Diophantine avoidance, Ruppert's conjecture, and normal basis theorem

Lenny Fukshansky
Claremont McKenna College
(joint work with Sehun Jeong)

University of Minnesota Duluth

Primitive Element Theorem

The following observation was first made by Évariste Galois in 1831 for the case of splitting fields of polynomials over $\mathbb{Q}$. It was proved in full generality by Ernst Steinitz in 1910.

Primitive Element Theorem

The following observation was first made by Évariste Galois in 1831 for the case of splitting fields of polynomials over $\mathbb{Q}$. It was proved in full generality by Ernst Steinitz in 1910.

Theorem 1

Let K be a number field. Then there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.

Primitive Element Theorem

The following observation was first made by Évariste Galois in 1831 for the case of splitting fields of polynomials over $\mathbb{Q}$. It was proved in full generality by Ernst Steinitz in 1910.

Theorem 1

Let K be a number field. Then there exists $\theta \in K$ such that $K = \mathbb{Q}(\theta)$.

Such θ is called a **primitive element** for K. In fact, each number field contains infinitely many primitive elements.

Sketch of proof

Let $d = [K : \mathbb{Q}]$ and write

$$\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$$

for the embeddings of K. Some $\theta \in K$ is primitive if and only if

$$\sigma_i(\theta) \neq \sigma_j(\theta), \ \forall \ 1 \leqslant i < j \leqslant d.$$

Sketch of proof

Let $d = [K : \mathbb{Q}]$ and write

$$\sigma_1, \ldots, \sigma_d : K \to \mathbb{C}$$

for the embeddings of K. Some $\theta \in K$ is primitive if and only if

$$\sigma_i(\theta) \neq \sigma_j(\theta), \ \forall \ 1 \leqslant i < j \leqslant d.$$

Let $\beta_1, \ldots, \beta_d$ be a basis for K over $\mathbb{Q}$ and let

$$\theta = z_1\beta_1 + \cdots + z_d\beta_d,$$

for some coefficients $z_1, \ldots, z_d \in \mathbb{Q}$. We want to choose these coefficients in such a way that

$$\begin{aligned} P(z_1, \ldots, z_d) &= \prod_{1 \leqslant i < j \leqslant d} (\sigma_i(\theta) - \sigma_j(\theta)) \\ &= \prod_{1 \leqslant i < j \leqslant d} \left(\sum_{k=1}^{d} z_k(\sigma_i(\beta_k) - \sigma_j(\beta_k)) \right) \neq 0. \end{aligned}$$

Sketch of proof

Since $\beta_1, \ldots, \beta_d$ form a basis for $K/\mathbb{Q}$, it is not possible that

$$\sigma_i(\beta_k) = \sigma_j(\beta_k), \ \forall\ 1 \leqslant k \leqslant d,$$

for some $i \neq j$, which implies that the polynomial P is not identically zero.

Sketch of proof

Since $\beta_1, \ldots, \beta_d$ form a basis for $K/\mathbb{Q}$, it is not possible that

$$\sigma_i(\beta_k) = \sigma_j(\beta_k), \ \forall\ 1 \leqslant k \leqslant d,$$

for some $i \neq j$, which implies that the polynomial P is not identically zero. Hence, it is possible to find

$$\boldsymbol{z} = (z_1, \ldots, z_d) \in \mathbb{Q}^d$$

such that $P(\boldsymbol{z}) \neq 0$.

Sketch of proof

Since $\beta_1, \ldots, \beta_d$ form a basis for $K/\mathbb{Q}$, it is not possible that

$$\sigma_i(\beta_k) = \sigma_j(\beta_k), \ \forall\ 1 \leqslant k \leqslant d,$$

for some $i \neq j$, which implies that the polynomial P is not identically zero. Hence, it is possible to find

$$\boldsymbol{z} = (z_1, \ldots, z_d) \in \mathbb{Q}^d$$

such that $P(\boldsymbol{z}) \neq 0$. For this choice of $\boldsymbol{z}$,

$$\theta = \sum_{k=1}^{d} z_k \beta_k$$

is a primitive element for K.

Some remarks

- The *avoidance* idea is intrinsic to this proof: we are looking for a point $\boldsymbol{z} \in \mathbb{Q}^n$ *outside* of the zero locus of the polynomial P.

Some remarks

- The *avoidance* idea is intrinsic to this proof: we are looking for a point $\boldsymbol{z} \in \mathbb{Q}^n$ *outside* of the zero locus of the polynomial P.
- The zero locus

$$Z_P = \{\boldsymbol{x} \in \mathbb{R}^d : P(\boldsymbol{x}) = 0\}$$

is a $(d-1)$-dimensional hypersurface in $\mathbb{R}^d$, thus "most" points in $\mathbb{R}^d$ (and, by continuity, in $\mathbb{Q}^d$) do not lie in Z_P. Therefore, "most" elements of K are primitive.

Some remarks

- The *avoidance* idea is intrinsic to this proof: we are looking for a point $\boldsymbol{z} \in \mathbb{Q}^n$ *outside* of the zero locus of the polynomial P.
- The zero locus

$$Z_P = \{\boldsymbol{x} \in \mathbb{R}^d : P(\boldsymbol{x}) = 0\}$$

is a $(d-1)$-dimensional hypersurface in $\mathbb{R}^d$, thus "most" points in $\mathbb{R}^d$ (and, by continuity, in $\mathbb{Q}^d$) do not lie in Z_P. Therefore, "most" elements of K are primitive.

- **Non-vanishing principle:** A polynomial in d variables of degree m that is not identically zero cannot vanish at every point of the grid

$$\left\{\boldsymbol{x} \in \mathbb{Z}^d : \max_{1 \leqslant i \leqslant d} |x_i| \leqslant \left[\frac{m}{2}\right] + 1\right\}.$$

This observation allows to make the above proof effective by controlling the "size" of θ.

Diophantine avoidance

The avoidance method aims to explicitly construct points outside of an algebraic set while controlling their "size". This method has been developed in a wide variety of situations:

Diophantine avoidance

The avoidance method aims to explicitly construct points outside of an algebraic set while controlling their "size". This method has been developed in a wide variety of situations:

- In a vector space avoiding a subspace – Faltings, 1992

Diophantine avoidance

The avoidance method aims to explicitly construct points outside of an algebraic set while controlling their "size". This method has been developed in a wide variety of situations:

- In a vector space avoiding a subspace – Faltings, 1992
- In a lattice avoiding a union of smaller-rank sublattices – L.F., 2006, 2010; Gaudron, 2009; Gaudron & Remond, 2012

Diophantine avoidance

The avoidance method aims to explicitly construct points outside of an algebraic set while controlling their "size". This method has been developed in a wide variety of situations:

- In a vector space avoiding a subspace – Faltings, 1992
- In a lattice avoiding a union of smaller-rank sublattices – L.F., 2006, 2010; Gaudron, 2009; Gaudron & Remond, 2012
- In a lattice avoiding a union of same-rank sublattices – Henk & Thiel, 2014

Diophantine avoidance

The avoidance method aims to explicitly construct points outside of an algebraic set while controlling their "size". This method has been developed in a wide variety of situations:

- In a vector space avoiding a subspace – Faltings, 1992
- In a lattice avoiding a union of smaller-rank sublattices – L.F., 2006, 2010; Gaudron, 2009; Gaudron & Remond, 2012
- In a lattice avoiding a union of same-rank sublattices – Henk & Thiel, 2014
- In a lattice avoiding a polynomial hypersurface – L.F., 2006, 2010

Diophantine avoidance

The avoidance method aims to explicitly construct points outside of an algebraic set while controlling their "size". This method has been developed in a wide variety of situations:

- In a vector space avoiding a subspace – Faltings, 1992
- In a lattice avoiding a union of smaller-rank sublattices – L.F., 2006, 2010; Gaudron, 2009; Gaudron & Remond, 2012
- In a lattice avoiding a union of same-rank sublattices – Henk & Thiel, 2014
- In a lattice avoiding a polynomial hypersurface – L.F., 2006, 2010
- In a lattice avoiding a polynomial hypersurface and a union of same-rank sublattices – L.F. & Jeong, 2024

Diophantine avoidance

The avoidance method aims to explicitly construct points outside of an algebraic set while controlling their "size". This method has been developed in a wide variety of situations:

- In a vector space avoiding a subspace – Faltings, 1992
- In a lattice avoiding a union of smaller-rank sublattices – L.F., 2006, 2010; Gaudron, 2009; Gaudron & Remond, 2012
- In a lattice avoiding a union of same-rank sublattices – Henk & Thiel, 2014
- In a lattice avoiding a polynomial hypersurface – L.F., 2006, 2010
- In a lattice avoiding a polynomial hypersurface and a union of same-rank sublattices – L.F. & Jeong, 2024

Additional related work with avoidance conditions has also been done in quadratic spaces and multilinear varieties.

Weil height

We need to define an appropriate measure of size. With notation as above, let $\alpha \in K$ and

$$m_\alpha(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$$

be the minimal polynomial of α with leading coefficient a_n.

Weil height

We need to define an appropriate measure of size. With notation as above, let $\alpha \in K$ and

$$m_\alpha(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$$

be the minimal polynomial of α with leading coefficient a_n.

The **Weil height** of θ is defined as

$$h(\alpha) = \left(|a_n| \prod_{i=1}^{d} \max\{1, |\sigma_i(\alpha)|\} \right)^{1/d}.$$

Weil height

We need to define an appropriate measure of size. With notation as above, let $\alpha \in K$ and

$$m_\alpha(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$$

be the minimal polynomial of α with leading coefficient a_n.

The **Weil height** of θ is defined as

$$h(\alpha) = \left(|a_n| \prod_{i=1}^{d} \max\{1, |\sigma_i(\alpha)|\} \right)^{1/d}.$$

Northcott property: The set

$$\{\alpha \in K : h(\alpha) \leqslant B\}$$

is finite for every $B \in \mathbb{R}_{>0}$.

Ruppert's conjecture

In view of the infinitude of primitive elements in a number field, it is natural to ask for one of small height. In 1998, W. Ruppert formulated the following conjecture.

Conjecture 2

Let K be a number field of degree $d \geqslant 2$ and discriminant Δ_K. Then there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and

$$h(\theta) \ll_d |\Delta_K|^{\frac{1}{2d}}.$$

Ruppert's conjecture

In view of the infinitude of primitive elements in a number field, it is natural to ask for one of small height. In 1998, W. Ruppert formulated the following conjecture.

Conjecture 2

Let K be a number field of degree $d \geqslant 2$ and discriminant Δ_K. Then there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and

$$h(\theta) \ll_d |\Delta_K|^{\frac{1}{2d}}.$$

The conjecture has been proved:

- By Ruppert (1998) in the case when K is a quadratic or a totally real number field of prime degree.

Ruppert's conjecture

In view of the infinitude of primitive elements in a number field, it is natural to ask for one of small height. In 1998, W. Ruppert formulated the following conjecture.

Conjecture 2

Let K be a number field of degree $d \geqslant 2$ and discriminant Δ_K. Then there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and

$$h(\theta) \ll_d |\Delta_K|^{\frac{1}{2d}}.$$

The conjecture has been proved:

- By Ruppert (1998) in the case when K is a quadratic or a totally real number field of prime degree.
- By Vaaler and Widmer (2013) in the case when K has at least one real embedding.

Ruppert's conjecture

In view of the infinitude of primitive elements in a number field, it is natural to ask for one of small height. In 1998, W. Ruppert formulated the following conjecture.

Conjecture 2

Let K be a number field of degree $d \geqslant 2$ and discriminant Δ_K. Then there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and

$$h(\theta) \ll_d |\Delta_K|^{\frac{1}{2d}}.$$

The conjecture has been proved:

- By Ruppert (1998) in the case when K is a quadratic or a totally real number field of prime degree.
- By Vaaler and Widmer (2013) in the case when K has at least one real embedding.
- Further technical results in the case of a totally complex field by Akhtari, Vaaler and Widmer (2025).

Further results

On the other hand, the following general result has been obtained by Pazuki and Widmer (2021).

Theorem 3

Let K be a number field of degree $d \geqslant 2$ and discriminant Δ_K. Then there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and

$$h(\theta) \leqslant |\Delta_K|^{\frac{1}{d}}.$$

Further results

On the other hand, the following general result has been obtained by Pazuki and Widmer (2021).

Theorem 3

Let K be a number field of degree $d \geqslant 2$ and discriminant Δ_K. Then there exists an element $\theta \in K$ such that $K = \mathbb{Q}(\theta)$ and

$$h(\theta) \leqslant |\Delta_K|^{\frac{1}{d}}.$$

In fact, Pazuki & Widmer argument can be easily adapted to guarantee that $\theta \in \mathcal{O}_K$, the ring of integers of K. Further, given an ideal $I \subseteq \mathcal{O}_K$, it follows from Theorem 3 that there exists a primitive element $\theta \in I$ with

$$h(\theta) \leqslant \left(\mathbb{N}_K(I)^2 |\Delta_K|\right)^{\frac{1}{d}},$$

where $\mathbb{N}_K(I) = |\mathcal{O}_K/I|$ is the norm of I.

Avoidance conditions

The proofs of the above bounds do not utilize the avoidance method. Our first result uses the avoidance method, along with height inequalities and the geometry of numbers to obtain the following bound with additional conditions.

Avoidance conditions

The proofs of the above bounds do not utilize the avoidance method. Our first result uses the avoidance method, along with height inequalities and the geometry of numbers to obtain the following bound with additional conditions.

Theorem 4 (L.F., S. Jeong (2024))

Let $I \subseteq \mathcal{O}_K$ be an ideal and let $J_1, \ldots, J_s \subset I$ be proper distinct subideals of I. Then there exists a primitive element $\theta \in I \setminus \bigcup_{k=1}^{s} J_k$ such that

$$h(\theta) \ll_{K,s} \frac{\mathbb{N}_K(J)^{d+1}}{\mathbb{N}_K(I)},$$

where $J = J_1 \cdots J_s$,

Basis bound

If $K = \mathbb{Q}(\theta)$ has degree d, then

$$1, \theta, \ldots, \theta^{d-1}$$

forms a basis for $K/\mathbb{Q}$. Thus, Ruppert's conjecture implies that there exists such a basis with

$$\max_{0 \leqslant k \leqslant d-1} h(\theta^k) \ll_d |\Delta_K|^{\frac{d-1}{2d}}.$$

Basis bound

If $K = \mathbb{Q}(\theta)$ has degree d, then

$$1, \theta, \ldots, \theta^{d-1}$$

forms a basis for $K/\mathbb{Q}$. Thus, Ruppert's conjecture implies that there exists such a basis with

$$\max_{0 \leqslant k \leqslant d-1} h(\theta^k) \ll_d |\Delta_K|^{\frac{d-1}{2d}}.$$

Consider the situation when $K/\mathbb{Q}$ is a Galois extension. Then for every element $\beta \in K$, all the algebraic conjugates of β (i.e., roots of its minimal polynomial) are also in K. A **normal basis** for $K/\mathbb{Q}$ is a basis $\beta_1, \ldots, \beta_d$ consisting of algebraic conjugates. This is equivalent to saying that β is a primitive element and all of its algebraic conjugates are $\mathbb{Q}$-linearly independent.

Normal Basis Theorem

The following theorem has been proved by Emmy Noether (1932) in case of some number fields and extended by her student Max Deuring (1932) to all number fields.

Normal Basis Theorem

The following theorem has been proved by Emmy Noether (1932) in case of some number fields and extended by her student Max Deuring (1932) to all number fields.

Theorem 5

If K is number field which is a Galois extension of $\mathbb{Q}$, then there exists a normal basis $\beta_1, \ldots, \beta_d$ for $K/\mathbb{Q}$.

Normal Basis Theorem

The following theorem has been proved by Emmy Noether (1932) in case of some number fields and extended by her student Max Deuring (1932) to all number fields.

Theorem 5

If K is number field which is a Galois extension of $\mathbb{Q}$, then there exists a normal basis $\beta_1, \ldots, \beta_d$ for $K/\mathbb{Q}$.

We want to establish an effective version of this theorem, producing a normal basis of bounded height. While Ruppert's conjecture gives a basis of bounded height, it does not guarantee that it is a *normal* basis.

Sketch of proof

We start by describing the standard proof of the Normal Basis Theorem. Let $G = \{\sigma_1, \ldots, \sigma_d\}$ be the Galois group of $K/\mathbb{Q}$ with σ_1 being the identity, where we are identifying elements of G with the embeddings of K into $\mathbb{C}$. Let $\alpha \in \mathcal{O}_K$ be a primitive element, $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α and define

$$g(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}.$$

Let $D(x) = \det(\sigma_i\sigma_j(g(x)))$. This is a nonzero polynomial with integer coefficients and

$$\deg(D(x)) = d(d-1).$$

We want to choose $\alpha \in \mathcal{O}_K$ so that $D(\alpha) \neq 0$: if this is the case, then the conjugates of $g(\alpha)$ are $\mathbb{Q}$-linearly independent, hence, form a normal basis for K over $\mathbb{Q}$.

Sketch of proof

Now, let $\theta \in \mathcal{O}_K$ be a primitive element, then $1, \theta, \ldots, \theta^{d-1} \in \mathcal{O}_K$ is a basis for K over $\mathbb{Q}$. For a given vector $\boldsymbol{z} = (z_0, \ldots, z_{d-1}) \in \mathbb{Z}^d$, define

$$\alpha_{\boldsymbol{z}} = \sum_{k=0}^{d-1} z_k \theta^k \in \mathcal{O}_K. \tag{1}$$

Then $D(\alpha_{\boldsymbol{z}})$ is a polynomial in d variables $z_0, \ldots, z_{d-1}$ of degree $d(d-1)$, which is not identically zero. Hence, we can use our *non-vanishing principle* to pick a point $\boldsymbol{z} \in \mathbb{Z}^d$ so that $D(\alpha_{\boldsymbol{z}}) \neq 0$.

Sketch of proof

Now, let $\theta \in \mathcal{O}_K$ be a primitive element, then $1, \theta, \ldots, \theta^{d-1} \in \mathcal{O}_K$ is a basis for K over $\mathbb{Q}$. For a given vector $\boldsymbol{z} = (z_0, \ldots, z_{d-1}) \in \mathbb{Z}^d$, define

$$\alpha_{\boldsymbol{z}} = \sum_{k=0}^{d-1} z_k \theta^k \in \mathcal{O}_K. \tag{1}$$

Then $D(\alpha_{\boldsymbol{z}})$ is a polynomial in d variables $z_0, \ldots, z_{d-1}$ of degree $d(d-1)$, which is not identically zero. Hence, we can use our *non-vanishing principle* to pick a point $\boldsymbol{z} \in \mathbb{Z}^d$ so that $D(\alpha_{\boldsymbol{z}}) \neq 0$.

The above argument again relies on the avoidance idea: we are picking a point outside of a hypersurface. Picking θ to be a small-height generator for K (in the spirit of *Ruppert's conjecture*) helps us to make this argument effective to obtain the following result.

Effective version of the Normal Basis Theorem

Theorem 6 (L.F., S. Jeong (2026))

Let $K/\mathbb{Q}$ be a Galois extension of degree $d \geqslant 2$. There exists a normal basis $\beta_1, \ldots, \beta_d$ for K over $\mathbb{Q}$ so that

$$h(\beta_i) \ll_d |\Delta_K|^{(d-1)(4d-3)},$$

for all $1 \leqslant i \leqslant d$.

Effective version of the Normal Basis Theorem

Theorem 6 (L.F., S. Jeong (2026))

Let $K/\mathbb{Q}$ be a Galois extension of degree $d \geqslant 2$. There exists a normal basis $\beta_1, \ldots, \beta_d$ for K over $\mathbb{Q}$ so that

$$h(\beta_i) \ll_d |\Delta_K|^{(d-1)(4d-3)},$$

for all $1 \leqslant i \leqslant d$.

The proof of this theorem follows the argument outlined above while carefully controlling all the choices and using a variety of height inequalities to obtain our bound.

Normal basis: quadratic case

In the case of a quadratic number field $K = \mathbb{Q}(\sqrt{t})$ for a squarefree integer t, we can obtain a better bound by a direct application of Ruppert's result.

Normal basis: quadratic case

In the case of a quadratic number field $K = \mathbb{Q}(\sqrt{t})$ for a squarefree integer t, we can obtain a better bound by a direct application of Ruppert's result.

Proposition 7 (L.F., S. Jeong (2026))

For all but at most finitely many quadratic extensions $K/\mathbb{Q}$, there exists a normal basis $\beta_1, \beta_2 \in K$ with

$$h(\beta_i) \ll |\Delta_K|^{\frac{1}{4}}, \text{ for } i = 1, 2.$$

Normal basis: quadratic case

In the case of a quadratic number field $K = \mathbb{Q}(\sqrt{t})$ for a squarefree integer t, we can obtain a better bound by a direct application of Ruppert's result.

Proposition 7 (L.F., S. Jeong (2026))

For all but at most finitely many quadratic extensions $K/\mathbb{Q}$, there exists a normal basis $\beta_1, \beta_2 \in K$ with

$$h(\beta_i) \ll |\Delta_K|^{\frac{1}{4}}, \text{ for } i = 1, 2.$$

To prove this result, we simply observe that the primitive element

$$a + b\sqrt{t}, \text{ for } a, b \in \mathbb{Q},$$

guaranteed by Ruppert's theorem must have $a \neq 0$ for all but finitely many quadratic fields. Then $a \pm b\sqrt{t}$ is the desired normal basis.

Normal basis: prime degree case

In the case of an odd prime-degree Galois extension $K/\mathbb{Q}$ we can also obtain a better bound using a different method, which is also based on the avoidance method.

Normal basis: prime degree case

In the case of an odd prime-degree Galois extension $K/\mathbb{Q}$ we can also obtain a better bound using a different method, which is also based on the avoidance method.

Theorem 8 (L.F., S. Jeong (2026))

Let $K/\mathbb{Q}$ be a Galois extension of prime degree $d \geqslant 3$. There exists a normal basis $\beta_1, \ldots, \beta_d$ for K over $\mathbb{Q}$ consisting of algebraic integers so that

$$h(\beta_i) \leqslant |\Delta_K|^{1/2}, \ 1 \leqslant i \leqslant d.$$

Normal basis: prime degree case

In the case of an odd prime-degree Galois extension $K/\mathbb{Q}$ we can also obtain a better bound using a different method, which is also based on the avoidance method.

Theorem 8 (L.F., S. Jeong (2026))

Let $K/\mathbb{Q}$ be a Galois extension of prime degree $d \geqslant 3$. There exists a normal basis $\beta_1, \ldots, \beta_d$ for K over $\mathbb{Q}$ consisting of algebraic integers so that

$$h(\beta_i) \leqslant |\Delta_K|^{1/2}, \ 1 \leqslant i \leqslant d.$$

Our proof is based on a result of Dubickas about linear independence of algebraic conjugates of prime degree and on Minkowski's Successive Minima Theorem in the geometry of numbers, along with an avoidance consideration.

References

- L.Fukshansky, S. Jeong. Diophantine avoidance and small-height primitive elements in ideals of number fields, *Combinatorics and Number Theory,* vol. 13 no. 4 (2024), pg. 333-350

- L.Fukshansky, S. Jeong. Normal bases of small height in Galois number fields, *Research in Number Theory*, vol 12. (2026), Article no. 21

References

- L.Fukshansky, S. Jeong. Diophantine avoidance and small-height primitive elements in ideals of number fields, *Combinatorics and Number Theory,* vol. 13 no. 4 (2024), pg. 333-350

- L.Fukshansky, S. Jeong. Normal bases of small height in Galois number fields, *Research in Number Theory*, vol 12. (2026), Article no. 21

Thank you!