ABSTRACT GEOMETRY OF NUMBERS: LINEAR FORMS

PETE L. CLARK

ABSTRACT. This paper concerns the **abstract geometry of numbers**: namely the pursuit of certain aspects of geometry of numbers over a suitable class of normed domains. (The standard geometry of numbers is then viewed as geometry of numbers over $\mathbb{Z}$ endowed with its standard absolute value.) In this work we study normed domains of "linear type", in which an analogue of Minkowski's linear forms theorem holds. We show that S-integer rings in number fields and coordinate rings of (smooth, geometrically integral) affine algebraic curves over an arbitrary ground field are of linear type. The theory is applied to quadratic forms in two ways, yielding a Nullstellensatz and a Small Multiple Theorem.

Contents

Introduction

In a previous paper [Cl12], I studied aspects of the theory of quadratic forms over a normed domain $(R, |\cdot|)$. The notion of a **Euclidean quadratic form** uses the norm structure in a key way and gives rise to some results of a geometry of numbers (GoN) flavor but in a more abstract algebraic context. Together with some work applying very elementary GoN to prove representation theorems for integral quadratic forms [GoN1], [GoN2], [GoN3] this has led me to pursue aspects of GoN over normed integral domains: in short an **abstract GoN**.

The main idea of the present paper is to pursue analogues of Minkowski's Linear Forms Theorem in a normed domain. In the first part of the paper we develop a theory of normed domains of **linear type**, in which an analogue of this result holds. We show that many domains of arithmetic interest – S-integer rings in number fields and coordinate rings of affine algebraic curves over any ground field – are of linear type. There is also a quantitative aspect in which we ask for the best constant in Minkowski's Theorem, which leads us to the **linear constants** $C(R, n)$ of a linear type normed domain. For the above domains we give explicit lower bounds on the linear constants. In simple cases – $\mathbb{Z}$ and $k[t]$ – our lower bounds are sharp, but in most cases the precise determination of the constants $C(R, n)$ remains open.

In the second part of the paper this theory is applied to prove two results for quadratic forms over a normed domain: the Nullstellensatz for isotropic forms and the Small Multiple Theorem for anisotropic forms.

Given an isotropic quadratic form over a normed domain, it is natural to ask for an upper bound on the size of an isotropic vector in terms of the size of the coefficients of the form. To be sure, there is room for interpretation in the precise meaning of "the size". There are classical results of J.W.S. Cassels in the case $R = \mathbb{Z}$ [Ca55] and A. Prestel in the case $R = k[t]$. [Pr87]. Cassels's result was generalized to $R = \mathbb{Z}_K$ for any number field K by S. Raghavan [Ra75], and Prestel's result was generalized to the coordinate ring of any nonsingular integral affine curve over an arbitrary field by A. Pfister [Pf97]. Our Nullstellensatz is an "abstract version": it holds over a suitable linear type normed Dedekind domain. It recovers the results of Cassels and Prestel but gives variants of those of Raghavan and Pfister because our measurement of "the size" agrees with theirs only when there is a single infinite place. It also applies to S-integer rings in number fields, a new result.

The Small Multiple Theorem holds for certain anisotropic quadratic forms over a suitable linear type normed Dedekind domain. This is new even over $\mathbb{Z}$, though it has precedent in work of Brauer-Reynolds [BR51] and Mordell [Mo51]. This result opens up an enormous terrain in which one may try to apply the – somewhat mysterious, but often effective – computational methods of [GoN1], [GoN2], [GoN3].

Both instances of "suitable" above mean the same thing. To adapt the arguments over $\mathbb{Z}$ and $k[t]$ one wants the norm to satisfy the triangle inequality, which is unfortunately *not* implied by the formalism of normed domains. In the case of an S-integer ring R, the norm satisfies the triangle inequality only when $R = \mathbb{Z}_K$ wih $K = \mathbb{Q}$ or an imaginary quadratic field. This is a disappointing limitation. For affine domains, the restricting to one infinite place is considerably less limiting, but it is still not the general case. Raghavan and Pfister prove results which go beyond these hypotheses, but each of their results involves switching to a different measurement of size: e.g. Raghavan takes as his "norm" the maximum of the absolute values at the infinite places: this satisfies the triangle inequality but is only submultiplicative: $|xy| \leq |x||y|$. There are so many signs that our norm is a natural one: § 1 of the present work is a rumination on this point – that the failure of the triangle inequality in so many examples of interest was most distressing.

Only late in the course of this work did a solution emerge: one can refine the definintion of linear constant so as to apply the triangle inequality separately to each of the metric factors of the norm. This leads to **multinormed linear constants**. Having come to regard the triangle inequality as my enemy, I found in this approach immense satisfaction (and relief), but I admit that it adds a layer of complexity. The reader may wish to start with the case of one infinite place.

Our approach is a perhaps amusing blend of high and low. On the algebraic side we work in the context of not necessarily free lattices over an arbitrary Dedekind domain. This necessitates some background algebra, to which § 1 is mostly devoted. However, on the GoN side we work mostly from scratch: in some cases – e.g. $R = \mathbb{Z}$, $R = \mathbb{F}_q[t]$ – the Pigeonhole Principle is sufficient. It is a piece of folklore that the Blichfeldt Lemma (which implies Minkowski's Convex Body Theorem) is a sort of "Measure Theoretic Pigeonhole Principle." We literally give a Measure Theoretic Pigeonhole Principle and use it to deduce a Blichfeldt Theorem in a measured group. This, together with the (old) result that an S-integer ring in a number field is discrete and cocompact in a suitable finite product of its completions, is the outer limit of our sophistication: we do not (yet!) need reduction theory, adeles, height functions...In the function field case, *in lieu* of using a fully fledged GoN as Mahler, Eichler, and others have developed, we simply invoke Riemann-Roch.

1. Normed Dedekind Domains

1.1. Elementwise Norms.

A **norm** on a ring R is a function $| \cdot | : R \to \mathbb{R}^{\geq 0}$ such that
(N0) $|x| = 0 \iff x = 0$,
(N1) $|x| \geq 1$ for all $x \in R^{\bullet}$; $|x| = 1 \iff x \in R^{\times}$,
(N2) $\forall x, y \in R$, $|xy| = |x||y|$.

A **normed ring** is a pair $(R, | \cdot |)$ where $| \cdot |$ is a norm on R. A nonzero ring admitting a norm is necessarily a domain. We denote the fraction field by K. The norm extends uniquely to a homomorphism of groups $(K^{\times}, \cdot) \to (\mathbb{R}^{>0}, \cdot)$.

Remark 1.1. *In* [Cl12] *our norm functions were required to take values in* $\mathbb{N}$*. This is a natural condition but one which is not needed in the present work.*

Let R be a domain with fraction field K. We say norms $|\cdot|_1, \cdot|\cdot|_2$ on R are **equivalent** – and write $|\cdot|_1 \sim |\cdot|_2$ – if there is $\alpha > 0$ such that for all $x \in K$, $|x|_2 = |x|_1^{\alpha}$.

Elementwise norms are especially easy to understand on a UFD. Indeed, to define an elementwise norm on a UFD one needs to assign to each nonzero principal prime ideal (π) of R an integer $a_\pi \geq 2$, and any such assignment yields an elementwise norm. In particular a DVR carries a unique equivalence class of norms.

The **norm group** $\mathcal{N}$ is $|K^\times| \subset \mathbb{R}^{>0}$. So long as $R \neq K$, its closure $\overline{\mathcal{N}}$ is a nontrivial closed subgroup of $\mathbb{R}^{>0}$, hence there are just two possibilities: either
(i) the closure $\overline{\mathcal{N}}$ of $\mathcal{N}$ is $\mathbb{R}^{>0}$; we say that R is **densely normed**, or
(ii) $\mathcal{N} \subset q^{\mathbb{Z}}$ for some $q > 1$; we say R is **q-normed**.[1]
In the q-normed case we will find it more convenient to work with

$$\deg(\cdot) = \log_q |\cdot|.$$

The corresponding axioms are: for all $x, y \in R$,
(N_q0) $\deg x = -\infty$ iff $x = 0$;
(N_q1) If $x \in R^\bullet$, $\deg x \in \mathbb{N}$; $\deg x = 0 \iff x \in R^\times$;
(N_q2) $\forall x, y \in R$, $\deg xy = \deg x + \deg y$.

1.2. Ideal norms.

Let R be a domain. Then the nonzero ideals of R form a monoid under multiplication, say $\mathcal{I}^+(R)$. An **ideal norm** on R is a homomorphism of monoids $|\cdot| : \mathcal{I}^+(R) \to \mathbb{R}^{\geq 1}$ such that $|I| = 1 \iff I = R$. An ideal norm extends to uniquely to a homomorphism from the monoid $\mathcal{I}(R)$ of fractional ideals of R to $\mathbb{R}^{>0}$.

Ideal norms are especially easy to understand on a Dedekind domain. Indeed, to define an ideal norm on a Dedekind domain one needs to assign to each nonzero prime ideal $\mathfrak{p}$ of R an integer $a_\mathfrak{p} \geq 2$, and any such assignment yields an ideal norm. Further, $\mathcal{I}(R)$ is a group iff R is Dedekind [M, Thm. 11.6].

In the present work R will always be a Dedekind domain, and a *normed ring* $(R, |\cdot|)$ means a Dedekind domain endowed with an *ideal norm*.

1.3. Overrings.

Let $(R, |\cdot|)$ be a normed Dedekind domain, and let R' be an **overring** of R, i.e., a ring intermediate between R and its fraction field K. The induced map on spectra $\iota^* : \operatorname{Spec} R' \to \operatorname{Spec} R$ is an injection, and R' is completely determined by the image $W := \iota^*(\operatorname{Spec} R')$. Namely [LM, Cor. 6.12]

$$R' = R_W := \bigcap_{\mathfrak{p} \in W} R_\mathfrak{p}.$$

[1]Thus $\mathcal{N} = (\tilde{q})^{\mathbb{Z}}$ for some $\tilde{q} = q^a$, $a \in \mathbb{Z}^+$, so the class of q-normed rings would have been the same if we had required $\mathcal{N} = q^{\mathbb{Z}}$. However, we will see that stating it this way is natural for our applications to coordinate rings of affine curves, since an affine algebraic curve over a non-algebraically closed field k need not have any k-rational points.

This allows us to identify the monoid $\mathcal{I}^+(R_W)$ of ideals of R_W as the free submonoid of the free monoid $\mathcal{I}^+(R)$ on the subset W of $\operatorname{Spec} R$ and thus define an **overring ideal norm** $|\cdot|_W$ on R_W as the composite map

$$\mathcal{I}^+(R_W) \xrightarrow{\iota^*} \mathcal{I}^+(R) \xrightarrow{|\cdot|} \mathbb{Z}^+.$$

We single out the following properties of $|\cdot|_W$:

• Every ideal $I \in \mathcal{R}$ may be uniquely decomposed as $W_I I'$ where W_I is divisible by the primes of W and I' is prime to W, and we have

$$|I|_W = |W_I I'|_S = |I'|_S = |I'|.$$

• For all ideals I, $|I|_W \leq |I|$.

1.4. **Extended Norms.**

Let $(R, |\cdot|)$ be a normed Dedekind domain with fraction field K. Let L/K be a finite field extension, and let S be the integral closure of R in L. Then S is a Dedekind domain [M, Thm. 11.7]. Let $N_{L/K} : L \to K$ be the norm in the sense of field theory. Since R is integrally closed, $N_{L/K}(S) \subset R$. The composite map

$$|\cdot|_S = |\cdot| \circ N_{L/K} : S \to \mathbb{R}^{>1}$$

is a norm function on S. We call it the **extended norm**.

1.5. **Almost Metric Norms and the Artin Constant.**

Let $|\cdot|$ be a norm on a ring R. Define

$$A(R) = \inf\{C \in \mathbb{R}^{>0} \mid \forall x, y \in R,\ |x+y| \leq C \max(|x|, |y|)\}.$$

If there is no such C, then $A(R) = \inf \varnothing = \infty$. If $A(R) < \infty$ we say that the norm is **almost metric** and call $A(R)$ the **Artin constant**. It follows that for all $x, y \in K$, $|x+y| \leq A(R) \max(|x|, |y|)$, and thus $|\cdot|$ is an absolute value on K in the sense of E. Artin.

When $A(R) = 1$ we say the norm is **non-Archimedean** or **ultrametric**.

Lemma 1.2. *Let R be a domain with fraction field K, and let $|\cdot|$ be an almost metric norm on R with Artin constant $A(R)$.*
a) $A(R) = \max(|1|, |2|)$.
b) For $\alpha \in \mathbb{R}^{>0}$, $A(R, |\cdot|^\alpha) = A(R)^\alpha$.
c) The map $(x, y) \mapsto |x-y|$ is a metric on K iff $A(R) \leq 2$.
d) For $x_1, \ldots, x_n \in K$, $|x_1 + \ldots + x_n| \leq |n| \max_i |x_i|$.

Proof. For part a), see [A, p. 16]. Part b) follows immediately. For part c), see [A, pp. 4-5]. As for part d): the non-Archmidean case is immediate from induction on $|x+y| \leq \max |x|, |y|$. For the Archimedean case: the assertion depends only on the equivalence class of the norm, so by scaling we may assume $A(R) = 2$. When the Artin constant is 2, then by Ostrowski's Theorem [A, p. 24], the absolute value on K is obtained by embedding K into $\mathbb{C}$ and restricting the standard Euclidean norm. In particular $|n| = n$ for all $n \in \mathbb{Z}^+$. Then by induction on part c),

$$|x_1 + \ldots + x_n| \leq |x_1| + \ldots + |x_n| \leq n \max_i |x_i| = |n| \max_i |x_i|. \qquad \square$$

In particular an almost metric norm is equivalent to a metric norm.

Lemma 1.3. *Let $|\cdot|$ be a q-norm on R. The following are equivalent:*
(i) $-\deg$ is a discrete valuation on K.
(ii) The norm $|\cdot|$ is ultrametric.
(iii) The norm $|\cdot|$ is metric.
(iv) The norm $|\cdot|$ is almost metric.

Proof. The implications (i) $\iff$ (ii) $\implies$ (iii) $\implies$ (iv) are all immediate. Assume (iv). We may adjust the norm within its equivalence class without affecting its ultrametricity, so seeking a contradiction we may suppose that $|\cdot|$ is *not* ultrametric but that it is metric with Artin constant 2, and thus for all $n \in \mathbb{Z}^+$, $n = |n| = q^{\deg n}$, i.e., $\deg n = \log_q n$. But this implies $\frac{\log_q 3}{\log_q 2} = \log_2 3 \in \mathbb{Q}$, a contradiction. □

Example 1.4. *Let R be a discrete valuation ring with uniformizer π. Then a norm $|\cdot|$ on R is freely determined by mapping π to any $q > 1$. Thus the norms on R lie in a single equivalence class, and they are all q-norms. The equivalent conditions of Lemma 1.3* do not hold*: we have $|1| = |\pi - 1| = 1$, but $|\pi| > \max |1|, |\pi - 1|$.*

Lemma 1.5. *Let $m \geq 2$, and let $|\cdot|_1, \ldots, |\cdot|_m$ be inequivalent absolute values on a ring K. Suppose that at least one of the following holds:*
(i) $(K, |\cdot|_2)$ is densely normed.
(ii) There is $\alpha > 1$ such that $\alpha \in \bigcap_{i=1}^m |K^\times|_i$.
Define $|\cdot| : K \to \mathbb{R}$ by $|x| = \prod_{i=1}^m |x|_i$. Then $|\cdot|$ is not *an absolute value on K.*

Proof. First suppose that (i) holds; let $\alpha > 1$ be an element of $|K^\times|_1$. Fix $n \in \mathbb{Z}^+$. By Artin-Whaples approximation [A, p. 9] there are $x_n, y_n \in K$ such that

$$|x_n|_1 \sim \alpha^n,\ |x_n|_2 \sim \alpha^{-n},\ |x_n|_k \sim 1\ \forall k \geq 3.$$

$$|y_n|_1 \sim \alpha^{-n},\ |y_n|_2 \sim \alpha^n,\ |y_n|_k \sim 1\ \forall k \geq 3.$$

Then $|x_n|, |y_n| \sim 1$, but $\lim_{n \to \infty} |x_n + y_n| = \infty$, so $|\cdot|$ is not an absolute value. If (ii) holds then the same argument works with α as in the statement of (ii). □

1.6. **Residually Finite Domains.**

A **residually finite domain** is a domain R in which the quotient by any *nonzero* ideal is finite [BW66], [CL70], [LM72]. A residually finite domain is Noetherian of Krull dimension at most one, hence Dedekind if and only if integrally closed.

Proposition 1.6. *Let R be a residually finite domain with fraction field K.*
a) Let L/K be a finite extension, and let S be a ring with $R \subset S \subset L$. Then S is a residually finite domain.
b) The integral closure $\tilde{R}$ of R in K is a residually finite domain.
c) The completion of R at a maximal ideal is a finite quotient domain.

Proof. Part a) is [LM72, Thm. 2.3]. In particular, it follows from part a) that $\tilde{R}$ is a residually finite domain. That $\tilde{R}$ is a Dedekind ring is part of the Krull-Akizuki Theorem. Part c) follows immediately from part a) and [CL70, Cor. 5.3]. □

Let R be a residually finite domain. For a nonzero ideal I of R, we define $|I| = \#R/I$. It is natural to ask whether $I \mapsto |I|$ gives an ideal norm on R.

Proposition 1.7. *Let I and J be nonzero ideals of the residually finite domain R.*
a) If I and J are comaximal – i.e., $I + J = R$ – then $|IJ| = |I||J|$.
b) If I is invertible, then $|IJ| = |I||J|$.
c) The map $I \mapsto |I|$ is an ideal norm on R iff R is integrally closed.

Proof. Part a) follows immediately from the Chinese Remainder Theorem. As for part b), we claim that the norm can be computed locally: for each $\mathfrak{p} \in \Sigma_R$, let $|I|_\mathfrak{p}$ be the norm of the ideal $IR_\mathfrak{p}$ in the local finite norm domain $R_\mathfrak{p}$. Then

$$|I| = \prod_{\mathfrak{p}} |I|_\mathfrak{p}. \tag{1}$$

To see this, let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a primary decomposition of I, with $\mathfrak{p}_i = \operatorname{rad}(\mathfrak{q}_i)$. It follows that $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_n\}$ is a finite set of pairwise comaximal ideals, so the Chinese Remainder Theorem applies to give

$$R/I \cong \prod_{i=1}^n R/\mathfrak{q}_i.$$

Since $R/\mathfrak{q}_i$ is a local ring with maximal ideal corresponding to $\mathfrak{p}_i$, it follows that $|\mathfrak{q}_i| = |\mathfrak{q}_i R_{\mathfrak{p}_i}|$, establishing the claim.
Using the claim reduces us to the local case, so that we may assume the ideal $I = (xR)$ is principal. In this case we use the short exact sequence of R-modules

$$0 \to \frac{xR}{xJ} \to \frac{R}{xJ} \to \frac{R}{(x)J} \to 0$$

together with the isomorphism

$$\frac{R}{J} \stackrel{\cdot x}{\to} \frac{xR}{xJ}.$$

c) If R is integrally closed (hence Dedekind), every ideal is invertible so this is an ideal norm. The converse is [BW66, Thm. 2]. □

Thus every residually finite Dedekind domain comes endowed with an ideal norm: $|I| = \#R/I$. We call this norm the **canonical norm**.

Proposition 1.8. *Let $(R, |\cdot|)$ be a residually finite Dedekind domain, endowed with its canonical norm. Let R_W be any overring. Then the associated overring norm $|\cdot|_W$ on R_W is the canonical norm.*

Proof. Let $\iota : R \hookrightarrow R_W$. It is enough to check $\#R_W/I = |I|_W$ for every maximal ideal $I = \mathcal{P}$ of R_W. Using the equality of local rings $(R_W)_\mathcal{P} = R_{\mathcal{P}\cap R}$ we get

$$|\mathcal{P}|_W = \#R/(\mathcal{P}\cap R) = \#R_{\mathcal{P}\cap R}/(\mathcal{P}\cap R)R_{\mathcal{P}\cap R} = \#(R_W)_\mathcal{P}/\mathcal{P}(R_W)_\mathcal{P} = \#R_W/\mathcal{P}.$$

□

Proposition 1.9. *Let R be a residually finite Dedekind domain with fraction field K, L/K a separable field extension, and S the integral closure of R in L. Then the extended norm $|\cdot|_S$ coincides with the canonical norm $|J| = \#S/J$.*

Proof. Put $n = [L : K]$. Let $\iota : R \hookrightarrow S$ be the inclusion map. By multiplicativity, it is enough to treat the case of $J = \mathcal{P}$ a maximal ideal. Let $\mathfrak{p} = \mathcal{P} \cap R$, and put $f = \dim_{R/\mathfrak{p}} S/\mathcal{P}$. Now recall:

$$N_{L/K}(\mathcal{P}) = \mathfrak{p}^f.$$

Indeed, when $\mathfrak{p}$ is principal this is [L, Prop. I.22]; since, like any ideal in a Dedekind domain, $N_{L/K}(\mathcal{P})$ can be computed locally, this suffices.[2] Thus

$$|\mathcal{P}|_S = |N_{L/K}(\mathfrak{p})| = |\mathfrak{p}^f| = \#(R/\mathfrak{p})^f = \#S/\mathcal{P}. \qquad \square$$

Remark 1.10. *Let the hypotheses be as in Propsition 1.9 except with L/K purely inseparable. Then $\mathcal{P}$ is the unique prime of S lying over $\mathfrak{p}$ in R, so $\iota_*\mathfrak{p} = \mathcal{P}^e$, hence*

$$|\mathcal{P}^e|_S = |N_{L/K}\iota_*\mathfrak{p}| = |\mathfrak{p}|^n,$$

so

$$|\mathcal{P}|_S = |\mathfrak{p}|^{\frac{n}{e}}.$$

*It follows that $|\mathcal{P}|_S = \#S/\mathcal{P}$ holds if and only if $ef = n$, i.e., iff L/K is **defectless** in the sense of valuation theory. If K has transcendence degree one over $\mathbb{F}_p$ then every finite extension is defectless* [Ku, p. 9]*, so – using a simple dévissage argument to combine the separable and purely inseparable cases – the conclusion of Proposition 1.9 also holds when K is a global field of positive characteristic.*

Example 1.11. *Let R be a DVR with valuation v, uniformizing element π and residue field $R/(\pi) \cong \mathbb{F}_q$. The canonical norm on R is $x \in R^\bullet \mapsto q^{v(x)}$. This is the* reciprocal *of the standard ultrametric associated to the valuation v. This norm is* not *almost metric: let $x = 1$, $y = \pi^n - 1$. Then $|x|, |y| = 1$, but $|x + y| = q^n$.*

1.7. **Hasse Domains.**

Let K be a global field: a finite degree extension of either $\mathbb{Q}$ or $\mathbb{F}_p$. A **place** on K is an equivalence class of almost metric norms on K. We denote by Σ_K the set of all places of K. Let S be a finite, nonempty subset of Σ_K containing all the Archimedean places, and let S_f be the subset of S consisting of all non-Archimedean places. We define $\mathbb{Z}_{K,S}$ as the set of all elements $x \in K$ such that $|x|_v \leq 1$ for every ultrametric place $|\cdot|_v \in \Sigma_K \setminus S$. Following O'Meara we call such a ring a **Hasse domain**. Every Hasse domain is a residually finite Dedekind domain hence comes equipped with the canonical ideal norm $|I| = \#R/I$.

For the convenience of the reader – and to fix notation – we recall some facts.

• Suppose $K \cong \mathbb{Q}[t]/(f)$ is a number field. Then the set of Archimedean places of K is finite and nonempty. More precisely, if f has r real roots and s conjugate pairs of complex roots, then K has r real places – i.e., such that the corresponding completion is isomorphic to the normed field $\mathbb{R}$ – and s complex places – i.e., such that the corrsponding completion is isomorphic to the normed field $\mathbb{C}$. We write out the infinite places as $\infty_1, \ldots, \infty_{r+s}$. The finite places correspond to maximal ideals of $\mathbb{Z}_K$, the integral closure of $\mathbb{Z}$ in K, which is the unique minimal Hasse domain with fraction field K: any other Hasse domain $\mathbb{Z}_{K,S}$ with fraction field K is an overring of R, obtained as $\bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} R \setminus S_f} R_{\mathfrak{p}}$.

• Suppose K has characteristic $p > 0$. Then there is a prime power $q = p^f$ such that $K/\mathbb{F}_q(t)$ is a regular extension – separable, with constant field $\mathbb{F}_q$. There is a unique smooth, projective geometrically integral curve $C_{/\mathbb{F}_q}$ such that $K = \mathbb{F}_q(C)$ is the field of rational functions on C. The places of K are Archimedean and correspond bijectively to closed points on C, or equivalently to complete $\mathfrak{g}_{\mathbb{F}_q} = \operatorname{Aut}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-orbits of $\overline{\mathbb{F}_q}$-valued points of C. Thus the Hasse domains with fraction field K

[2] What we have recalled is often taken as the *definition* of the norm of an ideal in a finite degree separable field extension. But our definition applies to the inseparable case as well.

correspond to finite unions of complete $\mathfrak{g}_{\mathbb{F}_q}$-orbits of $\overline{\mathbb{F}_q}$-points of C, and any such R is the ring of rational functions which are regular away from the support of D. There is no unique minimal Hasse domain in this case, because we cannot take $D = 0$: the ring of functions which are regular on all of C is just $\mathbb{F}_q$.

Proposition 1.12. *Let K be a number field and let $R = \mathbb{Z}_{K,S}$ be a Hasse domain, endowed with its canonical norm $|\cdot|$. Let $P \in S_f$, and suppose P lies over the rational prime p. Let $q_P = |P| = \#R/P$.*
a) For $x \in K^\times$, we have

$$|x| = \prod_{P \in S_f} q_P^{-v_P(x)} \prod_{i=1}^{r+s} |x|_{\infty_i}. \tag{2}$$

b) The norm $|\cdot|$ is almost metric iff $S_f = \varnothing$ and $K = \mathbb{Q}$ or is imaginary quadratic.
c) $A(\mathbb{Z}) = 2$. If K is imaginary quadratic, $A(\mathbb{Z}_K) = 4$.

Proof. a) We recall the **product formula**: for all $x \in K^\times$,

$$\prod_{P \in \operatorname{MaxSpec} \mathbb{Z}_K} q_P^{-v_P(x)} \prod_{i=1}^{r+s} |x|_{\infty_i} = 1.$$

Using this and (1) we get

$$|x| = \prod_{P \in \operatorname{MaxSpec} R} |x|_P = \prod_{P \in \operatorname{MaxSpec} R} q_P^{v_P(x)} = \prod_{P \in S_f} q_P^{-v_P(x)} \prod_{i=1}^{r+s} |x|_{\infty_i}.$$

b) Each factor on the right hand side of (2) is an almost metric norm on K. So if there is exactly one factor, $|x|$ is an almost metric norm. Since there is always at least one infinite place, this occurs iff there are no finite places and exactly one infinite place, i.e., when $S = S_\infty$ and $K = \mathbb{Q}$ or is imaginary quadratic. By Lemma 1.5, the norm is not almost metric if there is more than one factor on the right hand side of (2): hypothesis (i) is satisfied for every Archimedean place.
c) This is immediate from Lemma 1.2. □

Remark 1.13. *The condition that $S = S_\infty$ and $K = \mathbb{Q}$ or imaginary quadratic is precisely that of an S-integer ring in a number field to have finite unit group. Whenever the unit group is infinite, the set $\{|u + v| \mid u, v \in R^\times\}$ is unbounded.*

Proposition 1.12 has an analogue for Hasse domains of positive characteristic. In fact it is natural to consider a more general class of normed domains, namely coordinate rings of an affine curve over an arbitrary ground field. We do this next.

1.8. **Affine Domains.**

Let k be a field, let $C_{/k}$ be a smooth, projective geometrically integral curve, with fraction field $K = k(C)$. Let C° be an open affine subcurve of C obtained by removing a finite, nonempty set $S_\infty = \{\infty_1, \ldots, \infty_m\}$ of closed points of C.[3] For $1 \leq i \leq m$, let $d_i = [k(P_i) : k]$ be the degree of P_i. Let

$$R = k[C^\circ] = \bigcap_{P \notin S_\infty} R_P$$

[3]The Galois-theoretic description of divisors in § 1.7 relied on the perfection of $\mathbb{F}_q$. This fails for closed points $P \in C$ for which the residue field $k(P)$ is an inseparable extension of k.

be the ring of all functions regular away from $\infty_1, \ldots, \infty_m$. Then $R = k[C^\circ]$ is a Dedekind domain; we will call such a ring an **affine domain**.

The ring R carries a canonical norm up to equivalence: fix $q > 1$. If k is finite then we take $q = \#k$. By Zariski's Lemma and the Chinese Remainder Theorem, for all nonzero ideals I of R, R/I is a finite-dimensional k-vector space, and we put

$$|I| = q^{\dim_k R/I}.$$

When k is finite, this is the canonical norm on the Hasse domain R.

Proposition 1.14. *a) For $f \in R^\bullet$,*

$$|f| = q^{-\sum_{i=1}^m d_i v_{\infty_i}(x)}. \tag{3}$$

b) The following are equivalent:
(i) $m = 1$.
(ii) $(R, |\cdot|)$ is ultrametric.
(iii) $(R, |\cdot|)$ is almost metric.

Proof. The maximal ideals of R are in canonical bijection with the closed points of C°; we use P to denote either one. Let $f \in R^\bullet$; viewing x as a rational function on C, consider its divisor

$$\operatorname{div} f = \sum_{P \in C} \deg P v_P(f)[P].$$

Exponentiating the relation $\deg \operatorname{div} f = 0$ gives

$$q^{\sum_{P \in C^\circ} \deg P v_P(f)} = q^{-\sum_{i=1}^m d_i v_{\infty_i}(x)}.$$

On the other hand, $(f) = \prod_{P \in C^\circ} P^{v_P(f)}$, so by the Chinese Remainder Theorem

$$|f| = q^{\dim_k R/(f)} = q^{\sum_{P \in C^\circ} \dim_k R/P^{v_P(f)}}$$
$$= q^{\sum_{P \in C^\circ} v_P(f) \dim_k R/P} = q^{\sum_{P \in C^\circ} \deg P v_P(f)} = q^{-\sum_{i=1}^m d_i v_{\infty_i}(x)},$$

establishing part a). As for part b):
(i) $\implies$ (ii): if $m = 1$, then (3) shows that $|\cdot|$ is obtained by exponentiating the valuation v_∞, so of course gives an ultrametric.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i) follows by applying Lemma 1.5 to the absolute values $|x|_i = q^{-d_i v_{\infty_i}(x)}$. □

1.9. Finite Length Modules, Lattices and Covolumes.

Let R be a Dedekind domain with fraction field K, and let M be a finitely generated R-module. Let $M[\text{tors}]$ be its torsion submodule; we have a short exact sequence

$$0 \to M[\text{tors}] \to M \to P \to 0.$$

The quotient module P is finitely generated and torsionfree over a Dedekind domain, hence projective, so the sequence splits:

$$M \cong M[\text{tors}] \oplus P.$$

Further, there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_N$ of R and $n_1, \ldots, n_N \in \mathbb{Z}^+$ such that

$$M[\text{tors}] \cong \bigoplus_{i=1}^N R/\mathfrak{p}_i^{n_i}. \tag{4}$$

The **length** of $M[\text{tors}]$ is $\sum_{i=1}^{N} n_i$; an R-module has finite length if and only if it is finitely generated torsion. To a finite length R-module, following [CL, § I.5] we attach the invariant

$$\chi(M) = \prod_{i=1}^{n} \mathfrak{p}_i^{n_i}.$$

To see that $\chi(M)$ is well defined we may appeal to the uniqueness properties of the decomposition in (4) – which can be easily reduced to the corresponding uniqueness statement for torsion modules over a PID – or observe that $\chi(M)$ is the product of the annihilators of the Jordan-Hölder factors of M. Put $r = \dim_K(P \otimes_R K)$. Then

$$P \cong R^{r-1} \oplus I$$

for a fractional R-ideal I. The class of I in $\operatorname{Pic} I$ is an isomorphism invariant of P.

By an R-**lattice** in K^n we mean a finitely generated R-submodule $\Lambda \subset K^n$ such that the natural map $\Lambda \otimes_R K \to K^n$ is a K-vector space isomorphism. Since Λ is a finitely generated torsionfree module over a Dedekind domain, it is projective. More precisely, the structure theory for such modules shows that

$$\Lambda \cong R^{n-1} \oplus I$$

where I is a nonzero fractional R-ideal. The class of $I \in \operatorname{Pic} R$ is an invariant of Λ and indeed classifies Λ up to R-module isomorphism. Further, the group $\operatorname{GL}_n(K)$ acts on the set of lattices in K^n and the orbits are precisely the isomorphism classes of modules, i.e., are parameterized by $\operatorname{Pic} R$. In particular $K^\times$ acts on lattices in K^n via scalar matrices: for $\alpha \in K^\times$, we write $\alpha\Lambda$. Two lattices which are in the same orbit under this action of scalar matrices are **homothetic**.

We have the **standard** R-lattice $\mathcal{E}$ in K^n: the free R-module with basis $e_1, \ldots, e_n$. A lattice Λ is **integral** if $\Lambda \subset \mathcal{E}$. Every lattice is homothetic to an integral lattice.

If $\Lambda_1 \subset \Lambda_2 \subset K^n$ are R-lattices, then Λ_2/Λ_1 is a finite length R-module, so we may define $\chi(\Lambda_2/\Lambda_1)$, a nonzero ideal of R. For any pair of lattices Λ_1, Λ_2 we define a *fractional* R-ideal $\chi(\Lambda_2/\Lambda_1)$. Choose $\alpha \in R^\bullet$ such that $\alpha\Lambda_1 \subset \Lambda_2$ and put

$$\chi(\Lambda_2/\Lambda_1) = \alpha^{-1}\chi(\Lambda_2/\alpha\Lambda_1).$$

It is easy to check that this is independent of the choice of α (c.f. [CL, § III.1]). Finally, we put $\chi(\Lambda) = \chi(\mathcal{E}/\Lambda)$.

If $|\cdot|$ is an ideal norm on R, then for any R-lattice Λ in K^n we define

$$\operatorname{Covol} \Lambda = |\chi(\Lambda)|.$$

Proposition 1.15. *Let Λ be a lattice in K^n, and let $M \in \operatorname{GL}_n(K)$.*
a) If $\Lambda = A\mathcal{E}$ is free, then $\chi(\Lambda) = (\det A)R$.
b) In the general case we have

$$\operatorname{Covol}(M \cdot \Lambda) = |\det M| \operatorname{Covol} \Lambda. \tag{5}$$

Proof. Equalities of fractional ideals in a Dedekind domain may be checked locally, so we immediately reduce to the case of R a DVR.
a) For any $\alpha \in R^\bullet$ we have $\chi(\alpha\Lambda) = |\alpha|^n\chi(\Lambda)$ and $|\det \alpha A| = |\alpha|^n |\det A|$, so by scaling we may assume that $\Lambda \subset \mathcal{E}$ and thus $A \in M_n(R)$. Further, we may replace

A with PAQ for any $P,Q \in \mathrm{GL}_n(R)$, so we may assume that A is in Smith Normal Form: in particular, diagonal. The result is immediate in this case.
b) Since R is a DVR, $\Lambda = A\mathcal{E}$ is free and part a) applies: Then $\operatorname{Covol}\Lambda = |\det A|$ and $\operatorname{Covol}(M\cdot\Lambda) = |\det MA|$; (5) follows. □

Let k be a field, $C_{/k}$ a smooth, geometrically integral projective curve, and $\infty_1,\ldots,\infty_m$ closed point of C of degrees $d_1,\ldots,d_m$. Let $C^\circ = C\setminus\{\infty_1,\ldots,\infty_m\}$ and $R = k[C^\circ]$. As in §1.8, we fix $q > 1$ and endow R with the ideal q-norm $I \mapsto |I| = q^{\dim_k R/I}$.

Lemma 1.16. *For any integral lattice $\Lambda \subset R^n$, we have*

$$\operatorname{Covol}\Lambda = q^{\dim_k R^n/\Lambda}.$$

Proof. Let $\Lambda = \Lambda_0 \subset \Lambda_1 \subset \ldots \subset \Lambda_N = R^n$ be a maximal strictly ascending chain of R-submodules, so that $\Lambda_{i-1}/\Lambda_i \cong R/\mathfrak{p}_i$ for some maximal ideal $\mathfrak{p}_i$ of R. Then

$$\operatorname{Covol}\Lambda = |\prod_{i=1}^N \mathfrak{p}_i| = \prod_{i=1}^N |\mathfrak{p}_i| = \prod_{i=1}^N q^{\dim_k R/\mathfrak{p}_i}$$

$$= q^{\sum_{i=1}^N \dim_k R/\mathfrak{p}_i} = q^{\sum_{i=1}^N \dim_k \Lambda_i/\Lambda_{i-1}} = q^{\dim_k R^n/\Lambda}. \qquad \square$$

2. Linear Type Domains

2.1. Basic Definitions.

Let $(R,|\cdot|)$ be an ideal normed Dedekind domain with norm group $\mathcal{N}$ and fraction field K. We say that R is of **linear type** if for all $n \in \mathbb{Z}^+$ there is $C > 0$ such that: for all $M = (m_{ij}) \in \mathrm{GL}_n(K)$, an R-lattice $\Lambda \subset K^n$ and $\epsilon_1,\ldots,\epsilon_n \in \overline{\mathcal{N}}$ such that

$$|\det M| \operatorname{Covol}\Lambda \leq C \prod_{i=1}^n \epsilon_i, \tag{6}$$

there is $x = (x_1,\ldots,x_n) \in \Lambda^\bullet$ such that

$$\forall 1 \leq i \leq n, \ \left| \sum_{j=1}^n m_{ij}x_j \right| \leq \epsilon_i.$$

When R is of linear type, we let $C(R,n)$ be the supremum over all $C \in \overline{\mathcal{N}}$ such that (6) holds. We call the $C(R,n)$'s the **linear constants** of R.

Remark 2.1. *If $|\cdot|_1$ and $|\cdot|_2$ are equivalent norms on R, then if one is of linear type then so is the other. If $|\cdot|_2 = |\cdot|_1^\alpha$, then $C_2(R,n) = C_1(R,n)^\alpha$.*

When $(R,\cdot)$ is q-normed of linear type, then $C(R,n) \in q^{\mathbb{Z}}$, so it is convenient to put $c(R,n) = \log_q C(R,n) \in \mathbb{Z}$.

Proposition 2.2. *a) If $(R,|\cdot|)$ is densely normed of linear type, then for all $n \in \mathbb{Z}^+$,*

$$C(R,n) \leq 1.$$

b) Let $(R,|\cdot|)$ is q-normed, of linear type, and let $\alpha \in R^\bullet\setminus R^\times$. Then for all $n \in \mathbb{Z}^+$,

$$c(q,n) \leq (\deg\alpha)n - 1.$$

Proof. a) Fix $n \in \mathbb{Z}^+$, take $M = 1$, $\Lambda = R^n$ and $e_1 = \ldots = e_n = (1-\delta)$ for some $0 < \delta < 1$. There is no nonzero $x = (x_1, \ldots, x_n) \in R^n$ such that $|x_i| \leq (1-\delta)$ for all $1 \leq i \leq n$, so for any $C > 0$ satisfying the linear type condition we have $1 > C(1-\delta)^n$ or $C < (1-\delta)^{-n}$. Since this holds for all $\delta > 0$, we get $C(R,n) \leq 1$.
b) Fix $n \in \mathbb{Z}^+$, take $M = 1$, $\Lambda = R^n$ and $e_1 = \ldots = e_n = |x|^{-1}$. There is no nonzero $x = (x_1, \ldots, x_n) \in R^n$ such that $\deg x_i \leq e_i$ for all $1 \leq i \leq n$, so

$$0 = \deg(\det 1) \operatorname{covol} R^n > c(R,n) + \sum_{i=1}^{n} - \deg \alpha.$$

Thus $c(R,n) < (\deg \alpha)n$. Since $c(R,n) \in \mathbb{Z}$, we have $c(R,n) \leq (\deg \alpha)n - 1$. □

Example 2.3. ***Minkowski's Linear Forms Theorem*** *implies that $\mathbb{Z}$ is of linear type with $C(\mathbb{Z}, n) \leq 1$ for all $n \in \mathbb{Z}^+$. We will give a(n even) more elementary proof in § 3.2 using no more than the Pigeonhole Principle. Together with Proposition 2.2a) this gives $C(\mathbb{Z}, n) = 1$ for all $n \in \mathbb{Z}^+$ and also that this upper bound is sharp. There is a* boundary case *left open by our setup: is* 1 *an acceptable choice of C in the linear type condition? We will see that it is and actually prove a little more.*

Example 2.4. ***Tornheim's Linear Forms Theorem*** *implies that for any field k and $q > 1$, the ring $k[t]$ with norm $|f| = q^{\deg f}$ is q-normed and of linear type with $c(k[t], n) \geq n-1$. Together with Proposition 2.2b) applied with $\alpha = t$ this gives $c(k[t], n) = n-1$ for all $n \geq 1$ and also that this upper bound is sharp.*

It turns out to be useful to compare the linear type condition with the following *a priori* weaker one: an ideal normed Dedekind domain $(R, |\cdot|)$ with fraction field K is of **linear congruential type** if for all $n \in \mathbb{Z}^+$ there is $C' \in \overline{\mathcal{N}}$ such that: for all integral lattices $\Lambda \subset K^n$ and $\epsilon_1, \ldots, \epsilon_n \in \overline{\mathcal{N}}$ such that

$$\operatorname{Covol} \Lambda \leq C' \prod_{i=1}^{n} \epsilon_i, \tag{7}$$

there is $x = (x_1, \ldots, x_n) \in \Lambda^\bullet$ such that for all $1 \leq i \leq n$, $|x_i| \leq \epsilon_i$. If R is of linear congruential type, for $n \in \mathbb{Z}^+$ we let $C'(R,n)$ be the supremum over constants C'. We call the $C'(R,n)$'s the **linear congruential constants** of R.

Proposition 2.5. *A normed domain is of linear type iff it is of linear congruential type. Further, for all $n \in \mathbb{Z}^+$ we have $C(R,n) = C'(R,n)$.*

Proof. Step 0: It is clear that linear type implies linear congruential type and that $C'(R,n) \leq C(R,n)$ for all $n \in \mathbb{Z}^+$.
Step 1: Suppose R is of linear congruential type. Let Λ be *any* R-lattice in K^n and $\epsilon_1, \ldots, \epsilon_n \in \overline{\mathcal{N}}$ be such that

$$\operatorname{Covol} \Lambda \leq C'(R,n) \prod_{i=1}^{n} \epsilon_i.$$

We claim that there is $y \in \Lambda^\bullet$ with $|y_i| \leq C'(R,n)\epsilon_i$ for all $1 \leq i \leq n$. Choose $\alpha \in R^\bullet$ such that $\alpha\Lambda \subset \mathcal{E}$ and $|\alpha|\epsilon_i \in |R^\bullet|$ for all i. Then

$$\operatorname{Covol} \alpha\Lambda = |\alpha|^n \operatorname{Covol} \Lambda \leq C'(R,n) \prod_{i=1}^{n} |\alpha|\epsilon_i,$$

so there is $x = (x_1, \ldots, x_n) \in (\alpha\Lambda)^\bullet$ with $|x_i| \leq |\alpha|\epsilon_i$ for all $1 \leq i \leq n$. Put $y = \frac{1}{\alpha}x \in \Lambda^\bullet$. Then $|y_i| \leq \epsilon_i$ for all $1 \leq i \leq n$.
Step 2: Let $M \in \mathrm{GL}_n(K)$, $\Lambda \subset K^n$ be an R-lattice, and $\epsilon_1, \ldots, \epsilon_n \in \overline{\mathcal{N}}$ such that

$$|\det M| \operatorname{Covol} \Lambda \leq C'(R,n) \prod_{i=1}^n \epsilon_i.$$

Put $\Lambda_M = M\Lambda$. Suppose (6) holds. Then by Proposition 1.15,

$$|\det M| \operatorname{Covol} \Lambda = \operatorname{Covol} \Lambda_M \leq C(R,n) \prod_{i=1}^n \epsilon_i,$$

so by the assumed special case there is $y = (y_1, \ldots, y_n)^\bullet \in \Lambda_M = M\Lambda$ such that for all $1 \leq i \leq n$, $|y_i| \leq \epsilon_i$. But for $1 \leq i \leq n$, $y_i = \sum_{j=1}^n m_{ij}x_j$ for $x_j \in R$, so there is $x \in \mathcal{E}^\bullet$ such that for all $1 \leq i \leq n$, $\left|\sum_{j=1}^n m_{ij}x_j\right| \leq \epsilon_i$. □

Remark 2.6. *Consider the special case of the linear type condition in which $\Lambda = \mathcal{E}$. A linear change of variables shows that this is equivalent to the linear type condition for all* free lattices*, hence to the full linear type condition when R is a PID.*

2.2. **Overrings.**

Proposition 2.7. *Let $(R, |\cdot|)$ be a normed Dedekind domain. Let $W \subset \operatorname{MaxSpec} R$, and let R_W be the corresponding overring, endowed with the norm of* §1.5.
a) For all $n \in \mathbb{Z}^+$, we have $C(R_W, n) \leq C(R,n)$.
b) In particular, if R is of linear type, so is R_W.

Proof. By Proposition 2.5 we may deal with linear *congruential* type and the constants $C'(R,n)$, $C'(R_W,n)$ instead. Now everything works out easily: first, every integral R_W-lattice Λ is of the form $L \otimes_R R_W$ for some R-lattice L such that $\chi(L)$ is not divisible by any prime in W, and thus $\operatorname{Covol} \Lambda = \operatorname{Covol} L$. Thus, if $\epsilon_1, \ldots, \epsilon_n \in \overline{\mathcal{N}}$ are such that

$$\operatorname{Covol} \Lambda = \operatorname{Covol} L \leq c(R,n) \prod_{i=1}^n \epsilon_i,$$

then there is $x \in L^\bullet$ such that $|x_i| \leq \epsilon_i$ for all $1 \leq i \leq n$. Then $x \in \Lambda^\bullet$ and $|x_i|_W \leq |x_i| \leq \epsilon_i$ for all $1 \leq i \leq n$. □

2.3. **Extended Norms.**

Question 2.8. *Let R be a linear type normed Dedekind domain with fraction field K, L/K a finite field extension, and S the integral closure of R in L, endowed with its canonical norm of* §1.6. *Must S be of linear type?*

Although the question is a natural one, we are not able to give any kind of answer in this abstract setting. The problem is that when we convert a system of inequalities $|\sum_{j=1}^n m_{ij}x_j|_S \leq \epsilon_i$ over S to a system of inequalties over R – namely

$$\left| N_{L/K}\left(\sum_{j=1}^n m_{ij}x_j\right)\right|_R \leq \epsilon_i,$$

then the new system of inequalities is now not of a linear nature.

2.4. **Multinormed Linear Constants.**

We give here a refinement of the notion of linear constant which takes into account that in the examples of interest to us, the norm $|\cdot|$ on R need not be almost metric but is **multimetric**: a finite product of almost metric norms. Note in particular that the canonical norms on every Hasse domain and affine domain are multimetric.

We say an ideal normed Dedekind domain $(R, |\cdot|)$ is **multinormed** if there are elementwise norms $|\cdot|_1, \ldots, |\cdot|_m$ on R such that $|x| = \prod_{j=1}^{m} |x|_j$ for all $1 \leq j \leq m$. We say that $(R, |\cdot|)$ is **multimetric** if each norm $|\cdot|_j$ is almost metric. (This is is the case of interest to us.) For $1 \leq j \leq m$ we put $\mathcal{N}_j = |K^\times|_j$.

The norm $|\cdot|$ is of **q-type** iff there is $q > 0$ such that $\mathcal{N}_j \subset q^{\mathbb{Z}}$ for all j: this is the situation for affine domains. We emphasize that more than one choice of q is always possible but that such a choice will always be given as part of the structure. As in the $m = 1$ case we put $\deg_j = \log_q |\cdot|_j$. When each $-\deg j$ is a discrete valuation, we say the norm is **totally ultrametric**.

The norm is **totally dense** if $\mathcal{N}_j$ is dense for each j. If each $|\cdot|_j$ is metric, this is equivalent to each $|\cdot|_j$ being Archimedean, and we use the terminology **totally Archimedean**. The canonical norm on $R = \mathbb{Z}_K$, K a number field, is totally Archimedean. The norm is of **mixed type** if some $\mathcal{N}_j$ is dense and some $\mathcal{N}_{j'}$ is not. The canonical norm on $R = \mathbb{Z}_{K,S}$ when $S \neq \varnothing$ is of mixed multimetric type.

A multimetric ideal normed Dedekind domain R is of **multinormed linear type** if for all $n \in \mathbb{Z}^+$ there is $C \in \overline{\mathcal{N}}$ such that: given $M = (m_{ij}) \in \mathrm{GL}_n(K)$, an R-lattice $\Lambda \subset K^n$ and for all $1 \leq j \leq m$ constants $\epsilon_{1j}, \ldots, \epsilon_{nj} \in \overline{\mathcal{N}_j}$ such that

$$|\det M| \operatorname{Covol} \Lambda \leq C \prod_{i,j} \epsilon_{ij}, \tag{8}$$

there is $x = (x_1, \ldots, x_n) \in \Lambda^\bullet$ such that

$$\forall i, j, \ \left| \sum_{k=1}^{n} m_{ik} x_k \right|_j \leq \epsilon_{ij}.$$

When R is of multinormed linear type, we let $C_M(R, n)$ be the supremum over all $C \in \overline{\mathcal{N}}$ such that (6) holds. We call the $C_M(R, n)$'s the **multinormed linear constants** of R. We can now introduce the notion of **multinormed linear congruential type** and the associated constants $C'_M(R, n)$. Just as in the linear type case it turns out that multimetric linear congruential type is equivalent to multimetric linear type and $C'_M(R, n) = C_M(R, n)$ for all n. In the sequel we will estimate the multinormed linear constants using this equivalence.

2.5. **Diophantine Approximation.**

One of the most basic and important applications of Minkowski's Linear Forms Theorem is to Diophantine Approximation. The formalism of domains of linear type and q-linear type yields analogues of these classical results.

Theorem 2.9. *Let $(R, |\cdot|)$ be a multinormed linear type Dedekind domain. Let $n \in \mathbb{Z}^+$, $M \in \overline{\mathcal{N}} \cap (1, \infty)$, $\theta_1, \ldots, \theta_n \in K$.*

a) Suppose R is densely normed. If there is $C > 0$ with

$$|M|^{-1} < C < C_M(R, n+1),$$

then there are $x_1, \ldots, x_n \in R$ and $x_{n+1} \in R^\bullet$ such that
- *$\forall 1 \le j \le m$, $\forall 1 \le i \le n$, $|x_{n+1}\theta_i - x_i|_j \le (C|M|)^{\frac{-1}{mn}}$, and*
- *$\forall 1 \le j \le m$, $|x_{n+1}|_j < |M|^{\frac{1}{m}}$.*

b) Suppose R is q-normed. If

$$m(n+1) - \deg M \le c_M(R, n+1),$$

then there are $x_1, \ldots, x_n \in R$, $x_{n+1} \in R^\bullet$ such that both of the following hold:
- *For all $1 \le i \le n$, $1 \le j \le m$, $\deg_j(x_{n+1}\theta_i - x_i) \le \frac{m(n+1)-1-c_M(R,n+1)-\deg M}{mn}$,*
- *For all $1 \le j \le m$, $\deg_j x_{n+1} \le \deg_j M - 1$.*

c) Suppose R is of mixed multinormed linear type, with $\mathcal{N}_j$ dense for $1 \le j \le m'$ and q_j-normed for $m'+1 \le j \le m$. If there is $C > 0$ with

$$|M|^{-1} < C < C_M(R, n+1),$$

then there are $x_1, \ldots, x_n \in R$ and $x_{n+1} \in R^\bullet$ such that
- *$\forall 1 \le j \le m'$, $\forall 1 \le i \le n$, $|x_{n+1}\theta_i - x_i|_j \le (C|M|_j)^{\frac{-1}{n}}$,*
- *$\forall m' < j \le m$, $\forall 1 \le i \le n$, $|x_{n+1}\theta_i - x_i|_j \le 1$,*
- *$\forall 1 \le j \le m'$, $|x_{n+1}|_j < |M|_j$, and*
- *$\forall m' < j \le m$, $|x_{n+1}|_j \le 1$.*

Proof. In all cases we take $\Lambda = R^{n+1}$ and

$$A = \begin{bmatrix} -1 & 0 & \ldots & 0 & \theta_1 \\ 0 & -1 & \ldots & 0 & \theta_2 \\ \vdots & & & & \vdots \\ 0 & 0 & \ldots & -1 & \theta_n \\ 0 & 0 & \ldots & 0 & 1 \end{bmatrix}, \tag{9}$$

so $|\det A|_j = 1$ for all j.
a) For all $1 \le i \le n$ and all $1 \le j \le m$, put $\epsilon_{ij} = (C|M|)^{\frac{-1}{nm}}$; for all $1 \le j \le m$, put $\epsilon_{(n+1)j} = |M|^{\frac{1}{m}} - \delta$ for some $\delta > 0$. Then for sufficiently small δ, $C_M(R,n)\prod_{i,j}\epsilon_{ij} > |\det A| \operatorname{Covol}\Lambda$ and thus there is a nonzero $x = (x_1, \ldots, x_{n+1}) \in R^{n+1}$ such that $|x_{n+1}\theta_i - x_i|_j \le (C|M|)^{\frac{-1}{nm}}$ for all $1 \le i \le n$, $1 \le j \le m$ and $|x_{n+1}|_j < |M|_j$ for all $1 \le j \le m$. If $x_{n+1} = 0$ then we would have $|x_i| \le (C|M|)^{\frac{-1}{n}} < 1$, so $x_1 = \ldots = x_n = 0$ and thus $x = 0$, contradiction.
b) For $1 \le i \le n$ and $1 \le j \le m$, put

$$\begin{aligned} e_{ij} &= \lceil \frac{m - c_M(R,n+1) - \deg M}{mn} \rceil \\ &\le \frac{m - c_M(R,n+1) - \deg M}{mn} + \frac{mn-1}{mn} \\ &= \frac{m(n+1) - 1 - c_M(R,n+1) - \deg M}{mn}, \end{aligned}$$

and for all $1 \le j \le m$,

$$e_{(n+1)j} = (\deg_j M) - 1.$$

Then

$$c_M(R, n+1) + \sum_{1 \le i \le n+1, 1 \le j \le m} e_{ij} \ge 0 = \deg(\det A) + \operatorname{covol}\Lambda,$$

so by definition of $c_M(R, n+1)$ there is $x = (x_1, \ldots, x_n, x_{n+1}) \in (R^{n+1})^\bullet$, not all zero, such that

$$\forall 1 \leq i \leq n, \forall 1 \leq j \leq m,\ \deg_j(x_{n+1}\theta_i - x_i) \leq \lceil \frac{m - c_M(R, n+1) - \deg M}{mn} \rceil$$

$$\leq \frac{m(n+1) - 1 - c_M(R, n+1) - \deg M}{mn} < 0,$$

by our hypothesis, so for all $1 \leq i \leq n$,

$$\deg x_{n+1}\theta_i - x_i < 0.$$

As above, $x_{n+1} \neq 0$: otherwise $x_1 = \ldots = x_n = 0$ and thus $x = 0$, contradiction.
c) This is very similar to part a) and may be left to the reader. □

3. The Group Theoretic Pigeonhole Principle

3.1. The Group Theoretic Pigeonhole Principle.

Theorem 3.1. *(Group Theoretic Pigeonhole Principle) Let G be a group – not necessarily commutative, but written additively – and let Λ be a subgroup of G. Let $S \subset G$, and let $D(S) = \{s_1 - s_2 \mid s_1, s_2 \in S\}$. If for a cardinal number κ we have*

$$\#S > \kappa \cdot \#[G : \Lambda],$$

then there are at least κ nonzero elements of $D(S) \cap \Lambda$.

Proof. Let G/Λ be the set of right cosets of Λ in G, and let $\Phi : G \to G/\Lambda$ be the map $g \in G \mapsto \Lambda + g$. If $\#(\Phi^{-1}(y) \cap S) \leq \kappa$ for all $y \in G/H$ then $\#S \leq \kappa \cdot \#[G : \Lambda]$: contradiction. So there is $S' \subset S$ with $\#S' > \kappa$ and $\Phi(s_1) = \Phi(s_2)$ for all $s_1, s_2 \in S'$. Fix $s_0 \in S'$ and put $S'' = S' \setminus \{s_0\}$, so $\#S'' \geq \kappa$. As s runs through S'', $s - s_0$ are distinct nonzero elements of $D(S) \cap \Lambda$. □

3.2. The Classical Case.

Theorem 3.2. *For all $n \in \mathbb{Z}^+$, $C(\mathbb{Z}, n) = 1$.*

Proof. Let $\Lambda \subset \mathbb{Z}^n$ be a lattice and $\epsilon_1, \ldots, \epsilon_n \in \mathbb{R}^{>0}$ with

$$[\mathbb{Z}^n : \Lambda] = \operatorname{Covol} \Lambda \leq \prod_{i=1}^n \epsilon_i.$$

Let $G = \mathbb{Z}^n$. Put

$$S = \mathbb{Z}^n \cap \prod_{i=1}^n [0, \epsilon_i].$$

Then

$$\#S = \prod_{i=1}^n (\lfloor \epsilon_i \rfloor + 1) > \prod_{i=1}^n \epsilon_i \geq \#G_2, \tag{10}$$

so by Theorem 3.1 there are $s_1 \neq s_2 \in S$ with $s_1 - s_2 \in \Lambda$. Then $x = (x_1, \ldots, x_n) = s_1 - s_2 \in \Lambda^\bullet$ and has $|x_i| \leq \epsilon_i$ for all $1 \leq i \leq n$. It follows that $C(\mathbb{Z}, n) \geq 1$. Combining this with Proposition 2.2 gives $C(\mathbb{Z}, n) = 1$. □

In (10) we have $\lfloor \epsilon_i \rfloor + 1 > \epsilon_i$ for all i and thus $\prod_{i=1}^n (\lfloor \epsilon_i \rfloor + 1) > \prod_{i=1}^n \epsilon_i$. This is more than we need: it would be enough to have n inequalities any one of which is strict. Using this one obtains the following mild strengthening of Theorem 3.2.

Theorem 3.3. *Let $\Lambda \subset \mathbb{Q}^n$ be a $\mathbb{Z}$-lattice, and let $\epsilon_1, \ldots, \epsilon_n > 0$ be such that $\operatorname{Covol} \Lambda \leq \prod_{i=1}^n \epsilon_i$. Fix an index $i_\bullet \in \{1, \ldots, n\}$. Then there is $x \in \Lambda^\bullet$ such that $|x_i| < \epsilon_i$ for all $i \neq i_\bullet$ and $|x_{i_\bullet}| \leq \epsilon_{i_\bullet}$.*

Proof. As in the proof of Proposition 2.5, it is no loss of generality to assume that $\Lambda \subset \mathcal{E}$ is an integral lattice. The proof is the same as above except we take

$$S = \mathbb{Z}^n \cap \left([0, \epsilon_{i_\bullet}] \times \prod_{i \neq i_\bullet} [0, \epsilon_i) \right).$$

Then $\#(\mathbb{Z} \cap [0, \epsilon_i)) \geq \epsilon_i$ and $\#(\mathbb{Z} \cap [0, \epsilon_{i_\bullet}]) = \lfloor \epsilon_{i_\bullet} \rfloor + 1 > \epsilon_{i_\bullet}$, so $\#S > \prod_{i=1}^n \epsilon_i$. □

Corollary 3.4. *Let $n \in \mathbb{Z}^+$, $M > 1$, $\theta_1, \ldots, \theta_n \in \mathbb{R}$. There are $x_1, \ldots, x_{n+1} \in \mathbb{Z}$ with*

$$\forall 1 \leq i \leq n, \ |x_n \theta_i - x_i| \leq M^{\frac{-1}{n}},$$
$$0 < |x_{n+1}| < M.$$

Proof. The argument is the same as the proof of Theorem 2.5a) except using the slight strengthening of $C(\mathbb{Z}, n) = 1$ afforded by Theorem 3.3. □

Corollary 3.5. *Let $m, n \in \mathbb{Z}^+$, $d_1, \ldots, d_m \in \mathbb{Z}^+$, $\epsilon_1, \ldots, \epsilon_n \in \mathbb{R}^{>0}$, and suppose*

$$\prod_{j=1}^n \epsilon_j \geq \prod_{i=1}^m d_i. \tag{11}$$

Let $A = (a_{ij}) \in M_{m,n}(\mathbb{Z})$ and $j_0 \in \{1, \ldots, n\}$. Fix $j_\bullet \in \{1, \ldots, n\}$. There is $(x_1, \ldots, x_n) \in (\mathbb{Z}^n)^\bullet$ with
(i) $\sum_{j=1}^n a_{ij} x_j \equiv 0 \pmod{d_i}$ for $1 \leq i \leq m$ and
(ii) $|x_{j_\bullet}| \leq \epsilon_{i_\bullet}$, and $|x_i| < \epsilon_i$ for all $i \neq i_\bullet$.

Proof. For each $1 \leq i \leq m$, the set $\Lambda_i = \{x \in \mathbb{Z}^n \mid \sum_{j=1}^n a_{ij} x_j \equiv 0 \pmod{d_i}\}$ is a sublattice of $\mathbb{Z}^n$ of index at most d_i. Therefore $\Lambda = \bigcap_{i=1}^m \Lambda_i$ is a sublattice of $\mathbb{Z}^n$ of index at most $\prod_{i=1}^m d_i$. Now apply Theorem 3.3. □

Various special cases of Corollary 3.5 have appeared in the literature. The case $m = 1$, $n = 2$, $\epsilon_1 = \epsilon_2$ is due to A. Thue [Th02]; the case $m = 1$, $n = 2$ is due to I.M. Vinogradov [Vi27]. The case of m, n arbitrary, but all d_i's and ϵ_j's equal is due to Brauer-Reynolds [BR51]. The general case – but with strict inequalities in both the hypothesis and conclusion is due to Stevens-Kuty [SK68]. Most of all, the result with arbitrary m and $n = 3$ is due to Mordell [Mo51, p. 325].

3.3. **A Linear Type Criterion for Residually Finite Domains.**

Theorem 3.6. *Let R be an almost metric residually finite Dedekind domain, endowed with its canonical norm.*
a) Suppose R is densely normed and that there are $\kappa, E > 0$ such that for $e \geq E$, $\#\{x \in R \mid |x| \leq e\} \geq \kappa e$. Then

$$C(R, n) \geq \left(\frac{\kappa}{A(R)} \right)^n.$$

b) Suppose R is q-normed and that there are $k \in \mathbb{Z}$, $A \in \mathbb{N}$ such that for all integers $a \geq A$, $\#\{x \in R \mid \deg x \leq a\} \geq k + a$. Then

$$c(R, n) \geq nk - 1.$$

Proof. a) Let $C < \left(\frac{\kappa}{A(R)}\right)^n$, let Λ be an integral R-lattice in K^n, and let $\epsilon_1, \ldots, \epsilon_n \in \mathbb{R}^{>0}$ be such that $\operatorname{Covol} \Lambda \leq C \prod_{i=1}^n \epsilon_i$. Suppose first that $\epsilon_i \geq EA(R)$ for all i. Let $S = \{x \in R^n \mid |x_i| \leq \frac{\epsilon_i}{A(R)} \ \forall i\}$. By definition of κ and E we have

$$\#S \geq \prod_{i=1}^n \kappa \frac{\epsilon_i}{A(R)} > C \prod_{i=1}^n \epsilon_i \geq \operatorname{Covol} \Lambda,$$

so by Theorem 3.1 there are $s \neq s' \in S$ such that $x = s - s' \in \Lambda$. Then for all $1 \leq i \leq n$, $|x_i| = |s_i - s_i'| \leq A(R) \max |s_i|, |s_i|' \leq \epsilon_i$, so we have verified the linear congruential type condition in this case.

Now choose $a \in R^\bullet$ such that for all $1 \leq i \leq n$, $|a|\epsilon_i \geq EA(R)$. Then

$$\operatorname{Covol} a\Lambda = |a|^n \operatorname{Covol} \Lambda \leq C \prod_{i=1}^n |a|\epsilon_i,$$

so by the case done above there is $y \in (a\Lambda)^\bullet$ with $|y_i| \leq |a|\epsilon_i$ for all $1 \leq i \leq n$. Put $x = \frac{1}{a}y$, so $x \in \Lambda^\bullet$ and $|x_i| \leq \epsilon_i$ for all $1 \leq i \leq n$. It follows that $C(R,n) \geq \left(\frac{\kappa}{A(R)}\right)^n$.
b) The argument is entirely similar to that of part a). □

We denote Lebesgue measure in $\mathbb{R}^n$ by Vol. The following result is well known, but we include the proof for completeness and to show how little is up our sleeves.

Proposition 3.7. *For bounded $\Omega \subset \mathbb{R}^n$ and $r > 0$, let $r\Omega = \{rP \mid p \in \Omega\}$, let $\Lambda \subset \mathbb{R}^n$ be a lattice, and let*

$$L_{\Omega,\Lambda}(r) = \#r\Omega \cap \Lambda$$

be the ***lattice point enumerator****. If $\operatorname{Vol}(\partial\Omega) = 0$, then*

$$\lim_{r\to\infty} \frac{L_{\Omega,\Lambda}(r)}{r^n} = \frac{\operatorname{Vol}\Omega}{\operatorname{Covol}\Lambda}.$$

Proof. Let $M \in \operatorname{GL}_n(\mathbb{R})$ be such that $M\Lambda = \mathbb{Z}^n$. Then for all $r > 0$,

$$\#(r\Omega \cap \Lambda) = \#(rM\Omega \cap \mathbb{Z}^n)$$

and

$$\operatorname{Vol} M\Omega = \frac{\operatorname{Vol}\Omega}{|\det M|^{-1}} = \frac{\operatorname{Vol}\Omega}{\operatorname{Covol}\Lambda},$$

so we may replace (Ω, Λ) by $(M\Omega, \mathbb{Z}^n)$. Via a change of variable $r \mapsto \frac{r}{R}$ we may assume $M\Omega \subset (-1,1)^n$. Since $M\Omega$ is bounded and $\operatorname{Vol}(\partial M\Omega) = 0$, the characteristic function $\mathbf{1}_{M\Omega}$ is Riemann integrable. For $r \in \mathbb{Z}^+$, $\frac{L_{M\Omega,\mathbb{Z}^n}(r)}{r^n}$ is a Riemann sum for $\mathbf{1}_{M\Omega}$ and the partition of $[-1,1]^n$ into subsquares of side length $\frac{1}{r}$. □

Corollary 3.8. *Let K be an imaginary quadratic field. Then for all $n \in \mathbb{Z}^+$,*

$$C(\mathbb{Z}_K, n) \geq \left(\frac{\pi}{2\sqrt{|\Delta_K|}}\right)^n. \tag{12}$$

Proof. Step 1: The complex place of K gives an embedding $\sigma : K \to \mathbb{C}$ which realizes $\mathbb{Z}_K$ as a lattice in $\mathbb{C} \cong \mathbb{R}^2$; the norm $|\cdot|$ is the square of the usual Euclidean norm. The lattice $\sigma(\mathbb{Z}_K)$ has covolume[4] $2^{-1}\sqrt{|\Delta(K)|}$ and $\mathrm{Vol}(\{x \in \mathbb{R}^2 \mid |x| \leq e\}) = \pi e$. Applying Proposition 3.7 we get that as $e \to \infty$,

$$\#\{x \in \mathbb{Z}_K \mid |x| \leq e\} \sim \left(\frac{2\pi}{\sqrt{|\Delta(K)|}}\right) e.$$

Step 2: We have $A(\mathbb{Z}_K) = \max |1|, |2| = 4$. For each fixed $\delta > 0$, the hypotheses of Theorem 3.6a) apply with $\kappa = \frac{2\pi}{\sqrt{|\Delta(K)|}} - \delta$ and thus

$$C(\mathbb{Z}_K, n) \geq \left(\frac{\frac{2\pi}{\sqrt{|\Delta(K)|}} - \delta}{4}\right)^n.$$

Letting δ approach zero we get (12). $\square$

Corollary 3.9. *For all $n \in \mathbb{Z}^+$, $c(\mathbb{F}_q[t], n) = n - 1$.*

Proof. For all $a \in \mathbb{N}$,

$$\#\{x \in \mathbb{F}_q[t] \mid \deg x \leq a\} = q^{a+1},$$

Applying Theorem 3.6b) we get $c(\mathbb{F}_q[t], n) \geq n - 1$ for all $n \in \mathbb{Z}^+$. Combining this with Proposition 2.2b) gives the result. $\square$

We could now pursue the positive characteristic analogue of Corollary 3.8 by using GoN methods to give bounds on $\{x \in R \mid \deg x \leq a\}$. However, this would involve developing (or importing) GoN methods for Hasse domains of positive characteristic. But there is a more efficient approach which works for affine domains over an arbitrary ground field: observe that $\{x \in R \mid \deg x \leq a\}$ is a Riemann-Roch space and apply (Riemann's portion of) the Riemann-Roch Theorem. We do so next.

4. Affine Domains

Let k be a field, $C_{/k}$ a smooth, geometrically integral projective curve, and $\infty_1, \ldots, \infty_m$ closed points of C of degrees $d_1, \ldots, d_m$. Let $C^\circ = C \setminus \{\infty_1, \ldots, \infty_m\}$ and $R = k[C^\circ]$. As in §1.8, we fix $q > 1$ and endow R with the ideal q-norm $I \mapsto |I| = q^{\dim_k R/I}$. We will show that R is of linear q-type and give explicit lower bounds on the linear q-constants $c(R, n)$.

4.1. **Tornheim's Theorem.**

It is natural to look first at the case $R = k[t]$, $K = k(t)$. We have already seen that when k is finite, R is of linear type and indeed $c(k[t], n) = n - 1$. In this section we will show this same result over an arbitrary field k. In fact a result equivalent to this was first established in a(n apparently little known – it has no MathSciNet citations as of May 2013) work of L. Tornheim [To41].

Tornheim's original proof is more complicated than is necessary. Our desire to treat a more general case also brings certain complications, so we have decided to begin with a simple proof of Tornheim's Theorem.

---

[4]Later on we will take our Haar measure on $\mathbb{C}$ to be *twice* the standard Lebesgue measure: this would double both the covolume of $\sigma(\mathbb{Z}_K)$ and the volumes of the balls $\{x \mid |x| \leq e\}$, so it would not change the final result.

Lemma 4.1. *Let $C \in M_n(R) \cap \mathrm{GL}_n(K)$, and let $\Lambda = CR^n$. Then Λ is an R-submodule of R^n, so we may form the quotient R-module R^n/Λ. Then*

$$\dim_k(R^n/\Lambda) = \deg \det C.$$

Proof. This is an immediate consequence of Proposition 1.15 and Lemma 1.16. But let us also indicate a direct proof: since R is a PID, we may use Smith Normal Form to reduce to the case in which C is diagonal. The result is clear in this case. □

Lemma 4.2. *(Linear Algebraic Pigeonhole Principle) Let V be a k-vector space and W_1, W_2 be linear subspaces of V. If $\dim W_1 > \dim V/W_2$, then $W_1 \cap W_2 \neq \{0\}$.*

The proof is immediate.

Theorem 4.3. *(Tornheim* [To41]*) Let k be a field; let $C = (c_{ij}) \in \mathrm{GL}_n(K)$. For $1 \leq i \leq n$, put $L_i(x) = \sum_{j=1}^n c_{ij}x_j$. Let $e_1, \ldots, e_n \in \mathbb{N}$ be such that*

$$\deg \det C \leq n - 1 + \sum_{i=1}^n e_i. \tag{13}$$

Then there exists $x \in (R^N)^\bullet$ such that for all $1 \leq i \leq N$,

$$\deg L_i(x) \leq e_i.$$

Proof. Step 1: We suppose $C \in M_n(R)$. Consider the linear map $L : K^n \to K^n, x \mapsto Cx$, and put $\Lambda = L(R^n) \subset K^N$. Since $\det C \neq 0$, we have $L^{-1} : K^n \to K^n$, and thus $L^{-1}|_\Lambda : \Lambda \stackrel{\sim}{\to} R^n$. Put

$$\mathcal{B} = \{(x_1, \ldots, x_n) \in R^n \mid \forall 1 \leq i \leq n,\ \deg x_i \leq e_i\}.$$

Then $\mathcal{B}$ is a k-subspace of R^n with $\dim_k \mathcal{B} = \sum_{i=1}^n (e_i + 1)$. By Lemma 4.1, $\dim_k R^n/\Lambda = \deg \det C$. So (13) can be restated as

$$\dim_k \mathcal{B} > \dim_k R^n/\Lambda.$$

By Remark 4.2 there is a nonzero vector $y \in \Lambda \cap \mathcal{B}$. Taking $x = L^{-1}y$ does the job.
Step 2: In the general case, choose $f \in R^\bullet$ such that $fC \in M_n(R)$. Then

$$\deg \det fC \leq n - 1 + \sum_{i=1}^n (e_i + \deg f),$$

so by Step 1, there is $x \in (R^n)^\bullet$ with $\deg f + \deg L_i(x) = \deg fL_i(x) \leq e_i + \deg f$ for all $1 \leq i \leq n$, so $\deg L_i(x) \leq e_i$ for all $1 \leq i \leq n$. □

Corollary 4.4. *For all $n \geq 1$, $c(k[t], n) = n - 1$.*

Proof. Since $k[t]$ is a PID, all R-lattices are free, so by Remark 2.6 the special case of the linear q-type condition we've checked is equivalent to the general case: $c(k[t], n) \geq n - 1$. The upper bound comes from Proposition 2.2. □

4.2. **Affine Domains Are Of Multimetric Linear Type.**

Theorem 4.5. *Let k be a field and C°/k be a smooth, geometrically integral affine curve of genus g. Let $R = k[C^\circ]$ be its affine coordinate ring. Let $d = \min \deg \infty_1, \ldots, \infty_m$. Then*

$$c(R, n) \geq n(2 - d - g) - 1.$$

Proof. We will show that if $m = 1$ and $\deg \infty_1 = d$, then $c(R, n) \geq n(2 - d - g) - 1$. By Proposition 2.7, this suffices. Let $\Lambda \subset R^n$ be an integral R-lattice such that

$$\operatorname{covol} \Lambda \leq n(2 - d - g) - 1 + \sum_{i=1}^{n} e_i.$$

We must show there is $x = (x_1, \ldots, x_n) \in \Lambda^\bullet$ with $\deg x_i \leq e_i$ for all $1 \leq i \leq n$. By Lemma 1.16, $\operatorname{covol} \Lambda = \dim_k R^n/\Lambda$. Consider the k-vector space

$$\mathcal{B} = \{(x_1, \ldots, x_n) \in R^n \mid \deg x_i \leq e_i\}.$$

By Proposition 1.14, for $x \in K$, $\deg x = -d \operatorname{ord}_\infty(x)$, so for $x \in R$,

$$\deg x \leq e_i \iff -d \operatorname{ord}_\infty(x) \leq e_i \iff \operatorname{ord}_\infty(x) \geq \lceil -\frac{e_i}{d} \rceil = -\lfloor \frac{e_i}{d} \rfloor.$$

Thus $\{x \in R \mid \deg x \leq e_i\}$ is precisely the Riemann-Roch space $\mathcal{L}((\lfloor \frac{e_i}{d} \rfloor)\infty)$, so by Riemann-Roch its dimension is at least $d\lfloor \frac{e_i}{d} \rfloor - g + 1$. Therefore

$$\dim +k\mathcal{B} \geq \sum_{i=1}^{n} \left(d\lfloor \frac{e_i}{d} \rfloor - g + 1 \right) \geq d \sum_{i=1}^{n} \left(\frac{e_i}{d} - \frac{d-1}{d} \right) - ng + n = n(2-d-g) + \sum_{i=1}^{n} e_i.$$

It follows that

$$\dim_k \mathcal{B} > n(2 - d - g) - 1 + \sum_{i=1}^{n} e_i \geq \operatorname{covol} \Lambda = \dim_k R^n/\Lambda,$$

so by the Linear Algebraic Pigeonhole Principle $\mathcal{B} \cap \Lambda^\bullet \neq \varnothing$. □

Theorem 4.6. *Let k be a field and C/k be a smooth, geometrically integral projective curve of genus g, and let $C^\circ = C \setminus \{\infty_1, \ldots, \infty_m\}$ be the affine curve obtained by removing the given m closed points, of degrees $d_1, \ldots, d_m$. Let $R = k[C^\circ]$ be its affine coordinate ring. Then R is of multimetric linear type, and*

$$c_M(R, n) \geq n(m + 1 - \sum_{j=1}^{m} d_j - g) - 1.$$

Proof. Let $\Lambda \subset R^n$ be an integral R-lattice such that

$$\operatorname{covol} \Lambda \leq n(m + 1 - \sum_{j=1}^{m} d_j - g) - 1 + \sum_{i,j} e_{ij}.$$

We must show there is $x = (x_1, \ldots, x_n) \in \Lambda^\bullet$ with $\deg_j x_i \leq e_{ij}$ for all i, j. By Lemma 1.16, $\operatorname{covol} \Lambda = \dim_k R^n/\Lambda$. Consider the k-vector spaces

$$\forall 1 \leq i \leq n,\ \mathcal{B}_i = \{x_i \in R \mid \forall 1 \leq j \leq m,\ \deg_j x_i \leq e_{ij}\},$$

$$\mathcal{B} = \{(x_1, \ldots, x_n) \in R^n \mid \deg_j x_i \leq e_{ij}\} = \prod_{i=1}^{n} \mathcal{B}_i.$$

By Proposition 1.14, for $x_i \in K$,

$$\deg_j x_i \leq e_{ij} \iff -d_j \operatorname{ord}_{\infty_j} x_i \leq e_{ij} \iff \operatorname{ord}_{\infty_j} x_j \geq \frac{-e_{ij}}{d_j}.$$

Thus $\mathcal{B}_i$ is the Riemann-Roch space $\mathcal{L}(\sum_{j=1}^{m} \lfloor \frac{e_{ij}}{d_j} \rfloor \infty_j)$. By Riemann-Roch,

$$\dim_k \mathcal{B}_i \geq \sum_{j=1}^{m} d_j \lfloor \frac{e_{ij}}{d_j} \rfloor - g + 1$$

$$\geq \sum_{j=1}^{m} d_j \left(\frac{e_{ij}}{d_j} - \frac{d_{j-1}}{d_j} \right) - g + 1 = \sum_{j=1}^{m} e_{ij} - \sum_{j=1}^{m} d_j + m - g + 1.$$

It follows that

$$\dim_k \mathcal{B} > \sum_{i,j} e_{ij} + n(m + 1 - \sum_{j=1}^{m} d_j - g) - 1 \geq \operatorname{covol} \Lambda,$$

so by the Linear Algebraic Pigeonhole Principle $\mathcal{B} \cap \Lambda^\bullet \neq \varnothing$. □

5. Blichfeldt, Minkowski and Hasse Domains

5.1. **Abstract Blichfeldt and Minkowski Theorems.**

Proposition 5.1. *(Measure Theoretic Pigeonhole Principle) Let (X, μ) be a measure space, $\{S_i\}_{i \in I}$ a countable family of measurable subsets of X, $m \in \mathbb{N}$. If*

$$\sum_{i \in I} \mu(S_i) > m\mu(\bigcup_{i \in I} S_i), \tag{14}$$

then there is $x \in X$ with $\#\{i \in I \mid x \in S_i\} > m$.

Proof. By replacing X with $\bigcup_{i \in I} S_i$ we may assume that $\bigcup_{i \in I} S_i = X$. Further, it is no loss of generality to assume that $\mu(X) > 0$ and that no $x \in X$ lies in infinitely many of the sets S_i: indeed, in the former case the hypothesis does not hold and in the latter case the conclusion holds.

For a subset $S \subset X$, denote by 1_S the associated characteristic function: $1_S(x) = 1$ if $x \in S$, and otherwise $1_S(x) = 0$. Put

$$f = \sum_{i \in I} 1_{S_i}.$$

For any $x \in X$, $f(x) = \#\{i \in I \mid x \in S_i\}$, so $f : X \to \mathbb{R}$ is a measurable function. The condition (14) can be reexpressed as

$$\int_X f d\mu > m \int_X d\mu,$$

so we must have $\#\{i \in I \mid x \in S_i\} = f(x) > m$ for at least one $x \in X$. □

A **measured group** $(G, +, \mathcal{A}, \mu)$ is a group $(G, +)$ – not assumed to be commutative, though we write the group law additively – and a measure $(G, \mathcal{A}, \mu)$ which is right invariant: for all $A \in \mathcal{A}$ and $x \in G$, $\mu(A + x) = \mu(A)$. To avoid trivialities, we assume $\mu(G) > 0$.

Let Γ be a subgroup of G. A **fundamental domain** $\mathcal{F}$ for Γ in G is a measurable subset $\mathcal{F} \subset G$ such that
(FD1) $\bigcup_{g \in \Gamma} \mathcal{F} + g = \Gamma$, and
(FD2) Fo all $g_1, g_2 \in \Gamma$, $\mu((\mathcal{F} + g_1) \cap (\mathcal{F} + g_2)) = 0$.

Lemma 5.2. *If $\mathcal{F}_1$ and $\mathcal{F}_2$ are both fundamental domains for a countable subgroup Γ in G, then $\mu(\mathcal{F}_1) = \mu(\mathcal{F}_2)$.*

Proof. Observe that if $\{\mathcal{S}_i\}_{i \in I}$ is a countable family of subsets such that $\mu(S_i \cap S_j) = 0$ for all $i \neq j$, then

$$\mu(\bigcup_{i \in I} S_i) = \sum_{i \in I} \mu(S_i).$$

Now we have

$$\mathcal{F}_1 \supset \mathcal{F}_1 \cap (\bigcup_{g\in\Gamma} \mathcal{F}_2 + g) = \bigcup_{g\in\Gamma} \mu(\mathcal{F}_1 \cap (\mathcal{F}_2) + g),$$

so, using the above observation,

$$\mu(\mathcal{F}_1) \geq \sum_{h\in H} \mu(\mathcal{F}_1 \cap (\mathcal{F}_2 + g)) = \sum_{g\in\Gamma} \mu(\mathcal{F}_1 \cap (\mathcal{F}_2 - g)) = \sum_{g\in\Gamma} \mu((\mathcal{F}_1 + g) \cap \mathcal{F}_2)$$

$$= \mu(\bigcup_{g\in\Gamma} (\mathcal{F}_1 + g) \cap \mathcal{F}_2) = \mu(\mathcal{F}_2).$$

Interchanging $\mathcal{F}_1$ and $\mathcal{F}_2$ we get the result. □

A subgroup Λ of a measured group G is a **lattice** if it is countable and admits a measurable fundamental domain of finite measure. We define the **covolume** $\operatorname{Covol}\Lambda$ to be the measure of any such fundamental domain. Note that our assumption $\mu(G) > 0$ implies $\operatorname{Covol}\Lambda > 0$.

Theorem 5.3. *(Abstract Blichfeldt Lemma) Let Λ be a lattice in a measured group G, and let $M \in \mathbb{Z}^+$. Let $\Omega \subset G$ be measurable, and suppose*

$$\frac{\mu(\Omega)}{\operatorname{Covol}\Lambda} > M. \tag{15}$$

There are distinct $w_1, \ldots, w_{M+1} \in \Omega$ such that for all $1 \leq i, j \leq M+1$, $w_i - w_j \in \Lambda$.

Proof. Let $\mathcal{F}$ be a measurable fundamental domain for Λ in G. For $x \in \Lambda$, let

$$\Omega_x = \Omega \cap (\mathcal{F} + x).$$

Then $\Omega = \bigcup_{x\in\Gamma} \Omega_x$: this is a countable union which is essentially pairwise disjoint – for all $x \neq y \in \Gamma$, $\mu(\Omega_x \cap \Omega_y) = 0$ – so

$$\sum_{x\in\Gamma} \mu(\Omega_x - x) = \sum_{x\in\Lambda} \mu(\Omega_x) = \mu(\Omega) > M \operatorname{Covol}(\Lambda) = M\mu(\mathcal{F}). \tag{16}$$

We apply the Measure Theoretic Pigeonhole Principle with $X = \mathcal{F}$, $I = \Lambda$, $S_x = \Omega_x - x$: there is $v \in \mathcal{F}$ and $x_1, \ldots, x_{M+1} \in \Lambda$ such that

$$v \in \bigcap_{i=1}^{M+1} \Omega_{x_i} - x_i.$$

Thus for $1 \leq i \leq M+1$ there is $w_i \in \Omega_{x_i}$ – so $w_1, \ldots, w_{M+1}$ are distinct – with

$$\forall 1 \leq i \leq M+1, w_i - x_i = v.$$

It follows that for all $1 \leq i, j \leq M+1$, $w_i - w_j = (x_i + v) - (x_j + v) = x_i - x_j \in \Lambda$. □

Remark 5.4. *When μ is the counting measure on G, we essentially recover the Group Theoretic Pigeonhole Principle (more precisely, the case in which Γ is countable and κ is finite).*

A **measured ring** is a ring endowed with a measure such that the additive group of R is a measured group. Again we assume $\mu(R) > 0$ to avoid trivialities.

Theorem 5.5. *(Abstract Minkowski Theorem) Let* $M \in \mathbb{Z}^+$, $(R, +, \cdot, \mathcal{A}, \mu)$ *be a measured ring, and let* $\Lambda \subset R^N$ *be a countable subgroup. Let* $\Omega \subset R$ *be measurable and symmetric:* $x \in \Omega \implies -x \in \Omega$.
a) We suppose $2 \in R^\bullet$ *and all of the following:*
• Ω *is* ***midpoint closed:*** $x, y \in \Omega \implies \frac{x+y}{2} \in \Omega$.
• 2Λ *is a lattice in* R.
• $\frac{\mu(\Omega)}{\operatorname{Covol} 2\Lambda} > M$.
Then $\#(\Omega \cap \Lambda^\bullet) \geq M$.
b) We suppose all of the following:
• Ω *is closed under subtraction:* $x, y \in \Omega \implies x - y \in \Omega$.
• Λ *is a lattice in* R.
• $\frac{\mu(\Omega)}{(\operatorname{Covol} \Lambda} > M$.
Then $\#(\Omega \cap \Lambda^\bullet) \geq M$.

Proof. a) Apply the Abstract Blichfeldt Lemma with $G = (R, +)$ and 2Λ in place of Λ. We get distinct elements $w_1, \ldots, w_{M+1} \in \Omega$ such that for all $1 \leq i, j \leq M+1$, $\frac{w_i - w_j}{2} \in \Lambda$. Since Ω is symmetric and midpoint closed, $-w_j \in \Omega$ and thus $\frac{w_i - w_j}{2} \in \Omega$ for all $1 \leq i, j \leq M+1$. Fixing $i = 1$ and letting j run from 2 to $M+1$ gives us M nonzero elements of $\Omega \cap \Lambda$.
b) This is exactly the same as part a) except we use Λ instead of 2Λ and use the fact that Ω is closed under subtraction. □

Corollary 5.6. *(Minkowski Convex Body Theorem) Let* $\Omega \subset \mathbb{R}^n$ *be symmetric and convex, and let* $\Lambda \subset \mathbb{R}^n$ *be a lattice. If* $\operatorname{Vol} \Omega > 2^n \operatorname{Covol} \Lambda$, *then* $\Omega \cap \Lambda^\bullet \neq \varnothing$.

Proof. A convex subset is midpoint closed. Also $\operatorname{Covol}(2\Lambda) = 2^n \operatorname{Covol} \Lambda$. Now apply Theorem 5.5a). □

Corollary 5.7. *(Chonoles Convex Body Theorem* [Ch12]*) Let* $\mathcal{R} = \mathbb{F}_q((\frac{1}{t}))^n$ *and let* Λ *be an* $\mathbb{F}_q[t]$*-lattice in* R. *If* $\Omega \subset \mathcal{R}$ *is closed under subtraction and satisfies* $\operatorname{Vol} \Omega > \operatorname{Covol} \Lambda$, *then* $\Omega \cap \Lambda^\bullet \neq 0$.

Let $R = \mathbb{Z}_{K,S}$ be an S-integer ring in a number field K. Let $\mathcal{R} = \prod_{v \in S} K_v$. This is a locally compact ring. We endow it with the product of the Haar measures on each factor, where each factor isomorphic to $\mathbb{R}$ gets the standard Lebesgue measure, each factor isomorphic to $\mathbb{C}$ gets twice the standard Lebesgue measure, and each non-Archimedean local field K_v gets the Haar measure which gives its maximal compact subring $\mathcal{O}_v$ volume 1. It is a standard fact that $\sigma(R)$ is discrete and cocompact in $\mathcal{R}$: see e.g. [Co]. Let $\mathcal{V}(R)$ denote the μ-volume of a fundamental domain for $\sigma(R)$ in $\mathcal{R}$.

On $\mathcal{R}^n$, let μ the product Haar measure. Let $\Lambda \subset K^n$ be an R-sublattice, and let $\hat{\sigma} : K^n \to \mathcal{R}^n$ be the natural embedding. It follows that $\hat{\sigma}(\Lambda)$ is discrete and cocompact in $\mathcal{R}^n$, and that its covolume in the measure theoretic sense is equal to $|\chi(\Lambda)|\mathcal{V}(R)^n$. Thus if we take Vol to be $\mathcal{V}(R)^{-n}\mu$, then Vol is a Haar measure on $\mathcal{R}^n$ such that $\operatorname{Covol} \Lambda$ means both the covolume in the sense of § 1.9 and the measure of a fundamental domain for Λ in $\mathcal{R}^n$.

Corollary 5.8. *Let* $\Omega \subset \mathcal{R}^n$ *be a measurable subset such that*

$$\operatorname{Vol} \Omega > \operatorname{Covol} \Lambda.$$

Then there are distinct $x, y \in \Omega$ *such that* $x - y \in \Lambda$.

5.2. **Hasse Domains Are of Multimetric Linear Type.**

For $z = x + yi \in \mathbb{C}$, recall that we have taken the normalization $|z| = x^2 + y^2$.

Lemma 5.9. *a) When $S_f = \varnothing$, we have $\mathcal{V}(R) = |\Delta(K)|^{\frac{1}{2}}$.*
b) Let $r, s \in \mathbb{N}$, $d = r + 2s$, $t \in \mathbb{R}$, and let

$$B_t = \{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s \mid \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j|^{\frac{1}{2}} \leq t\}.$$

Then for all $t \geq 0$,

$$\operatorname{Vol} B_t = \mathcal{V}(R)^{-n} 2^r \pi^s \frac{t^d}{d!}.$$

Proof. Both assertions are part of the standard application of geometry of numbers to algebraic number theory. For proofs see e.g. [S, Ch. IV]. □

Theorem 5.10. *Let K be a number field. Suppose K has r real places and s complex places, and put $d = r + 2s = [K : \mathbb{Q}]$. Let $\mathbb{Z}_K$ be the ring of integers of K, and let $\mathbb{Z}_K \subset R \subset K$ be an overring. Then for all $n \in \mathbb{Z}^+$,*

$$C(R, n) \geq M(K)^{-n}, \tag{17}$$

where

$$M(K) = \left(\frac{4}{\pi}\right)^s \frac{d!}{d^d} |\Delta_K|^{\frac{1}{2}}$$

is Minkowski's constant.

Proof. By Proposition 2.6, we may assume $R = \mathbb{Z}_K$. Consider the embedding $\hat{\sigma} : K^n \hookrightarrow \mathbb{R}^{nd}$, $(x_1, \ldots, x_n) \mapsto (\sigma(x_1), \ldots, \sigma(x_n))$. For any R-sublattice Λ of R^n, $\hat{\sigma}(\Lambda)$ is a lattice in $\mathbb{R}^{nd}$. For $\epsilon = (\epsilon_1, \ldots, \epsilon_n) \in (\mathbb{R}^{>0})^n$, we define $S_1(\epsilon) \subset \mathbb{R}^{nd}$ as the set of all $x \in \mathbb{R}^{nd}$ satisfying

$$|x_{i1}| \cdots |x_{ir}||x_{i(r+1)}^2 + x_{i(r+2)}^2| \cdots |x_{i(d-1)}^2 + x_{id}^2| \leq \epsilon_i$$

for $1 \leq i \leq n$. By the arithmetic geometric mean inequality, $S_1(\epsilon)$ contains the symmetric compact convex body $S_2(\epsilon)$ defined by

$$|x_{i1}| + \ldots + |x_{ir}| + 2|x_{i(r+1)}^2 + x_{i(r+2)}^2|^{\frac{1}{2}} + \ldots + 2|x_{i(d-1)}^2 + x_{id}^2|^{\frac{1}{2}} \leq d\epsilon_i^{\frac{1}{d}}$$

for all $1 \leq i \leq n$. By Lemma 5.9,

$$\operatorname{Vol} S_2(\epsilon) = \mathcal{V}(R)^{-n} \left(2^r \pi^s \frac{d^d}{d!}\right)^n \epsilon_1 \cdots \epsilon_n.$$

Applying Minkowski's Convex Body Theorem, there is a nonzero point of Λ in $S_2(\epsilon)$ (hence also in $S_1(\epsilon)$ if

$$\mathcal{V}(R)^{-n} \left(2^r \pi^s \frac{d^d}{d!}\right)^n (\epsilon_1 \cdots \epsilon_N) = \operatorname{Vol}(S_2(\epsilon)) \geq 2^{nd},$$

i.e., if and only if

$$\operatorname{Covol} \Lambda \leq M(K)^{-n} \epsilon_1 \cdots \epsilon_n.$$

Since a point in $S_1(\lambda)$ satisfies $|x_i| \leq \epsilon_i$ for all i, this shows that $M(K)^{-n}$ is a linear constant for $\mathbb{Z}_K$ in dimension n. □

Remark 5.11. *When K is an imaginary quadratic field, the lower bound on $C(\mathbb{Z}_K, n)$ given in (17) is precisely the same lower bound given in (12).*

Theorem 5.12. *The Hasse domain $R = \mathbb{Z}_{K,S}$ is of multimetric linear type. More precisely, for all $n \in \mathbb{Z}^+$,*

$$C_M(R,n) \geq (\frac{\pi}{4})^s \mathcal{V}(R)^{-n}.$$

Proof. Consider the embedding $\hat{\sigma} : K^n \hookrightarrow \mathcal{R}^n$, $(x_1, \ldots, x_n) \mapsto (\sigma(x_1), \ldots, \sigma(x_n))$. For any R-sublattice Λ of R^n, $\hat{\sigma}(\Lambda)$ is a lattice in $\mathbb{R}^{nd}$ with covolume $[R^n : \Lambda]$. Fix $\epsilon_{i,j} > 0$ and $e_{i,P_j} \in \mathbb{Z}$. Let Ω be the set of $(x_1, \ldots, x_n) \in \mathcal{R}^n$ such that $|x_i|_{\infty_j} \leq \epsilon_{ij}$ and $\deg_{P_j} x_i \leq e_{iP_j}$ for all i and j. Then

$$\operatorname{Vol} \Omega = \mathcal{V}(R)^{-n} 2^r \pi^s \prod_{i,j} \epsilon_{ij} \prod_{j=1}^{s} q_{P_j}^{e_{1P_j} + \ldots + e_{nP_j}}.$$

By Corollary 5.8, if

$$2^r \pi^s \prod_{i,j} \epsilon_{ij} \prod_{j=1}^{s} q_{P_j}^{e_{1P_j} + \ldots + e_{nP_j}} > [R^n : \Lambda] \mathcal{V}(R)^n,$$

then there are distinct $x, y \in \Omega$ such that $x - y \in \Lambda$. Thus if we define ϵ'_{ij} to be $\frac{\epsilon_{ij}}{2}$ when ∞_j is real and $\frac{\epsilon_{ij}}{4}$ when ∞_j is complex, we find that if

$$2^r \pi^s \prod_{i,j} \epsilon'_{ij} \prod_{j=1}^{s} q_{P_j}^{e_{1P_j} + \ldots + e_{nP_j}} > [R^n : \Lambda] \mathcal{V}(R)^n,$$

then there is $x \in \Omega \cap \Lambda^\bullet$. Thus any number larger than $2^r \pi^s 2^{-r-2s} \mathcal{V}(R)^{-n} = 2^{-2s} \pi^s \mathcal{V}(R)^{-n}$ is a linear multimetric constant in dimension n. □

Remark 5.13. *In Theorem 5.12 we are more concerned with the qualitative result that S-integer rings in number fields are of multimetric linear type than with the value of the constant. Thus we have not used the arithmetic geometric mean maneuver of the proof of Theorem 5.8 or even computed $\mathcal{V}(R)$ in the general case.*

6. Quadratic Forms: the Nullstellensatz

6.1. **The Nullstellensatz.**

Let $(R, |\cdot|)$ be a normed Dedekind domain of multimetric linear type. We renormalize so that each norm $|\cdot|_j$ has Artin constant at most 2. Thus the triangle inequality holds and $|n|_j \leq n$ for all Archimedean j and $|n|_j = 1$ for all non-Archimedean j.

For $x = (x_1, \ldots, x_n) \in K^n$, we put

$$|x|_j = \max_i |x_i|_j, \; |x| = \prod_{j=1}^{m} |x|_j.$$

For a matrix $M = (m_{ij}) \in M_n(R)$, we put

$$|M|_j = \max_{i,k} |m_{ik}|_j$$

when j is a q-norm and

$$|M|_j = \sum_{i,k} |m_{ik}|_j$$

when j is Archimedean. Also put

$$|M| = \prod_{j=1}^{m} |M|_j.$$

For a quadratic form

$$f = \sum_{1 \leq i \leq k \leq n} m_{ik} x_i x_j$$

with coefficients in R, we let $M = (m_{ik})$ be the corresponding upper triangular matrix and put

$$|f| = |M|.$$

An **isotropic vector** for a quadratic form f is a nonzero vector $v \in R^n$ with $f(v) = 0$. A form f is **isotropic** if it has an isotropic vector and otherwise **anisotropic**.

There is a rival notion of the size of a vector $x = (x_1, \ldots, x_n) \in K^n$, namely we could take $\max_i |x_i|$. Curiously, this is the measure we will use in the statement of the Nullstellensatz, although both will occur in the proof! For later use we note the relationship between them:

$$\forall x = (x_1, \ldots, x_n) \in K^n, \ \max_i |x_i| \leq |x|. \tag{18}$$

Theorem 6.1 (Nullstellensatz)**.** *Let $(R, |\cdot|)$ be a normed Dedekind domain of multimetric linear type, with fraction field K. We suppose that $|R|$ is a discrete subset of $\mathbb{R}$ (e.g. if some equivalent norm is $\mathbb{Z}$-valued). Let $f = \sum_{i,j} m_{ij} t_i t_j \in R[t_1, \ldots, t_n]$ be a nonzero isotropic quadratic form.*
a) If the norm is of q-type, then f admits an isotropic vector $a \in R^n$ with

$$\max_i \deg a_i \leq mn - 1 - c_M(R, n) + \binom{n-1}{2} \deg f. \tag{19}$$

b) Suppose there is at least one j such that $|\cdot|_j$ is Archimedean and m' of them altogether. Let $0 < \delta < C_M(R, n)$ and $0 < \eta < 1$. Then f admits an isotropic vector a with

$$\max_i |a_i| \leq \max\left(\frac{(1 - \eta^{\frac{1}{m'}})^{-m'(n-1)}}{\eta(C_M(R, n) - \delta)} \right), \left(\frac{1}{\eta(C_M(R, n) - \delta)} \right) |3f|^{\frac{n-1}{2}}. \tag{20}$$

c) If $R = \mathbb{Z}$ then q admits an isotropic vector $a \in R^n$ with

$$|a| \leq (3|f|)^{\frac{n-1}{2}}.$$

Proof. In Steps 0 and 1 we treat the part of the proof which is essentially the same in all cases. Then we treat the q-normed case in Step 2, the densely normed case in Step 3, and the $R = \mathbb{Z}$ case in Step 4.
Step 0: Since $|R|$ is discrete, there is an f-isotropic vector $a = (a_1, \ldots, a_n) \in R^n$ with $|a|$ minimal. By permuting the variables, we may assume that $\max_i |a_i| = |a_n|$. For $x, y \in K^n$, we define a bilinear form

$$\langle x, y \rangle = f(x + y) - f(x) - f(y) = \sum_{1 \leq i \leq j \leq n} m_{ij}(x_i y_j + x_j y_i).$$

Step 1: We CLAIM: for all $b \in R^n$ with $f(b) \neq 0$ and all $c \in K$,

$$|f|^{-1} \leq |3||b - ca|^2. \tag{21}$$

PROOF OF CLAIM: Let

$$a^* = f(b)a - \langle a, b\rangle b.$$

A calculation – which can be interpreted in terms of reflection through b – gives

$$f(a^*) = f(b)^2 f(a) - f(b)\langle a, b\rangle\langle a, b\rangle + \langle a, b\rangle^2 f(b) = 0.$$

By the minimality of a, we have

$$|a| \leq |a^*|. \tag{22}$$

Now put $d = b - ca$, so $b = d + ca$. Then

$$a^* = f(d + ca)a - \langle a, d + ca\rangle(d + ca) = f(d)a - \langle a, d\rangle d.$$

Fix $1 \leq j \leq m$. Suppose first that $|\cdot|_j$ is Archimedean. Then:

$$|a^*|_j = |f(d)a - \langle a, d\rangle d|_j \leq |\sum_{i,j} m_{ij} d_i d_j|_j |a|_j + |2|_j |\sum_{i,j} m_{ij} a_i d_j|_j |d|_j$$

$$\leq \sum_{i,j} |m_{ij}|_j |a|_j |d|_j^2 + |2|_j \sum_{i,j} |m_{ij}|_j |a|_j |d|_j^2 = |3|_j |f|_j |a|_j |d|_j^2.$$

The ultrametric case is similar. Multiplying from $j = 1$ to m we get

$$|a^*| \leq |3||f||a||d|^2. \tag{23}$$

Combining (22) and (23) and dividing through by $|a||f|$, we get (21).
Step 2: Suppose the norm is of q-type. We may assume that

$$\deg a_n \geq mn - c_M(R, n),$$

for (19) holds otherwise. Apply Theorem 2.9b) with $n-1$ in place of n, $M = \deg a_n$ and $\theta_i = \frac{a_i}{a_n}$ for $1 \leq i \leq n-1$: there is $b = (b_1, \ldots, b_n) \in R^n$ with $b_n \neq 0$ such that

$$\forall 1 \leq i \leq n-1, \forall 1 \leq j \leq m,\ \deg_j b_n\theta_i - b_i \leq \frac{mn - 1 - c_M(R, n) - \deg a_n}{m(n-1)}, \tag{24}$$

$$\forall 1 \leq j \leq m,\ \deg_j b_n \leq \deg_j a_n - 1. \tag{25}$$

We CLAIM that for all i, j, $\deg_j b_i \leq \deg_j a - 1$. When $i = n$, this follows from (25). Suppose $1 \leq i \leq n-1$. Then for all $1 \leq j \leq m$,

$$\deg_j b_i \leq \max\left(\frac{mn - 1 - c_M(R, n) - \deg a_n}{m(n-1)}, \deg_j b_n + \deg_j a_i - \deg_j a_n\right).$$

If $b_i = 0$ then for all j, $\deg_j b_i = -\infty \leq \deg_j a_n - 1$. If $b_i \neq 0$, then since $\left(\frac{mn-1-c_M(R,n)-\deg a_n}{m(n-1)}\right) < 0$, we have

$$\deg_j b_i \leq \deg_j a_i + (\deg_j b_n - \deg_j a_n) \leq \deg_j a_i - 1,$$

establishing the claim. Thus for all j, $\deg_j b = \max_i \deg_j b_i \leq \deg_j a - 1$, so

$$\deg b = \sum_{j=1}^{m} \deg_j b \leq \deg_j a - m < \deg a,$$

so by minimality of a, $f(b) \neq 0$. Put $c = \frac{b_n}{a_n}$; then

$$\deg b - ca \leq \frac{mn - 1 - c_M(R, n) - \deg a_n}{n-1}. \tag{26}$$

In this case (21) can be restated as

$$-\deg f \leq 2\deg(b - ca). \tag{27}$$

Combining (27) and (26) we get

$$-\deg f \leq 2\left(\frac{mn - 1 - c_M(R,n) - \deg a_n}{n-1}\right),$$

which is equivalent to

$$\max_i \deg a_i = \deg a_n \leq (mn-1) - c_M(R,n) + \left(\frac{n-1}{2}\right)\deg f.$$

Step 3: Suppose that the number m' of Archimedean infinite places is at least one. For $\delta > 0$, we put $C_\delta = C_M(R,n) - \delta$: we will take δ to be small enough so that $C_\delta > 0$. We introduce an auxiliary parameter $\eta \in (0,1)$. From the form of the claimed inequality on $|a_n| = \max_i |a_i|$ we may assume

$$|a_n| > \frac{(1 - \eta^{\frac{1}{m'}})^{-m'(n-1)}}{\eta C_\delta}. \tag{28}$$

Let us also put

$$\kappa = (C_\delta \eta |a_n|)^{\frac{-1}{m'(n-1)}};$$

then (28) is equivalent to

$$\kappa < 1 - \eta^{\frac{1}{m'}}. \tag{29}$$

Apply Theorem 2.9 with $n-1$ in place of n, $M = \eta|a_n|$ and $\theta_i = \frac{a_i}{a_n}$ for $1 \leq i \leq n-1$: there is $b = (b_1, \ldots, b_n) \in R^n$ with $b_n \neq 0$ such that: if j is Archimedean then

$$\forall 1 \leq i \leq n-1,\ |b_n\theta_i - b_i|_j \leq (C_\delta \eta |a_n|)^{\frac{-1}{m'(n-1)}} = \kappa < 1$$

$$|b_n|_j \leq \eta^{\frac{1}{m'}}|a_n|_j,$$

whereas for every non-Archimedean j we have

$$\forall 1 \leq i \leq n-1,\ |b_n\theta_i - b_i|_j \leq 1,$$

$$|b_n|_j \leq 1.$$

For all non-Archimedean j and all i we have $|b_i|_j \leq 1 \leq |a_n|_j$ and thus $|b|_j \leq |a|_j$. Now let j be Archimedean. We have

$$|b_n|_j \leq \eta^{\frac{1}{m'}}|a_n|_j < |a_n|_j.$$

Further, for $1 \leq i \leq n-1$,

$$|b_i|_j = |b_n\frac{a_i}{a_n} - b_i - b_n\frac{a_i}{a_n}|_j \leq |b_i - b_n\frac{a_i}{a_n}|_j + \frac{|b_n|_j}{|a_n|_j}|a_i|_j \leq \kappa + \eta^{\frac{1}{m'}}|a_i|_j.$$

If $a_i = 0$, then this gives

$$|b_i|_j \leq \kappa < 1 \leq |a_n|_j \leq |a|_j.$$

Otherwise $|a_i|_j \geq 1$, so by (29)

$$\left(1 - \eta^{\frac{1}{m'}}\right)|a_i|_j \geq 1 - \eta^{\frac{1}{m'}} > \kappa$$

and thus

$$|b_i|_j \leq \kappa + \eta^{\frac{1}{m'}}|a_i|_j < |a_i|_j \leq |a|_j.$$

Thus we have $|b|_j \leq |a|_j$ for all j with strict inequality at each Archimedean place hence $|b| < |a|$. By minimality of a, $f(b) \neq 0$. Put $c = \frac{b_n}{a_n}$; then

$$(30) \qquad |b - ca| \leq \prod_{j=1}^{m'} (C_\delta \eta |a_n|)^{\frac{-1}{m'(n-1)}} = (C_\delta \eta |a_n|)^{\frac{-1}{n-1}}.$$

Combining (21) and (30) as above yields

$$\max_i |a_i| = |a_n| \leq \frac{1}{\eta C_\delta} |3f|^{\frac{n-1}{2}}.$$

Step 4: If $R = \mathbb{Z}$, then it is no loss of generality to suppose that $|a| \geq 2$, as the claimed bound certainly holds otherwise. Using Corollary 3.4 there is $b = (b_1, \ldots, b_n) \in R^n$ with $b_n \neq 0$ such that

$$\forall 1 \leq i \leq n-1, |b_n \theta_i - b_i| \leq |a|^{\frac{-1}{n}},$$

$$|b_n| < |a|.$$

Then – exploiting that the norm on $\mathbb{Z}$ is $\mathbb{N}$-valued – for all $1 \leq i \leq n-1$,

$$|b_i| \leq |b_n \theta_i - b_i| + |b_n \frac{a_i}{a_n}| < 1 + |b_n| \leq |a|.$$

The rest of the argument is the same as in Step 3 above and leads to

$$|a| \leq (3|f|)^{\frac{n-1}{2}}. \qquad \square$$

6.2. **Some Cases of the Nullstellensatz.**

In every case, Theorem 6.1 takes the form: for a suitable normed domain $(R, |\cdot|)$ and $n \in \mathbb{Z}^+$, there is a constant $Q(R,n)$ such that every nonzero isotropic n-ary quadratic form f over a normed domain $(R, |\cdot|)$ admits an isotropic vector $|a|$ with

$$(31) \qquad |a| \leq Q(R,n) |f|^{\frac{n-1}{2}}.$$

When $R = \mathbb{Z}$ the existence of a bound of the form (31) was shown by Cassels [Ca55]. In his textbook [C], Cassels gave an improved argument leading to the better bound $Q(R,n) = 3^{\frac{n-1}{2}}$. We have essentially reproduced this argument in our Theorem 6.1c). Cassels gives examples to show that the exponent $\frac{n-1}{2}$ cannot be improved upon, and thus Theorem 6.1b) is sharp up to the constant $Q(\mathbb{Z}, n)$. Whether one can improve upon $Q(\mathbb{Z}, n) = 3^{\frac{n-1}{2}}$ seems to be an open question. There is certainly no room for improvement coming from linear forms: we have used that the linear constants $C(\mathbb{Z}, n)$ are all equal to 1 – the largest possible value – and even a little more via Theorem 3.4.

By Theorem 5.12, the hypotheses of part b) hold when $R = \mathbb{Z}_K$ for an imaginary quadratic field K. A result of this form was first proved by [Ra75], who showed that one can take $Q(R,n) = \operatorname{disc}(K)^{\frac{n}{4}} 5^{\frac{n-1}{2}}$. To apply Theorem 6.1 in this case we take the square root of the canonical norm on $\mathbb{Z}_K$, giving $C(R,n) \geq \left(\frac{2}{\pi}\right)^{\frac{n}{2}} (\operatorname{disc} K)^{\frac{n}{4}}$. Our approach gives a better constant, at least asymptotically: assuming that $|f|$ is large enough so that the "eta factor" in (20) can be ignored, we get a constant arbitrarily close to $\left(\frac{2}{\pi}\right)^{\frac{n}{2}} 3^{\frac{n-1}{2}} (\operatorname{disc} K)^{\frac{n}{4}}$.

(We admit that the eta factor in (20) seems to be an artifice of the proof. Unfortunately we do not know how to remove it, but probably someone else will.)

When K is a number field with more than one infinite place, the canonical norm is not metric. This did not stop Raghavan from proving a generalization of Cassels's Theorem in this context: the constant he gets is $\mathrm{disc}(K)^{\frac{n}{2[K:\mathbb{Q}]}} 5^{\frac{n-1}{2}}$. However he does not use (an equivalent norm to) the canonical norm: in fact his measure of the size of the coefficients is not a norm at all in our sense, as it is only submultiplicative (but satisfies the triangle inequality).

Combining the Nullstellensatz with Theorem 5.12 for $R = \mathbb{Z}_K$ we recover a variant of Ragahvan's result. But moreover we may take $R = \mathbb{Z}_{K,S}$ to be any S-integer ring. This is a new result, but as we will see it is a natural one, being an analogue of a result of Pfister in the function field case.

Turning now to the q-normed case of Theorem 6.1, we get cleaner results.

Corollary 6.2. *(Prestel* [Pr87]*) Let k be a field, and let f be a nonzero n-ary quadratic form with coefficients in $k[t]$. If f is isotropic, there is an isotropic vector v with $\deg v \leq \frac{n-1}{2} \deg f$.*

Proof. Apply Corollary 4.4 and Theorem 6.1. □

Our method of proof of Theorem 6.1 owes a lot to [Pr87]: roughly, we have replaced an argument on linear systems over $k[t]$ with our theory of linear constants.

Again Prestel gives an example to show that the exponent $\frac{n-1}{2}$ in (31) is best possible, again whether the constant is best possible remains open, and again there is no possible improvement coming from the theory of linear constants, since $c(k[t], n) = n - 1$ is the largest possible value.

In the same paper, Prestel considers the ring $R = \mathbb{R}[x, y]$. Writing $\deg f$ for the total degree of an element of R, notice that for fixed $q > 1$, $|f| = q^{\deg f}$ gives an *elementwise* multiplicative q-norm function on the UFD R. It is sensible to define the linear q-constants $c(R, n)$ in this context – since R is not a Dedekind domain, one ought to restrict to free lattices – and if $c(R, n) > -\infty$, the proof of Theorem 6.1c) would apply to give a bound on the degree of an isotropic vector for an isotropic quadratic form in terms of the total degrees of the coefficients of the form. However, for $n = 16$, Prestel exhibits for each $v \in \mathbb{N}$ a quadratic form $f_v \in R[t_1, \ldots, t_n]$ with total degree 2 and such that the least degree of an isotropic vector is at least v [Pr87, Thm. 2]. Thus $\mathbb{R}[x, y]$ is not of linear type!

Corollary 6.3. *Let $C_{/k}$ be a smooth, geometrically integral projective curve over k, let $\infty_1, \ldots, \infty_m$ be closed points of degrees $d_1, \ldots, d_m$. Let $C^\circ = C \setminus \{\infty_1, \ldots, \infty_m\}$, and let $k = k[C^\circ]$ endowed with its canonical q-norm of § 1.8. Let $f \in R[t_1, \ldots, t_n]$ be a nonzero isotropic quadratic form. Then f admits an isotropic vector v with*

$$\deg v \leq \left(\sum_j d_j + g - 1 \right) n + \left(\frac{n-1}{2} \right) \deg f. \tag{32}$$

Proof. Apply Theorems 4.6 and 6.1. □

Corollary 6.3 is a variant of the Nullstellensatz of A. Pfister. For $f \in k(C)^\bullet$, let $\deg_P f$ be the degree of the polar part of $\operatorname{div} f$; by taking maxima we extend this notion of $\deg_P$ to vectors and matrices with coefficients in $k(C)$. Then:

Theorem 6.4. *(Pfister* [Pf97]*) With hypotheses as in Corollary 6.3, f admits an isotropic vector v with*

$$\deg_P v \leq (\max_i d_i + g - 1)n + \left(\frac{n-1}{2}\right) \deg_P f. \tag{33}$$

For $x \in k[C^\circ]^\bullet$, $\deg x$ is the sum of all of the infinite degrees $\deg_j x$ whereas $\deg_P x$ is the sum over only the non-negative terms $\deg_j x$, so $\deg x \leq \deg_P f$. (Further, $\deg x$ depends on the chosen set of infinite places whereas $\deg_P f$ does not.) When $m = 1$ we have $\deg_P = \deg$ and indeed Corollary 6.3 and Theorem 6.4 coincide. For $m > 1$ the constant in Theorem 6.4 is smaller than that of Corollary 6.3, but because the norms are different the results do not appear to be directly comparable. However, Pfister himself showed that a variant of Theorem 6.4 follows easily from the common special case $m = 1$ by a short argument involving the Riemann-Roch Theorem. Thus the following result is also a corollary of our Nullstellensatz.

Corollary 6.5. *(Pfister* [Pf97, p. 230]*) With hypotheses as in Corollary 6.3, f admits an isotropic vector v with*

$$\deg_P v \leq \left(\frac{3n-1}{2}\right)(\min_j d_j + g - 1) + \left(\frac{n-1}{2}\right) \deg_P f.$$

Thus we recover Pfister's Theorem 6.4 up to a different value of the constant $Q(R, n)$. In fact Pfister remarked that the constant given in Corollary 6.5 is sometimes worse and sometimes better than that of Theorem 6.4.

7. Quadratic Forms: The Small Multiple Theorem

An ideal I in a ring R is **odd** if it is coprime to $2R$. An element x of R is odd if the principal ideal (x) is odd.

Theorem 7.1. *Let R be a Dedekind domain with fraction field K, let $q(x) = q(x_1, \ldots, x_n)$ be a nondegenerate quadratic form over R, and let I be an odd ideal of R which is coprime to* $\operatorname{disc} q$. *We further assume:*
(H) The base change of q to R/I is hyperbolic, i.e., isomorphic to $\bigoplus_{i=1}^{\frac{n}{2}} \mathbb{H}$. Then:
a) There is an R-sublattice $\Lambda_I \subset R^n$ such that:
(i) We have $R^n/\Lambda_I \cong (R/I)^{\frac{n}{2}}$ and thus $\chi(\Lambda_I) = I^{\frac{n}{2}}$.
(ii) We have $q(v) \equiv 0 \pmod{I}$ for all $v \in \Lambda_I$.
b) The R-module Λ_I is free iff $I^{\frac{n}{2}}$ is principal.
c) Each of the following conditions implies (H):
(H1) $n = 2$ and $-d(q)$ is a square in R/I.
(H2) Every residue field of R/I has u-invariant at most 2 (e.g. this holds when every residue field is finite), n is even and $(-1)^{\frac{n}{2}} d(q)$ is a square in R.

Proof. a) Step 1: We suppose $I = \mathfrak{p}^e$ is an odd prime power. Then $k := R/\mathfrak{p}$ is a field of characteristic different from 2. Let $R_\mathfrak{p}$ be the completion of R at $\mathfrak{p}$; then $R_\mathfrak{p}$ is a nondyadic CDVR with fraction field $K_\mathfrak{p}$, and since m is prime to $\operatorname{Disc} q$, the base change $\hat{q}$ of q to $R_\mathfrak{p}$ is **nonsingular**. Since the reduction of $\hat{q}$ modulo $\mathfrak{p}$ is isotropic, by Hensel's Lemma so is $\hat{q}$. Thus $\hat{q}_{/K_\mathfrak{p}}$ is universal and similar to a Pfister form, hence is itself an isotropic Pfister form. Every isotropic Pfister form

is hyperbolic, so $\hat{q}_{K_\mathfrak{p}} \cong_{K_\mathfrak{p}} \bigoplus_{i=1}^{\frac{n}{2}} \mathbb{H}$. Since $\hat{q}$ is nonsingular, it follows that $\hat{q} \cong_{R_\mathfrak{p}} \bigoplus_{i=1}^{\frac{n}{2}} \mathbb{H}$ (e.g. [Sc, Thm. 1.6.13]), and thus $q_{/R/(m)} \cong \bigoplus_{i=1}^{\frac{n}{2}} \mathbb{H}$. If the ith copy of the hyperbolic plane is the free R/I-module with basis e_i, f_i, put $M = \langle e_1, \ldots, e_{\frac{n}{2}} \rangle_{R/I}$. Let $\varphi : R^n \to (R/I)^n$ be the canonical map, and let $\Lambda_I = \varphi^{-1}(M)$. Then Λ_I is an R-submodule of Λ_I with finite length quotient, so it is an R-lattice in K^n. Clearly $\chi(R^n/\Lambda_I) = I^{\frac{n}{2}}$, and by construction, $q(v) \equiv 0 \pmod{m}$ for all $v \in \Lambda_I$, so this completes the proof of Theorem 7.1 in this case.
Step 2: Suppose $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. For $1 \leq i \leq r$, put $I_i = \mathfrak{p}_i^{e_i}$. By Step 1, for $1 \leq i \leq r$ there is a sublattice $\Lambda_i \subset R^n$ such that $\chi(R^n/\Lambda_i) = I_i^{\frac{n}{2}}$ and $q|_{\Lambda_i} \equiv 0 \pmod{I_i}$. Put $\Lambda_I = \bigcap_{i=1}^r \Lambda_i$. Then Λ_I is a sublattice of R^n; by the Chinese Remainder Theorem $\chi(R^n/\Lambda_I) = \prod_{i=1}^r \chi(R^n/\Lambda_i) = I^{\frac{n}{2}}$ and $q(v) \equiv 0 \pmod{I}$ for all $v \in \Lambda_I$.
b) This follows easily from the fact that $R^n/\Lambda_I \cong (R/I)^{\frac{n}{2}}$. □

Theorem 7.2. *Let $(R, |\cdot|)$ be a multimetric linear type normed Dedekind domain, with fraction field K. Let $f = f(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n]$ be an anisotropic quadratic form. Let d be an odd element of R which is coprime to $\operatorname{disc} q$. We suppose* ***hypothesis (H)****: the base change of q to $R/(d)$ is isomorphic to $\bigoplus_{i=1}^{\frac{n}{2}} \mathbb{H}$.*
a) If $|\cdot|_j$ is Archimedean for at least one j, then for any $0 < c < C_M(R,n)$ there is $v \in R^n$ and $k \in R$ such that

$$q(v) = kd, \ 0 < |k| \leq c^{\frac{-2}{n}} |f|. \tag{34}$$

b) If the norm is of q-type, there is $v \in R^n$ and $k \in R^\bullet$ such that

$$q(v) = kd, \ \deg k \leq \deg f + \frac{2(mn-1)}{n} - \frac{2c_M(R,n)}{n}.$$

Proof. By Theorem 7.1 there is an integral lattice Λ_d with $\operatorname{Covol} \Lambda_d = |d|^{\frac{n}{2}}$ and such that $q(v) \equiv 0 \pmod{d}$ for all $v \in \Lambda_d$.
a) Suppose that $|\cdot|_j$ is Archimedean for $1 \leq j \leq m'$ and ultrametric for $m' < j \leq m$. For all $1 \leq i \leq n, \ 1 \leq j \leq m'$, take

$$\epsilon_{i,j} = \epsilon = c^{\frac{-1}{m'n}} |d|^{\frac{1}{2m'}}.$$

For all $1 \leq i \leq n, \ m' < j \leq m$, take

$$\epsilon_{i,j} = 1.$$

Then $\operatorname{Covol} \Lambda_d \leq c \prod_{i,j} \epsilon_{i,j}$, so there is $v = (v_1, \ldots, v_n) \in \Lambda_d^\bullet$ with $|v_i|_j \leq c^{\frac{-1}{m'n}} |d|^{\frac{1}{2m'}}$ for all $1 \leq i \leq n$, $1 \leq j \leq m'$ and $|v_i|_j \leq 1$ for all $1 \leq i \leq n$, $m' < j \leq m$. Then

$$|f(v)| = |\sum_{i,k} a_{ik} v_i v_k| = \prod_{j=1}^m |\sum_{i,k} a_{ik} v_i v_k|_j \leq \prod_{j=1}^{m'} \sum_{i,k} |a_{ik} v_i v_k|_j \prod_{j=m'+1}^m \max_{ik} |a_{ik} v_i v_k|_j$$

$$\leq \epsilon^{2m'} \prod_{j=1}^{m'} \sum_{i,k} |a_{ik}|_j \prod_{j=m'+1}^m \max_{ik} |a_{ik}|_j = \epsilon^{2m'} |f| = c^{\frac{-2}{n}} |d| |f|.$$

Writing $f(v) = kd$ and using $|f(v)| = |k||d|$, we get

$$|k| \leq c^{\frac{-2}{n}} |f|.$$

b) For all $1 \leq i \leq n, \ 1 \leq j \leq m$ we take

$$e_{ij} = e = \lceil \frac{\frac{n}{2} \deg d - c_M(R,n)}{mn} \rceil.$$

Then $\operatorname{covol}\Lambda_d = \frac{n}{2}\deg d \leq c_M(R,n) + \sum_{i,j} e_{ij}$, so there is $v = (v_1, \ldots, v_n) \in \Lambda_d^\bullet$ such that

$$\forall 1 \leq i \leq n,\ 1 \leq j \leq m,\ \deg_j v_i \leq \lceil \frac{\frac{n}{2}\deg d - c_M(R,n)}{mn} \rceil$$
$$\leq \frac{\frac{n}{2}\deg d - c_M(R,n)}{mn} + \frac{mn-1}{mn}.$$

Then

$$\deg f(v) = \sum_{j=1}^m \deg_j f(v) = \sum_{j=1}^m \deg_j \sum_{ik} a_{ik} v_i v_k$$
$$\leq \sum_{j=1}^m \max_{ik}(\deg_j a_{ik} + \deg_j v_i + \deg_j v_k) \leq \sum_{j=1}^m \max_{ik}(\deg_j a_{ik} + 2e)$$
$$= \deg f + 2me \leq \deg f + \frac{2(mn-1)}{n} - \frac{2c_M(R,n)}{n} + \deg d.$$

Writing $f(v) = kd$ for $k \neq 0$ and using $\deg f(v) = \deg k + \deg d$, we get

$$\deg k \leq \deg f + \frac{2(mn-1)}{n} - \frac{2c_M(R,n)}{n}.$$

□

Theorem 7.3. *Let* $f = \sum_{i,j} a_{ij} t_i t_j \in \mathbb{Z}[t_1, \ldots, t_n]$ *be an anisotropic quadratic form. Let* $d \in \mathbb{Z}^\bullet$ *be an odd integer coprime to* $\operatorname{disc} f$ *and such that the base change of* f *to* $\mathbb{Z}/d\mathbb{Z}$ *is hyperbolic. Then there is* $v \in \mathbb{Z}^n$ *such that*

$$f(v) = kd,\ 0 < |k| < |f|. \tag{35}$$

Proof. Using $C(\mathbb{Z}, n) = 1$ for all n and a simple limiting argument we get (35) with "$\leq$". Using instead the sharper Theorem 3.3 one extracts a strict inequality. □

See [Mo66] for the use of Theorem 7.3 to prove representation theorems for binary integral quadratic forms. Here we content ourselves with one classical case.

Example 7.4. *(Brauer-Reynolds* [BR51]*): Let* $f = x^2 + y^2 + z^2 + w^2$ *over* $\mathbb{Z}$*. For every odd positive integer* d*, there is* $v \in \mathbb{Z}^4$ *with* $f(v) = kd$*,* $0 < k < 4$*. We can deduce Lagrange's Theorem that* q *represents all positive integers. Indeed, since* $f(\mathbb{Z}^4)$ *is closed under multiplication and certainly contains* 1 *and* 2*, it suffices to show that* f *represents every odd prime* p*. We know that there is* v *with*

$$x^2 + y^2 + z^2 + w^2 = p \tag{36}$$

or

$$x^2 + y^2 + z^2 + w^2 = 2p \tag{37}$$

or

$$x^2 + y^2 + z^2 + w^2 = 3p. \tag{38}$$

If (36) holds, we're done. If (37) holds, parity considerations show: after reordering the variables we may assume $x \equiv y \pmod 2$ *and* $z \equiv w \pmod 2$ *and then*

$$p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2.$$

If (38) holds, then one of x, y, z, w – say x – must be divisible by 3*; replacing y, z, w with their negatives if necessary we may assume $y \equiv z \equiv w \pmod 3$, and then*

$$p = \left(\frac{y+z+w}{3}\right)^2 + \left(\frac{x+z-w}{3}\right)^2 + \left(\frac{x-y+w}{3}\right)^2 + \left(\frac{x+y-z}{3}\right)^2.$$

Theorem 7.5. *Let k be a field and C/k be a smooth, geometrically integral projective curve of genus g, and let $C^\circ = C \setminus \{\infty_1, \ldots, \infty_m\}$ be the affine curve obtained by removing the given m closed points, of degrees $d_1, \ldots, d_m$. Let $R = k[C^\circ]$. Let $f \in R[t_1, \ldots, t_n]$ be an anisotropic quadratic form. Let $d \in R^\bullet$ be odd and coprime to* $\operatorname{disc} f$ *and such that the base change of f to R/dR is hyperbolic. Then there is $v \in R^n$ such that*

$$f(v) = kd,\ 0 \leq \deg k \leq \deg f + 2\left(\sum_{j=1}^{m} d_j + g - 1\right). \tag{39}$$

Proof. Apply Theorems 4.6 and 7.2. □

References

[A] E. Artin, *Algebraic numbers and algebraic functions.* Gordon and Breach Science Publishers, New York-London-Paris 1967.

[BR51] A. Brauer and R.L. Reynolds, *On a theorem of Aubry-Thue.* Canadian J. Math. 3 (1951), 367-374.

[BW66] H.S. Butts and L.I. Wade, *Two criteria for Dedekind domains.* Amer. Math. Monthly 73 (1966), 14–21.

[C] J.W.S. Cassels, *An introduction to the geometry of numbers.* Corrected reprint of the 1971 edition. Classics in Mathematics. Springer-Verlag, Berlin, 1997.

[Ca55] J.W.S. Cassels, *Bounds for the least solutions of homogeneous quadratic equations.* Proc. Cambridge Philos. Soc. 51 (1955), 262-264.

[Ch12] Z. Chonoles, *Hermite's Theorem for Function Fields.* Honors Thesis, Brown University, 2012.

[CF] Algebraic number theory. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich Academic Press, London; Thompson Book Co., Inc., Washington, D.C. 1967.

[CL] J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962.

[CL70] K.L. Chew and S. Lawn, *Residually finite rings.* Canad. J. Math. 22 1970 92–101.

[Cl12] P.L. Clark, *Euclidean Quadratic Forms and ADC-forms I.* Acta Arithmetica 154 (2012), 137–159.

[Co] B. Conrad, *The Lattice of S-Integers.* `http://math.stanford.edu/~conrad/249BPage/handouts/Sintlattice.pdf`

[GoN1] P.L. Clark, J. Hicks, H. Parshall and K. Thompson, *GoNI: Primes represented by binary quadratic forms.* . INTEGERS 13 (2013), A37, 18 pp.

[GoN2] P.L. Clark, J. Hicks, K. Thompson and N. Walters, *GoNII: Universal quaternary quadratic forms.* INTEGERS 12 (2012), A50, 16 pp.

[GoN3] J. Hicks and K. Thompson, *GoNIII: More universal quaternary forms*, preprint.

[Ku] F.-V. Kuhlmann, *The defect.* Commutative algebra–Noetherian and non-Noetherian perspectives, 277-318, Springer, New York, 2011.

[L] S. Lang, *Algebraic Number Theory.* Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[LM] M.D. Larsen and P.J. McCarthy, *Multiplicative theory of ideals.* Pure and Applied Mathematics, Vol. 43. Academic Press, New York-London, 1971.

[LM72] K.B. Levitz and J.L. Mott, *Rings with finite norm property.* Canad. J. Math. 24 (1972), 557–565.

[M] H. Matsumura, *Commutative ring theory.* Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

[Ma41] K. Mahler, *An analogue to Minkowski's geometry of numbers in a field of series.* Ann. of Math. (2) 42, (1941), 488-522.

[Mo51] L.J. Mordell, *On the equation* $ax^2+by^2-cz^2=0$. Monatsh. Math. 55 (1951), 323-327.

[Mo66] L.J. Mordell, *Solvability of the equation* $ax^2+by^2=p$. J. London Math. Soc. 41 (1966), 517-522.

[Pf97] A. Pfister, *Small zeros of quadratic forms over algebraic function fields.* Acta Arith. 79 (1997), 221-238.

[Pr87] A. Prestel, *On the size of zeros of quadratic forms over rational function fields.* J. Reine Angew. Math. 378 (1987), 101-112.

[Ra75] S. Raghavan, *Bounds for minimal solutions of Diophantine equations.* Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II 1975, no. 9, 109-114.

[S] P. Samuel, *Théorie algébrique des nombres.* Hermann, Paris 1967.

[Sc] W. Scharlau, *Quadratic and Hermitian forms.* Grundlehren der Mathematischen Wissenschaften 270. Springer-Verlag, Berlin, 1985.

[SK68] H. Stevens and L. Kuty, *Applications of an elementary theorem to number theory.* Arch. Math. (Basel) 19 (1968), 37-42.

[Th02] A. Thue, *Et par antydninger ti1 en taltheoretisk metode*, Kra. Vidensk. Selsk. Forh. 7 (1902), 57-75.

[To41] L. Tornheim, *Linear forms in function fields.* Bull. Amer. Math. Soc. 47 (1941), 126-127.

[Vi27] I.M. Vinogradov, *On a general theorem concerning the distribution of the residues and non-residues of powers.* Trans. Amer. Math. Soc. 29 (1927), 209–17.

Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602-7403, USA

E-mail address: `pete@math.uga.edu`