On fields with finitely many points of bounded height: around property (N)

Sara Checcoli
(Institut Fourier, Université Grenoble-Alpes)

VaNTAGe Seminar

February 27th, 2024

§1. Measuring algebraic numbers

Def Let $\alpha \in \overline{\mathbb{Q}}$ and let $p_\alpha(x) = a \cdot (x - \alpha_1) \cdots (x - \alpha_d) \in \mathbb{Z}[x]$ be its minimal polynomial. The (absolute logarithmic Weil) height of α is

$$h(\alpha) = \frac{1}{d} \log \underbrace{\left(|a| \cdot \prod_{i=1}^{d} \max(1, |\alpha_i|) \right)}_{\text{Mahler measure of } \alpha}$$

Good for computing h

from Ziyang's talk

Rem Other definition of $h(\alpha)$

✎ Arbitrary number field K: For $[x_0 : \cdots : x_n] \in \mathbb{P}^n(K)$ with each $x_j \in K$,
$h([x_0 : \cdots : x_n]) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in \Sigma_K} \log \max\{\|x_0\|_v, \ldots, \|x_n\|_v\}$.

→ here $h(\alpha) = h([\alpha : 1])$

Good for proving theorems on h

§1. Measuring algebraic numbers

Def Let $\alpha \in \overline{\mathbb{Q}}$ and let $p_\alpha(x) = a \cdot (x-\alpha_1) \cdots (x-\alpha_d) \in \mathbb{Z}[x]$ be its minimal polynomial. The <u>(absolute logarithmic Weil) height of α</u> is

$$h(\alpha) = \frac{1}{d} \log\left(|a| \cdot \prod_{i=1}^{d} \max(1, |\alpha_i|)\right)$$

Ex If $\alpha = \frac{a}{b} \in \mathbb{Q}$, $\gcd(a,b) = 1 \Rightarrow h(\alpha) = \log\max(|a|, |b|)$

Rem (1) h "measures the arithmetic complexity" on $\overline{\mathbb{Q}}$

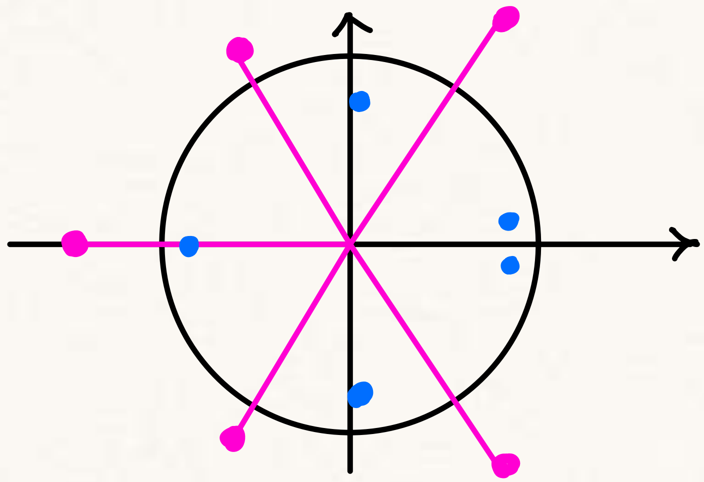
Ex $\dfrac{2^{1000}-1}{2^{1000}} \sim 1$ but $h\left(\dfrac{2^{1000}-1}{2^{1000}}\right) = 1000 \log 2$ while $h(1) = 0$!

(2) h gives informations on the distribution of the conjugates of α around the unit circle

Ex If α is a root of

$$x^{10} + 3x^7 - 6x^4 + 3$$

$$h(\alpha) = 0.59085\ldots$$



§1. Measuring algebraic numbers

Def Let $\alpha \in \overline{\mathbb{Q}}$ and let $p_\alpha(x) = a \cdot (x-\alpha_1) \cdots (x-\alpha_d) \in \mathbb{Z}[x]$ be its minimal polynomial. The (absolute logarithmic Weil) height of α is

$$h(\alpha) = \frac{1}{d} \log\left(|a| \cdot \prod_{i=1}^{d} \max(1, |\alpha_i|)\right)$$

(3) Some properties of h:

- $h(\alpha^n) = |n| \cdot h(\alpha)$ for $n \in \mathbb{Z}$
- $h(\alpha\beta) \leq h(\alpha) + h(\beta)$
- $h(\alpha+\beta) \leq h(\alpha) + h(\beta) + \log 2$
- $h(\sigma(\alpha)) = h(\alpha)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$
- $h(\alpha) \geq 0$ for all $\alpha \in \overline{\mathbb{Q}}$

Q: What are the algebraic numbers of height 0?

Thm (Kronecker) Let $\alpha \in \overline{\mathbb{Q}}^*$. Then $h(\alpha) = 0 \iff \alpha$ is a root of unity.

Q (vague): What can be said on algebraic numbers having non-zero, but "small" height?

§2. Small height

Q. Let $B > 0$. How many algebraic numbers have height $\leq B$?
Infinitely many!
Ex. · All roots of unity
· If $n \geq \frac{\log 2}{B} \Rightarrow h(2^{1/n}) = \frac{\log 2}{n} \leq B$

Q. How many algebraic numbers have bounded height & degree?

<u>Theorem</u> (Northcott, '49) For any integer $d \geq 1$ and real $B > 0$ we have
$$\#\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha):\mathbb{Q}] \leq d,\ h(\alpha) \leq B\} < \infty.$$

NORTHCOTT (D. G.). - An inequality in the theory of arithmetic on algebraic varieties, Proc. Cambridge philos. Soc., t. 45, 1949, p. 502-509.

§2. Small height

Q. Let $B>0$. How many algebraic numbers have height $\leq B$?
Infinitely many!
Ex. · All roots of unity
· If $n \geq \frac{\log 2}{B} \Rightarrow h(2^{1/n}) = \frac{\log 2}{n} \leq B$

Q. How many algebraic numbers have bounded height & degree?

Theorem (Northcott, '49) For any integer $d \geq 1$ and real $B>0$ we have
$$\#\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha):\mathbb{Q}] \leq d,\ h(\alpha) \leq B\} < \infty.$$

Rem · Proof is effective!
· Height: important tool in Diophantine geometry
E.g. bound for the height of rational points on some curve $\Rightarrow$ finiteness of the set + explicit list of its elements!
↑ **Effective Mordell** (cf Ziyang's talk)

§2. Small height

Q. Let $B>0$. How many algebraic numbers have height $\leq B$?
Infinitely many!
Ex · All roots of unity
· If $n \geq \frac{\log 2}{B} \Rightarrow h(2^{1/n}) = \frac{\log 2}{n} \leq B$

Q. How many algebraic numbers have bounded height & degree?

Theorem (Northcott, '49) For any integer $d \geq 1$ and real $B>0$ we have
$$\#\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha):\mathbb{Q}] \leq d,\ h(\alpha) \leq B\} < \infty.$$

Rem
- Proof is effective!
- Height: important tool in Diophantine geometry
  E.g. bound for the height of rational points on some curve $\Rightarrow$ finiteness of the set + explicit list of its elements!
- By Northcott, if $(\alpha_n)_n$ infinite sequence of small points
  $\Rightarrow$ the degrees $[\mathbb{Q}(\alpha_n):\mathbb{Q}]$ must grow. How?

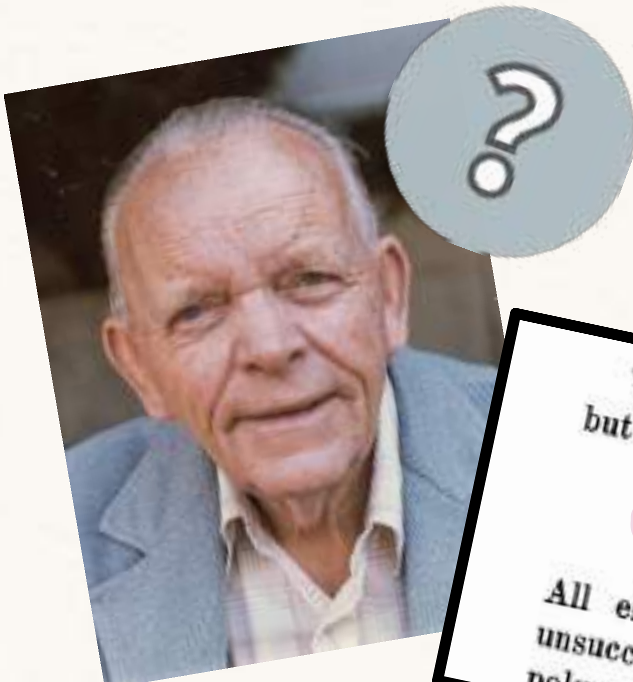
§2. Small height

Lehmer's Conjecture ('33) [Small non-zero height $\Rightarrow$ big degree]
There exists a real number $c>0$ such that, for every $\alpha \in \overline{\mathbb{Q}}$, the product $[\mathbb{Q}(\alpha):\mathbb{Q}] \cdot h(\alpha)$ is either 0 or $\geq c$.

§2. Small height

Lehmer's ~~Conjecture~~ ('33) [Small non-zero height ⇒ big degree]

There exists a real number $c>0$ such that, for every $\alpha \in \overline{\mathbb{Q}}$, the product $[\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha)$ is either 0 or $\geq c$.



13. A problem in the theory of equations. The following problem arises immediately. *If ε is a positive quantity, to find a polynomial of the form*

$$f(x) = x^r + a_1 x^{r-1} + \cdots + a_r$$

where the a's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 *and* $1+\varepsilon$.

This problem, of interest in itself, is especially important for our pur- ... Whether or not the problem has a solution for $\varepsilon < 0.176$ we do

We have not made an examination of all 10th degree symmetric polynomials but a rather intensive search has failed to reveal a better polynomial than

$$x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1, \quad \Omega = 1.176280821.$$

All efforts to find a better equation of degree 12 and 14 have been unsuccessful. Poulet has made a similar investigation of symmetric polynomials with practically the same results.

Factorization of Certain Cyclotomic Functions
Author(s): D. H. Lehmer
Source: *Annals of Mathematics*, Second Series, Vol. 34, No. 3 (Jul., 1933), pp. 461-479

§2. Small height

Lehmer's Conjecture ('33) [Small non-zero height ⇒ big degree]
There exists a real number $c>0$ such that, for every $\alpha\in\overline{\mathbb{Q}}$, the product $[\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha)$ is either 0 or $\geq c$.

Rem. Proved for many classes of $\alpha\in\overline{\mathbb{Q}}$, but open in general

→ Some known cases

* Easy if α not algebraic integer ($h(\alpha)\geq \frac{\log 2}{d}$)
* (Smyth, '71) α not reciprocal (ie α and $1/\alpha$ not conj.) with $c=\log(1.324717\ldots)=\log M(x^3-x-1)$
* (Amoroso-David, '99) $\alpha\in\overline{\mathbb{Q}}$ such that $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois
  ↳ Even better result by Amoroso-Masser ('14)

§2. Small height

Lehmer's Conjecture ('33) [Small non-zero height $\Rightarrow$ big degree]
There exists a real number $c>0$ such that, for every $\alpha \in \overline{\mathbb{Q}}$, the product $[\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha)$ is either 0 or $\geq c$.

<u>Rem</u> · Proved for many classes of $\alpha \in \overline{\mathbb{Q}}$, but open in general

· Best unconditional result by Dobrowolski ('79): if $d = [\mathbb{Q}(\alpha):\mathbb{Q}]$ and $d\,h(\alpha) \neq 0$, then $d\,h(\alpha) \geq c\left(\frac{\log\log d}{\log d}\right)^3$ ($c = \frac{1}{4}$, Voutier, '96)

· Conjectural constant
$c = \log(1.17628\ldots)$

· Dimitrov ('19): proved the Schinzel-Zassenhaus Conj. (weak form of Lehmer's conjecture)

Conj $\exists\, c>0$ such that, if $\alpha \in \overline{\mathbb{Q}}$, $h(\alpha) \neq 0$ and $\overline{|\alpha|} := \max\begin{pmatrix}\text{absolute values of}\\ \text{conjugates of } \alpha\end{pmatrix} \Rightarrow \log \overline{|\alpha|} \geq \frac{c}{[\mathbb{Q}(\alpha):\mathbb{Q}]}$

$c = (\log 2)/4$ in Dimitrov's proof

<u>Rem</u> Lehmer $\Rightarrow$ SZ (as $\log\overline{|\alpha|} \geq h(\alpha)$)

§2. Small height

Lehmer's Conjecture ('33) [Small non-zero height $\Rightarrow$ big degree]
There exists a real number $c>0$ such that, for every $\alpha \in \overline{\mathbb{Q}}$, the product $[\mathbb{Q}(\alpha):\mathbb{Q}]\cdot h(\alpha)$ is either 0 or $\geq c$.

Rem. • Proved for many classes of $\alpha \in \overline{\mathbb{Q}}$, but open in general

• Best unconditional result by Dobrowolski ('79): if $d=[\mathbb{Q}(\alpha):\mathbb{Q}]$ and $d\,h(\alpha)\neq 0$, then $d\,h(\alpha) \geq c\left(\frac{\log\log d}{\log d}\right)^3$ ($c=\frac{1}{4}$, Voutier, '96)

• Conjectural constant
$c = \log(1.17628\ldots)$

• Dimitrov ('19): proved the Schinzel-Zassenhaus Conj.

• Breuillard & Varjú ('21): Lehmer $\Longleftrightarrow$ Uniform growth conjecture

Conj For all $d>1$, $\exists\, c=c(d)>0$ such that:
if $S \subset GL_d(\mathbb{C})$ finite, then $\rho(S) := \lim_{n\to\infty} \frac{1}{n} \log|S^n|$

set of all products of n elements in S

rate of exponential growth

§2. Small height

<u>Lehmer's Conjecture</u> ('33) [Small non-zero height $\Rightarrow$ big degree]
There exists a real number $c > 0$ such that, for every $\alpha \in \overline{\mathbb{Q}}$, the product $[\mathbb{Q}(\alpha):\mathbb{Q}] \cdot h(\alpha)$ is either 0 or $\geq c$.

<u>Theorem</u> (Northcott, '49) For any integer $d \geq 1$ and real $B > 0$ we have
$$\#\{\alpha \in \overline{\mathbb{Q}} \mid [\mathbb{Q}(\alpha):\mathbb{Q}] \leq d,\ h(\alpha) \leq B\} < \infty.$$

<u>Q</u> Are there subsets of $\overline{\mathbb{Q}}$ where even stronger statements hold?

§3. Properties (N) and (B)

Def (Bombieri–Zannier, '01)

A subfield $L \subseteq \overline{\mathbb{Q}}$ is said to have:

- the Northcott property (N) if $\forall B > 0$, $\#\{\alpha \in L \mid h(\alpha) \leq B\} < \infty$.
- the Bogomolov property (B) if $\exists c = c(L) > 0$ such that $\forall \alpha \in L$ either $h(\alpha) = 0$ or $h(\alpha) \geq c$.

Rem
- Fields with (N) satisfy a strong form of Northcott's theorem.
- Fields with (B) satisfy a strong form of Lehmer's conj.
- (N) $\Rightarrow$ (B) [easy]
- (B) $\not\Rightarrow$ (N)

Ex (1) $L = \mathbb{Q}^{ab}$ maximal abelian ext. of $\mathbb{Q}$

$\to$ has (B) (Amoroso–Dvornicich, 2000)

§3. Properties (N) and (B)

<u>Def</u> (Bombieri-Zannier, '01)

A subfield $L \subseteq \overline{\mathbb{Q}}$ is said to have:

- the <u>Northcott property (N)</u> if $\forall B>0$, $\#\{\alpha \in L \mid h(\alpha) \leq B\} < \infty$.
- the <u>Bogomolov property (B)</u> if $\exists c = c(L) > 0$ such that $\forall \alpha \in L$ either $h(\alpha) = 0$ or $h(\alpha) \geq c$.

<u>Rem</u>
- Fields with (N) satisfy a strong form of Northcott's theorem.
- Fields with (B) satisfy a strong form of Lehmer's conj.
- (N) $\Rightarrow$ (B) [easy]
- (B) $\not\Rightarrow$ (N)

<u>Ex</u> (2) $L = \mathbb{Q}^{tr}$ field of totally real numbers

$\rightarrow$ L has (B) (Schinzel, '73)

$\rightarrow$ L has not (N): $\zeta_n + \zeta_n^{-1} \in \mathbb{Q}^{tr}$ & $h(\zeta_n + \zeta_n^{-1}) \leq \log 2$

§3. Properties (N) and (B)

<u>Def</u> (Bombieri–Zannier, '01)

A subfield $L\subseteq\overline{\mathbb{Q}}$ is said to have:

- the <u>Northcott property (N)</u> if $\forall B>0$, $\#\{\alpha\in L \mid h(\alpha)\le B\}<\infty$.
- the <u>Bogomolov property (B)</u> if $\exists\, c=c(L)>0$ such that $\forall \alpha\in L$ either $h(\alpha)=0$ or $h(\alpha)\ge c$.

<u>Rem</u>.

L number field
has (N) & (B)
[by Northcott's thm]

?

$L=\overline{\mathbb{Q}}$
neither (B) nor (N)
$[\,h(2^{1/n})=\frac{\log 2}{n}\to 0\,]$

Pb Given a subfield $L\subseteq\overline{\mathbb{Q}}$ of infinite degree over $\mathbb{Q}$, decide whether it has or not property (N) or (B)

HARD in general!

§3. Properties (N) and (B)

- We will see what is known on this problem
- Nowadays: many examples of fields with (B) or (N) but they essentially can be all put in one of the following families

fields obtained "adding some torsion"

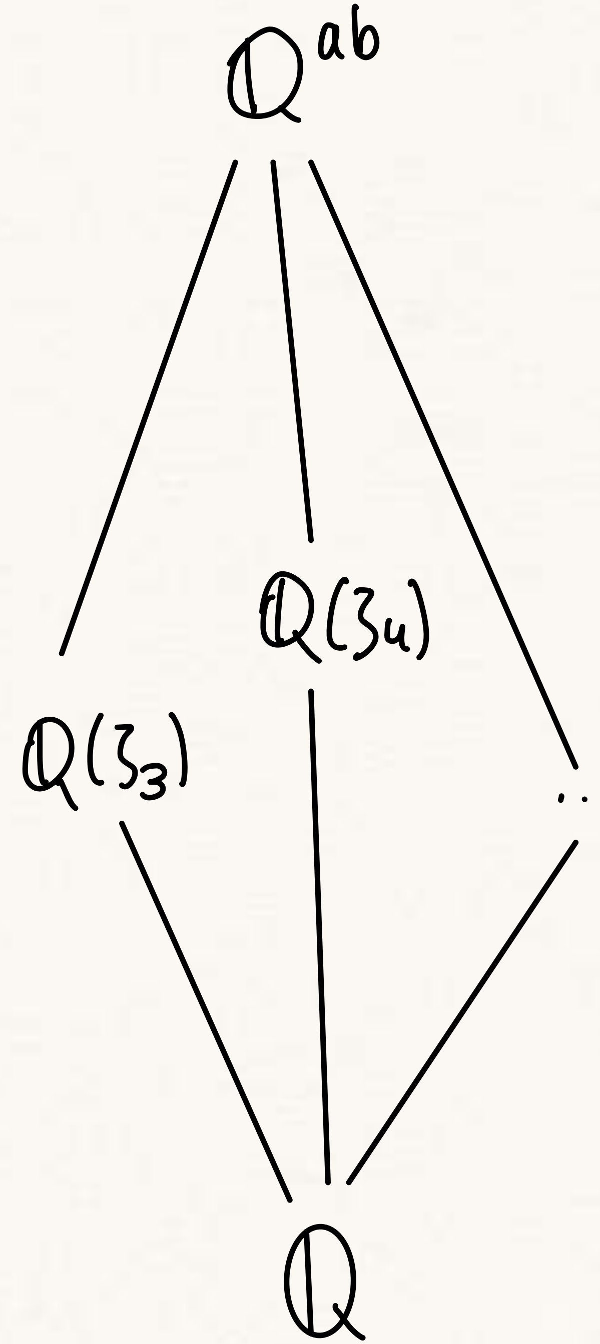
fields satisfying "some local conditions"

§4. Fields obtained "adding torsion"

Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B)
(Amoroso - Dvornicich, '00)



§4. Fields obtained "adding torsion"

Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B)
(Amoroso - Dvornicich, '00)

Rem More generally if K number field K^{ab} has (B)
(Amoroso - Zannier, '00 - '10)

$\mathbb{Q}^{ab}$

$\mathbb{Q}$

§4. Fields obtained "adding torsion"

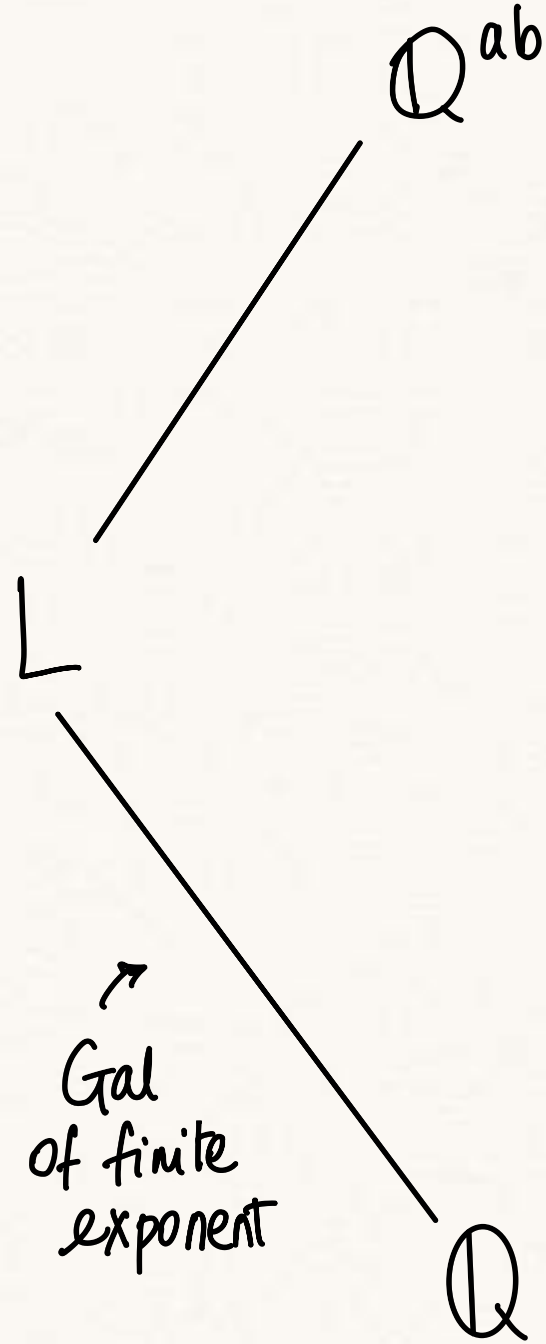
Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B) (Amoroso-Dvornicich, '00)

(ii) it has not (N)

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}^{ab}$ & $\mathrm{Gal}(L/\mathbb{Q})$ has finite exponent $\Rightarrow$ L has (N) (Bombieri, Zannier, '01)



§4. Fields obtained "adding torsion"

Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B)
(Amoroso-Dvornicich, '00)

(ii) it has not (N)

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}^{ab}$ & $Gal(L/\mathbb{Q})$ has finite exponent
$\Rightarrow L$ has (N)
(Bombieri, Zannier, '01)

$\mathbb{Q}^{ab}$

L

Gal of finite exponent

$\mathbb{Q}$

Recall

A group G has finite exponent if there exists an integer n>0 such that g^n is the identity for all g in G.

Examples:

- $L = \mathbb{Q}^{(d)}_{ab}$ compositum of all abelian extensions of $\mathbb{Q}$ of deg $\leq d$
  - $[\mathbb{Q}^{(d)}_{ab} : \mathbb{Q}] = \infty$ for $d \geq 2$
  - $\exp(Gal) \leq d!$

§4. Fields obtained "adding torsion"

Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B) (Amoroso - Dvornicich, '00)

(ii) it has not (N)

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}^{ab}$ & $\mathrm{Gal}(L/\mathbb{Q})$ has finite exponent $\Rightarrow L$ has (N) (Bombieri, Zannier, '01)

$\mathbb{Q}^{ab}$

Recall

A group G has finite exponent if there exists an integer n>0 such that g^n is the identity for all g in G.

More generally: K numb. field

- $K^{(d)}_{ab}$ = compositum of all ext's of K of deg $\leq d$ and has (N) (Bz '01)
- L/K Galois abelian. $\mathrm{Gal}(L/K)$ has bounded exp $\Leftrightarrow L \subseteq K^{(d)}_{ab}$ for some d (C. Zannier, '11)

d

r $d \geq 2$

d!

of ... exponent

$\mathbb{Q}$

§4. Fields obtained "adding torsion"

Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B)
(Amoroso - Dvornicich, '00)

(ii) it has not (N)

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}^{ab}$ & $\mathrm{Gal}(L/\mathbb{Q})$ has finite exponent
$\Rightarrow$ L has (N)
(Bombieri, Zannier, '01)

Q. What if try with another G?

$\mathbb{Q}^{ab}$

Recall

s finite
xists an
hat g^n
all g in G.

L

Gal of finite exponent

$\mathbb{Q}$

- $L = \mathbb{Q}^{(d)}_{ab}$

compositum of all abelian extensions of $\mathbb{Q}$ of deg $\leq d$

* $[\mathbb{Q}^{(d)}_{ab} : \mathbb{Q}] = \infty$ for $d \geq 2$

* $\exp(\mathrm{Gal}) \leq d!$

§4. Fields obtained "adding torsion"

Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B) ☐

(Amoroso-Dvornicich, '00)

(ii) it has (N)

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}^{ab}$ & $Gal(L/\mathbb{Q})$ has finite exponent $\Rightarrow L$ has (N)

(Bombieri, Zannier, '01)

Rem It is true more generally that $K(E_{tors})$ has (B) when $K/\mathbb{Q}$ is Galois and $Gal(K/\mathbb{Q})$ has bounded exponent [but E still defined $/\mathbb{Q}$!] (Frey, '22)

Recipe

elliptic diet

- Take $\mathbb{Q}$
- Add coord. of all torsion pts of $G = E$ elliptic curve $/\mathbb{Q}$
- Get $\mathbb{Q}(E_{tors})$: not abelian over $\mathbb{Q}$, but ...

(i) it has (B) ☑

(Habegger, '13)

§4. Fields obtained "adding torsion"

Recipe

- Take $\mathbb{Q}$
- Add to it all torsion points of $G = \mathbb{G}_m(\overline{\mathbb{Q}})$
- Get $\mathbb{Q}^{ab}$ = max abelian ext. of $\mathbb{Q}$

(i) it has (B) ✓
(Amoroso-Dvornicich, '00)

(ii) it has not (N) ✓

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}^{ab}$ & $\mathrm{Gal}(L/\mathbb{Q})$ has finite exponent $\Rightarrow L$ has (N) ✓
(Bombieri, Zannier, '01)

Recipe

elliptic diet

- Take $\mathbb{Q}$
- Add coord. of all torsion pts of $G = E$ elliptic curve $/\mathbb{Q}$
- Get $\mathbb{Q}(E_{tors})$: not abelian over $\mathbb{Q}$, but ...

(i) it has (B) ✓
(Habegger, '13)

(ii) it has not (N) ✓
(∞ many roots of unity)

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}(E_{tors})$ & $\mathrm{Gal}(L/\mathbb{Q})$ has finite exponent $\Rightarrow$ L has (N) ✓
(C. Dill, '23)

§4. Fields obtained "adding torsion"

★ More generally & more precisely

Thm (C. Dill '23) Let K be a number field and A an abelian variety $/K$. If $L \subseteq K(A_{tors})$, L/K is Galois and $\exp(Gal(L/K)) \leq d$, then $L \subseteq M_{ab}^{(d)}$ for some number field M depending only on K, A and d.

Rem (1) No new fields with (N)!
($M_{ab}^{(d)}$ has (N) by Bombieri-Zannier)

(2) New analogy between $\mathbb{Q}(A_{tors})$ and $\mathbb{Q}^{ab}$

Q $\mathbb{Q}(A_{tor})$ has (B)? **OPEN!**

Recipe — elliptic diet

- Take $\mathbb{Q}$
- Add coord. of all torsion pts of $G = E$ elliptic curve $/\mathbb{Q}$
- Get $\mathbb{Q}(E_{tors})$: not abelian over $\mathbb{Q}$, but ...

(i) it has (B) ☑
(Habegger, '13)

(ii) it has not (N) ☑
(∞ many roots of unity)

(iii) If $L/\mathbb{Q}$ Galois, ☑
$L \subseteq \mathbb{Q}(E_{tors})$ & $Gal(L/\mathbb{Q})$ has finite exponent $\Rightarrow$ L has (N)
(C. Dill, '23) ★

§4. Fields obtained "adding torsion"

☆ More generally & more precisely

Thm (C. Dill '23) Let K be a number field and A an abelian variety $/K$. If $L \subseteq K(A_{tors})$, L/K is Galois and $\exp(Gal(L/K)) \leq d$, then $L \subseteq M_{ab}^{(d)}$ for some number field M depending only on K, A and d.

Rem (3) Recently (11 Jan 2024) Gajda & Petersen showed that our thm holds also over other base fields K (ie. K/k finitely generated ext. with k finite field or alg. closed field or local field)

Recipe

elliptic diet

- Take $\mathbb{Q}$
- Add coord. of all torsion pts of $G = E$ elliptic curve $/\mathbb{Q}$
- Get $\mathbb{Q}(E_{tors})$: not abelian over $\mathbb{Q}$, but ...

(i) it has (B) ☑
(Habegger, '13)

(ii) it has not (N) ☑
(∞ many roots of unity)

(iii) If $L/\mathbb{Q}$ Galois, $L \subseteq \mathbb{Q}(E_{tors})$ & $Gal(L/\mathbb{Q})$ has finite exponent $\Rightarrow$ L has (N) ☑
(C. Dill, '23) ☆

§5. Fields satisfying local conditions

Property (B)

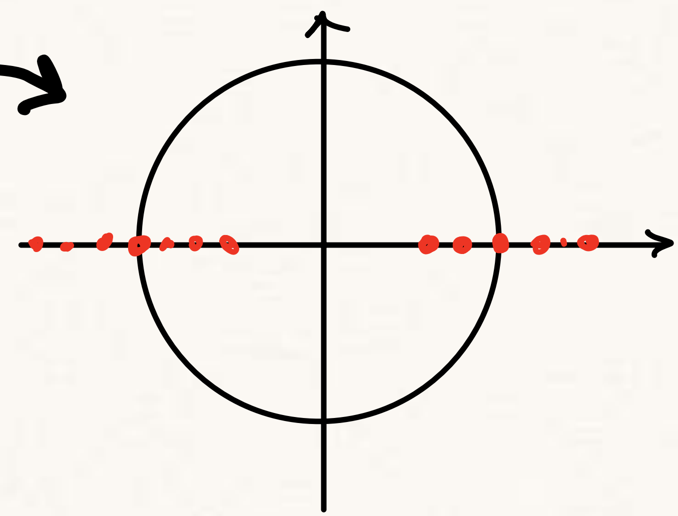
- $\mathbb{Q}^{tr}$ = field of totally real numbers has (B)

  (Schinzel, '73) If $\alpha \in \mathbb{Q}^{tr} \setminus \{\pm 1\}$, $h(\alpha) \geq \frac{1}{2} \log\left(\frac{1+\sqrt{5}}{2}\right)$

  Rem Non quantitative version follows from Bilu's theorem

  Roughly: Galois orbits of sequences of points with height tending to 0 must be "equidistributed" around the unit circle

But points in $\mathbb{Q}^{tr}$ are clearly not equidistributed...
so they can't be too small



§5. Fields satisfying local conditions

Property (B)

- $\mathbb{Q}^{tr}$ = field of totally real numbers has (B)

  (Schinzel, '73) If $\alpha \in \mathbb{Q}^{tr} \setminus \{\pm 1\}$, $h(\alpha) \geq \frac{1}{2} \log\left(\frac{1+\sqrt{5}}{2}\right)$

  Rem A 1 page proof
  for algebraic integers in $\mathbb{Q}^{tr}$
  was given by
  Höhn & Skoruppa ('93)

Journal de Théorie des Nombres
de Bordeaux 5 (1993), 185

Un résultat de Schinzel

par G. Höhn et N.-P. Skoruppa

$$H(\alpha) \geq \left(\frac{1+\sqrt{5}}{2}\right)^{1/2}.$$

$$\max(1, |x|) \cdot \left(\frac{1+\sqrt{5}}{2}\right)^{-1/2} \geq f(x).$$

D'autre part on a

Bibliographie

[5] A. Schinzel, Addendum to the paper "On the product of the conjugates outside the unit circle of an algebraic number" Acta Arith.

Max-Planck-Institut für Mathematik
Gottfried-Claren-Strasse 26
Bonn
ALLEMAGNE

§5. Fields satisfying local conditions

Property (B)

- $\mathbb{Q}^{tr}$ = field of totally real numbers has (B)
- $\mathbb{Q}^{tp}$ = field of totally p-adic numbers has (B) (Bombieri, Zannier '01)

  ↖ compositum of all Galois extensions of $\mathbb{Q}$ in which p splits totally

More generally:

<u>Thm</u> (Bombieri, Zannier, '01) Let $L|\mathbb{Q}$ be a Galois ext.
Let $S(L) = \{p \text{ prime} \mid L \text{ has bounded local degree at } p\}$
(i.e. $\forall p \in S(L)$, L can be embedded in a finite ext. of $\mathbb{Q}_p$)
Then, if $S(L) \neq \emptyset$, L has (B) and

$$\liminf_{\alpha \in L} h(\alpha) \geq \frac{1}{2} \sum_{p \in S(L)} \frac{\log p}{e_p(p^{f_p} + 1)}$$

inertial degree of L at p

ramification index of L at p

§5. Fields satisfying local conditions

Property (B)

- (Amoroso, David, Zannier, '14):
  K number field, $L|K$ Galois & Z = center of $\mathrm{Gal}(L|K)$.
  If L^Z has bounded local degrees at some prime, L has (B).

→ This implies:

- BZ theorem
- K^{ab} has (B) $(L^Z = K)$

§5. Fields satisfying local conditions

Property (N)

- (Bombieri, Zannier, '01) $K_{ab}^{(d)}$ has (N)
- (Widmer, '13) Let $K = K_0 \subsetneq K_1 \subsetneq \dots$ tower of n. fields s.t. the relative discriminants have "sufficiently rapid" growth at each non-trivial step within the tower $\Rightarrow \bigcup_{i=0}^{\infty} K_i$ has (N).

§5. Fields satisfying local conditions

Property (N)

- (Bombieri, Zannier, '01) $K_{ab}^{(d)}$ has (N)
- (Widmer, '13) Let $K = K_0 \subsetneq K_1 \subsetneq \ldots$ tower [...] the relative discriminants have "suffici[...] [...]h at each non-trivial step within the to[...] [...]N).

(Widmer, 24)
New criterion (based again on discriminants growth) that implies both his previous result and BZ's thm

§5. Fields satisfying local conditions

Property (N)

- (Bombieri, Zannier, '01) $K^{(d)}_{ab}$ has (N)
- (Widmer, '13) Let $K = K_0 \subsetneq K_1 \subsetneq \dots$ tower
  the relative discriminants have "suffic
  at each non-trivial step within the t (N).

(Widmer, 24)
New criterion (based again on discriminants growth) that implies both his previous result and Bz's thm

Q Other results on (N)?

→ Recall: if $L|\mathbb{Q}$ Galois with bounded local deg. at all $p \in S(L) \neq \emptyset$

$$\liminf_{\alpha \in L} h(\alpha) \geq \beta(L) = \frac{1}{2} \sum_{p \in S(L)} \frac{\log p}{e_p(p^{f_p}+1)} \qquad \text{(Bz '01)}$$

Rem Bz remarked that:

- if $\beta(L) = +\infty \Rightarrow L$ has also (N)
- if L number field $\Rightarrow \beta(L) = +\infty$

Q: $\exists\, L|\mathbb{Q}$ of infinite degree st. $\beta(L) = +\infty$?
And that moreover do not satisfy some previous criteria for (N)?

§5. Fields satisfying local conditions

Property (N)

- (Bombieri, Zannier, '01) $K^{(d)}_{ab}$ has (N)
- (Widmer, '13) Let $K = K_0 \subsetneq K_1 \subsetneq \dots$ tower
  the relative discriminants have "suffic
  at each non-trivial step within the to

Q Other results on (N)?

→ Recall: if $L/\mathbb{Q}$ Galois with bounded loca ϕ

$$\liminf_{\alpha \in L} h(\alpha) \geq \beta(L) = \frac{1}{2} \sum_{p \in S(L)} \frac{\log p}{e_p (p^{f_p}}$$

Rem BZ remarked that:

* if $\beta(L) = +\infty \Rightarrow L$ has also (N)
* if L number field $\Rightarrow \beta(L) = +\infty$

Q: $\exists\, L/\mathbb{Q}$ of infinite degree st. $\beta(L) = +\infty$?
And that moreover do not satisfy some previous criteria for (N)?

(Widmer, '24)
New criterion (based again on discriminants growth) that implies

(C. Fehm, '21) Yes!
There are "many" Galois ext. $L/\mathbb{Q}$ st.

* $[L:\mathbb{Q}] = \infty$
* $\beta(L) = +\infty$
* L does not satisfy the conditions neither of BZ's thm nor of Widmer's 1st result

§5. Fields satisfying local conditions

Property (N)

- (Bombieri, Zannier, '01) $K^{(d)}_{ab}$ has (N)
- (Widmer, '13) Let $K = K_0 \subsetneq K_1 \subsetneq \dots$ tower ... h
  the relative discriminants have "suffic... at each non-trivial step within the t... .

(Widmer, 24) New criterion (based again on discriminants growth) that implies

Q Other results on (N)?

→ Recall: if $L|\mathbb{Q}$ Galois with bounded loca... ϕ

$$\liminf_{\alpha \in L} h(\alpha) \geq \beta(L) = \frac{1}{2} \sum_{p \in S(L)} \frac{\log p}{e_p(p^{f_p} \dots}$$

Rem BZ remarked that:

* if $\beta(L) = +\infty \Rightarrow L$ has also (N)
* if L number field $\Rightarrow \beta(L) = +\infty$

Q: $\exists\, L|\mathbb{Q}$ of infinite degree st. $\beta(L) = +\infty$?
And that moreover do not satisfy some previous criteria for (N)?

(C. Fehm, '24) Yes! There are "many" Galois ext. $L|\mathbb{Q}$ st.

* $[L:\mathbb{Q}] = \infty$
* $\beta(L) = +\infty$
* L does not satisfy the conditions neither of BZ's thm nor of Widmer's 1st result nor of Widmer's new thm

§6. Some open problems

(1) <u>On property (N)</u>. We saw that:

if $L/\mathbb{Q}$ abelian & $\mathrm{Gal}(L/\mathbb{Q})$ has bounded exponent $\Rightarrow$ L has (N)

§6. Some open problems

(1) <u>On property (N)</u>. We saw that:

Q. if $L/\mathbb{Q}$ ~~abelian~~ & $\mathrm{Gal}(L/\mathbb{Q})$ has bounded exponent $\overset{?}{\Rightarrow}$ L has (N)

Simplest case:

Does $\mathbb{Q}^{(3)} =$ compositum of all n.fields of deg ≤ 3 have (N)? **Open!**

§6. Some open problems

(2) On property (B).

- We saw that Lehmer Conjecture was proved for generators of Galois extensions (Amoroso, David, '99). Moreover
- (Amoroso, Masser, '16) $\forall \varepsilon > 0$, $\exists c(\varepsilon)$ such that if $\alpha \in \overline{\mathbb{Q}}^*$ not a root of unity and $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois then $h(\alpha) \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}]^{\varepsilon} \geq c(\varepsilon)$.

Open!

Q. Does the set $S = \{\alpha \in \overline{\mathbb{Q}} \mid \mathbb{Q}(\alpha)/\mathbb{Q} \text{ Galois}\}$ have (B)?

□ One can study subsets $S_G = \{\alpha \in S \mid \mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q}) = G\}$

* (Amoroso, Dvornicich '00) S_G has (B) when G abelian.
* (Amoroso, '16) If $G = S_n$ and $\alpha \in S_G$ is a product of conjugated units or linear comb. of conjugates $\Rightarrow h(\alpha) \xrightarrow[n \to \infty]{} +\infty$
* (Jenvrin, '24) Same conclusion for $G = A_n$

Conj. (Amoroso '16) If $\mathbb{Q}(\alpha)/\mathbb{Q}$ Galois of group S_n, then $h(\alpha) \geq f(n) \to +\infty$ when $n \to +\infty$.

Thank you!