SEARCH BOUNDS FOR DIOPHANTINE EQUATIONS

LENNY FUKSHANSKY

Contents

1. Hilbert's 10th problem and search bounds

Consider a system of m Diophantine equations in n variables, i.e.

$$\left.\begin{array}{l} P_1(X_1,\dots,X_n)=0 \\ \vdots \\ P_m(X_1,\dots,X_n)=0 \end{array}\right\} \tag{1.1}$$

where $P_1,\dots,P_m$ are polynomials with integer coefficients.

Question 1. *Does this system have a nontrivial integral solution?*

Question 2. *Assuming it does, how do we find such a solution?*

The famous result of Y. Matijasevich (1970; building on the previous work by M. Davis, H. Putnam and J. Robinson - 1961) implies that Question 1 in general is undecidable. Suppose that we could prove a theorem of the following kind:

If the system (1.1) *has a nontrivial solution vector $\boldsymbol{x} \in \mathbb{Z}^n$, then there exists such a solution vector with*

$$|\boldsymbol{x}| := \max_{1\le i\le n} |x_i| \le B \tag{1.2}$$

for some explicit constant $B = B(P_1,\dots,P_m)$.

Then to answer Question 1, it would be enough to check whether any of the vectors in the finite set

$$\left\{ \boldsymbol{x} \in \mathbb{Z}^n : \max_{1\le i\le n} |x_i| \le B \right\}$$

is a solution to (1.1), reducing it to a *finite search algorithm.* Moreover, if Question 1 is answered affirmatively, then this finite search algorithm simultaneously provides an answer to Question 2. We will refer to a constant B satisfying (1.2) as an explicit *search bound* (with respect to $|\ |$) for the polynomial system $P_1,\dots,P_M$. Hence Questions 1 and 2 can be replaced by -

Question 3. *Assuming the polynomial system $P_1,\dots,P_M$ has a nontrivial integral solution, can we find an explicit search bound?*

This search-bounds approach to the problem was proposed by D. W. Masser in [Mas02]. Existence of search bounds for general polynomial systems like (1.1) would contradict Matijasevich's theorem, and hence search bounds in general cannot exist. Moreover, it was proved by J. P. Jones (1980) that the question whether a single Diophantine equation of degree four or larger has a solution in positive integers is already undecidable. This suggests that search bounds for equations of degree ≥ 4 may be out of reach, and relatively little is known even for degree 3 (although some work has been done, especially in the recent years). There is however a wealth of results for polynomials of degree 1 and 2, which is going to be the focus of these lectures.

2. Integral linear equations

We start by discussing a search bound for a system of homogeneous linear equations. This is Siegel's Lemma, the simplest version of which was originally observed by Axel Thue in 1909 and then formally proved by Carl Ludwig Siegel in 1929. While Siegel's Lemma originated as a tool used in transcendence arguments (in particular, for construction of auxiliary polynomials with bounded coefficients), it took on a separate life in the more recent years as a first case of a result on points of bounded height on algebraic varieties.

Our presentation here partially follows [Sch91]. Let

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

be an $m \times n$ matrix with integer entries and rank equal to $m < n$. Define

$$\Lambda = \{\boldsymbol{x} \in \mathbb{Z}^n : A\boldsymbol{x} = \boldsymbol{0}\}.$$

Theorem 2.1 (Siegel's Lemma, version 1)**.** *With notation as above, there exists* $\boldsymbol{0} \neq \boldsymbol{x} \in \Lambda$ *with*

$$|\boldsymbol{x}| < 2 + (n|A|)^{\frac{m}{n-m}}, \tag{2.1}$$

where $|\boldsymbol{x}| = \max\{|x_i| : 1 \leq i \leq n\}$*,* $|A| = \max\{|a_{ij}| : 1 \leq i \leq m,\ 1 \leq j \leq n\}$*.*

Proof. Let $R \in \mathbb{Z}_{>0}$, and let

$$C_R^n = \{\boldsymbol{x} \in \mathbb{R}^n : |\boldsymbol{x}| \leq R\}$$

be the cube centered at the origin in $\mathbb{R}^n$ with sidelength $2R$. Then

$$|C_R^n \cap \mathbb{Z}^n| = (2R+1)^n.$$

Let $T_A : \mathbb{R}^n \to \mathbb{R}^m$ be a linear map, given by $T_A(\boldsymbol{x}) = A\boldsymbol{x}$ for each $\boldsymbol{x} \in \mathbb{R}^n$. Notice that for every $\boldsymbol{x} \in C_R^n$,

$$|T_A(\boldsymbol{x})| \leq n|A|R,$$

i.e. T_A maps C_R^n into $C_{n|A|R}^m \subseteq \mathbb{R}^m$, since $\operatorname{rk}(A) = l$. Now

$$|C_{n|A|R}^m \cap \mathbb{Z}^m| = (2n|A|R+1)^m.$$

Now let us choose R to be a positive integer satisfying

$$(n|A|)^{\frac{m}{n-m}} \leq 2R < (n|A|)^{\frac{m}{n-m}} + 2.$$

Then

$$\begin{aligned} |C_R^n \cap \mathbb{Z}^n| &= (2R+1)^n = (2R+1)^m(2R+1)^{n-m} \\ &\geq (2R+1)^m(n|A|)^m > (2n|A|R+1)^m \\ &= |C_{n|A|R}^m \cap \mathbb{Z}^m|. \end{aligned}$$

This means that T_A cannot be mapping $C_R^n \cap \mathbb{Z}^n$ into $C_{n|A|R}^m \cap \mathbb{Z}^m$ in a one-to-one manner. Hence, there must exist $\boldsymbol{x} \neq \boldsymbol{y} \in C_R^n \cap \mathbb{Z}^n$ such that $T_A(\boldsymbol{x}) = T_A(\boldsymbol{y})$, i.e.

$$T_A(\boldsymbol{x} - \boldsymbol{y}) = 0,$$

and so $\boldsymbol{x} - \boldsymbol{y} \in \Lambda$. On the other hand,

$$|\boldsymbol{x} - \boldsymbol{y}| \leq |\boldsymbol{x}| + |\boldsymbol{y}| \leq 2R < (n|A|)^{\frac{m}{n-m}} + 2,$$

and this finishes the proof. □

Notice that the main underlying idea in the proof of Siegel's Lemma was the pigeon hole principle. It is remarkable that the exponent $\frac{m}{n-m}$ in the upper bound of (2.1) cannot be improved. To see this, let for instance $m = n-1$ and for a positive integer R consider the $(n-1) \times n$ matrix

$$A = \begin{pmatrix} R & -1 & 0 & \dots & 0 & 0 \\ 0 & R & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & R & -1 \end{pmatrix}.$$

Then $|A| = R$, and every nonzero integer solution of the system of linear equations $A\boldsymbol{x} = \boldsymbol{0}$ must have $x_n = R^{n-1}x_1$. Therefore, if

$$\Lambda = \{\boldsymbol{x} \in \mathbb{Z}^n : A\boldsymbol{x} = \boldsymbol{0}\},$$

and $\boldsymbol{0} \neq \boldsymbol{x} \in \Lambda$, then

$$|\boldsymbol{x}| \geq R^{n-1} = |A|^{\frac{m}{n-m}}.$$

In the theorem above, we did not have to assume that the system of polynomial equations has a solution: an underdetermined homogeneous linear system always has a nontrivial integer solution. On the other hand, we can consider an inhomogeneous integral linear system

$$A\boldsymbol{x} = \boldsymbol{b}, \tag{2.2}$$

for a matrix A as above and a nonzero integer vector $\boldsymbol{b} \in \mathbb{Z}^m$. A system like this does not necessarily have a solution, so let us start with a criterion to determine whether it has a solution. Define

$$\gcd(A) := \gcd(\det A' : A' \text{ is an } m \times m \text{ submatrix of } A),$$

and in the same manner define $\gcd(A\ \boldsymbol{b})$ for the augmeneted $(n+1) \times m$ matrix $(A\ \boldsymbol{b})$ with $\boldsymbol{b}$ added as the last column. The following theorem was originally proved by I. Heger in 1856.

Theorem 2.2. *The linear system* (2.2) *has an integer solution if and only if*

$$\gcd(A\ \boldsymbol{b}) = \gcd(A).$$

A much more recent result of Borosh, Flahive, Rubin and Treybig [BFRT89] gives a search bound for this inhomogeneous problem.

Theorem 2.3. *Assume that the linear system* (2.2) *has an integer solution. Then there exists such a solution* $\boldsymbol{x}$ *with*

$$|\boldsymbol{x}| \leq \max\left\{\det A' : A' \textit{ is an } m \times m \textit{ submatrix of } A\right\}.$$

3. Some geometry of numbers

In this section we will discuss some of the famous theorems related to the following very classical problem in the geometry of numbers: given a set M and a lattice Λ in $\mathbb{R}^n$, how can we tell if M contains any points of Λ?

Theorem 3.1 (Blichfeldt, 1914)**.** *Let M be a Jordan measurable set in $\mathbb{R}^n$. Suppose that $\operatorname{Vol}(M) > 1$, or that M is closed, bounded and $\operatorname{Vol}(M) \geq 1$. Then there exist $\boldsymbol{x}, \boldsymbol{y} \in M$ such that $\boldsymbol{0} \neq \boldsymbol{x} - \boldsymbol{y} \in \mathbb{Z}^n$.*

Proof. First suppose that $\operatorname{Vol}(M) > 1$. Let

$$P = \{\boldsymbol{x} \in \mathbb{R}^n : 0 \leq x_i < 1 \ \forall\ 1 \leq i \leq n\},$$

and let

$$S = \{\boldsymbol{u} \in \mathbb{Z}^n : M \cap (P + \boldsymbol{u}) \neq \emptyset\}.$$

Since M is bounded, S is a finite set, say $S = \{\boldsymbol{u}_1, \dots, \boldsymbol{u}_{r_0}\}$. Write $M_r = M \cap (P + \boldsymbol{u}_r)$ for each $1 \leq r \leq r_0$. Also, for each $1 \leq r \leq r_0$, define

$$M_r' = M_r - \boldsymbol{u}_r,$$

so that $M_1', \dots, M_{r_0}' \subseteq P$. On the other hand, $\bigcup_{r=1}^{r_0} M_r = M$, and $M_r \cap M_s = \emptyset$ for all $1 \leq r \neq s \leq r_0$, since $M_r \subseteq P + \boldsymbol{u}_r$, $M_s \subseteq P + \boldsymbol{u}_s$, and $(P + \boldsymbol{u}_r) \cap (P + \boldsymbol{u}_s) = \emptyset$. This means that

$$1 < \operatorname{Vol}(M) = \sum_{r=1}^{r_0} \operatorname{Vol}(M_r).$$

However, $\operatorname{Vol}(M_r') = \operatorname{Vol}(M_r)$ for each $1 \leq r \leq r_0$,

$$\sum_{r=1}^{r_0} \operatorname{Vol}(M_r') > 1,$$

but $\bigcup_{r=1}^{r_0} M_r' \subseteq P$, and so

$$\operatorname{Vol}\left(\bigcup_{r=1}^{r_0} M_r'\right) \leq \operatorname{Vol}(P) = 1.$$

Hence the sets $M_1', \dots, M_{r_0}'$ are not mutually disjoined, meaning that there exist indices $1 \leq r \neq s \leq r_0$ such that there exists $\boldsymbol{x} \in M_r' \cap M_s'$. Then we have $\boldsymbol{x} + \boldsymbol{u}_r, \boldsymbol{x} + \boldsymbol{u}_s \in M$, and

$$(\boldsymbol{x} + \boldsymbol{u}_r) - (\boldsymbol{x} + \boldsymbol{u}_s) = \boldsymbol{u}_r - \boldsymbol{u}_s \in \mathbb{Z}^n.$$

Now suppose M is closed, bounded, and $\operatorname{Vol}(M) = 1$. Let $\{s_r\}_{r=1}^{\infty}$ be a sequence of numbers all greater than 1, such that

$$\lim_{r \to \infty} s_r = 1.$$

By the argument above we know that for each r there exist

$$\boldsymbol{x}_r \neq \boldsymbol{y}_r \in s_r M$$

such that $\boldsymbol{x}_r - \boldsymbol{y}_r \in \mathbb{Z}^n$. Then there are subsequences $\{\boldsymbol{x}_{r_k}\}$ and $\{\boldsymbol{y}_{r_k}\}$ converging to points $\boldsymbol{x}, \boldsymbol{y} \in M$, respectively. Since for each r_k, $\boldsymbol{x}_{r_k} - \boldsymbol{y}_{r_k}$ is a nonzero lattice point, it must be true that $\boldsymbol{x} \neq \boldsymbol{y}$, and $\boldsymbol{x} - \boldsymbol{y} \in \mathbb{Z}^n$. This completes the proof. □

As a corollary of Theorem 3.1 we can prove the following version of *Minkowski Convex Body Theorem.*

Theorem 3.2 (Minkowski)**.** *Let $M \subset \mathbb{R}^n$ be a compact convex $\mathbf{0}$-symmetric set with* $\operatorname{Vol}(M) \geq 2^n$*. Then there exists $\mathbf{0} \neq \boldsymbol{x} \in M \cap \mathbb{Z}^n$.*

Proof. Notice that the set

$$\frac{1}{2}M = \left\{ \frac{1}{2}\boldsymbol{x} : \boldsymbol{x} \in M \right\} = \begin{pmatrix} 1/2 & 0 & \dots & 0 \\ 0 & 1/2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1/2 \end{pmatrix} M$$

is also convex, $\mathbf{0}$-symmetric, and by Problem 11.3 its volume is

$$\det \begin{pmatrix} 1/2 & 0 & \dots & 0 \\ 0 & 1/2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1/2 \end{pmatrix} \operatorname{Vol}(M) = 2^{-n} \operatorname{Vol}(M) \geq 1.$$

Thererfore, by Theorem 3.1, there exist $\frac{1}{2}\boldsymbol{x} \neq \frac{1}{2}\boldsymbol{y} \in \frac{1}{2}M$ such that

$$\frac{1}{2}\boldsymbol{x} - \frac{1}{2}\boldsymbol{y} \in \mathbb{Z}^n.$$

But, by symmetry, since $\boldsymbol{y} \in M$, $-\boldsymbol{y} \in M$, and by convexity, since $\boldsymbol{x}, -\boldsymbol{y} \in M$,

$$\frac{1}{2}\boldsymbol{x} - \frac{1}{2}\boldsymbol{y} = \frac{1}{2}\boldsymbol{x} + \frac{1}{2}(-\boldsymbol{y}) \in M.$$

This completes the proof. □

Remark 3.1. This result is sharp: for any $\varepsilon > 0$, the cube

$$C = \left\{ \boldsymbol{x} \in \mathbb{R}^n : \max_{1 \leq i \leq n} |x_i| \leq 1 - \frac{\varepsilon}{2} \right\}$$

is a convex $\mathbf{0}$-symmetric set of volume $(2 - \varepsilon)^n$, which contains no nonzero integer lattice points.

Problem 11.4 extends Blichfeldt and Minkowski theorems to arbitrary lattices as follows:

- If $\Lambda \subset \mathbb{R}^n$ is a lattice of full rank and $M \subset \mathbb{R}^n$ is a compact convex set with $\operatorname{Vol}(M) \geq \det \Lambda$, then there exist $\boldsymbol{x}, \boldsymbol{y} \in M$ such that $\mathbf{0} \neq \boldsymbol{x} - \boldsymbol{y} \in \Lambda$.
- If $\Lambda \subset \mathbb{R}^n$ is a lattice of full rank and $M \subset \mathbb{R}^n$ is a compact convex $\mathbf{0}$-symmetric set with $\operatorname{Vol}(M) \geq 2^n \det \Lambda$, then there exists $\mathbf{0} \neq \boldsymbol{x} \in M \cap \Lambda$.

As an application of these results, we prove *Minkowski's Linear Forms Theorem.*

Theorem 3.3. *Let $B = (b_{ij})_{1 \leq i,j \leq n} \in \mathrm{GL}_n(\mathbb{R})$, and for each $1 \leq i \leq n$ define a linear form with coefficients $b_{i1}, \dots, b_{in}$ by*

$$L_i(\boldsymbol{X}) = \sum_{j=1}^{n} b_{ij} X_j.$$

Let $c_1, \dots, c_n \in \mathbb{R}_{>0}$ be such that

$$c_1 \dots c_n \geq |\det(B)|.$$

Then there exists $\mathbf{0} \neq \boldsymbol{x} \in \mathbb{Z}^n$ such that

$$|L_1(\boldsymbol{x})| \leq c_1, \ |L_i(\boldsymbol{x})| < c_i \ \forall \ 1 \leq i \leq n.$$

Proof. Let us write $\boldsymbol{b}_1, \dots, \boldsymbol{b}_n$ for the row vectors of B, then

$$L_i(\boldsymbol{x}) = \boldsymbol{b}_i \boldsymbol{x},$$

for each $\boldsymbol{x} \in \mathbb{R}^n$. Let $0 < \varepsilon < 1$ and consider the parallelepiped

$$P_\varepsilon = \{\boldsymbol{x} \in \mathbb{R}^n : |L_1(\boldsymbol{x})| < c_1(1+\varepsilon),\ |L_i(\boldsymbol{x})| < c_i\ \forall\ 2 \le i \le n\} = B^{-1}R_\varepsilon,$$

where $R_\varepsilon = \{\boldsymbol{x} \in \mathbb{R}^n : |x_1| < c_1(1+\varepsilon),\ |x_i| < c_i\ \forall\ 2 \le i \le n\}$ is the open rectangular box with sides of length $2c_1(1+\varepsilon), 2c_2, \dots, 2c_n$ centered at the origin in $\mathbb{R}^n$. Then by Problem 11.3,

$$\operatorname{Vol}(P_\varepsilon) = |\det(B)|^{-1} \operatorname{Vol}(R_\varepsilon) = |\det(B)|^{-1} 2^n (1+\varepsilon) c_1 \dots c_n \ge 2^n(1+\varepsilon) > 2^n,$$

and so by Theorem 3.2 there exists $\boldsymbol{0} \ne \boldsymbol{x}_\varepsilon \in P_\varepsilon \cap \mathbb{Z}^n$. This is true for every ε and $P_{\varepsilon_1} \subset P_{\varepsilon_2}$ whenever $\varepsilon_1 < \varepsilon_2$. Further, each $P_\varepsilon \subset P_1$, which is bounded, and hence contains only finitely many points of $\mathbb{Z}^n$. There is a nonzero integer in each of P_ε, and hence there must be a nonzero integer point $\boldsymbol{x} \in \bigcap_\varepsilon P_\varepsilon$, which is precisely the point we are looking for. □

Corollary 3.4. *Let $\theta_1, \dots, \theta_n$ be real numbers, and let $M > 1$ be an integer. There exists a positive integer $m < M$ and integers $b_1, \dots, b_n$ such that*

$$|m\theta_j - b_j| \le M^{-1/n},\ \forall\ 1 \le j \le n.$$

Proof. Define $n+1$ linear forms in $n+1$ variables:

$$L_j(\boldsymbol{X}) = \theta_j X_{n+1} - X_j,\ \forall\ 1 \le j \le n,$$
$$L_{n+1}(\boldsymbol{X}) = X_{n+1}.$$

Let us apply Theorem 3.3 with this choice of the linear forms, so the corresponding matrix B is of the form

$$B = \begin{pmatrix} -1 & 0 & \dots & 0 & \theta_1 \\ 0 & -1 & \dots & 0 & \theta_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & \theta_n \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

hence $\det(B) = \pm 1$. Let us take $c_j = M^{-1/n}$ for each $1 \le j \le n$ and $c_j = M$, then

$$c_1 \cdots c_{n+1} = 1.$$

Then Theorem 3.3 guarantees the existence of a nonzero point $(\boldsymbol{b}, m) \in \mathbb{Z}^{n+1}$ such that

$$|L_i(\boldsymbol{b})| \le c_i,\ \forall\ 1 \le i \le n,\ m < M.$$

This establishes the corollary. □

4. Cassels' theorem on quadratic forms

In this section, we consider the case of a quadratic hypersurface. Namely, let

$$F(\boldsymbol{X}) = \sum_{i=1}^{n} \sum_{j=1}^{n} f_{ij} X_i X_j \in \mathbb{Z}[X_1, \dots, X_n]$$

be a quadratic form in n variables with integer coefficients. We say that F is *isotropic* if there exists $\boldsymbol{0} \neq \boldsymbol{x} \in \mathbb{Z}^n$ such that $F(\boldsymbol{x}) = 0$; noticed that F has an integral zero if and only if it has a rational zero, by homogeneity. Provided that F is isotropic, we are interested in proving the existence of a nonzero point of bounded height in the zero-set

$$\mathcal{V}(F) = \{\boldsymbol{x} \in \mathbb{Z}^n : F(\boldsymbol{x}) = 0\}$$

with an explicit bound on height. Define

$$|F| = \max\{|f_{ij}| : 1 \leq i, j \leq n\}.$$

The following theorem was originally proved by Cassels in 1955.

Theorem 4.1. *Let F be an isotropic integral quadratic form, as above. Then there exists $\boldsymbol{0} \neq \boldsymbol{a} \in \mathcal{V}(F)$ such that*

$$|\boldsymbol{a}| \leq \left(3n^2|F|\right)^{\frac{n-1}{2}}. \tag{4.1}$$

Proof. Let $\boldsymbol{0} \neq \boldsymbol{a} \in \mathcal{V}(F)$ be a vector of minimal sup-norm $|\boldsymbol{a}|$. Permuting the indices and taking $-\boldsymbol{a}$ instead of $\boldsymbol{a}$, if necessary, we can assume that $a_1 = |\boldsymbol{a}|$. If $a_1 = 1$, then (4.1) is satisfied, so assume $a_1 \geq 2$. Define the numbers

$$\theta_j = a_j/a_1 \ \forall\ 2 \leq j \leq n,$$

and apply Corollary 3.4 with this choice of θ_j's and $M = a_1$. Then there exists $b_1 < a_1$ and $\boldsymbol{b} = (b_1, \dots, b_n) \in \mathbb{Z}^{n-1}$ such that

$$|b_1(a_j/a_1) - b_j| \leq a_1^{-1/(n-1)},\ \forall\ 2 \leq j \leq n.$$

Hence, for all $2 \leq j \leq n$,

$$|b_j| \leq |b_1\theta_j| + a_1^{-1/(n-1)} \leq b_1 + a_1^{-1/(n-1)} < b_1 + 1,$$

and so $|\boldsymbol{b}| = b_1 < a_1 = |\boldsymbol{a}|$. By minimality of $|\boldsymbol{a}|$, it must be that $F(\boldsymbol{b}) \neq 0$. Define

$$\boldsymbol{a}' = F(\boldsymbol{b})\boldsymbol{a} - 2F(\boldsymbol{a}, \boldsymbol{b})\boldsymbol{b} \in \mathbb{Z}^n.$$

Notice that $\boldsymbol{a}' \neq \boldsymbol{0}$. Indeed, assume $\boldsymbol{a}' = \boldsymbol{0}$, then $F(\boldsymbol{b})\boldsymbol{a} = 2F(\boldsymbol{a}, \boldsymbol{b})\boldsymbol{b}$, hence $F(\boldsymbol{a}, \boldsymbol{b}) \neq 0$, since $\boldsymbol{a} \neq 0$. On the other hand,

$$F(\boldsymbol{b})^2 F(\boldsymbol{a}) = 4F(\boldsymbol{a}, \boldsymbol{b})^2 F(\boldsymbol{b}) = 0,$$

meaning that $F(\boldsymbol{b}) = 0$, which is a contradiction.

It is also easy to verify that

$$F(\boldsymbol{a}') = F(\boldsymbol{b})^2 F(\boldsymbol{a}) + 4F(\boldsymbol{a}, \boldsymbol{b})^2 F(\boldsymbol{b}) - 4F(\boldsymbol{a}, \boldsymbol{b})^2 F(\boldsymbol{b}) = 0.$$

Now, for each $1 \leq j \leq n$, we can write

$$b_j = \left(\frac{b_1}{a_1}\right) a_j + d_j,$$

where

$$d_1 = 0,\ |d_j| \leq a_1^{-1/(n-1)} \ \forall\ 2 \leq j \leq n.$$

Writing $\boldsymbol{d} = (d_1, \ldots, d_n)$, we see that

$$|\boldsymbol{d}| \leq a_1^{-1/(n-1)} = |\boldsymbol{a}|^{-1/(n-1)}.$$

Also, $\boldsymbol{b} = \left(\frac{b_1}{a_1}\right)\boldsymbol{a} + \boldsymbol{d}$, and so

$$F(\boldsymbol{a}, \boldsymbol{b}) = F(\boldsymbol{a}, \boldsymbol{d}) \text{ and } F(\boldsymbol{b}) = 2\left(\frac{b_1}{a_1}\right)F(\boldsymbol{a}, \boldsymbol{d}) + F(\boldsymbol{d}).$$

Therefore

$$\begin{aligned}\boldsymbol{a}' &= \left(2\left(\frac{b_1}{a_1}\right)F(\boldsymbol{a}, \boldsymbol{d}) + F(\boldsymbol{d})\right)\boldsymbol{a} - 2F(\boldsymbol{a}, \boldsymbol{d})\left(\left(\frac{b_1}{a_1}\right)\boldsymbol{a} + \boldsymbol{d}\right) \\ &= F(\boldsymbol{d})\boldsymbol{a} - 2F(\boldsymbol{a}, \boldsymbol{d})\boldsymbol{d}.\end{aligned}$$

We can now roughly estimate the size of $\boldsymbol{a}'$:

$$|\boldsymbol{a}'| \leq 3n^2|F||\boldsymbol{d}|^2|\boldsymbol{a}|.$$

Since $\boldsymbol{a}$ is a minimal zero of F, we must have $|\boldsymbol{a}'| \geq |\boldsymbol{a}|$, and so

$$|\boldsymbol{a}| \leq 3n^2|F||\boldsymbol{d}|^2|\boldsymbol{a}|,$$

meaning that $3n^2|F||\boldsymbol{d}|^2 \geq 1$. On the other hand, $|\boldsymbol{d}| \leq |\boldsymbol{a}|^{-1/(n-1)}$, and so

$$1 \leq 3n^2|F||\boldsymbol{a}|^{-2/(n-1)},$$

meaning that $|\boldsymbol{a}| \leq \left(3n^2|F|\right)^{\frac{n-1}{2}}$, as asserted. □

The dependence on $|F|$ in the upper bound of Theorem 4.1 is best possible, as demonstrated by the following example due to M. Kneser [Cas56]. Consider an integral quadratic form

$$F(\boldsymbol{X}) = X_1^2 - \sum_{i=2}^{n}(X_i - cX_{i-1})^2 = (1-c^2)X_1^2 - (1+c^2)\sum_{i=2}^{n-1}X_i^2 - X_n^2 + 2c\sum_{i=2}^{n}X_{i-1}X_i$$

for some large positive integer c. Then $|F| = 1 + c^2$. Now, if $F(\boldsymbol{x}) = 0$ for some $\boldsymbol{0} \neq \boldsymbol{x} \in \mathbb{Z}^n$, then it must be true that

$$0 \neq x_1^2 = \sum_{i=2}^{n}(x_i - cx_{i-1})^2 = y_2^2 + \cdots + y_n^2,$$

where $y_i = x_i - cx_{i-1}$ for each $2 \leq i \leq n$. We can express

$$x_n = y_n + cy_{n-1} + \cdots + c^{n-1}y_2 + c^{n-1}x_1.$$

Then the smallest possible absolute value of x_n becomes

$$(c^{n-1} - c^{n-2})|x_1| > \frac{1}{2}c^{n-1} = \frac{1}{2}\left(|F| - 1\right)^{\frac{n-1}{2}}.$$

5. Inhomogeneous quadratic polynomials

Let us now consider the case when instead of being a quadratic form, F is an inhomogeneous quadratic polynomial over K. In other words, let

$$F(\boldsymbol{X}) = \sum_{i=1}^{n} \sum_{j=1}^{n} f_{ij} X_i X_j + \sum_{i=1}^{n} f_{0i} X_i + f_{00} \in K[X_1, \dots, X_n],$$

and suppose that

$$\mathcal{V}_K(F) = \{\boldsymbol{x} \in K^n : F(\boldsymbol{x}) = 0\}$$

is not empty. We want to prove the existence of a point $\boldsymbol{x} \in \mathcal{V}_K(F)$ of bounded height. Notice that we can "homogenize" F by adding one more variable X_0, i.e. consider the quadratic form in $n+1$ variables

$$F(\boldsymbol{X}) = \sum_{i=0}^{n} \sum_{j=1}^{n} f_{ij} X_i X_j \in K[X_0, \dots, X_n].$$

Problem 11.20 guarantees that a point $\boldsymbol{x} = (x_0, x_1, \dots, x_n) \in K^{n+1}$ with $x_0 \neq 0$ is a zero of $F(X_0, \dots, X_n)$ if and only if the point $\boldsymbol{x}' = (x_1, \dots, x_n) \in K^n$ is a zero of

$$F_1(X_1, \dots, X_n) := F(1, X_1, \dots, X_n).$$

Hence we want to look for small-height zeros of F with additional condition $x_0 \neq 0$. The following theorem was proved by D. Masser in 1998 [Mas98].

Theorem 5.1. *Let F be a quadratic form in $n+1 \geq 2$ variables with coefficients in K. Suppose that there exists $\boldsymbol{x} = (x_0, ..., x_n) \in K^{n+1}$ such that $F(\boldsymbol{x}) = 0$ and $x_0 \neq 0$, then there exists such $\boldsymbol{x}$ with*

$$|\boldsymbol{x}| \ll_n |F|^{\frac{n+1}{2}}, \tag{5.1}$$

where the implied constant depends only on n.

This implies that if an inhomogeneous quadratic polynomial in n variables with coefficients in K has a zero over K, then it has such a zero of height bounded as in (5.1). The exponent in the upper bound of (5.1) is best possible as demonstrated by an example of Masser presented in [Mas98]: for a fixed integer $a \geq 2$, consider the inhomogeneous quadratic polynomial

$$F(X_1, \dots, X_n) = 2X_1 - (X_2 - aX_1)^2 - \dots - (X_n - aX_{n-1})^2 - 2a^2.$$

The height of this polynomial is a constant multiple of a^2. It is not very difficult to show that the "smallest" rational zeros this polynomial has are of the height $\geq c(n)a^{n+1} = c'(n)H(F)^{\frac{n+1}{2}}$ for appropriate dimensional constants $c(n)$, $c'(n)$.

Masser's theorem provides a search bound for an inhomogeneous quadratic equation over $\mathbb{Q}$. The problem of obtaining an inhomogeneous result over $\mathbb{Z}$ instead of $\mathbb{Q}$ is substantially more difficult. Some state-of-the art results for integer solutions to inhomogeneous integral quadratic equations were obtained by R. Dietmann in [Die03].

Theorem 5.2. *Let $F(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$ be a nonsingular integral quadratic form. Suppose that there exists a vector $\boldsymbol{x} \in \mathbb{Z}^n$ such that $F(\boldsymbol{x}) = t$ for some integer t. Then there is a vector $\boldsymbol{x} \in \mathbb{Z}^n$ such that $F(\boldsymbol{x}) = t$ and*

$$|\boldsymbol{x}| \ll |F_t|^{\ell(n)},$$

where $F_t(\boldsymbol{X}) = F(\boldsymbol{X}) - t$*, the implied constant depends only on* n*, and*

$$\ell(n) = \begin{cases} 2100 & \text{if } n = 3, \\ 84 & \text{if } n = 4, \\ 5n + 19 + 74/(n-4) & \text{if } n \geq 5. \end{cases}$$

6. Multilinear forms

In this section, we study a special class of polynomials of arbitrary degree. Let $n \geq 1$ be an integer and let us define $[n] := \{1, \dots, n\}$. Given an integer d with $1 \leq d \leq n$, we put $\mathcal{I}_d(n) := \{I \subseteq [n] : |I| = d\}$. For each indexing set $I = \{i_1, \dots, i_d\} \in \mathcal{I}_d(n)$ with $1 \leq i_1 < \cdots < i_d \leq n$, we define the monomial x_I in the variables $x_{i_1}, \dots, x_{i_d}$ out of $x_1, \dots, x_n$ as $x_I := x_{i_1} \cdots x_{i_d}$. An *integer multilinear (n,d)-form* is a polynomial of the form

$$F(x_1, \dots, x_n) = \sum_{I \in \mathcal{I}_d(n)} f_I x_I,$$

where the coefficients f_I are integers for all $I \in \mathcal{I}_d(n)$. Such an F is a homogeneous polynomial in n variables of degree d which has degree 1 in each of the variables $x_1, \dots, x_n$. We will say that F *represents* an integer b it there exists an integer vector $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$. Under what conditions on F does such a polynomial represent all integers? The first observation is that the coefficients f_I of F must be relatively prime: if $g = \gcd(f_I)_{I \in \mathcal{I}_d(n)} > 1$, then g must divide $F(\boldsymbol{a})$ for every $\boldsymbol{a} \in \mathbb{Z}^n$, and hence an integer b that is not a multiple of g is not represented by F. We will say that our form *is coprime* if $\gcd(f_I)_{I \in \mathcal{I}_d(n)} = 1$.

We will provide some sufficient conditions for a multilinear (n,d)-form F to represent all integers. Further, our results are effective in the sense that we provide algorithms that yield an integer solution $\boldsymbol{a}$ of the equation $F(\boldsymbol{a}) = b$ (theoretically but not necessarily practically) in a finite number of steps. The following theorem was proved in [BF20].

Theorem 6.1. *Let $F(\boldsymbol{x})$ be a coprime integer multilinear (n,d)-form. Suppose in addition that at least one of the following two conditions holds:*

(a) *The nonzero coefficients of F are pairwise coprime,*

(b) *$n = d+1$ and F has a pair of coprime coefficients.*

Then F represents all integers. Further, for each $b \in \mathbb{Z}$ there exists an $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$ and

$$|\boldsymbol{a}| \leq |b| \left(2|F|\right)^{d!\,\mathrm{e}},$$

where $|\boldsymbol{a}| = \max_{1 \leq i \leq n} |a_i|$, $|F| = \max_{I \in \mathcal{I}_d(n)} |f_I|$, and $\mathrm{e} = 2.71828\dots$.

Proof of Theorem 6.1(a). By the remark after Theorem 6.1, we may assume that $d \geq 2$. We define

$$\nu_d = \sum_{k=0}^{d} \frac{d!}{k!} \tag{6.1}$$

and will show the theorem with the bound

$$|\boldsymbol{a}| \leq |b| \left(2|F|\right)^{\nu_d}. \tag{6.2}$$

As $\nu_d < d!\,\mathrm{e}$, this is actually sharper than the bound given in Theorem 6.1.

Since $F(\boldsymbol{x}) := F(x_1, \dots, x_n)$ is homogeneous, $F(\boldsymbol{0}) = 0$. Hence from here on we assume that $b \neq 0$. First suppose that $F(\boldsymbol{x})$ has only one monomial, i.e.,

$$F(\boldsymbol{x}) = f_I \prod_{i \in I} x_i$$

for some $I \subseteq [n]$ and $f_I \in \mathbb{Z}$. Since the gcd of the coefficients of F is 1, we must have $f_I = \pm 1$. Take some $j \in I$ and put $a_j = \pm b$ and $a_i = 1$ for $i \in I \setminus \{j\}$. We so obtain a vector $\boldsymbol{a} \in \mathbb{Z}^n$ such that $F(\boldsymbol{a}) = b$ and $|\boldsymbol{a}| = \max\{1, |b|\} = |b|$, which is smaller than the bound (6.2).

Next assume that $F(\boldsymbol{x})$ has exactly two monomials, i.e.,

$$F(\boldsymbol{x}) = f_{I_1} \prod_{i \in I_1} x_i + f_{I_2} \prod_{i \in I_2} x_i$$

for some $I_1, I_2 \subseteq [n]$ and coprime $f_{I_1}, f_{I_2} \in \mathbb{Z}$. Then the index sets I_1 and I_2 must be distinct (since otherwise there would be only one monomial) of the same cardinality d, and so there must exist some $k \in I_1 \setminus I_2$ and $m \in I_2 \setminus I_1$. Let $a'_k, a'_m \in \mathbb{Z}$ be such that

$$a'_k f_{I_1} + a'_m f_{I_2} = 1.$$

The Euclidean algorithm allows us to find such a'_k, a'_m with

$$|a'_k|, |a'_m| \leq \max\{|f_{I_1}|, |f_{I_2}|\}.$$

Letting $a_k = ba'_k$, $a_m = ba'_m$, and $a_i = 1$ for $i \neq k, m$, we get

$$F(\boldsymbol{a}) = a_k f_{I_1} + a_m f_{I_2} = b$$

with $|\boldsymbol{a}| \leq |b||F|$, which is again smaller than the bound (6.2).

We now argue by induction on $\ell \geq 1$, the number of monomials of F. Since the base of induction is already established, we assume that $\ell \geq 3$ and that the result is proved for polynomials with no more than $\ell - 1$ monomials. First notice that we can assume without loss of generality that F depends on all variables (if not, then F is a polynomial in $< n$ variables) and that no variable is present in all monomials (if it is, then just set it equal to 1). Let $d \geq 2$ be the degree of F. Every monomial is indexed by a subset I of $[n] = \{1, \ldots, n\}$ of cardinality d.

Suppose first that the variable x_1 is present in $\ell - 1$ monomials. We then may write

$$F(\boldsymbol{x}) = x_1 G(x_2, \ldots, x_n) + f_I \prod_{i \in I} x_i, \tag{6.3}$$

where $I \subset \{2, \ldots, n\}$ with $|I| = d$ and G is a homogeneous polynomial of degree $d-1$ that is linear in each of the $n-1$ variables with pairwise coprime integer coefficients. By the induction hypothesis, there exists a vector $\boldsymbol{a}' = (a_2, \ldots, a_n) \in \mathbb{Z}^{n-1}$ such that $G(\boldsymbol{a}') = 1$ and

$$|\boldsymbol{a}'| \leq |1|(2|G|)^{\nu_{d-1}} \leq (2|F|)^{\nu_{d-1}}.$$

Put $a_1 = b - f_I \prod_{i \in I} a_i$. Then

$$F(a_1, \boldsymbol{a}') = \left(b - f_I \prod_{i \in I} a_i \right) G(\boldsymbol{a}') + f_I \prod_{i \in I} a_i = b, \tag{6.4}$$

that is, $F(\boldsymbol{a}) = b$ for $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$. Furthermore,

$$|\boldsymbol{a}| \leq |b| + |f_I||\boldsymbol{a}'|^d \leq 2|b||F||\boldsymbol{a}'|^d$$

since $|b|$, $|f_I||\boldsymbol{a}'|^d$ are positive integers and f_I is a coefficient of F. Therefore

$$|\boldsymbol{a}| \leq 2|b||F| \left(2|F|\right)^{\nu_{d-1} d} = \left(2|F|\right)^{1 + d\nu_{d-1}} |b|,$$

and because, by (6.1),

$$1 + d\nu_{d-1} = 1 + d \sum_{k=0}^{d-1} \frac{(d-1)!}{k!} = \sum_{k=0}^{d} \frac{d!}{k!} = \nu_d,$$

we obtain the bound (6.2).

On the other hand, assume that x_1 is not present in at least two different monomials. Then set $x_1 = 0$ and apply the induction hypothesis to the resulting polynomial

$$P(x_2, \dots, x_n) := F(0, x_2, \dots, x_n) \tag{6.5}$$

in $n-1$ variables. This polynomial has no more than $\ell - 1$ and no fewer than two monomials and satisfies all the other conditions of the theorem. Take $\boldsymbol{a}' \in \mathbb{Z}^{n-1}$ to be the point guaranteed by the induction hypothesis, so that $P(\boldsymbol{a}') = b$ and

$$|\boldsymbol{a}'| \leq (2|P|)^{\nu_d}\ |b| \leq (2|F|)^{\nu_d}\ |b|. \tag{6.6}$$

Setting $\boldsymbol{a}$ to be $\boldsymbol{a}'$ with inserted 0 in the first coordinate, we obtain the necessary solution $F(\boldsymbol{a}) = b$ with $|\boldsymbol{a}| = |\boldsymbol{a}'|$ bounded as in (6.6), which gives the bound (6.2). □

Proof of Theorem 6.1(b). We argue by induction on $d \geq 1$. As said, if $d = 1$, then $n = 2$ and $F(x_1, x_2) = f_1 x_1 + f_2 x_2$ with $\gcd(f_1, f_2) = 1$. Thus, the result follows from the Euclidean algorithm.

Suppose now $d \geq 2$. Since $n = d + 1 \geq 3$, the set $\mathcal{I}_d(n)$ consists of the indexing sets $I(k) = [n] \setminus \{k\}$ with $1 \leq k \leq n$, and so

$$F(x_1, \dots, x_n) = \sum_{k=1}^{n} f_{I(k)} x_{I(k)}.$$

Since F has a pair of coprime coefficients, there must exist $1 \leq j < m \leq n$ such that $\gcd(f_{I(j)}, f_{I(m)}) = 1$. Assume without loss of generality that $j = n-1$, $m = n$, and notice that each monomial $x_{I(k)}$ for $k \neq 1$ is divisible by x_1. Thus, writing $I'(k) = I(k) \setminus \{1\}$ we obtain

$$F(x_1, \dots, x_n) = x_1 G(x_2, \dots, x_n) + f_{I(1)} x_{I(1)} = x_1 G(x_2, \dots, x_n) + f_{I(1)} \prod_{i=2}^{n} x_i$$

with

$$G(x_2, \dots, x_n) = \sum_{k=2}^{n} f_{I(k)} x_{I'(k)}.$$

The polynomial G is a coprime integer multilinear $(n-1, d-1)$-form with $n - 1 = (d-1) + 1$ and G still has the same pair of coprime coefficients $f_{I(n-1)}, f_{I(n)}$. We can therefore apply the induction hypothesis to G and can argue in the same way as in the proof of Theorem 6.1(a) to get the desired result. □

7. Siegel's Lemma over number fields

In this section, we present a basic version of Siegel's Lemma over number fields. Let K be a number field of degree d with embeddings $\sigma_1, \dots, \sigma_d$. For each $\alpha \in K$, define its *height*

$$\mathcal{H}(\alpha) := \max\{|\sigma_k(\alpha)| : 1 \leq k \leq d\}.$$

Height functions more generally are devices meant to measure arithmetic complexity of objects, in a certain well-defined sense. This is a somewhat simplified version of a height function, which takes into account only partial information about the arithmetic properties of an algebraic number. We will discuss the theory of height functions and introduce more sophisticated machinery in Section 8 below.

As we know, the ring of integers $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank d. In other words, $\mathcal{O}_K$ has a $\mathbb{Z}$-basis: there exists a linearly independent collection $\omega_1, \dots, \omega_d \in \mathcal{O}_K$ such that

$$\mathcal{O}_K = \left\{ \sum_{k=1}^{d} a_k \omega_k : a_1, \dots, a_d \in \mathbb{Z} \right\}.$$

Define the corresponding $d \times d$ basis matrix $W := (\sigma_\ell(\omega_k))_{1 \leq \ell, k \leq d}$, which of course is nonsingular. With this notation and information in mind, we can now prove our next result, following [MR14].

Theorem 7.1 (Siegel's Lemma, version 2)**.** *Let K be a number field of degree d, and let $A = (\alpha_{ij})$ be an $l \times n$ matrix of rank $l < n$ with entries $\alpha_{ij} \in \mathcal{O}_K$. Define*

$$\mathcal{H}(A) := \max\{\mathcal{H}(\alpha_{ij}) : 1 \leq i \leq l, 1 \leq j \leq n\}.$$

There exists a solution $\mathbf{0} \neq \boldsymbol{x} = (x_1, \dots, x_n) \in \mathcal{O}_K^n$ to the homogeneous linear system $A\boldsymbol{x} = \mathbf{0}$ with

$$\max_{1 \leq j \leq n} \mathcal{H}(x_j) < B_K(l,n) \mathcal{H}(A)^{\frac{l}{n-l}}, \tag{7.1}$$

where $B_K(l,n)$ is some constant depending only on l, n and the number field K.

Proof. Let $\omega_1, \dots, \omega_d \in \mathcal{O}_K$ be a $\mathbb{Z}$-basis for $\mathcal{O}_K$, as described above, and let W be the corresponding basis matrix. Then for each entry α_{ij} of our matrix A, there exist $a_{ijk} \in \mathbb{Z}$, $1 \leq k \leq d$, such that

$$\alpha_{ij} = \sum_{k=1}^{d} a_{ijk} \omega_k.$$

Applying embeddings $\sigma_1, \dots, \sigma_d$ to the above equation, we obtain

$$\sigma_\ell(\alpha_{ij}) = \sum_{k=1}^{d} a_{ijk} \sigma_\ell(\omega_k)$$

for each $1 \leq \ell \leq d$, and hence

$$\boldsymbol{\alpha}_{ij} := (\sigma_1(\alpha_{ij}), \dots, \sigma_d(\alpha_{ij}))^t = W(a_{ij1}, \dots, a_{ijd})^t.$$

Since W is invertible, we have

$$\boldsymbol{a}_{ij} := (a_{ij1}, \dots, a_{ijd})^t = W^{-1} \boldsymbol{\alpha}_{ij}.$$

If we write $v_{k\ell}$ for the entries of W^{-1}, then

$$a_{ijk} = \sum_{\ell=1}^{d} v_{k\ell} \sigma_\ell(\alpha_{ij}),$$

and so

$$|a_{ijk}| \leq d \max_{1 \leq \ell \leq d} |v_{k\ell} \sigma_\ell(\alpha_{ij})| \leq d C_K \mathcal{H}(A), \tag{7.2}$$

where C_K is a constant depending only on the number field K such that $C_K \geq \max_{1 \leq k, \ell \leq d} |v_{k\ell}|$.

Now suppose $\boldsymbol{x} \in \mathcal{O}_K^n$ is a nontrivial solution of the system $A\boldsymbol{x} = \boldsymbol{0}$, and write

$$\boldsymbol{x} = \left(\sum_{\ell=1}^d b_{1\ell}\omega_\ell, \dots, \sum_{\ell=1}^d b_{n\ell}\omega_\ell \right) \tag{7.3}$$

for some $b_{j\ell} \in \mathbb{Z}$ for $1 \leq j \leq n$, $1 \leq \ell \leq d$. Then i-th entry of the vector $A\boldsymbol{x}$ is

$$\sum_{j=1}^n \sum_{\ell=1}^d \sum_{k=1}^d a_{ijk} b_{j\ell} \omega_k \omega_\ell = 0.$$

Since $\omega_k \omega_\ell \in \mathcal{O}_K$, it can also be expressed as a linear combination of ω_m's with $\mathbb{Z}$-coefficients:

$$\omega_k \omega_\ell = \sum_{m=1}^d c_{k\ell m} \omega_m$$

for each $1 \leq k, \ell \leq d$, and hence we have

$$\sum_{m=1}^d \sum_{j=1}^n \sum_{\ell=1}^d \sum_{k=1}^d a_{ijk} b_{j\ell} c_{k\ell m} \omega_m = 0.$$

Since $\omega_1, \dots, \omega_d$ are linearly independent over $\mathbb{Z}$, all the coefficients in the above equations must be zero, and hence we have a system of ld homogeneous linear equations with integer coefficients in the nd variables $b_{j\ell}$:

$$\sum_{j=1}^n \sum_{\ell=1}^d \sum_{m=1}^d a_{ijk} b_{j\ell} c_{k\ell m} = 0,$$

for all $1 \leq i \leq l$, $1 \leq m \leq d$. Applying Theorem 2.1 along with (7.2), we see that there exists a solution with

$$\max_{j,\ell} |b_{j\ell}| \leq 2 + (nd^2 C_K \mathcal{H}(A))^{\frac{ld}{nd - ld}},$$

and hence, by (7.3),

$$\max_{1 \leq j \leq n} \mathcal{H}(x_j) \leq d \left(2 + (nd^2 C_K \mathcal{H}(A))^{\frac{l}{n-l}} \right) \max_{1 \leq \ell \leq d} \mathcal{H}(\omega_\ell).$$

Since the choice of $\omega_1, \dots, \omega_\ell$ depends only on K, the conclusion of the theorem follows. □

Recall that for any $\beta \in K$, there exists $c \in \mathbb{N}$ such that $c\beta \in \mathcal{O}_K$. In fact, for any collection $\beta_1, \dots, \beta_n \in K$, let us define their *common denominator* to be

$$D(\beta_1, \dots, \beta_n) = \min\{c \in \mathbb{N} : c\beta_k \in \mathcal{O}_K \ \forall \ 1 \leq k \leq n\}.$$

For an $l \times n$ matrix A with entries in K, we will write $D(A)$ for the common denominator of all of its entries, i.e.,

$$D(A) = D(\alpha_{ij} : 1 \leq i \leq l, 1 \leq j \leq n).$$

With this notation in mind, we have one more version of Siegel's lemma.

Corollary 7.2 (Siegel's Lemma, version 3)**.** *Let K be a number field of degree d, and let $A = (\alpha_{ij})$ be an $l \times n$ matrix of rank $l < n$ with entries $\alpha_{ij} \in K$. There exists a solution $\mathbf{0} \neq \boldsymbol{x} = (x_1, \ldots, x_n) \in \mathcal{O}_K^n$ to the homogeneous linear system $A\boldsymbol{x} = \mathbf{0}$ with*

$$\max_{1 \leq j \leq n} \mathcal{H}(x_j) < B_K(l, n)(D(A)\mathcal{H}(A))^{\frac{l}{n-l}}, \tag{7.4}$$

where $B_K(l, n)$ is the same constant as in Theorem 7.1 above.

Proof. Let $A' = D(A)A$, then A' is an $l \times n$ matrix with entries in $\mathcal{O}_K$, and $A\boldsymbol{x} = \mathbf{0}$ if and only $A'\boldsymbol{x} = \mathbf{0}$. Then apply Theorem 7.1 to the system $A'\boldsymbol{x} = \mathbf{0}$ while keeping in mind that $\mathcal{H}(A') = D(A)\mathcal{H}(A)$. □

8. Absolute values and height functions

In this section we introduce the basic machinery of absolute values and heights, which is used to investigate further questions in Diophantine Approximations and Diophantine Geometry.

Definition 8.1. Let K be a field. An *absolute value* on K is a function $|\ |: K \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in K$ we have:

(1) $|x| \geq 0$ with equality if and only if $x = 0$,
(2) $|xy| = |x||y|$,
(3) *Triangle inequality:* $|x+y| \leq |x| + |y|$.

Sometimes (3) can be replaced by the stronger property:

(4) *Ultrametric inequality:* $|x+y| \leq \max\{|x|, |y|\}$.

If $|\ |$ satisfies (1), (2), (3), but fails (4), we say that it is *archimedean* absolute value; if it also satisfies (4), it is called *non-archimedean.*

Here is the most basic example of an absolute value on K: it is called the *trivial* absolute value, and is defined by

$$|x| = \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \neq 0. \end{cases}$$

This is the only possible absolute value on a finite field.

We will say that two absolute values $|\ |_1$ and $|\ |_2$ on K are *equivalent* if there exists $\theta \in \mathbb{R}_{>0}$ such that

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

for all $x \in K$. In this case we will write $|\ |_1 \sim |\ |_2$. It is easy to see that an archimedean absolute value cannot be equivalent to a non-arhimedean one. This relation $\sim$ is an actual equivalence relation (Problem 11.5), and the only absolute value equivalent to the trivial one is itself (Problem 11.6).

Equivalence classes of nontrivial absolute values on K are called *places.* The set of all places of K will be denoted by $M(K)$. Notice that an absolute value $|\ |$ defines a metric on K:

$$(x, y) \to |x - y|$$

for every $x, y \in K$. Therefore $|\ |$ induces a metric topology on K. Moreover, we can talk about the *completion* of K with respect to this topology. K equipped with the metric induced by $|\ |$ is a metric space, we will write $(K, |\ |)$ to mean that we are thinking of K as a metric space with respect to this metric. Recall that a metric space $(K, |\ |)$ is called *complete* if every Cauchy sequence in K converges to a point in K. The *completion* of $(K, |\ |)$ is the set of all equivalence classes of Cauchy sequences on $(K, |\ |)$, where two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ are equivalent if

$$\lim_{n \to \infty} |a_n - b_n| = 0.$$

Notice that $|\ |$ is also defined on the completion of $(K, |\ |)$, and so this completion also has a metric topology induced by $|\ |$. Then $(K, |\ |)$ is complete if and only if it is equal to its completion; by "equal" here we mean isometrically isomorphic as fields: it is a well known fact that completion of a field is also a field, where addition and multiplication on Cauchy sequences are defined component-wise.

Notice that for an absolute value $|\ |$ on K, $x \to |x|$ is a homomorphism from the multiplicative group $K^\times = \{x \in K : x \neq 0\}$ to multiplicative group $\mathbb{R}_{>0}$. Therefore:

(1) $|1| = 1$,
(2) $|\zeta| = 1$ for every root of unity $\zeta \in K$, i.e. for every $\zeta \in K$ such that $\zeta^n = 1$ for some $n \in \mathbb{Z}_{>0}$,
(3) $|-x| = |x|$, for all $x \in K^\times$,
(4) $|x^{-1}| = |x|^{-1}$, for all $x \in K^\times$.

If L/K is an extension of fields and $|\ |$ is an absolute value on L, then its restriction to K is an absolute value on K. It is in general possible that $|\ |$ is non-trivial on L, but is trivial on K.

We will now demonstrate some standard absolute values on $\mathbb{Q}$. The first one is the usual absolute value, which we will denote by $|\ |_\infty$:

$$|x|_\infty = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$$

This is an archimedean absolute value (Problem 11.8), which induces the usual metric topology on $\mathbb{Q}$; the completion of $\mathbb{Q}$ with respect to this topology is $\mathbb{R}$. Sometimes we will write $\mathbb{Q}_\infty$ instead of $\mathbb{R}$ to stress this fact.

Now let $p \in \mathbb{Z}$ be a prime, and define the *p-adic* absolute value $|\ |_p$ on $\mathbb{Q}$ as follows. For each $n \in \mathbb{Z}$, let

$$|n|_p = p^{-\mu(n)},$$

where $p^{\mu(n)}$ is the largest power of p dividing n, hence $|n|_p \leq 1$ for each $n \in \mathbb{Z}$. Now for each $\frac{m}{n} \in \mathbb{Q}$, let

$$\left|\frac{m}{n}\right|_p = \frac{|m|_p}{|n|_p}.$$

This is a non-archimedean absolute value on $\mathbb{Q}$ for every prime p (Problem 11.9). The topology induced by $|\ |_p$ on $\mathbb{Q}$ is called *p-adic topology*; the completion of $\mathbb{Q}$ with respect to this is called the field of *p-adic numbers*, denoted by $\mathbb{Q}_p$. The set

$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p : |a|_p \leq 1\}$$

is a ring, and is called the ring of *p-adic integers.* Problem 11.10 implies that $\mathbb{Z} \subseteq \mathbb{Z}_p$ for every prime $p \in \mathbb{Z}$. Moreover, if we write $\mathcal{P}$ for the set of all primes in $\mathbb{Z}$, then

$$\mathbb{Z} = \bigcap_{p \in \mathcal{P}} \mathbb{Z}_p.$$

The important result classifying all absolute values on $\mathbb{Q}$ is Ostrowski's theorem.

Theorem 8.1 (Ostrowski, 1935)**.** *Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to either $|\ |_\infty$ or $|\ |_p$ for some $p \in \mathcal{P}$.*

Proof. We start with the following fact, the proof of which is deferred to Problem 11.11.

Lemma 8.2. *An absolute value $|\ |$ on $\mathbb{Q}$ is non-archimedean if and only if $|n| \leq 1$ for every $n \in \mathbb{Z}$. Moreover, for any absolute value $|\ |$ on $\mathbb{Q}$ there exists $\rho \in \mathbb{R}_{>0}$ such that*

$$|n| \leq |n|_\infty^\rho. \tag{8.1}$$

Now suppose $|\ |$ is an absolute value on $\mathbb{Q}$. We will use Lemma 8.2 throughout this proof, assuming without loss of generality that $\rho = 1$ in (8.1); indeed, $|\ |^{\frac{1}{\rho}}$ is equivalent to $|\ |$, so it is not important whether we prove that $|\ |^{\frac{1}{\rho}}$ or $|\ |$ is equivalent to $|\ |_{\infty}$ or $|\ |_p$ for some $p \in \mathcal{P}$.

Let $a, b \in \mathbb{Z}_{>0}$, $a > 1, b > 1$. For any $\nu \in \mathbb{Z}_{>0}$, there exists integers $c_0, \dots, c_n$ with $0 \leq c_i < a$ and $c_n \neq 0$ such that

$$b^{\nu} = c_0 + c_1 a + \dots + c_n a^n.$$

Notice that by Lemma 8.2 for each $0 \leq i \leq n$,

$$|c_i| \leq |c_i|_{\infty} \leq |a|_{\infty} = a.$$

Also notice that

$$a^n \leq c_n a^n \leq b^{\nu},$$

and so $n \leq \frac{\nu \log b}{\log a}$. Then

$$\begin{aligned} |b|^{\nu} = |b^{\nu}| &\leq \sum_{i=0}^{n} |c_i||a|^i \leq (n+1)\ a \max\{1, |a|\}^n \\ &\leq \left(1 + \frac{\nu \log b}{\log a}\right) a \max\{1, |a|\}^n. \end{aligned}$$

Therefore

$$|b| \leq \left(1 + \frac{\nu \log b}{\log a}\right)^{1/\nu} a^{1/\nu} \max\{1, |a|\}^{\frac{\log b}{\log a}} \to \max\left\{1, |a|^{\frac{\log b}{\log a}}\right\},$$

as $\nu \to \infty$, in other words

$$|b| \leq \max\left\{1, |a|^{\frac{\log b}{\log a}}\right\}. \tag{8.2}$$

Case 1. Assume $|\ |$ is archimedean. Then by Lemma 8.2, there exists $b \in \mathbb{Z}$ such that $|b| > 1$. Then by (8.2), $|a| > 1$ for every $a \in \mathbb{Z}$ except for -1,0,1. Therefore if $a, b \in \mathbb{Z}$, $a, b > 1$, then

$$|b|^{\frac{1}{\log b}} \leq |a|^{\frac{1}{\log a}} \leq |b|^{\frac{1}{\log b}},$$

and so

$$|b|^{\frac{1}{\log b}} = |a|^{\frac{1}{\log a}}.$$

We have

$$1 < |b| \leq |b|_{\infty} = b,$$

so $|b| = |b|_{\infty}^{\rho} = b^{\rho}$ for some $0 < \rho \leq 1$, and hence

$$|a| = |b|^{\frac{\log a}{\log b}} = b^{\rho \frac{\log a}{\log b}} = a^{\rho} = |a|_{\infty}^{\rho}.$$

Same way therefore $|\alpha| = |\alpha|_{\infty}^{\rho}$ for every $\alpha \in \mathbb{Q}$.

Case 2. Assume $|\ |$ is non-archimedean. Then by Lemma 8.2, $|n| \leq 1$ for every $n \in \mathbb{Z}$, and since $|\ |$ is non-trivial, there exists $a \in \mathbb{Z}$ such that $|a| < 1$. Let

$$I = \{a \in \mathbb{Z} : |a| < 1\}.$$

This is an ideal in $\mathbb{Z}$ (Problem 11.12). Therefore there exists a prime $p \in \mathbb{Z}$ such that $I = p\mathbb{Z}$. Let $0 \neq \alpha \in \mathbb{Q}$. Write

$$\alpha = p^r \frac{x}{y}$$

with $x, y \in \mathbb{Z}$ such that $p \nmid xy$. Then $x, y \notin I$, hence

$$|x| = |y| = 1,$$

and so

$$|\alpha| = |p^r| = |p|^r.$$

Since $p \in I$, $|p| < 1$, so $|p| = p^{-s}$ for some $s > 0$. Then

$$|\alpha| = p^{-rs} = |r|_p^s.$$

We have shown that $|\ |$ must be equivalent to either $|\ |_\infty$ or $|\ |_p$ for some prime p. This completes the proof. □

Therefore we can write

$$M(\mathbb{Q}) = \{\infty\} \cup \mathcal{P},$$

this way indexing the archimedean place by ∞, and non-archimedean places by p for each $p \in \mathcal{P}$.

Theorem 8.3 (Artin - Whaples Product Formula)**.** *If $0 \neq a \in \mathbb{Q}$, then*

$$|a|_\infty \prod_{p \in \mathcal{P}} |a|_p = 1.$$

Proof. Problem 11.13. □

Next we discuss absolute values on a number field K. If $|\ |$ is an absolute value on K, its restriction to $\mathbb{Q}$ is an absolute value on $\mathbb{Q}$, and so must belong to either ∞ or one of the p-adic places on $\mathbb{Q}$. Hence absolute values on K are precisely extensions of those on $\mathbb{Q}$. If $v \in M(K)$, we will write $|\ |_v$ for an absolute value that represents it. We know that $|\ |_v$ extends either $|\ |_\infty$ or $|\ |_p$ for some $p \in \mathcal{P}$, and we say that v *lies over* ∞ or p respectively; we denote it by writing $v|\infty$ or $v|p$. The place $v \in M(K)$ is archimedean if and only if $v|\infty$. Sometimes we will write $v \nmid \infty$ to mean that v is non-archimedean, i.e. lies over some p-adic place of $\mathbb{Q}$. For each place $u \in M(\mathbb{Q})$ there may be more than one place $v \in M(K)$ such that $v|u$, however each places $v \in M(K)$ lies over precisely one place $u \in M(\mathbb{Q})$.

First we describe all archimedean places of K. Let $\sigma_1, \dots, \sigma_r$ be real embeddings of K, and $\tau_1, \overline{\tau}_1, \dots, \tau_s, \overline{\tau}_s$ conjugate pairs of complex embeddings, then

$$r + 2s = d = [K : \mathbb{Q}].$$

Notice that since $\mathbb{Q}_\infty = \mathbb{R} \subset \mathbb{C}$, the absolute value $|\ |_\infty$ is defined on $\mathbb{R}$ and on $\mathbb{C}$. Also, for each $a \in K$

$$\sigma_i(a) \in \mathbb{R},\ \tau_j(a), \overline{\tau}_j(a) \in \mathbb{C}$$

for each $1 \leq i \leq r$ and $1 \leq j \leq s$. If ρ is one of these embeddings, then we define an absolute value $|\ |_\rho$ on K by

$$|a|_\rho = |\rho(a)|_\infty.$$

It is easy to notice that if $|\ |_{\tau_j} = |\ |_{\overline{\tau}_j}$ for each $1 \leq j \leq s$. However, the absolute values

$$|\ |_{\sigma_1}, \dots, |\ |_{\sigma_r}, |\ |_{\tau_1}, \dots, |\ |_{\tau_s}$$

are not equivalent to each other. These represent all the archimedean places of K. For each $v \in M(K)$, we will write K_v for the completion of K at v. If $v|u$ for some $u \in M(\mathbb{Q})$, then $K_v/\mathbb{Q}_u$ is an extension of fields, and we will define the *local degree* of K at v to be the degree of this extension, and denote it by

$$d_v = [K_v : \mathbb{Q}_u].$$

We will also write sometimes $\mathbb{Q}_v$ where $v \in M(K)$ to mean $\mathbb{Q}_u$, where $u \in M(\mathbb{Q})$ is the unique place over which v lies. Notice that if $v \in M(K)$ is archimedean, then K_v is either $\mathbb{R}$ or $\mathbb{C}$, depending on whether v is real or complex, i.e. corresponds to a real or to a complex embedding. Therefore, for each $v|\infty$

$$d_v = [K_v : \mathbb{Q}_\infty] = [K_v : \mathbb{R}] = \begin{cases} 1 & \text{if } v \text{ is real} \\ 2 & \text{if } v \text{ is complex.} \end{cases}$$

Therefore

$$\sum_{v|\infty} d_v = r + 2s = d.$$

Next we describe non-archimedean places of K. Let p be a prime in $\mathbb{Z}$, so that $(p) = p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. Recall that $\mathcal{O}_K$, the ring of algebraic integers of K, is a Dedekind domain, which means that there is unique factorization into prime ideals in $\mathcal{O}_K$. Notice that $\mathbb{Z} \in \mathcal{O}_K$, and so $p\mathcal{O}_K$ is an ideal in $\mathcal{O}_K$, although it may no longer be prime. Then there exist prime ideals $P_1, \dots, P_k$ and positive integers $e_1, \dots, e_k$ such that

$$p\mathcal{O}_K = P_1^{e_1} \dots P_k^{e_k},$$

and $\sum_{i=1}^k e_i = d$; each such e_i is called the *ramification degree* of P_i over p. First we define $|0|_{P_i} = 0$. Now let $0 \neq a \in \mathcal{O}_K$, then for each P_i, $1 \leq i \leq k$, define

$$\operatorname{ord}_{P_i} a = \max\{j \in \mathbb{Z} : a \in P_i^j\},$$

and let

$$|a|_{P_i} = p^{-\frac{\operatorname{ord}_{P_i} a}{e_i}}.$$

The number $\operatorname{ord}_{P_i} a$ is well-defined due to unique factorization of ideals into powers of prime ideals: it is precisely the power to which P_i divides $a\mathcal{O}_K$. Notice that K is the field of fractions of $\mathcal{O}_K$, i.e.

$$K = \left\{ \frac{a}{b} : a, b \in \mathcal{O}_K \right\}.$$

Then for each $\alpha = \frac{a}{b} \in K$ with $a, b \in \mathcal{O}_K$, define

$$|\alpha|_{P_i} = \frac{|a|_{P_i}}{|b|_{P_i}}. \tag{8.3}$$

This is an absolute value on K, which restricts to the usual p-adic absolute value on $\mathbb{Q}$ (Problem 11.14). Hence for each prime p in $\mathbb{Z}$, we defined absolute values lying over it; these are all the non-archimedean places of K. Suppose $v \in M(K)$ lies over p, and P_i is the corresponding prime ideal of $\mathcal{O}_K$ with ramification degree e_i over p. In a Dedekind domain every nonzero prime ideal is maximal, hence P_i is a maximal ideal, and so $\mathcal{O}_K/P_i$ is a field; in fact, it is a finite field of characteristic p, meaning that

$$|\mathcal{O}_K/P_i| = p^{f_i},$$

for some $f_i \in \mathbb{Z}_{>0}$. This f_i is called the *inertia degree* of P_i over p. Its significance for our purposes is that the local degree $d_v = [K_v : \mathbb{Q}_p]$ is equal to $e_i f_i$. A result from algebraic number theory implies that if $P_1, \ldots, P_k$ are prime ideals in $\mathcal{O}_K$ lying over a rational prime p with respective ramification degrees $e_1, \ldots, e_k$ and ramification degrees $f_1, \ldots, f_k$, then

$$\sum_{i=1}^{k} e_i f_i = d.$$

In particular this means that

$$\sum_{v|u} d_v = d$$

is true for any $u \in M(\mathbb{Q})$. The Artin - Whaples product formula works over a number field in a similar way as over $\mathbb{Q}$: we state here without proof.

Theorem 8.4. *If $0 \neq a \in K$, then*

$$\prod_{v \in M(K)} |a|_v^{d_v} = 1.$$

Example 8.1. *Let $K = \mathbb{Q}(\sqrt{2})$, then $d = 2$. Since K is totally real, there are no complex embeddings. Hence if $v \in M(K)$ is archimedean, then $K_v = \mathbb{R}$, and so $d_v = 1$. Since*

$$\sum_{v|\infty} d_v = 2,$$

K must have two archimedean places. These are precisely the places corresponding to embeddings $\sigma_1, \sigma_2 : K \to \mathbb{R}$, given by

$$\sigma_1(\sqrt{2}) = \sqrt{2},\ \sigma_2(\sqrt{2}) = -\sqrt{2},$$

and fixing $\mathbb{Q}$, hence σ_1 is the identity. Let v_1, v_2 be the archimedean places corresponding to embeddings σ_1, σ_2 respectively. Notice that for every $\alpha \in K$, there exist $a, b \in \mathbb{Q}$ such that $\alpha = a + b\sqrt{2}$, hence

$$|\alpha|_{v_1} = |\sigma_1(a + b\sqrt{2})|_\infty = |a + b\sqrt{2}|_\infty,$$

and

$$|\alpha|_{v_2} = |\sigma_2(a + b\sqrt{2})|_\infty = |a - b\sqrt{2}|_\infty.$$

Now let us look at non-archimedean places of K. Consider for instance all places $v \in M(K)$ lying over 7. Notice that

$$7 = (3 + \sqrt{2})(3 - \sqrt{2}),$$

therefore the ideal $7\mathcal{O}_K$ no longer prime in $\mathcal{O}_K$ splits as the product of these two prime ideals:

$$7\mathcal{O}_K = P_1 P_2,$$

where $P_1 = (3+\sqrt{2})\mathcal{O}_K$ and $P_2 = (3-\sqrt{2})\mathcal{O}_K$. This means that there are two places lying over 7, corresponding to P_1 and P_2, call them u_1 and u_2 respectively. Then $d_{u_1} = d_{u_2} = 1$. Notice for instance that

$$3+\sqrt{2} \in P_1,\ 3+\sqrt{2} \notin P_1^2,\ 3+\sqrt{2} \notin P_2,$$
$$3-\sqrt{2} \in P_2,\ 3-\sqrt{2} \notin P_2^2,\ 3-\sqrt{2} \notin P_1,$$

hence

$$|3+\sqrt{2}|_{u_1} = 7^{-1},\ |3-\sqrt{2}|_{u_1} = 7^0,$$
$$|3+\sqrt{2}|_{u_2} = 7^0,\ |3-\sqrt{2}|_{u_2} = 7^{-1}.$$

Recall that prime ideals in $\mathcal{O}_K$ are maximal. This implies that $3 \pm \sqrt{2}$ are not contained in any other prime ideal of $\mathcal{O}_K$, hence for every place $v \in M(K)$ which is not equal to v_1, v_2, u_1, or u_2, $|3 \pm \sqrt{2}|_v = 1$. Hence

$$\prod_{v \in M(K)} |3 \pm \sqrt{2}|_v = |3+\sqrt{2}|_\infty |3-\sqrt{2}|_\infty 7^{-1} = 1.$$

This is a demonstration of the product formula at work.

Remark 8.1. The same construction of absolute values as described in this section can be carried out for any field extension of number fields L/K. In this case, we would replace the ground field $\mathbb{Q}$ with K, and talk about places of L lying over places of K in the same precise manner. We will assume this more general construction going forward.

We now introduce *height functions*, which serve as the main tool used to measure arithmetic complexity. We have already seen an example of a height function $\mathcal{H}$ in Section 7, however $\mathcal{H}$ only carries archimedean information: it only measured the size of a given algebraic number at the archimedean places. We are now prepared to define more general heights on vectors, which incorporate arithmetic information at all the places of a number field. As above, K is a number field of degree d over $\mathbb{Q}$ and $M(K)$ is its set of places. Let $n \geq 2$ be an integer. For each place v of K we define a *local height* H_v for each vector $\boldsymbol{x} \in K_v^n$ by

$$H_v(\boldsymbol{x}) = \begin{cases} \left(\sum_{i=1}^n |x_i|_v^2\right)^{\frac{1}{2}} & \text{if } v|\infty, \\ \max_{1 \leq i \leq n} |x_i|_v & \text{if } v \nmid \infty. \end{cases}$$

Then for each $\mathbf{0} \neq \boldsymbol{x} \in K^n$, define the *global height* H_K by

$$H_K(\boldsymbol{x}) = \prod_{v \in M(K)} H_v(\boldsymbol{x})^{d_v}. \tag{8.4}$$

Notice that for each $\mathbf{0} \neq \boldsymbol{x} \in K^n$, $H_v(\boldsymbol{x}) = 1$ for all but finitely many places v of K, hence the product in (8.4) is actually finite, therefore convergent, meaning that H_K is well-defined. Also notice that if $0 \neq \alpha \in K$ and $\mathbf{0} \neq \boldsymbol{x} \in K^n$, then

$$\begin{aligned} H_K(\alpha\boldsymbol{x}) &= \prod_{v \in M(K)} |\alpha|_v^{d_v} H_v(\boldsymbol{x})^{d_v} \\ &= \left(\prod_{v \in M(K)} |\alpha|_v^{d_v}\right) \prod_{v \in M(K)} H_v(\boldsymbol{x})^{d_v} = H_K(\boldsymbol{x}) \qquad (8.5) \end{aligned}$$

by the product formula. This means that H_K is a *homogeneous* function, and so is *projectively defined.* Indeed, define an equivalence relation on $K^n \setminus \{\mathbf{0}\}$ by writing

$\boldsymbol{x} \sim \boldsymbol{y}$ whenever $\boldsymbol{x} = \alpha \boldsymbol{y}$ for some $0 \neq \alpha \in K$. It is easy to check that this indeed is an equivalence relation, and we write $[x_1 : \cdots : x_n]$ for the equivalence class of the vector $\boldsymbol{x} = (x_1, \dots, x_n) \in K^n$, which is called the *projective point* corresponding to $\boldsymbol{x}$. The space of all projective points on K^n is called the $(n-1)$-dimensional *projective space* over K, i.e.

$$\mathbb{P}^{n-1}(K) = \{[x_1 : \cdots : x_n] : (x_1, \dots, x_n) \in K^n \setminus \{\mathbf{0}\}\}.$$

Notice that this is precisely the space of all lines through the origin in K^n, i.e. the space of 1-dimensional subspaces of K^n. This is the simplest example of the more general construction of Grassmannian that we will encounter later. Then (8.5) implies that H_K is well-defined on $\mathbb{P}^{n-1}(K)$, i.e. it can be viewed as a function $H_K : \mathbb{P}^{n-1}(K) \to \mathbb{R}_{>0}$.

Notice that the definition of H_K depends on K. Let L be an extension of K of degree e, hence $[L : \mathbb{Q}] = de$. For each place $v \in M(L)$, we will write $e_v = [L_v : K_v]$, hence $[L_v : \mathbb{Q}_v] = d_v e_v$. Also notice that

$$\sum_{v \in M(L), v|u} e_v = e$$

for each place $u \in M(K)$. Suppose that $\mathbf{0} \neq \boldsymbol{x} \in K^n$, then

$$H_L(\boldsymbol{x}) = \prod_{v \in M(L)} H_v(\boldsymbol{x})^{d_v e_v} = \prod_{u \in M(K)} \prod_{v \in M(L), v|u} H_v(\boldsymbol{x})^{d_u e_v},$$

but since $\boldsymbol{x} \in K^n$, $H_v(\boldsymbol{x}) = H_{v'}(\boldsymbol{x})$ whenever $v, v' \in M(L)$ lie over the same place $u \in M(K)$. Hence:

$$H_L(\boldsymbol{x}) = \prod_{u \in M(K)} H_u(\boldsymbol{x})^{d_u \sum_{v \in M(L), v|u} e_v} = \prod_{u \in M(K)} H_u(\boldsymbol{x})^{d_u e} = H_K(\boldsymbol{x})^e.$$

This suggests that if we want a height function that does not depend on the field of definition, we may want to introduce the normalizing exponent $\frac{1}{[K:\mathbb{Q}]}$.

Definition 8.2. Let $\overline{\mathbb{Q}}$ be the field of all algebraic numbers, as before. Define the *absolute height* $H : \overline{\mathbb{Q}}^n \setminus \{\mathbf{0}\} \to \mathbb{R}_{>0}$ by

$$H(\boldsymbol{x}) = H_K(\boldsymbol{x})^{\frac{1}{[K:\mathbb{Q}]}}$$

for every $\mathbf{0} \neq \boldsymbol{x} \in \overline{\mathbb{Q}}^n$, where K is any number field containing the coordinates of $\boldsymbol{x}$. By the discussion above, H does not depend on the choice of this number field. Once again, notice that H is projectively defined. We will also adopt a convention that $H(\mathbf{0}) = 1$.

We also define the *inhomogeneous height* $h_K : K^n \to \mathbb{R}_{>0}$ by

$$h_K(\boldsymbol{x}) = H_K(1, \boldsymbol{x}),$$

for every $\boldsymbol{x} \in K^n$, and the *absolute inhomogeneous height* $h : \overline{\mathbb{Q}}^n \to \mathbb{R}_{>0}$ by

$$h(\boldsymbol{x}) = h_K(\boldsymbol{x})^{\frac{1}{[K:\mathbb{Q}]}},$$

for every $\boldsymbol{x} \in \overline{\mathbb{Q}}^n$, where K is any number field containing the coordinates of $\boldsymbol{x}$. Notice that h_K and h are no longer projectively defined, i.e. if $\alpha \in \overline{\mathbb{Q}}$, then $h(\alpha \boldsymbol{x})$ is not necessarily equal to $h(\boldsymbol{x})$. Also notice that for every $\boldsymbol{x} \in \overline{\mathbb{Q}}^n$,

$$H(\boldsymbol{x}) \leq h(\boldsymbol{x}).$$

For any algebraic number $\alpha \in \overline{\mathbb{Q}}$, we define its *Weil height* to be

$$h(\alpha) = H(1, \alpha).$$

We now briefly outline the basic properties of heights, proofs of which are left to the exercises.

Lemma 8.5. *The following statements are true:*

(1) *If* $\boldsymbol{x} \in \mathbb{Z}$ *is such that* $\gcd(x_1, \dots, x_n) = 1$*, then*

$$H(\boldsymbol{x}) = \|\boldsymbol{x}\|_2 = \left(x_1^2 + \dots + x_n^2\right)^{\frac{1}{2}},$$

i.e. height of an integer vector is the Euclidean norm of the corresponding primitive vector.

(2) *If* $0 \neq x_0 \in \mathbb{Z}$*, and*

$$\boldsymbol{x} = \left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{Q}^n,$$

is such that $\gcd(x_0, x_1, \dots, x_n) = 1$*, then*

$$h(\boldsymbol{x}) = \left(x_0^2 + x_1^2 + \dots + x_n^2\right)^{\frac{1}{2}},$$

i.e. the inhomogeneous height of a rational vector is the Euclidean norm of the corresponding reduced integer vector $(x_0, x_1, \dots, x_n)$*.*

Proof. Problem 11.15. □

Lemma 8.6. *If* $m_1, \dots, m_k \in \mathbb{Z}$*, and* $\boldsymbol{x}_1, \dots, \boldsymbol{x}_k \in \overline{\mathbb{Q}}^n$*, then*

$$h\left(\sum_{i=1}^k m_i \boldsymbol{x}_i\right) \leq \left(\sum_{i=1}^k m_i^2\right)^{\frac{1}{2}} \prod_{i=1}^k h(\boldsymbol{x}_i).$$

In particular, if $\alpha_1, \dots, \alpha_k \in \overline{\mathbb{Q}}$*, then*

$$h\left(\sum_{i=1}^k m_i \alpha_i\right) \leq \left(\sum_{i=1}^k m_i^2\right)^{\frac{1}{2}} \prod_{i=1}^k h(\alpha_i).$$

Additionally, for any $\alpha, \beta \in \overline{\mathbb{Q}}$*,*

$$h(\alpha\beta) \leq h(\alpha)h(\beta).$$

Proof. Problem 11.16. □

Lemma 8.7. *Suppose that* K *and* L *are isomorphic number fields with* $\sigma : K \to L$ *an isomorphism, and let us also write* σ *for the isomorphism it induces from* K^n *to* L^n *for each integer* $n \geq 1$*. Then*

$$H(\sigma(\boldsymbol{x})) = H(\boldsymbol{x})$$

for each $\boldsymbol{x} \in K$*. Hence conjugate vectors have the same height. Notice in particular that this implies that conjugate algebraic numbers have the same height.*

Proof. Problem 11.17. □

The notion of height also extends to polynomials. In particular, if F is a polynomial with coefficients $a_1, \dots, a_n \in \overline{\mathbb{Q}}$, then we define

$$H(F) = H(a_1, \dots, a_n).$$

Lemma 8.8. *Let $P(X), Q(X) \in \overline{\mathbb{Q}}[X]$ be polynomials in one variable with coefficients in $\overline{\mathbb{Q}}$ of degrees n_1, n_2 respectively, and let $n = \min\{n_1, n_2\}$. Then*

$$H(PQ) \leq \sqrt{n+1}\ H(P)H(Q).$$

Proof. Let K be a number field containing coefficients of P and Q, and suppose it has degree d over $\mathbb{Q}$. It is easy to observe that for every $v \in M(K)$ such that $v \nmid \infty$,

$$H_v(PQ) = H_v(P)H_v(Q),$$

where these are precisely the local heights of corresponding coefficient vectors. Let $v \in M(K)$, $v|\infty$, then by Problem 11.18

$$H_v(PQ) \leq \sqrt{n+1}\ H_v(P)H_v(Q).$$

Therefore we have:

$$\begin{aligned} H(PQ) &= \prod_{v \in M(K)} H_v(PQ)^{\frac{d_v}{d}} \\ &\leq \prod_{v \nmid \infty} (H_v(P)H_v(Q))^{\frac{d_v}{d}} \prod_{v | \infty} \left(|n+1|_v^{\frac{1}{2}}\ H_v(P)H_v(Q) \right)^{\frac{d_v}{d}} \\ &= H(P)H(Q) \prod_{v|\infty} |n+1|_v^{\frac{d_v}{2d}} \\ &= \left(\sqrt{n+1}\right)^{\frac{\sum_{v|\infty} d_v}{d}} H(P)H(Q) = \sqrt{n+1}\ H(P)H(Q). \end{aligned}$$

This completes the proof. □

Corollary 8.9. *Suppose that*

$$P(X) = a_d(X - \alpha_1) \dots (X - \alpha_d),$$

where $a_d, \alpha_1, \dots, \alpha_d \in \overline{\mathbb{Q}}$. Then

$$H(P) \leq 2^{\frac{d-1}{2}} h(\alpha_1) \dots h(\alpha_d). \tag{8.6}$$

Proof. Notice that here we can view $P(X)$ as a product of d linear polynomials in one variable, hence applying Lemma 8.8 $d-1$ times yields (8.6). □

For a vector $\boldsymbol{x} \in \overline{\mathbb{Q}}^n$, we define its *degree* to be

$$\deg(\boldsymbol{x}) = [\mathbb{Q}(x_1, \dots, x_n) : \mathbb{Q}].$$

Also, for a projective point $[\boldsymbol{x}]$ we write $\deg([\boldsymbol{x}])$ to mean the minimum of $\deg(\boldsymbol{x})$ taken over all representatives of $[\boldsymbol{x}]$. We are now ready to prove the fundamental property of heights, which was first established by Northcott in 1949 [Nor49]: this result is known as Northcott's theorem, and any height function satisfying this theorem (there are others, not only our H) is said to satisfy *Northcott's finiteness property.*

Theorem 8.10. *Let n, d, B be positive integers. Then the set*

$$S_n(B,d) = \left\{ [\boldsymbol{x}] \in \mathbb{P}^{n-1}(\overline{\mathbb{Q}}) : \deg([\boldsymbol{x}]) \leq d,\ H(\boldsymbol{x}) \leq B \right\}$$

is finite.

Proof. If $\boldsymbol{x} = (x_1, x_2, \dots, x_n) \in \overline{\mathbb{Q}}^n$ with $x_i \neq 0$ for some $1 \leq i \leq n$, then $H(\boldsymbol{x}) = H\left(\frac{\boldsymbol{x}}{x_i}\right)$. Therefore we can always choose a representative $\boldsymbol{x}$ of $[\boldsymbol{x}] \in \mathbb{P}^{n-1}(\overline{\mathbb{Q}})$ with one coordinate equal to 1. Without loss of generality assume $\boldsymbol{x} = (1, x_2, \dots, x_n) \in \overline{\mathbb{Q}}^n$, then

$$H(\boldsymbol{x}) \geq H(1, x_i) = h(x_i), \ \forall\ 2 \leq i \leq n.$$

Therefore it suffices to prove that the set

$$S(B,d) = \left\{\alpha \in \overline{\mathbb{Q}} : \deg(\alpha) \leq d,\ h(\alpha) \leq B\right\}$$

is finite. Notice that if $\alpha \in S(B,d)$, then it must be a root of a monic polynomial with rational coefficients of degree at most d

$$P(X) = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_d),$$

where $\alpha = \alpha_1, \alpha_2, \dots, \alpha_d$ are conjugates of α. By Lemma 8.7, $h(\alpha) = h(\alpha_i)$ for every $1 \leq i \leq d$, and so $h(\alpha_i) \leq B$ for all $1 \leq i \leq d$. By Corollary 8.9,

$$H(P) \leq 2^{\frac{d-1}{2}} h(\alpha_1) \dots h(\alpha_d) \leq 2^{\frac{d-1}{2}} B^d. \tag{8.7}$$

Since $P(x)$ is monic, let $\left(\frac{m_0}{m}, \dots, \frac{m_{d-1}}{m}, 1\right) \in \mathbb{Q}$ be the coefficient vector of P, written is such a way that $\gcd(m, m_0, \dots, m_{d-1}) = 1$. Then by Lemma 8.5,

$$H(P) = \sqrt{m^2 + m_0^2 + \dots + m_{d-1}^2} = \|\boldsymbol{m}\|_2,$$

where $\boldsymbol{m} = (m, m_0, \dots, m_{d-1}) \in \mathbb{Z}^{d+2}$, and $\|\ \|_2$ stands for the Euclidean norm, as usual. It is now easy to see that there are only finitely many integral vectors $\boldsymbol{m}$ with $\|\boldsymbol{m}\|_2 \leq 2^{\frac{d-1}{2}} B^d$, and so there are only finitely many polynomials P satisfying (8.7). This means that $S(B,d)$ must be finite, and so completes the proof. □

Remark 8.2. The cardinality of $S_n(B,d)$ has been investigated by various authors, starting with a result of Schanuel in 1979. More recently there were upper and lower bounds produced by Schmidt, Gao, Thunder, Masser, Vaaler, and Widmer among others, however there still is no known general asymptotic formula for $|S_n(B,d)|$ (see [Wid09] and [Wid10] for some recent results and a more detailed bibliogrpahy).

Next we will show how the notion of height can be extended to subspaces of K^n. Let $V \subseteq K^n$ be an ℓ-dimensional subspace, $1 \leq \ell \leq n$. Let $\boldsymbol{x}_1, \dots, \boldsymbol{x}_\ell$ be a basis for V, and write $X = (\boldsymbol{x}_1\ \dots\ \boldsymbol{x}_\ell)$ for the corresponding $n \times \ell$ basis matrix. Let $\mathcal{I}$ be the set of subsets of $\{1, \dots, n\}$ of cardinality ℓ, then

$$|\mathcal{I}| = \binom{n}{\ell}.$$

For each $I \in \mathcal{I}$, let X_I be the $\ell \times \ell$ submatrix of X whose rows are indexed by elements of I. We introduce lexicographic ordering on elements of $\mathcal{I}$, and write

$$\mathcal{I} = \left\{I_1, \dots, I_{\binom{n}{\ell}}\right\}$$

with respect to that order. Then define a vector of *Grassmann coordinates* (also known as *Plücker coordinates*) of V with respect to the basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_\ell$ to be

$$g(X) = \left(\det(X_{I_1}), \dots, \det\left(X_{I_{\binom{n}{\ell}}}\right)\right) \in K^{\binom{n}{\ell}}.$$

Suppose $\boldsymbol{y}_1, \dots, \boldsymbol{y}_\ell$ is a different basis for V, and write Y for the corresponding basis matrix. Then there exists a matrix $U \in GL_\ell(K)$ such that

$$Y = XU,$$

and so it is easy to see that

$$g(Y) = \det(U) g(X).$$

As before, we write $[g(X)]$ for the projective point in $\mathbb{P}^{\binom{n}{\ell}-1}$ represented by the vector $g(X)$, hence $[g(X)] = [g(Y)]$, and so we denote this projective point $[g(V)]$ to indicate that it does not depend on the choice of the basis. Define

$$\mathbb{G}_n^\ell(K) = \{[g(V)] : V \subseteq K^n,\ \dim_K(V) = \ell\}.$$

$\mathbb{G}_n^\ell(K)$ is called the $\binom{n}{\ell}$-*Grassmann component* of K^n, and this is the projective space whose points correspond to ℓ-dimensional subspaces of K^n. Notice that this is a generalization of the projective space $\mathbb{P}^{n-1}(K)$, which can be thought of as the space of one-dimensional subspaces of K^n. This is perhaps the simplest example of a parameter space, i.e. of a general type of objects in algebraic geometry which are called *moduli spaces.*

Using this notation, we can now define height of an ℓ-dimensional subspace V of K^n by

$$H(V) = H(g(V)). \tag{8.8}$$

Of course, this works in precisely the same manner for subspaces of $\overline{\mathbb{Q}}^n$. This height function on subspaces of a vector space was originally introduced by W. M. Schmidt in [Sch67] and is called the *Schmidt height.* We also define Schmidt height on matrices: for an $n \times m$ matrix A over K, $1 \leq m \leq n$ we let

$$H(A) = H\left(\operatorname{span}_K \{\boldsymbol{a}_1, \dots, \boldsymbol{a}_m\}\right),$$

where $\boldsymbol{a}_1, \dots, \boldsymbol{a}_m$ are column vectors of A. If $m > n$, we define $H(A)$ to be $H(A^\top)$. Suppose the m-dimensional vector subspace $V \subset K^n$ is described as

$$V = \{A\boldsymbol{x} : \boldsymbol{x} \in K^m\} = \{\boldsymbol{y} \in K^n : B\boldsymbol{y} = \boldsymbol{0}\}$$

for the $n \times m$ matrix A and $(n-m) \times n$ matrix B over K, respectively. Then the Brill-Gordan duality principle [Gor73] (also see Theorem 1 on page 294 of [HP47]) states that

$$H(A) = H(B) = H(V). \tag{8.9}$$

We also recall here a useful property of height functions that we will need: this is Lemma 4.7 of [RT96].

Lemma 8.11. *Let V be a subspace of K^n and let $U_1, \dots, U_m$ be subspaces of V such that $V = \operatorname{span}_K\{U_1, \dots, U_m\}$. Then*

$$H(V) \leq H(U_1) \cdots H(U_m).$$

Height can also be defined for more general objects, such as algebraic varieties and intersection cycles; this is done in a manner similar in spirit to the simplest case of linear varieties (namely vector subspaces) that we considered here, namely by parametrizing these objects in an appropriate manner. This, however, is more in the realm of arithmetic geometry, and out of the scope of our exposition.

9. Siegel's lemma revisited

In this section, we revisit Siegel's lemma we introduced in Sections 2 and 7, but this time in a more powerful form. Let us look back at Theorems 2.1 and 7.1: they provide a bound on the height of a solution to a homogeneous linear system in terms of the height of the coefficient matrix A of this system. Notice, however, that if we multiply A by 2 the solution space does not change, but height of A certainly changes in a way that would affect the upper bounds of these theorems. This problem is circumvented by using Schmidt height (8.8) on the solution space instead of the height of a coefficient matrix. The following version of Siegel's lemma was proved by Bombieri and Vaaler in 1983, see [BV83].

Theorem 9.1. *Let V be an m-dimensional subspace of K^n, $m < n$. Then there exists a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m \in \mathcal{O}_K^n$ for V such that*

$$\prod_{i=1}^{m} H(\boldsymbol{x}_i) \leq \left\{ n|\Delta_K|^{1/d} \right\}^{m/2} H(V), \tag{9.1}$$

where Δ_K is the discriminant of K, and $d = [K : \mathbb{Q}]$ as usual.

In other words, Theorem 9.1 states that a subspace V of K^n has a basis of relatively small height with coordinates in $\mathcal{O}_K$, where the bound on the height is explicit and depends on the height of V. In particular, it implies the existence of a non-zero point of small height in V, bounded as follows.

Corollary 9.2. *Let V be an m-dimensional subspace of K^n, $m < n$. Then there exists $\boldsymbol{0} \neq \boldsymbol{x} \in \mathcal{O}_K^n \cap V$ such that*

$$H(\boldsymbol{x}) \leq \left\{ n|\Delta_K|^{1/d} \right\}^{1/2} H(V)^{1/m}. \tag{9.2}$$

This corollary can be viewed as a generalization of Minkowski's Convex Body Theorem (Problem 11.19). The dependence on $H(V)$ in (9.1) and (9.2) is sharp. An analogous bound has been proved for a small-height basis of a subspace V of $\overline{\mathbb{Q}}^n$ by Roy and Thunder, see [RT96], where the constant in the upper bound does not depend on any number field; this is often desired, since Δ_K can be quite large.

Theorem 9.3. *Let V be an m-dimensional subspace of $\overline{\mathbb{Q}}^n$, $m < n$. Then for every $\varepsilon > 0$, there exists a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m \in \overline{\mathbb{Q}}^n$ for V such that*

$$\prod_{i=1}^{m} H(\boldsymbol{x}_i) \leq \left(e^{\frac{m(m-1)}{4}} + \varepsilon \right) H(V).$$

While the Roy-Thunder bound does not depend on any number field, the basis vectors $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$ they produce are also not guaranteed to lie over a fixed number field. Bridging between the Bombieri-Vaaler and the Roy -Thunder results, we establish [FF24] the existence of a small-height basis for an m-dimensional subspace of K^n (i.e., the space of solutions to a system of simultaneous linear equations), and the inequalities we prove are free of constants that depend on a number field. While we bound the individual heights of the vectors instead of the product, our basis lies over a fixed number field K and our bound is particularly simple.

Theorem 9.4. *Let $V \subset K^n$ be an m-dimensional subspace, $1 \leq m < n$. Then there exists a basis $\boldsymbol{x}_1, \dots, \boldsymbol{x}_m$ for V such that*

$$\max_{1 \leq j \leq m} H(\boldsymbol{x}_j) \leq H(V). \tag{9.3}$$

Proof. Since $\dim_K V = m$, there exists an $(n-m)\times n$ matrix A of rank $n-m$ with entries in K so that

$$V = \{\boldsymbol{x} \in K^n : A\boldsymbol{x} = \boldsymbol{0}\},$$

then $H(A) = H(V)$. Since $\operatorname{rk}(A) = n-m$, there must exist standard basis vectors $\boldsymbol{e}_{i_1},\dots,\boldsymbol{e}_{i_m} \in K^n$ so that the matrix $B := \begin{pmatrix} A \\ E \end{pmatrix}$ with $E := (\boldsymbol{e}_{i_1} \ \dots \ \boldsymbol{e}_{i_m})^\top$ is in $\mathrm{GL}_n(K)$. Now, for each $1 \leq j \leq m$ define the vector

$$\boldsymbol{x}_j = B^{-1}\boldsymbol{e}_{j+n-m},$$

which is the $(j+n-m)$-th column vector of the matrix B^{-1}. Notice then that for every $1 \leq j \leq m$, $A\boldsymbol{x}_j = 0$, i.e. $\boldsymbol{x}_j \in V$. Further, these vectors are linearly independent since they are columns of a nonsingular matrix B^{-1}, and so they form a basis for V. We will now estimate their heights.

Let us write B_j for the $(n-1)\times n$ submatrix of B without the $(j+n-m)$-th row, then $B_j\boldsymbol{x}_j = \boldsymbol{0}$ since the $(j+n-m)$-th is the only row of B whose dot-product with the $(j+n-m)$-th column of B^{-1} is nonzero. Then we have

$$\operatorname{span}_K \boldsymbol{x}_j = \{\boldsymbol{y} \in K^n : B_j\boldsymbol{y} = \boldsymbol{0}\},$$

and so $H(\boldsymbol{x}_j) = H(B_j)$ by (8.9). On the other hand, $H(B_j) = H(B_j^\top)$ is equal to the height of the $(n-1)$-dimensional subspace of K^n spanned by the row-vectors of B_j. These row-vectors are the row-vectors of A and all but one row-vectors of E, therefore by Lemma 8.11,

$$H(\boldsymbol{x}_j) = H(B_j) \leq H(A) \prod_{k=1, k\neq j+n-m}^{m} H(\boldsymbol{e}_k) = H(A) = H(V),$$

since height of a standard basis vector is equal to 1. This completes the proof. □

Remark 9.1. While (9.1) is a stronger result than (9.3), in general it does not imply a better bound on $\max_{1\leq j\leq m} H(\boldsymbol{x}_j)$ than (9.3). Further, the bound of (9.3) does not depend on the number field K: this is a feature of a so-called *absolute* result such as the absolute Siegel's lemma given in [RT96]. While the bound presented in [RT96] is analogous to (9.1) with the constant in the bound independent of any number field, the basis vectors constructed there lie in $\overline{\mathbb{Q}}$ and not in a fixed number field either. On the other hand, our Theorem 9.4 guarantees vectors lying in K^n. Due to these features, our Theorem 9.4 may be preferable to these classical results in some specific situations where $|\Delta_K|$ dominates $H(V)$.

10. Some generalizations over number fields

In this section we state (without proof) generalizations over number fields of some of the above results on quadratic and multilinear polynomials.

First, consider the case of a quadratic hypersurface. Namely, let

$$F(\boldsymbol{X}) = \sum_{i=1}^{n} \sum_{j=1}^{n} f_{ij} X_i X_j \in K[X_1, \dots, X_n]$$

be a quadratic form in n variables with coefficients in the number field K of degree d over $\mathbb{Q}$. We say that F is *isotropic* over K if there exists $\boldsymbol{0} \neq \boldsymbol{x} \in K^n$ such that $F(\boldsymbol{x}) = 0$. Provided that F is isotropic over K, we are interested in proving the existence of a non-zero point of bounded height in the quadratic variety

$$\mathcal{V}_K(F) = \{\boldsymbol{x} \in K^n : F(\boldsymbol{x}) = 0\}$$

with an explicit bound on height. The following number-field generalization of Cassels' theorem (Theorem 4.1) was obtained by Raghavan in 1975; see [Rag75].

Theorem 10.1. *Let F be a quadratic form, which is isotropic over K as above, then there exists $\boldsymbol{0} \neq \boldsymbol{x} \in \mathcal{V}_K(F)$ such that*

$$H(\boldsymbol{x}) \leq c_1(K, n) H(F)^{\frac{n-1}{2}},$$

where the constant $c_1(K, n)$ in the upper bound is explicit and depends on K and n.

For the case of an inhomogeneous quadratic polynomial F over a number field K, given by

$$F(\boldsymbol{X}) = \sum_{i=1}^{n} \sum_{j=1}^{n} f_{ij} X_i X_j + \sum_{i=1}^{n} f_{0i} X_i + f_{00} \in K[X_1, \dots, X_n],$$

we suppose that

$$\mathcal{V}_K(F) = \{\boldsymbol{x} \in K^n : F(\boldsymbol{x}) = 0\}$$

is not empty. Then we have the following number-field generalization of Masser's theorem (Theorem 5.1); see [Fuk04].

Theorem 10.2. *Let F be a quadratic form in $n+1 \geq 2$ variables with coefficients in K. Suppose that there exists $\boldsymbol{x} = (x_0, ..., x_n) \in K^{n+1}$ such that $F(\boldsymbol{x}) = 0$ and $x_0 \neq 0$, then there exists such $\boldsymbol{x}$ with*

$$H(\boldsymbol{x}) \leq c_2(K, n) H(F)^{\frac{n+1}{2}},$$

where the constant in the upper bound is explicit, and depends in particular on Δ_K.

See also [Fuk13] for a survey of a vast variety of further results on Cassels' and Masser's theorems and their many generalizations, including the more complicated inhomogeneous situation over the ring of integers instead of a field.

What can be said about bounds on height of solutions of polynomials of degree higher than 2 in an arbitrary number of variables over a fixed number field K of degree d and discriminant Δ_K? We can state a rather general result for a system of polynomials of arbitrary degree, linear in some of the variables. Specifically, let $F(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ and let $1 \leq k < n$. Let $[n] = \{1, \dots, n\}$, $I =$

$\{i_1, \dots, i_k\} \subset [n]$, and $I' = [n] \setminus I$. Let $\boldsymbol{x}_{I'} = (x_j)_{j \in I'}$. We will say that F is linear in I-separated variables if

$$F(x_1, \dots, x_n) = \sum_{j=1}^{k} x_{i_j} F_j(\boldsymbol{x}_{I'}) + F_{k+1}(\boldsymbol{x}_{I'}), \tag{10.1}$$

where $F_j(\boldsymbol{x}_{I'}) \in K[\boldsymbol{x}_{I'}]$ for $1 \leq j \leq k+1$ are any polynomials in $n-k$ variables indexed by I' with coefficients in K. For a polynomial $F(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$, we define its zero-set over K

$$Z_K(F) = \{\boldsymbol{z} \in K^n : F(\boldsymbol{z}) = 0\}.$$

We also write $\mathcal{N}(F)$ for the number of nonzero monomials of F and $h(\Box) = H(1, \Box)$ for the inhomogeneous height, as before. The following result is proved in [FF23].

Theorem 10.3. *Let I be as above and let*

$$F_l(x_1, \dots, x_n) = \sum_{j=1}^{k} x_{i_j} F_{l,j}(\boldsymbol{x}_{I'}) + F_{l,k+1}(\boldsymbol{x}_{I'}),\ 1 \leq l \leq k$$

be polynomials over K of respective degrees $m_1, \dots, m_k$ linear in I-separated variables as in (10.1)*. Consider the inhomogeneous system*

$$\left.\begin{array}{rl} F_1(x_1, \dots, x_n) = \sum_{j=1}^{k} x_{i_j} F_{1,j}(\boldsymbol{x}_{I'}) + F_{1,k+1}(\boldsymbol{x}_{I'}) & = 0 \\ & \vdots \\ F_k(x_1, \dots, x_n) = \sum_{j=1}^{k} x_{i_j} F_{k,j}(\boldsymbol{x}_{I'}) + F_{k,k+1}(\boldsymbol{x}_{I'}) & = 0 \end{array}\right\} \tag{10.2}$$

of linear equations in the variables $x_{i_1}, \dots, x_{i_k}$ with coefficients $F_{l,j}(\boldsymbol{x}_{I'})$, $1 \leq l \leq k$, $1 \leq j \leq k+1$. Assume that the matrix $\mathcal{F} := (F_{l,j}(\boldsymbol{x}_{I'}))_{1 \leq l \leq k, 1 \leq j \leq k}$ of the corresponding homogeneous system has the same rank as the coefficient matrix of inhomogeneous system, i.e., $\mathcal{F}$ augmented by the column $(F_{l,k+1}(\boldsymbol{x}_{I'}))_{1 \leq l \leq k}$. Then $\bigcap_{l=1}^{k} Z_K(F_l) \neq \emptyset$ and there exists a point $\boldsymbol{z} \in \bigcap_{l=1}^{k} Z_K(F_l)$ with

$$h(\boldsymbol{z}) \leq k^{k+1} |\Delta_K|^{\frac{1}{d}} \left(\frac{D+2}{2}\right)^{2km+1} (\mathcal{N}\mathfrak{H})^{2k},$$

where

$$D = \sum_{l=1}^{k} m_l,\ m = \max_{1 \leq l \leq k} m_l,$$
$$\mathcal{N} = \max_{1 \leq l \leq k} \mathcal{N}(F_l),\ \mathfrak{H} = \max_{1 \leq l \leq k} h(F_l).$$

There are some known results in this direction for rational cubic forms in large enough number of variables: the current state of the art in this direction is a rather technical result obtained in [BDE12]. For sufficiently general polynomials of higher degree, this problem seems to be out of reach at the present time. In fact, such a bound would provide an algorithm to decide whether a Diophantine equation has an integral solution, and so would imply a positive answer to Hilbert's 10th problem in this case, i.e. this would mean that there exists an algorithm to decide whether such an equation has nontrivial integral solutions. However, by the famous theorem of Matijasevich [Mat70] Hilbert's 10th problem is undecidable. This means that in general such bounds do not exist over $\mathbb{Q}$; in fact, they seem unlikely to exist over any fixed number field even for a quartic polynomial (see [Mas02] for further details).

One can ask if it is possible to obtain a search bound for a system of quadratic equations. There is a reduction method (sometimes called Skolem reduction) that allows to describe the solution set of a single polynomial of arbitrary degree in terms of a system of quadratic equations, albeit in more variables. For instance, here is an example from [Mas02]:

$$x^3 + y^3 + z^3 = 3$$

is equivalent over $\mathbb{Z}$ to the system

$$xu + yv + zw = 3,\ u = x^2,\ v = y^2,\ w = z^2.$$

Since it is unlikely that there are search bounds for polynomial of high degree, it seems equally unlikely that they exist for systems of quadratic equations.

The problem becomes easier if we allow for solutions to lie over some extension of K of bounded degree. The following basic bound is easy to prove (see [Fuk09]).

Proposition 10.4. *Let $d \geq 1$, $n \geq 2$, and $F(X_1, ..., X_n)$ be a homogeneous polynomial in n variables of degree d with coefficients in a number field K. There exists $\mathbf{0} \neq \boldsymbol{z} \in \overline{\mathbb{Q}}^n$ with $\deg_K(\boldsymbol{z}) \leq d$ such that $F(\boldsymbol{z}) = 0$ and*

$$H(\boldsymbol{z}) \leq \sqrt{2}\ H(F)^{1/d}.$$

Here $\deg_K(\boldsymbol{z})$ is the degree $[L : K]$, where L is the number field generated over K by the coordinates of the point $\boldsymbol{z}$.

Additional (although somewhat technical and difficult to state) results on systems of quadratic equations over $\overline{\mathbb{Q}}$ can be found in [Fuk15]. Further investigations of small-height solutions of polynomial equations have strong connections with arithmetic geometry via the study of points of bounded height on algebraic varieties. This subject requires a more extensive theory of height functions. An excellent source for further reading in this direction is [BG06].

11. Problems

Problem 11.1. *Let A be an $m \times n$ integer matrix, $1 \leq m < n$ and $\boldsymbol{b} \in \mathbb{Z}^m$ a nonzero vector. Assume that the linear system $A\boldsymbol{x} = \boldsymbol{b}$ has integer solutions. Prove that*

$$\gcd(A\ \boldsymbol{b}) = \gcd(A).$$

Problem 11.2. *An $m \times n$ integer matrix A with $1 \leq m < n$ is called unimodular if there exists an $(n-m) \times n$ integer matrix B so that*

$$\begin{pmatrix} A \\ B \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}).$$

Use Theorem 2.2 to prove that if A is unimodular, then $\gcd(A) = 1$.

Problem 11.3. *Let S be a compact convex set in $\mathbb{R}^n$, $A \in \mathrm{GL}_n(\mathbb{R})$, and define*

$$T = AS = \{A\boldsymbol{x} : \boldsymbol{x} \in S\}.$$

Prove that $\mathrm{Vol}(T) = |\det(A)| \mathrm{Vol}(S)$.

Hint: If we treat multiplication by A as coordinate transformation, prove that its Jacobian is equal to $\det(A)$. *Now use it in the integral for the volume of T to relate it to the volume of S.*

Problem 11.4. *Prove versions of Theorems 3.1 - 3.2 where $\mathbb{Z}^n$ is replaced by an arbitrary lattice $\Lambda \subseteq \mathbb{R}^n$ or rank n and the lower bounds on volume of M are multiplied by* $\det(\Lambda)$.

Hint: Let $\Lambda = A\mathbb{Z}^n$ for some $A \in \mathrm{GL}_n(\mathbb{R})$. Then a point $\boldsymbol{x} \in A^{-1}M \cap \mathbb{Z}^n$ if and only if $A\boldsymbol{x} \in M \cap \Lambda$. Now use Problem 11.3 to relate the volume of $A^{-1}M$ to the volume of M.

Problem 11.5. *Prove that $\sim$ as defined in Definition 8.1 is an equivalence relation on the set of all absolute values on a field K.*

Problem 11.6. *Prove that the only absolute value equivalent to the trivial one is itself.*

Problem 11.7. *Prove that two absolute values $|\ |_1$ and $|\ |_2$ on a field K are equivalent if and only if they induce the same topology.*

Problem 11.8. *Prove that $|\ |_\infty$ is an archimedean absolute value on $\mathbb{Q}$.*

Problem 11.9. *Prove that $|\ |_p$ is a non-archimedean absolute value on $\mathbb{Q}$ for each prime $p \in \mathbb{Z}$.*

Problem 11.10. *Prove that*

$$\mathbb{Z} = \{a \in \mathbb{Q} : |a|_p \leq 1\ \forall \textit{ primes } p \in \mathbb{Z}\}.$$

Problem 11.11. *Prove Lemma 8.2.*

Problem 11.12. *Prove that $I = \{a \in \mathbb{Z} : |a| < 1\}$ is a prime ideal in $\mathbb{Z}$.*

Problem 11.13. *Prove Theorem 8.3 (Artin - Whaples Product Formula over $\mathbb{Q}$): if $0 \neq a \in \mathbb{Q}$, then*

$$|a|_\infty \prod_{p \in \mathcal{P}} |a|_p = 1.$$

Problem 11.14. *Prove that* (8.3) *defines an absolute value on a number field K, which restricts to the usual p-adic absolute value on $\mathbb{Q}$.*

Problem 11.15. *Prove Lemma 8.5.*

Problem 11.16. *Prove Lemma 8.6.*

Problem 11.17. *Prove Lemma 8.7.*

Problem 11.18. *Let K be a number field, $v \in M(K)$, $v|\infty$, and let P and Q be polynomials in one variable of degree $\leq n$ with coefficients in K. Use Cauchy's inequality to prove that*

$$H_v(PQ) \leq \sqrt{n+1}\ H_v(P)H_v(Q).$$

Problem 11.19. *Let A be an $n \times \ell$ integer matrix of rank $\ell < n$. Let $\Lambda = A\mathbb{Z}^\ell$ be a sublattice of $\mathbb{Z}^n$ of rank ℓ. Let*

$$V = \operatorname{span}_{\mathbb{R}} \Lambda = A\mathbb{R}^\ell$$

be the ℓ-dimensional subspace of $\mathbb{R}^n$ spanned by Λ, then $\Lambda = V \cap \mathbb{Z}^n$. The famous Cauchy-Binet formula then implies that the Schmidt height

$$H(V) = \sqrt{\det(A^\top A)} = \det \Lambda.$$

Use Cauchy-Binet formula along with Problem 11.4 to prove that there exists $\mathbf{0} \neq \boldsymbol{x} \in \Lambda$ such that

$$H(\boldsymbol{x}) \leq c_n H(V)^{1/\ell},$$

for some constant c_n depending only on n.

Problem 11.20. *Let K be a number field. Prove that a point $\boldsymbol{x} = (x_0, x_1, \dots, x_n) \in K^{n+1}$ with $x_0 \neq 0$ is a zero of a quadratic form $F(X_0, \dots, X_n)$ if and only if the point $\boldsymbol{x}' = (x_1, \dots, x_n) \in K^n$ is a zero of the quadratic polynomial*

$$F_1(X_1, \dots, X_n) := F(1, X_1, \dots, X_n).$$

References

[BDE12] T. D. Browning, R. Dietmann, and P. D. T. A. Elliott. Least zero of a cubic form. *Math. Ann.*, 352(3):745–778, 2012.

[BF20] A. Böttcher and L. Fukshansky. Representing integers by multilinear polynomials. *Res. Number Theory*, 6:Paper No. 38, 8 pp., 2020.

[BFRT89] I. Borosh, M. Flahive, D. Rubin, and L. Treybig. A sharp bound for solutions of linear diophantine equations. *Proc. Amer. Math. Soc.*, 105(4):844–846, 1989.

[BG06] E. Bombieri and W. Gubler. *Heights in Diophantine geometry*. New Mathematical Monographs, 4. Cambridge University Press, Cambridge, 2006.

[BV83] E. Bombieri and J. D. Vaaler. On Siegel's lemma. *Invent. Math.*, 73(1):11–32, 1983.

[Cas56] J. W. S. Cassels. Addendum to the paper: Bounds for the least solutions of homogeneous quadratic equations. *Proc. Cambridge Philos. Soc.*, 52:602, 1956.

[Die03] R. Dietmann. Small solutions of quadratic diophantine equations. *Proc. London Math. Soc.*, 86(3):545–582, 2003.

[FF23] M. Forst and L. Fukshansky. On zeros of multilinear polynomials. *J. Number Theory*, 245:169–186, 2023.

[FF24] M. Forst and L. Fukshansky. On a new absolute version of siegel's lemma. *Res. Math. Sci.*, 11(1):Paper No. 10, 16 pp., 2024.

[Fuk04] L. Fukshansky. Small zeros of quadratic forms with linear conditions. *J. Number Theory*, 108(1):29–43, 2004.

[Fuk09] L. Fukshansky. Search bounds for zeros of polynomials over $\overline{\mathbb{Q}}$. *Rocky Mountain J. Math.*, 39(3):789–804, 2009.

[Fuk13] L. Fukshansky. Heights and quadratic forms: on Cassels' theorem and its generalizations. In W. K. Chan, L. Fukshansky, R. Schulze-Pillot, and J. D. Vaaler, editors, *Diophantine methods, lattices, and arithmetic theory of quadratic forms*, Contemp. Math., 587, pages 77–94. Amer. Math. Soc., Providence, RI, 2013.

[Fuk15] L. Fukshansky. Height bounds on zeros of quadratic forms over $\overline{\text{ıı}}$. *Res. Math. Sci.*, 2:Art. 19, 26 pp., 2015.

[Gor73] P. Gordan. Uber den grossten gemeinsamen factor. *Math. Ann.*, 7:443–448, 1873.

[HP47] W. V. D. Hodge and D. Pedoe. *Methods of Algebraic Geometry, Volume 1*. Cambridge Univ. Press, 1947.

[Mas98] D. W. Masser. How to solve a quadratic equation in rationals. *Bull. London Math. Soc.*, 30(1):24–28, 1998.

[Mas02] D. W. Masser. Search bounds for Diophantine equations. *A panorama of number theory or the view from Baker's garden (Zurich, 1999)*, pages 247–259, 2002.

[Mat70] Yu. V. Matijasevich. The diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[MR14] M. R. Murty and P. Rath. *Transcendental Numbers*. Springer, New York, 2014.

[Nor49] D. G. Northcott. An inequality in the theory of arithmetic on algebraic varieties. *Proc. Camb. Phil. Soc.*, 45:502–509, 510–518, 1949.

[Rag75] S. Raghavan. Bounds of minimal solutions of diophantine equations. *Nachr. Akad. Wiss. Gottingen, Math. Phys. Kl.*, 9:109–114, 1975.

[RT96] D. Roy and J. L. Thunder. An absolute Siegel's lemma. *J. Reine Angew. Math.*, 476:1–26, 1996.

[Sch67] W. M. Schmidt. On heights of algebraic subspaces and Diophantine approximations. *Ann. of Math.*, 85(2):430–472, 1967.

[Sch91] W. M. Schmidt. *Diophantine Approximations and Diophantine Equations*. Springer-Verlag, 1991.

[Wid09] M. Widmer. Counting points of fixed degree and bounded height. *Acta Arith.*, 140(2):145–168, 2009.

[Wid10] M. Widmer. Counting points of fixed degree and bounded height on linear varieties. *J. Number Theory*, 130(8):1763–1784, 2010.

Department of Mathematics, Claremont McKenna College, 850 Columbia Ave, Claremont, CA 91711, USA

Email address: lenny@cmc.edu