1|_v\} \\ &= h_{K[x_0,x_1]}(P). \end{aligned}$$

This computation allows to define a notion of canonical height over the $\overline{K}$-points of $\mathbb{P}^1_K$.

Definition 4. Let $(K, \{|\cdot|_v, n_v\}_{v\in\mathfrak{M}})$ be an adelic field satisfying the product formula. Let P be a $\overline{K}$-rational point of $\mathbb{P}^1_K$. The **canonical height** (or the **Weil height**) **of** P is defined as $h_{\overline{K}}(P) := h_L(P)$, where L is any finite field extension of K such that P is a L-rational point of $\mathbb{P}^1_K$, and L is endowed with the canonical adelic structure of Proposition 2.

The rational case. We consider now the case of the field $\mathbb{Q}$, with the adelic structure given in Proposition 1, which satisfies the product formula. Definition 4 gives a notion of height of algebraic points over the projective line. Including $\overline{\mathbb{Q}}$ into $\mathbb{P}^1_{\mathbb{Q}}\left(\overline{\mathbb{Q}}\right)$ via

$$\alpha \mapsto [1 : \alpha]$$

allows to define the height of an algebraic number, which is an element of $\overline{\mathbb{Q}}$. Explicitely, for every $\alpha \in \overline{\mathbb{Q}}$ one has, directly by Definition 4:

$$h(\alpha) = \sum_{w\in\mathfrak{N}} n_v \log\max\{1, |\alpha|_v\},$$

where $(K, \{|\cdot|_v, n_v\}_{v\in\mathfrak{M}})$ is the canonical adelic structure described above of any number field K containing α. In particular:

- $h(\alpha) \geq 0$ for every $\alpha \in \overline{\mathbb{Q}}$
- $h(\alpha^q) = q \cdot h(\alpha)$ for every $\alpha \in \overline{\mathbb{Q}}$ and $q \in \mathbb{Q}_{\geq 0}$[3].

[3]It is not difficult to show that, more generally, $h(\alpha^q) = |q| \cdot h(\alpha)$ for every $\alpha \in \overline{\mathbb{Q}}$ and $q \in \mathbb{Q}$.

In a certain sense, $h(\alpha)$ *measures the arithmetic complexity of* α, as it can be seen in the case of $\alpha \in \mathbb{Q}$.

Proposition 3. *Suppose* $\frac{a}{b} \in \mathbb{Q}$, *with* $\gcd(a, b) = 1$. *Then*

$$h\left(\frac{a}{b}\right) = \max\{\log|a|, \log|b|\}.$$

Proof. One can use Definition 3 with respect to the base field $\mathbb{Q}$. Then:

$$h\left(\frac{a}{b}\right) = h\left(\left[1 : \frac{a}{b}\right]\right) = h([b : a]) = \sum_{v \in \mathfrak{M}_{\mathbb{Q}}} \log \max\{|a|_v, |b|_v\}.$$

Let p be a prime number. Since a and b are integer numbers, they have p-adic absolute value at most equal to 1. The fact that a and b are coprime implies that at least one of them has p-adic absolute value exactly equal to 1. Hence, for every non-archimedean absolute value v over $\mathbb{Q}$, $\max\{|a|_v, |b|_v\} = 1$. So:

$$h\left(\frac{a}{b}\right) = \log \max\{|a|_\infty, |b|_\infty\} = \max\{\log|a|, \log|b|\}.$$

□

Example. Proposition 3 allows us to answer Question 2 in a satisfactory way. In fact, it turns out that $h(1) = 0$, while $h\left({}^{2016}/_{2017}\right) = \log(2017)$. Hence, 1 has a far lower height than ${}^{2016}/_{2017}$, justifying the intuitive idea of its lower arithmetic complexity.

The following theorem suggests how the theory of heights can help for finiteness result as in the case of the answer to Question 1. Recall that the *degree* of an algebraic number α is defined as the degree of its minimal polynomial over $\mathbb{Q}$.

Theorem 2 (Northcott's property)**.** *There are only finitely many algebraic numbers with bounded degree and bounded height.*

In other words, for every pair of constants $A, B \in \mathbb{R}_{\geq 0}$, the set

$$\left\{\alpha \in \overline{\mathbb{Q}} : \deg(\alpha) \leq A \text{ and } h(\alpha) \leq B\right\}$$

is finite. When $A = 1$, this fact is a trivial consequence of Proposition 3.

Lehmer's problem. Since the height of an algebraic number measures its arithmetic complexity, it is natural to ask which are the "simplest" elements of $\overline{\mathbb{Q}}$. The value $h(\alpha)$ being non-negative for all $\alpha \in \overline{\mathbb{Q}}$ and being $h(1) = 0$, the question is equivalent to the description of the family of algebraic numbers with height equal to zero.

Theorem 3 (Kronecker)**.** *The height of* $\alpha \in \overline{\mathbb{Q}}^\times$ *is* 0 *if and only if* α *is a root of unity.*

Proof. If α is a root of unity, then there exists $n \in \mathbb{N}$ for which $\alpha^n = 1$. Basic properties of the height imply that:

$$n \cdot h(\alpha) = h(\alpha^n) = h(1) = 0,$$

hence $h(\alpha) = 0$.
Conversely, suppose that $h(\alpha) = 0$. For all $k \in \mathbb{N}$, one has that $\alpha^k \in \mathbb{Q}[\alpha]$ and $h(\alpha^k) = k \cdot h(\alpha) = 0$. As a consequence of Northcott's property, the set

$$\{1, \alpha, \alpha^2, \dots\}$$

is finite. Then, there exist $k, l \in \mathbb{N}$ such that $\alpha^k = \alpha^l$, implying that α is a root of unity. □

Having understood which are the algebraic numbers with height equal to 0, the next natural question is the following: how close to 0 can the height of a non-zero algebraic number be, if one excludes roots of unity? The answer is simple: it can be arbitrarely small, as the following example shows.

Example. For every $k \in \mathbb{N}$, the height of $\sqrt[k]{2}$ is

$$h(\sqrt[k]{2}) = \frac{1}{k} h(2) = \frac{1}{k} \log(2),$$

which tends to 0 as k grows. Remark that the set $\{\sqrt[k]{2}\}_{k \in \mathbb{N}}$ is infinite with bounded height; of course, it does not contradict Northcott's property, as the degree of the algebraic numbers $\sqrt[k]{2}$ is not bounded.

One can then refine the question to the following one.

Question 3. *How small can the quantity* $\deg(\alpha) \cdot h(\alpha)$ *be for* $\alpha \in \overline{\mathbb{Q}}^\times$*, if one excludes roots of unity?*

This apparently harmless question is still without answer, even if progresses have been made towards the following conjecture.

Conjecture (Lehmer)**.** *There exists a constant* $c > 0$ *such that* $\deg(\alpha) \cdot h(\alpha) \geq c$ *for all* $\alpha \in \overline{\mathbb{Q}}^\times \setminus \{$*roots of unity*$\}$.

Despite the long time passed since the conjecture was formulated in 1933, the candidate for the constant c is still the one suggested by Lehmer himself, i.e. $\log(1.17628081\dots)$, which is reached by any root of the polynomial

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1^4.$$

[4]The best results known today are the following: C.J. Smyth proved that every root of a non-reciprocal polynomial gives a higher value than the conjectured one. In a different direction, E. Dobrowolski proved that the quantity $\deg(\alpha) \cdot h(\alpha)$ cannot decrease to 0 too fast as $d = \deg(\alpha)$ grows (the quantity is bounded below by a term in $(\log\log d / \log d)^3$).

2

...idèles

by Eduardo SOTO

Motivation

A central object of study in number theory is the understanding of number fields, which are finite field extensions of $\mathbb{Q}$. The finite field extensions which are better understood are the ones which can be studied via Galois theory. Recall that a finite field extension is said to be a **Galois extension** if it is normal and separable. In the case of number fields, the separability assumption is automatically satisfied (this is a more general result for fields of characteristic zero); as a consequence, a finite field extension K of $\mathbb{Q}$ is Galois if and only it is normal, that is if and only if K is the splitting field over $\mathbb{Q}$ of a polynomial with coefficients in $\mathbb{Q}$. This means that there exists a polynomial f with rational coefficients such that $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$, where $\alpha_1, \dots, \alpha_n$ are *all* the roots of f in some algebraic closure of $\mathbb{Q}$. The **Galois group of the extension** $K/\mathbb{Q}$ is defined as

$$\mathrm{Gal}_{\mathbb{Q}}(K) := \{\sigma \in \mathrm{Aut}(K) : \sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}\},$$

$\mathrm{Aut}(K)$ being the group of field isomorphisms of K, together with the composition of morphism. It represents a tremendously useful tool to study Galois extensions, thanks to Galois main theorem. The cardinality of $\mathrm{Gal}_{\mathbb{Q}}(K)$ coincides with the degree of the extension $K/\mathbb{Q}$.

Cyclotomic extensions. Among all finite field extensions of $\mathbb{Q}$, a special role is played by the so-called *cyclotomic extensions*, which we introduce here. Let n be a positive integer number, denote by μ_n the group of n-th roots of

unity and by ζ_n a primitive n-th root of unity (that is, a generator of the group μ_n).

Definition 1. The number field $\mathbb{Q}[\zeta_n]$ is called a **cyclotomic** field extension of $\mathbb{Q}$.

The extension $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is a Galois extension ($\mathbb{Q}[\zeta_n]$ is the splitting field of $f = T^n - 1$ over $\mathbb{Q}$) and it has degree $\phi(n)$, the Euler function of n. Moreover, it is not difficult to verify that

$$\mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}[\zeta_n]) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}.$$

The isomorphism is described as follows: for every σ in the Galois group, $\sigma(\zeta_n) = \zeta_n^l$ for some $l \in \{1, \ldots, n-1\}$, not depending on the choice of the primitive root ζ_n; send σ to such l.

Abelian extensions. A Galois extension $K/\mathbb{Q}$ is said to be **abelian** if the Galois group $\mathrm{Gal}_{\mathbb{Q}}(K)$ is an abelian group. The description of the Galois group of the cyclotomic extension in the previous paragraph shows that *each cyclotomic extension of $\mathbb{Q}$ is abelian*. Also, *each quadratic extension of $\mathbb{Q}$ is abelian*; indeed, every degree two extension is Galois and its Galois group has cardinality 2: it has to be the cyclic group of two elements.
Of course, there exist extensions of $\mathbb{Q}$ which are not abelian, as shown in the following example.

Example. Consider the polynomial $f = T^3 - 2$. Let K be the splitting field of f over $\mathbb{Q}$, that is $K = \mathbb{Q}\left[\sqrt[3]{2}, \zeta_3\right]$, where ζ_3 denotes a primitive third root of unity. The field extension $K/\mathbb{Q}$ is a Galois extension of degree 6. Hence $G := \mathrm{Gal}_{\mathbb{Q}}(K)$ is a finite group of order 6. The group G is not abelian; indeed, denote by σ, τ the two elements of G acting on the $\mathbb{Q}$-generators of K as follows:

$$\begin{aligned} \sigma : \sqrt[3]{2} &\mapsto \sqrt[3]{2} \\ \zeta_3 &\mapsto \zeta_3^2 \end{aligned}$$

and

$$\begin{aligned} \tau : \sqrt[3]{2} &\mapsto \sqrt[3]{2} \cdot \zeta_3 \\ \zeta_3 &\mapsto \zeta_3 \end{aligned}$$

One easily checks that $\sigma\tau \neq \tau\sigma$ (indeed, $\sigma\tau = \tau^2\sigma$). A simple computation shows that

$$G = \langle \sigma, \tau |\, \sigma^2, \tau^3, (\sigma\tau)^2 \rangle = S_3,$$

the 3-dihedral group, which is the smallest non abelian group.

Describing all Galois extensions of $\mathbb{Q}$ is a difficult task. The situation is clearer for quadratic extensions, which are automatically Galois extensions.

Proposition 1. *Any quadratic extension of $\mathbb{Q}$ is included in a cyclotomic field extension of $\mathbb{Q}$.*

Proof. Every quadratic extension of $\mathbb{Q}$ is of the form $\mathbb{Q}[\sqrt{n}]$, for some $n \in \mathbb{Z}$ squarefree. We claim that for every $n \in \mathbb{Z}$ one has

$$\mathbb{Q}\left[\sqrt{n}\right] \subseteq \mathbb{Q}\left[\zeta_{4|n|}\right].$$

In order to prove the previous inclusion, let's start with the case of $n = p$ a prime positive number. Denoting by $\left(\frac{a}{p}\right)$ the Legendre symbol of a over p, one considers

$$\alpha := \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \zeta_p^j \in \mathbb{Q}\left[\zeta_p\right].$$

Some computations show that $\alpha^2 = \left(\frac{-1}{p}\right) \cdot p$, from which $\alpha \in \mu_4 \cdot \sqrt{p}$ (recall that $\mu_4 = \{\pm 1, \pm i\}$). Hence,

$$\sqrt{p} \in \mu_4 \cdot \alpha \subseteq \mathbb{Q}\left[\zeta_4, \zeta_p\right] \subseteq \mathbb{Q}\left[\zeta_{4p}\right].$$

The same argument proves that $\sqrt{-p} \in \mathbb{Q}\left[\zeta_{4p}\right]$. Regarding the general case, $n = \pm p_1 \cdot \cdots \cdot p_l$ (it is squarefree), from which

$$\sqrt{n} = \sqrt{\pm p_1}\sqrt{p_2} \cdot \cdots \cdot \sqrt{p_l} \in \mathbb{Q}\left[\zeta_4, \zeta_{p_1}, \ldots, \zeta_{p_l}\right] \subseteq \mathbb{Q}\left[\zeta_{4p_1 \cdots p_l}\right] \subseteq \mathbb{Q}\left[\zeta_{4|n|}\right],$$

completing the proof. □

The previous Proposition is only the tip of the iceberg. The following more general result holds, concerning abelian extensions of $\mathbb{Q}$.

Theorem 1 (Kronecker-Weber)**.** *Every finite Galois abelian extension of $\mathbb{Q}$ is contained in some cyclotomic extension of $\mathbb{Q}$.*

The previous theorem, whose first complete proof is due to Hilbert (1896), underlines the idea that cyclotomic field extensions play a prominent role among the abelian field extensions of $\mathbb{Q}$. Moreover, using Galois main theorem, one can classify abelian extensions of $\mathbb{Q}$ by looking at subgroups of $(\mathbb{Z}/n\mathbb{Z})^\times$ for $n \in \mathbb{N}$, which is the Galois group of the n-cyclotomic extension of $\mathbb{Q}$.

A question. The content of Kronecker-Weber theorem is the possibility of generating every abelian extension of $\mathbb{Q}$ using cyclotomic numbers. What happens for abelian extensions of a general number field? The following question is then natural.

Question 1. *How can one classify every finite Galois abelian extensions of a number field K? Otherwise said, which are the algebraic numbers needed to construct all finite Galois abelian extensions of K?*

Though its simple formulation, the problem is far from being fully resolved. Some progresses have been made since 1900, when Hilbert included the question in his list of 23 problems. The language of idèles offers a useful tool to develop a class field theory over general number fields, helping in the understanding of the posed question.

Basics in algebraic number theory

We recall in this section some basic definitions and results that are necessary to introduce the machinery of idèles.

Places over number fields. A **place** over a number field K is an equivalence class of absolute values, where two absolute values are said to be equivalent if they induce the same topology on K. The family of places over a given number field is perfectly understood. First of all, one distinguishes between *non-archimedean absolute values*, the ones satisfying the ultrametric property $|x+y| \leq \max\{|x|, |y|\}$ for every $x, y \in K$, and *archimedean absolute values*, the ones which does not. The property of being archimedean or not is stable under equivalence of absolute values and then induces a distinction between *archimedean* (or *infinite*) *places* and *non-archimedean* (or *finite*) *places*. We next describe the full picture.

Infinite places. For a fixed number field K, denote by $\mathcal{S}_K$ the set of the endomorphisms $\sigma : K \to \mathbb{C}$. An element $\sigma \in \mathcal{S}_K$ is said to be a **real embedding** if $\sigma(K) \subseteq \mathbb{R}$, a **complex embedding** otherwise.

Example. Let $K := \mathbb{Q}[T]/\left(T^3 - 2\right)$. It is a number field of degree 3 over $\mathbb{Q}$. It admits three embeddings: a real embedding, sending T to $\sqrt[3]{2}$, and two complex embeddings, sending T to $\sqrt[3]{2} \cdot \zeta_3$ or to $\sqrt[3]{2} \cdot \zeta_3^2$ respectively. Notice that the two complex embedding are obtained one from the other after composing with the complex conjugation.

The observations in the previous example still holds in the general case. The complex embeddings of a number field K always come in pairs, and one is the complex conjugate of the other. This means that if σ is a complex embedding of K, then $\overline{\sigma} := J \circ \sigma$ is such as well, where J denotes the complex conjugation. Moreover, if r_1 and r_2 denote the number of real embeddings of K and the number of *pairs* of complex embeddings of K, respectively, the following equality holds:

$$[K : \mathbb{Q}] = r_1 + 2r_2.$$

Denote now by $|\cdot|$ the usual absolute value in $\mathbb{C}$. It is clear that every embedding σ of K into $\mathbb{C}$ gives an archimedean absolute value on K by $|\cdot|_\sigma := |\sigma(\cdot)|$. Also, if σ and $\overline{\sigma}$ are conjugate complex embeddings, they produce the same absolute value over K. As a result, this construction provides $r_1 + r_2$ archimedean absolute values over K.

Dedekind domains and finite places. Given an extension of rings $A \subseteq B$, one says that the *integral closure of A into B* is the set of elements in B which satisfy a integral relation over A, that is the set of elements of B which are roots

of a monic polynomial with coefficients in A. This is the straightforward generalization of the notion of algebraic closure of a field inside another field. A domain A is said to be *integrally closed* if it coincides with its integral closure in its field of fractions.

Definition 2. A **Dedekind domain** is an integrally closed, Noetherian domain with Krull dimension one, that is, it is not a field and every non-zero prime ideal is maximal.

The notion of Dedekind domain can be considered as the "globalization" of the notion of discrete valuation rings. In fact, a noetherian domain is a Dedekind domain if and only if the localization at each maximal ideal is a DVR. A peculiar and useful properties of Dedekind domains is the fact that any non-zero proper ideal admits a unique decomposition into a product of prime ideals.

The main number theoretic interest into Dedekind domains is the following. For a number field K, the **ring of integers of** K is defined as the integral closure of $\mathbb{Z}$ into K, that is the set of elements in K satisfying an integral relation over $\mathbb{Z}$. It is commonly denoted by $\mathcal{O}_K$.

Proposition 2. *The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain.*

A direct consequence of the previous proposition is that any non-zero proper ideal of $\mathcal{O}_K$ factors into a product of prime ideals in $\mathcal{O}_K$. Using this property, any non-zero prime ideal of $\mathcal{O}_K$ gives a non-archimedean absolute value over K as follows. Fix a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Its *norm* is defined to be $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$. Consider an element $x \in \mathcal{O}_K \setminus \{0\}$ and let $(x) = x\mathcal{O}_K$ be the corresponding non-zero principal ideal in $\mathcal{O}_K$. This ideal admits a unique factorization into prime ideals of $\mathcal{O}_K$, that is

$$x\mathcal{O}_K = \mathfrak{p}^e \cdot \mathfrak{p}_1^{e_1} \cdot \cdots \cdot \mathfrak{p}_l^{e_l}.$$

Define

$$\|x\|_{\mathfrak{p}} := N(\mathfrak{p})^{-e}.$$

One can extend this function to K by setting $\|0\|_{\mathfrak{p}} := 0$ and $\|a/b\|_{\mathfrak{p}} := \|a\|_{\mathfrak{p}}/\|b\|_{\mathfrak{p}}$. This is easily verified to be a non-archimedean absolute value over K. One remarks that

$$\{x \in K : \|x\|_{\mathfrak{p}} \leq 1\} = \mathcal{O}_{K,\mathfrak{p}}$$

(the localization of $\mathcal{O}_K$ at $\mathfrak{p}$); it is a local domain with maximal ideal $\mathcal{M}_{K,\mathfrak{p}} = \{x \in K : \|x\|_{\mathfrak{p}} < 1\}$.

Generalized Ostrowski theorem. A classical result by Ostrowski (1916) states that the only absolute values on $\mathbb{Q}$ are, up to equivalence: the trivial absolute value, the Euclidean absolute value and the p-adic absolute values, for p prime. A similar version for number fields holds.

Theorem 2 (Generalized Ostrowski)**.** *Let K be a number field. The only absolute values over K are, up to equivalence: the trivial absolute value, the archimedean absolute values coming from embeddings of K in $\mathbb{C}$ and the non-archimedean absolute values associated to non-zero prime ideals of $\mathcal{O}_K$.*

The language of idèles

For a number field K, denote by $\mathfrak{M}_K$ the family of places over K. For a given place v of K, let K_v denote its v-completion and by $\mathcal{O}_{K,v}$ the ring of integers of K_v.

Definition 3. The **group of idèles of a number field** K is defined as the set

$$\mathcal{J}_K := \left\{ (x_v)_v \in \prod_{v \in \mathfrak{M}_K} K_v \ : \ x_v \in \mathcal{O}_{K,v}^{\times} \text{ for almost all } v \in \mathfrak{M}_K \right\},$$

together with componentwise multiplication.

Remark first of all that the defined operation is internal. Indeed, whenever x_v, y_v lie in $\mathcal{O}_{K,v}^{\times}$, so does $x_v \cdot y_v$. Moreover, no dependence on the choice of an absolute value for the given place appears in the definition.

TO BE CONTINUED