GEOMETRY OF NUMBERS EXPLAINED

PETE L. CLARK

Contents

1. Introduction

Despite the pretentious working title, our aspiration here is *not* to explain the Geometry of Numbers (GoN) but rather how to apply GoN techniques and results to prove representation theorems for quadratic forms, and to do so in a rather general algebraic context.

2. $\mathcal{G}$-Lattices

An ideal I in a ring R is **odd** if it is coprime to $2R$.

Theorem 1. *Let $(R, |\ |)$ be a normed 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 suppose:*
- *The base change of q to K is similar to a Pfister form.*
- *The base change of q to R/I is isotropic.*

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 $\chi(R^n/\Lambda_I) = I^{\frac{n}{2}}$.

(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.

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 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 $R^n/\Lambda_I \cong (R/I)^{\frac{n}{2}}$. □

Remark 2.1: a) Let $q = q(x_1, \ldots, x_n)$ be a Pfister form over a field K. Then: (i) q must be **principal**, i.e., must K-represent 1; and n must be a power of 2. Observe that every nondegenerate form is similar to a principal form: if q K-represents $a \in K^\times$, then $\frac{1}{a}q$ is principal.
b) The hypotheses exclude the (trivial) $n = 1$ case: the base change of q to $R/(m)$ is assumed to be isotropic and (since m is prime to $\operatorname{disc} q$) nondegenerate, and this requires at least two variables.
c) A nondegenerate binary quadratic form over K is a Pfister form iff it K-represents 1. Thus *every* nondegenerate binary form is similar to a Pfister form.
c) A nondegenerate quaternary form is similar to a Pfister form iff its discriminant is 1. Indeed, by rescaling we may assume q K-represents 1 and thus we have a diagonalization $q \cong \langle 1, a, b, c \rangle$. Setting $abc = \operatorname{disc} q = 1$, we find that as square classes in k, $c \cong ab$ and thus $q \cong \langle 1, a, b, ab \rangle$.
d) As k increases, the Pfister forms become sparser among all nondegenerate (2^k)-ary quadratic forms. There are many beautiful characterization theorems for Pfister forms – for instance, a form is a Pfister form iff the base change to its generic splitting field is hyperbolic – but, so far as I know, starting with $k = 3$ there is no concrete description of k-fold Pfister forms which is any simpler than the definition:

$$q \cong \bigotimes_{i=1}^{k} \langle 1, a_i \rangle.$$

3. Normed Domains

Now we give the formalism of elementwise norms and ideal norms on an integral domain R. This material was first introduced in [FID] and then used in [ADCI].

The first four subsections are reproduced verbatim from [ADCI]; the last two subsections are "new", although in truth they seem rather routine.

3.1. **Elementwise Norms.**

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

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.

Let R be a domain with fraction field K. We say that two norms $|\cdot|_1, \cdot|\cdot|_2$ on R are **equivalent** – and write $|\cdot|_1 \sim |\cdot|_2$ if for all $x \in K$, $|x|_1 < 1 \iff |x|_2 < 1$.

Remark 3.1: Let $(R, |\cdot|)$ be a normed domain with fraction field K. By (N1) and (N2), $|\cdot| : (R^\bullet, \cdot) \to (\mathbb{Z}^+, \cdot)$ is a homomorphism of commutative monoids. It therefore extends uniquely to a homomorphism on the group completions, i.e., $|\cdot| : K^\times \to \mathbb{Q}^{>0}$ via $|\frac{x}{y}| = \frac{|x|}{|y|}$. This map factors through the **group of divisibility** $G(R) = K^\times/R^\times$ to give a map $K^\times/R^\times \to \mathbb{Q}^{>0}$.

Example 3.2: The usual absolute value $|\cdot|_\infty$ on $\mathbb{Z}$ (inherited from $\mathbb{R}$) is a norm.

Example 3.3: Let k be a field, $R = k[t]$, and let $a \geq 2$ be an integer. Then the map $f \in k[t]^\bullet \mapsto a^{\deg f}$ is a non-Archimedean norm $|\cdot|_a$ on R and the norms obtained for various choices of a are equivalent. As we shall see, when k is finite, the most natural normalization is $a = \#k$. Otherwise, we may as well take $a = 2$.

Example 3.4: Let R be a discrete valuation ring (DVR) with valuation $v : K^\times \to \mathbb{Z}$ and residue field k. For any integer $a \geq 2$, we may define a norm on R, $|\cdot|_a : R^\bullet \to \mathbb{Z}^{>0}$ by $x \mapsto a^{v(x)}$. (Note that these are the *reciprocals* of the norms $x \mapsto a^{-v(x)}$ attached to R in valuation theory.) Using the fact that $G(R) = K^\times/R^\times \cong (\mathbb{Z}, +)$ one sees that these are all the norms on R. That is, a DVR admits a unique norm up to equivalence.

Example 3.5: Let R be a UFD. Then $\mathrm{Prin}(R)$ is a free commutative monoid on the set Σ_R of height one primes of R [B-CA, VII.3.2]. Thus, to give a norm map on R it is necessary and sufficient to map each prime element π to an integer $n_\pi \geq 2$ in such a way that if $(\pi) = (\pi')$, $n_\pi = n_{\pi'}$.

3.2. **Ideal norms.**

For a domain R, let $\mathcal{I}^+(R)$ be the monoid of nonzero ideals of R under multiplication and $\mathcal{I}(R)$ be the monoid of nonzero fractional R-ideals under multiplication.

An **ideal norm** on R is a nondegenerate homomorphism of monoids $|\cdot| : \mathcal{I}^+(R) \to (\mathbb{Z}^{>0}, \cdot)$. We extend the norm to the zero ideal by putting $|(0)| = 0$. In plainer language, to each nonzero ideal I we assign a positive integer $|I|$, such that $|I| = 1 \iff I = R$ and $|IJ| = |I||J|$ for all ideals I and J.

3.3. **Finite Quotient Domains.**

A commutative ring R has the property of **finite quotients** (FQ) if for all nonzero ideals I of R, the ring R/I is finite [BW], [CL70], [LeMo].

Obviously any finite ring satisfies (FQ). On the other hand, it can be shown that any infinite ring satisfying property (FQ) is necessarily a domain. We define an **finite quotient domain** to be an infinite integral domain satisfying (FQ) which is not a field. A finite quotient domain is a Noetherian domain of Krull dimension one, hence it is a Dedekind domain iff it is integrally closed.

Example 3.6: The rings $\mathbb{Z}$ and $\mathbb{F}_p[t]$ are finite quotient domains. From these many other examples may be derived using the following result.

Proposition 2. *Let R be a finite quotient 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, if not a field, S is a finite quotient domain.
b) The integral closure $\tilde{R}$ of R in K is a finite quotient domain.
c) The completion of R at a maximal ideal is a finite quotient domain.

Proof. Part a) is [LeMo, Thm. 2.3]. In particular, it follows from part a) that $\tilde{R}$ is a finite quotient 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 finite quotient 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 3. *Let I and J be nonzero ideals of the finite quotient 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

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

To see this, let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a primary decomposition of I, with $\mathfrak{p}_i = \mathrm{rad}(\mathfrak{q}_i)$. 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 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

$$\frac{R}{J} \xrightarrow{\cdot x} \frac{xR}{xJ}$$

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

In all of our applications, R is either an S-integer ring in a global field or a completion of such at a height one prime. By the results of this section, the map $I \mapsto |I| = \#R/I$ is an ideal norm on these rings. We will call this norm **canonical**. We ask the reader to verify that the norm of Example 1.1 is canonical, as are the norms $|\cdot|_{\#k}$ of Examples 1.2 and 1.3 when the field k is finite.

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

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

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

Remark 3.7: As above, 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, $|I|_W \leq |I|$.

Theorem 4. *Let R be a Dedekind domain with fraction field K, $|\cdot|$ an ideal norm on R, $W \subset \Sigma_R$ and $R_W = \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}$ the corresponding overring. Let $q(x) \in R[x]$ be a quadratic form, and suppose that $E \in \mathbb{R}^{>0}$ is a constant such that for all $x \in K^n$, there exists $y \in R^n$ such that $|q(x-y)| \leq E$. Then for all $x \in K^n$, there exists $y_W \in R_W^n$ such that $|q(x - y_W)|_W \leq E$.*

3.5. **Extended Norms.**

Suppose $|\cdot|$ is a norm on the integrally closed domain R with fraction field K. Let L/K be a finite field extension, and let S be the integral closure of R in L. Let $N_{L/K} : L \to K$ be the norm map in the sense of field theory. Since R is integrally closed, $N_{L/K}(S) \subset R$. Consider the composite map

$$|\cdot|_S = |\cdot| \circ N_{L/K} : S \to \mathbb{N}.$$

Proposition 5. *a) The map $|\cdot|_S : S \to \mathbb{N}$ is a norm function on S.*
b) If R is a Dedekind domain and $|\cdot|$ is an ideal norm on S, then S is a Dedekind domain and $|\cdot|_S$ is an ideal norm on S.

c) If R is a finite-quotient domain with canonical norm $|\ |$, then S is a finite-quotient domain and $|\ |_S$ is its canonical norm. Moreover, since R is assumed to be integrally closed, it is a Dedekind domain and thus so is S, and the canonical norms $|\cdot|$ and $|\cdot|_S$ are ideal norms.

The proof is straightforward and left to the reader.

3.6. **Finite Length Modules, Lattices and Covolumes.**

Let R be a Dedekind domain with fraction field K. Recall that a finitely generated R-module is projective iff it is torsionfree [CA, Thm. 451].

Let M be a finite length R-module: that is, M admits a composition series

$$0 = M_0 \subset M_1 \subset \ldots \subset M_N = M$$

with successive quotients M_{i+1}/M_i simple R-modules. The simple R-module M_i/M_{i-1} is isomorphic to $R/\mathfrak{p}_i$ for a unique nonzero prime ideal $\mathfrak{p}_i$ of R. Following Serre, we define the ideal $\chi(M) = \prod_{i=1}^N \mathfrak{p}_i$: note that the Jordan-Hölder Theorem ensures that $\chi(M)$ is is independent of the choice of composition series. Note that the length of M and $\chi(M)$ can be computed locally.

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.

If $\Lambda_1 \subset \Lambda_2 \subset K^n$ are two R-lattices, then Λ_2/Λ_1 is a finite length R-module, so $\chi(\Lambda_2/\Lambda_1)$ is defined. But moreover, observe that *any* two R-lattices $\Lambda_1, \Lambda_2 \subset K^n$ are **commensurable** in the sense that there exists $a \in R^\bullet$ such that $a\Lambda_1 \subset \Lambda_2$. Thus we may define $\chi(\Lambda_1/\Lambda_2)$ to be the fractional R-ideal $\chi(\Lambda_2/a\Lambda_1)a^{-1}$; it is easy to check that this is independent of the choice of a (c.f. [CL, § III.1]).

Now let $|\cdot|$ be an ideal norm on R. For a finite length R-module M we define

$$|M| = |\chi(M)|,$$

and for any R-lattice $\Lambda \subset K^n$ we define its **covolume**

$$\operatorname{Covol} \Lambda = |\chi(R^n/\Lambda)|.$$

4. Hermite Constants

4.1. **The Hermite Invariant of a Quadratic Form.**

Let R be a Dedekind domain of characteristic not 2, with fraction field K, and let $|\cdot|$ be an ideal norm on R. We use this structure to carry over one of the core notions from GoN to this abstract algebraic context, the **Hermite constant**.

For $n \in \mathbb{Z}^+$, let $Q_n(R)$ be the set of all nondegenerate n-ary quadratic forms $q(t) = q(t_1, \ldots, t_n) \in R[t] = R[t_1, \ldots, t_n]$.[1] Similarly define $Q_n(K)$ to be the nondegenerate n-ary quadratic forms with coefficients in the fraction field K.

[1]Identifying a quadratic form with its Hessian matrix, we may naturally view $Q_n(R)$ as a Zariski open subspace of affine $\frac{n(n+1)}{2}$-space over R. This pleasant geometric remark is doubtless useful for something, but we will not need it here.

For any $q \in Q_n(K)$, we define the **Hermite invariant**

$$\gamma(q) = \frac{\inf_{v \in (R^n)^\bullet} |q(v)|}{|\operatorname{disc} q|^{\frac{1}{n}}}.$$

Let $\mathcal{H}_n$ be the subgroup of $\mathrm{GL}_n(K)$ generated by $\mathrm{GL}_n(R)$ and the homotheties $K^\times$. Two quadratic forms $q_1, q_2 \in Q_n(K)$ are **H-equivalent** if there exists $m \in \mathcal{H}_n$ such that $q_2(t) = q_1(mt)$. It is immediate from the definition that H-equivalent forms have the same Hermite invariant.

We define the **n-dimensional Hermite constant**

$$\gamma_n(R) = \sup_{q \in Q(K,n)} \gamma(q).$$

Remark: $q \in Q_n(K)$ is isotropic iff $\gamma(q) = 0$. Thus in considerations involving Hermite constants $\gamma_n(R)$ we may always restrict to *anisotropic* forms.

It is natural and useful to make the following generalization: for any nonempty $\mathcal{S}_n \subset Q_n(K)$, put

$$\gamma(R, \mathcal{S}_n) = \sup_{q \in \mathcal{S}_n} \gamma(q).$$

In particular, let $Q_n(K)^+$ be the subset of **totally positive definite** forms, i.e., forms which are positive definite with respect to every ordering of K. Then we put

$$\gamma_n^+(R) = \gamma(R, Q_n(K)^+) = \sup_{q \in Q_n(K)^+} \frac{\inf_{v \in (R^n)^\bullet} |q(v)|}{|\operatorname{disc} q|^{\frac{1}{n}}}.$$

Example: The constant $\gamma_n^+(\mathbb{Z})$ is the Hermite constant that appears in the classical geometry of numbers and is often simply denoted by γ_n.

Notice that our definition allows $\gamma_n(R) = +\infty$. This motivates the following key definition: an ideal norm $|\ |$ on a Dedekind domain R is **of Hermite type** if for all $n \in \mathbb{Z}^+$, $\sup_n \gamma_n(R) < \infty$.

Even when $\gamma_n(R) = \infty$, there will be *some* subsets $\mathcal{S}_n \subset Q_n(K)$ for which $\gamma(R, \mathcal{S}_n)$ is finite – e.g., when $\mathcal{S}_n$ is finite! – so let us say that the norm $|\cdot|$ is $\mathcal{S}_n$-finite when $\gamma(R, \mathcal{S}_n) < \infty$.

It is convenient to be able to make K-linear changes of variables, so let us agree to only consider subsets $\mathcal{S}_n \subset Q_n(K)$ which are $\mathrm{GL}_n(K)$-**stable**, i.e., for $q(t) \in \mathcal{S}_n$ and $m \in \mathrm{GL}_n(K)$, $q(mt) \in \mathcal{S}_n$.

For $q \in Q_n(K)$ we may also define the **isotropic Hermite invariant**

$$\gamma_I(q) = \frac{\inf_{v \in R^n \ |\ q(v) \neq 0} |q(v)|}{|\operatorname{disc} q|^{\frac{1}{n}}}.$$

For anisotropic q, $\gamma_I(q) = \gamma(q)$; for q isotropic, $\gamma(q) = 0$ while $\gamma_I(q) \geq |\operatorname{disc} q|^{\frac{-1}{n}}$.

We may also define the **isotropic Hermite constant**

$$\gamma_{n,I}(R) = \sup_{q \in Q(K,n)} \gamma_I(q).$$

Example 4.1: Let $R = \mathbb{Z}$ and $q(x,y) = xy$. Then $\gamma_I(q) = 2$, so $\gamma_{2,I}(\mathbb{Z}) \geq 2$. In fact we have equality, as the following result of H. Blaney shows.

Theorem 6. *(Blaney* [Bl48]*) For all $n \in \mathbb{Z}^+$, we have $\gamma_{n,I}(\mathbb{Z}) \leq 2^{n-1}$.*

However we will not further consider the isotropic Hermite invariant here.

Conjecture 7. *Let R be a Dedekind domain and $|\cdot|$ a Hermite type norm on R.*
a) For $W \subset \operatorname{MaxSpec} R$, let $R_W = \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}$. Then the overring norm $|\cdot|_W$ on R_W is of Hermite type.
b) For L/K a finite field extension, let S be the integral closure of R in L. Then the extended norm $|\cdot|_S$ on S is of Hermite type.

Remark 4.2: Calling this a "conjecture" is premature: I haven't yet thought much about it or even tried to prove it (although somewhat similar results in the case of overring norms are given in [ADCI]). My feeling is rather that this is an appealingly clean, general result, so it would certainly be nice if it were true.

Moreover, using Theorems 15 and 17, we see that Conjecture 7 has the following appealing consequences.

Theorem 8. *If Conjecture 7 holds, then the canonical norm on a Hasse domain is of Hermite type.*

Remark 4.3: It seems very likely to me that the conclusion of Theorem 8 holds independently of Conjecture 7. In fact, I will be mildly surprised if Theorem 8 is not already known to the experts in this area. For instance it is known that for any totally real number field K and all $n \in \mathbb{Z}^+$, the positive Hermite constant $\gamma_n^+(\mathbb{Z}_F)$ is finite: this follows from a theorem of Icaza.

Theorem 9. *Let k be a field with* $\operatorname{char}(k) \neq 2$*, and let $C_{/k}$ be an integral, normal affine algebraic curve. If Conjecture 7 holds, then the coordinate ring $k[C]$ admits a norm of Hermite type.*

4.2. **Almost metric norms.**

A norm $|\cdot|$ on a ring R is **metric** if for all $x, y \in R$, $|x+y| \leq |x| + |y|$. A norm is **ultrametric** if for all $x, y \in R$, $|x+y| \leq \max |x|, |y|$.

Example 4.4: The standard norm (Euclidean absolute value) on $\mathbb{Z}$ is metric.

Example 4.5: For any field k and any $a \geq 2$, on the ring $R = k[t]$ the norm $f \in R \mapsto a^{\deg f}$ is ultrametric: indeed, for $f, g \in R$,

$$|f+g| = a^{\deg(f+g)} \leq a^{\max \deg f, \deg g} = \max a^{\deg f}, a^{\deg g} = \max |f|, |g|.$$

Nonexample: Let R be a discrete valuation ring which is not a field, with valuation $v : R^\bullet \to \mathbb{Z}$, $v(0) = -\infty$. Then for any $a \geq 2$ and $x \in R$, putting $|x| = a^{v(x)}$ gives a norm on R. But **beware**: this norm is *not* ultrametric nor even metric. Indeed, let π be a uniformizing element $x = \pi^2 - 1$, $y = 1$. Then

$$a^{v(x+y)} = a^{v(\pi^2)} = a^2 > 1 + 1 = a^{v(\pi^2-1)} + a^{v(1)}.$$

Notice in particular that our definition of the norm attached to a discrete valuation is *the reciprocal* of the usual definition, and thus the metric properties are lost.

In fact among all normed rings, examples of metric norms – and still more, ultrametric norms – seem to be quite rare. We get a slightly larger class of examples by relaxing the metric condition, as follows.
Let $|\cdot|$ be a norm on a ring R. Define

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

The following result connects some simple facts about these quantities.

Lemma 10. *a) If $A(R) < \infty$, then for all $x, y \in K$, $|x+y| \leq A(R)(|x|+|y|)$.*
b) If $C(R) < \infty$, then for all $x, y \in K$, $|x+y| \leq C(R)\max|x|, |y|)$.
c) We have $A(R) \leq C(R) \leq 2A(R)$.
d) In particular, $A(R) < \infty \iff C(R) < \infty$.

Proof. ... □

We call a norm **almost metric** if $A(R) < \infty$ (equivalently by Lemma 10, if $C(R) < \infty$). Note that a norm is metric if $A(R) \leq 2$ and ultrametric iff $C(R) = 1$.

Theorem 11. *Let K_0 denote either $\mathbb{Q}$ or $\mathbb{F}_p(t)$. Let K/K_0 be a finite separable extension of degree d. Let S be a finite, nonempty set of places of K containing all Archimedean places (if any), and let R be the ring of S-integers of K. TFAE:*
(i) $\#S = 1$. (ii) The unit group $R^\times$ is finite.
(iii) The canonical norm function $x \in R^\bullet \mapsto \#R/(x)$ is almost metric.
(iv) $C(R) = 2^d$.

Proof. ... □

Corollary 12. *Let R be an S-integer ring in a number field K.*
a) The canonical norm on R is almost metric iff
(i) $K = \mathbb{Q}$ and $R = \mathbb{Z}$, or
(ii) K is imaginary quadratic and $R = \mathbb{Z}_K$ is the full ring of integers.
b) In case (i) above, $C = 2$. In case (ii) above, $C = 4$.

4.3. **Euclidean norms.**

For a normed Dedekind domain $(R, |\cdot|)$, we define the **Euclideanity**

$$E(R) = \sup_{x \in K} \inf_{y \in R} |x - y|.$$

As usual, we say that $|\cdot|$ is a **Euclidean norm** on R if for all $x \in K$ there exists $y \in R$ with $|x-y| < 1$. Thus in particular R is Euclidean if $E(R) < 1$ and is not Euclidean if $E(R) > 1$. Because of the supremum in the definition of $E(R)$, the case $E(R) = 1$ is ambiguous: *a priori* it is possible for a ring with $E(R) = 1$ to be Euclidean, but in every example I know with $E(R) = 1$, the norm is *not* Euclidean. In any case, we really will want to use the stronger condition $E(R) < 1$ in our work below, so this distinction is not really relevant for us.

As is well-known, in a Euclidean ring every ideal is generated by each element of minimal norm, so a Euclidean ring is a PID.

Example 4.6: Let $R = \mathbb{Z}$ endowed with the standard absolute value. Then $E(R) = \frac{1}{2}$, so $\mathbb{Z}$ is Euclidean.

Example 4.7: Let k be any field, $R = k[t]$, and let $a \geq 2$ be an integer. Endow R with the nom $|f|_a = a^{\deg f}$. Then $E(R) = \frac{1}{a}$, so R is Euclidean.

Note that we may have $E(R) = \infty$; we say R is **E-finite** if $E(R) < \infty$.

Lemma 13. *Let R be a PID with fraction field K, and let $|\cdot|$ be a metric norm on R. Let L/K be a finite separable field extension, and let S be the integral closure of R in L, endowed with its extended norm. Then S is an E-finite Dedekind domain.*

Proof. Let $n = [L : K]$. It is a standard result in algebraic number theory that S is a Dedekind domain (this does not use the hypothesis of separability) and that $S \cong R^n$ (this does!). Let $\sigma_1, \ldots, \sigma_n : L \hookrightarrow \overline{K}$ be the n-distinct K-algebra embeddings into an algebraic closure, so for $x \in L$, $|x| = |\prod_{i=1}^n \sigma_i(x)|$. Let $x_1, \ldots, x_n$ be an R-basis for S, hence also a K-basis for L. Therefore, for any $x \in L$, there are unique $\alpha_1, \ldots, \alpha_n \in L$ such that $x = \sum_i \alpha_i x_i$. Fix $\epsilon > 0$, and choose for all i an element $\beta_i \in R$ such that $|\alpha_i - \beta_i| \leq E(R) + \epsilon$. Then

$$|x - \sum_{i=1}^n \beta_i x_i| \leq \sum_{i=1}^n |\alpha_i - \beta_i||x_i| \leq (E(R) + \epsilon) \sum_{i=1}^n |x_i|.$$

Thus S is E-finite. □

4.4. **An Abstract Hermite Theorem.**

Theorem 14. *Let $(R, |\cdot|)$ be an almost metric normed ring with $E(R) < 1$.*
a) Suppose $A(R)E(R)^2 < 1$. Then for all $n \geq 2$,

$$\gamma_n(R) \leq \left(\frac{A(R)}{1 - A(R)E(R)^2}\right)^{\frac{n-1}{2}}.$$

b) Suppose $C(R)E(R)^2 < 1$. Then for all $n \geq 2$,

$$\gamma_n(R) \leq C(R)^{\frac{n-1}{2}}.$$

c) If R is ultrametric, $\gamma_n(R) \leq 1$ for all $n \in \mathbb{Z}^+$.

Proof. The greater part of the argument involves deriving the inequality (1). Combining this with $|x + y| \leq A(R)(|x| + |y|)$ we deduce part a); combining it with $|x + y| \leq C(R) \max |x|, |y|$, we deduce part b).

Since $E(R) < 1$, R is Euclidean and thus a PID, so Hermite's Lemma applies. Let $q = \sum_{ij} a_{ij} t_i t_j : K^n \to K$ be an anisotropic quadratic form. By Hermite's Lemma, after making a unimodular change of variables we may assume that the minimum of q on R^n is attained at the first standard basis vector e_1.

Let $\varphi : K^n \to K^n$ be the K-linear map given by $e_1 \mapsto e_1' = e_1$, $e_j \mapsto e_j' = e_j - \frac{a_{1j}}{a_{11}}$ for $2 \leq j \leq n$, so e_1 is orthogonal to the subspace $\langle e_2', \ldots, e_n' \rangle$. Note also that $\det \varphi = 1$. Let

$$q'(t) = q(\varphi(t)) = a_{11} t_1^2 + q_2(t_2, \ldots, t_n).$$

Then $\operatorname{disc} q_2 = \frac{\operatorname{disc} q'}{a_{11}} = \frac{\operatorname{disc} q}{a_{11}}$. Now for $\lambda_1, \ldots, \lambda_n \in R$, write

$$w = (\lambda_1 + \frac{a_{12}}{a_{11}}\lambda_2 + \ldots + \frac{a_{1n}}{a_{11}}\lambda_n)e_1 + \lambda_2 e_2' + \ldots + \lambda_n e_n' = \gamma e_1 + z,$$

say. Suppose z is chosen so as to be minimal for q_2 on $\bigoplus_{i=2}^n Re_i'$. Then

$$|q(z)| = |q_2(\lambda_2, \ldots, \lambda_n)| \leq \gamma_{n-1}(R)|\operatorname{disc} q_2|^{\frac{1}{n-1}} = \gamma_{n-1}(R)|a_{11}|^{\frac{-1}{n-1}}|\operatorname{disc} q|^{\frac{1}{n-1}}.$$

Let $\epsilon > 0$ be small enough so that $E(R) + \epsilon < 1$. By definition of $E(R)$, there is $\lambda_1 \in R$ with $|\gamma| \leq E(R) + \epsilon < 1$. Thus we have

$$\min(q) = |a_{11}| \leq |q(w)| = |\gamma^2 a_{11} + q_2(\lambda_2, \ldots, \lambda_n)|. \tag{1}$$

a) By definition of $A(R)$, we have

$$|a_{11}| \leq |\gamma^2 a_{11} + q_2(\lambda_2, \ldots, \lambda_n)| \leq A(R)\left(|\gamma^2||a_{11}| + |q_2(\lambda_2, \ldots, \lambda_n)|\right)$$

$$\leq A(R)(E(R)+\epsilon)^2|a_{11}| + A(R)\gamma_{n-1}(R)|a_{11}|^{\frac{-1}{n-1}}|\operatorname{disc} q|^{\frac{1}{n-1}}.$$

Since this inequality holds for all sufficiently small ϵ, it also holds for $\epsilon = 0$:

$$|a_{11}| \leq A(R)E(R)^2|a_{11}| + A(R)\gamma_{n-1}(R)|a_{11}|^{\frac{-1}{n-1}}|\operatorname{disc} q|^{\frac{1}{n-1}}.$$

Multiplying through by $|a_{11}|^{\frac{1}{n-1}}$ gives

$$|a_{11}|^{\frac{n}{n-1}} \leq A(R)E(R)^2|a_{11}|^{\frac{n}{n-1}} + A(R)\gamma_{n-1}(R)|\operatorname{disc} q|^{\frac{1}{n-1}},$$

and thus

$$\frac{|a_{11}|^n}{|\operatorname{disc} q|} \leq \left(\frac{A(R)}{1 - A(R)E(R)^2}\right)^{n-1} \gamma_{n-1}(R)^{n-1}.$$

This implies

$$\gamma_n(R)^n \leq \left(\frac{A(R)}{1 - A(R)E(R)^2}\right)^{n-1} \gamma_{n-1}(R)^{n-1}$$

and thus

$$\gamma_n(R) \leq \left(\frac{A(R)}{1 - A(R)E(R)^2}\right)^{\frac{n-1}{n}} \gamma_{n-1}(R)^{\frac{n-1}{n}}.$$

Using $\gamma_1(R) = 1$, an easy induction argument gives

$$\gamma_n(R) \leq \left(\frac{1}{1 - A(R)E(R)^2}\right)^{\frac{n-1}{2}},$$

completing the proof of part a). As for part b), starting again from (1) we get

$$|a_{11}| \leq= |\gamma^2 a_{11} + q_2(\lambda_2, \ldots, \lambda_n)| \leq C(R)\max(|\gamma|^2|a_{11}|, |q_2(\lambda_2, \ldots, \lambda_n)|)$$

and thus (inserting and then removing an $\epsilon > 0$ as above) we get

$$|a_{11}| \leq C(R)\max(E(R)^2|a_{11}|, \gamma_{n-1}(R)|a_{11}|^{\frac{-1}{n-1}}|\operatorname{disc} q|^{\frac{1}{n-1}}).$$

But by our hypothesis, $|a_{11}| > C(R)E(R)^2|a_{11}|$, so we must have

$$|a_{11}| \leq C(R)\gamma_{n-1}(R)|a_{11}|^{\frac{-1}{n-1}}|\operatorname{disc} q|^{\frac{1}{n-1}}).$$

Thus

$$|a_{11}|^{\frac{n}{n-1}} \leq C(R)\gamma_{n-1}(R)|\operatorname{disc} q|^{\frac{1}{n-1}}$$

and hence

$$\frac{|a_{11}|^n}{|\operatorname{disc} q|} \leq C^{n-1}\gamma_{n-1}^{n-1}(R).$$

Taking nth roots gives

$$\gamma_n(R) \leq C^{\frac{n-1}{n}} \gamma_{n-1}^{\frac{n-1}{n}}.$$

Exactly as in part a), an easy induction argument gives $\gamma_n(R) \leq C^{\frac{n-1}{2}}$.
c) Since $|\cdot|$ is ultrametric iff $C(R) = 1$, this follows immediately from part b). □

Corollary 15. *(Hermite, 1850) For all $n \in \mathbb{Z}^+$, we have $\gamma_n(\mathbb{Z}) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}}$.*

Proof. Since $E(\mathbb{Z}) = \frac{1}{2}$, $A(\mathbb{Z}) = 1$, $A(\mathbb{Z})E(\mathbb{Z})^2 < 1$, and Theorem 14a) applies. □

Remark: Indeed $\gamma_2(\mathbb{Z}) = \frac{2}{\sqrt{3}}$, so the bound of Theorem 14a) can be attained.

Corollary 16. *Let $R = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ be the ring of integers of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-3})$. Then for all $n \in \mathbb{Z}^+$, we have*

$$\gamma_n(\mathbb{Z}) \leq \left(\frac{36}{5}\right)^{\frac{n-1}{2}}.$$

Proof. For the ring of integers $\mathbb{Z}_K$ of an imaginary quadratic field K we have

$$E(\mathbb{Z}_K) = \frac{|m|+1}{4},\ Z_K = \mathbb{Z}[\sqrt{-m}],$$

$$E(\mathbb{Z}_K) = \frac{(|m|+1)^2}{16m},\ \mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{-m}}{2}].$$

By Lemma 10 and Theorem 11, $A(R) \leq C(R) = 4$. Since $A(R)E(R)^2 < 1$, Theorem 14a) applies. □

Remark: Rather disappointingly, it turns out that $R = \mathbb{Z}$ and $R = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ are the only two S-integer rings to which the hypotheses of Theorem 14 apply!

Corollary 17. *(Gerstein* [Ge73]*, Quebbemann) Let k be a field of characteristic different from 2. Let $a \geq 2$ be an integer. Endow $R = k[t]$ with the norm $|f|_a = a^{\deg f}$. Then $\gamma_n(k[t]) \leq 1$ for all $n \in \mathbb{Z}^+$.*

Proof. Since $E(R) = \frac{1}{a}$, $C(R) = 1$, $C(R)E(\mathbb{R})^2 < 1$, and Theorem 14c) applies. □

Remark 4.8: A field k of characteristic not 2 admits an ordering iff for all $n \in \mathbb{Z}^+$ the quadratic form $q_n = \langle 1, \ldots, 1\rangle = t_1^2 + \ldots + t_n^2$ is anisotropic. Such a field k is necessarily infinite, and then an easy specialization argument shows that any anisotropic form q over k remains anisotropic upon base extension to $k[t]$. So let k be a field admitting an ordering – e.g. $k = \mathbb{R}$ or any of its subfields. Then for all $n \in \mathbb{Z}^+$, $|\operatorname{disc} q_n| = 1$ and $m(q_n) = 1$, so $\gamma(q_n) = 1$ and thus $\gamma_n(k[t]) = 1$. This shows that the bound of Corollary 17 is best possible without further restrictions on k. On the other hand, if $k = \mathbb{F}_q$ then every quadratic form in at least 5 variables over $k[t]$ is isotropic, and thus $\gamma_n(\mathbb{F}_q[t]) = 0$ for all $n \geq 5$.

Theorem 18. *(Samuel* [Sa71]*) Suppose that X is a curve of genus zero. Then $S = k[X]$ is Euclidean with respect to the extended norm iff the projective closure $\overline{X}$ of X is isomorphic to $\mathbb{P}^1$ and the gcd of the degrees of the points at infinity is 1.*

If $L \cong k(t)$ and $\overline{X} \setminus X$ contains a k-rational point then S is isomorphic to a localization of $k[t]$. And conversely: thus if for instance k admits a degree 2 and a degree 3 field extension, then we get an ultrametric Euclidean affine ring S which is not simply a localization of $k[t]$. For all such rings, Theorem 14c) applies: we get $\gamma_n(S) \leq 1$ for all $n \in \mathbb{Z}^+$.

4.5. **The Main Theorem.**

Theorem 19. *Let R be a Dedekind domain of characteristic different from 2, with fraction field K, and let $|\cdot|$ be a norm on R of Hermite type. Let $q(t) = q(t_1, \ldots, t_n) \in R[t]$ be an anisotropic quadratic form. Let d be an odd element of R coprime to $\operatorname{disc} q$. We suppose:*
• *$q_{/K}$ is similar to a Pfister form, and*
• *$q_{/R/(d)}$ is isotropic.*
Let $\mathcal{S}$ be any $\mathrm{GL}_n(K)$-stable subset of $Q(K, n)$ containing q.
Then for all $\epsilon > 0$, there exists $v \in (R^n)^\bullet$ and $k \in R$ such that

$$q(v) = kd,\ 0 < |k| \leq \gamma(\mathcal{S})|\operatorname{disc} q|^{\frac{1}{n}}.$$

Proof. ... □

Remark 4.13: Of course Theorem 19 becomes more or less useful according to how much one knows about Hermite constants over R. It has been stated in a form which gives a large degree of flexibility: for instance, over $\mathbb{Z}$ the known information about Hermite constants is quite different for definite forms versus indefinite forms, and the statement of Theorem 19 allows this to be taken into account.

Remark 4.14: Immediately from the definitions, for anisotropic q we have

$$\gamma(\mathcal{S})|\operatorname{disc}(q)|^{\frac{1}{n}} \geq 1.$$

On the other hand, it is natural to separate out three cases: if $\gamma(\mathcal{S})|\operatorname{disc} q|^{\frac{1}{n}} < 2$, we say $(q, \mathcal{S})$ is **subcritical**; if $\gamma(\mathcal{S})|\operatorname{disc} q|^{\frac{1}{n}} = 2$, we say $(q, \mathcal{S})$ is **critical**; and when $\gamma(\mathcal{S})|\operatorname{disc} q|^{\frac{1}{n}} > 2$, we say $(q, \mathcal{S})$ is **supercritical**. The subcritical case is the most auspicious for Diophantine applications. Indeed:

Corollary 20. *Let R be a Dedekind domain, with Hermite type ideal norm $|\cdot|$. Let $q(t) = q(t_1, \ldots, t_n) \in R[t]$ be an anisotropic quadratic form such that $q_{/K}$ is similar to a Pfister form. Let $\mathcal{S}$ is a $\mathrm{GL}_n(K)$-stable subset containing q such that $(q, \mathcal{S})$ is subcritical.*
a) Then for every odd element d of R coprime to $\operatorname{disc}(q)$ such that $q_{/R/(d)}$ is isotropic, q R-represents d up to a unit: there exists $v \in R^n$ and $u \in R^\times$ such that $q(v) = ud$.
b) Suppose R is a finite quotient domain. If $n = 2$, then $q_{/R/(d)}$ is isotropic iff $-\operatorname{disc}(q)$ is a square modulo d. If $n > 2$, then $q_{R/(d)}$ is always isotropic.

4.6. **Hermite Constants Over Totally Real Number Rings.**

Let K be a totally real number field, and let $R = \mathbb{Z}_K$ be its ring of integers, endowed with the canonical norm. Let $q(t)_{/R}$ be a totally definite quadratic form. In this case it is easy to see that $q(v)$ actually achieves a *minimum* on $(R^n)^\bullet$, so the ϵ in Theorem 19 may be removed.

Here we present some results – entirely due to other people! – on the positive Hermite constants $\gamma_n^+(\mathbb{Z}_K)$.

Theorem 21. *(Icaza* [Ic97]*) Let K be a totally real number field of degree m, and with discriminant Δ_K. Let $\mathbb{Z}_K$ be the ring of integers of K. For all $n \in \mathbb{Z}^+$,*

$$\gamma_n^+(\mathbb{Z}_K) \leq 4^m V_n^{\frac{-2m}{n}} |\Delta_K|,$$

where V_n is the volume of the unit ball in Euclidean n-space.

Remark 4.15: In fact Icaza proves a result about Hermite constants for an arbitrary number field K, but when K has complex places her definition of the Hermite constant is different from ours.

Theorem 22. *(*[BCIO01, Thms. 3.2, 3.4, 3.6]*)*
a) For $K = \mathbb{Q}(\sqrt{2})$, we have

$$\gamma_2^+(\mathbb{Z}_K) = \frac{4}{2\sqrt{6}-3} = 2.1063945\ldots.$$

b) For $K = \mathbb{Q}(\sqrt{3})$, we have

$$\gamma_2^+(\mathbb{Z}_K) = 4.$$

c) For $K = \mathbb{Q}(\sqrt{5})$, we have

$$\gamma_2^+(\mathbb{Z}_K) = \frac{4}{\sqrt{5}} = 1.78885438\ldots.$$

Theorem 23. *(Pohst-Wagner* [PW09]*)*
a) For $K = \mathbb{Q}(\sqrt{6})$, we have

$$\gamma_2^+(\mathbb{Z}_K) = 5.$$

b) For $K = \mathbb{Q}(\sqrt{13})$, we have

$$\gamma_2^+(\mathbb{Z}_K) = \sqrt{\frac{1476 + 144\sqrt{91}}{175}} = 4.0353\ldots$$

c) For $K = \mathbb{Q}(\sqrt{21})$, we have

$$\gamma_2^+(\mathbb{Z}_K) = \frac{16}{3}.$$

Theorem 24. *Let $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}] = \mathbb{Z}_{\mathbb{Q}(\sqrt{5})}$, a PID. Let ρ be an odd prime element of R which is prime to 5.*
a) The following are equivalent:
(i) $\left(\frac{-1}{\rho}\right) = 1$, i.e., -1 is a nonzero square in $R/(\rho)$.
(ii) There exist $x, y \in R$ and $u \in R^\times$ such that $x^2 + y^2 = u\rho$.
b) The following are equivalent:
(i) $\left(\frac{-3}{\rho}\right) = 1$, i.e., -3 is a nonzero square in $R/(\rho)$.
(ii) There exist $x, y \in R$ and $u \in R^\times$ such that $x^2 + xy + y^2 = u\rho$.

Proof. ... □

Remark 4.16: The implication (i) $\implies$ (ii) of Theorem 24 is proved in [De02] by "pushing down to $\mathbb{Z}$" and applying the Convex Body Theorem. Having Theorem 22c) at our disposal enabled us to give a morally similar, but much quicker, proof.

Theorem 25. *Let $R = \mathbb{Z}[\sqrt{3}] = Z_{\mathbb{Q}(\sqrt{3})}$, a PID. Let ρ be an odd prime element of R which is prime to 3. TFAE:*
(i) $\left(\frac{-3}{\rho}\right) = 1$, i.e., -3 is a nonzero square in $R/(\rho)$.
(ii) There exist $x, y \in R$ and $u \in R^\times$ such that $x^2 + xy + y^2 = u\rho$.

5. Linear Forms, Vinogradov's Lemma and Brauer-Reynolds

There are contexts in which one can prove results qualitatively similar to Theorem 19 but with the Hermite constant input replaced by information about *systems of linear forms*. For instance, successful applications of linear forms techniques to the representation of integers by quadratic forms over $\mathbb{Z}$ appear in [BrRe51], [Mo66], [GoN0]. As usual, we wish to abstract and (if possible) extend these classical results so as to hold over a suitable class of normed rings.

The results in this section are especially preliminary. In particular, a paper of T. Cochrane [Co87] is highly relevant and useful to this goal, but we have not yet had the chance to absorb and include his results here.

References

[ADCI] P.L. Clark, *Euclidean Quadratic Forms and ADC-forms I.* To appear in *Acta Arith.* Preprint available at `http://math.uga.edu/ pete/ADCForms1.pdf`.

[AM] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading Mass.-London-Don Mills, Ont. 1969.

[B-CA] N. Bourbaki, *Commutative algebra. Chapters 17.* Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998.

[BCIO01] R. Baeza, R. Coulangeon, M. Icaza and M. O'Ryan, *Hermite's constant for quadratic number fields*. Experiment. Math. 10 (2001), 543-551.

[BaIc97] R. Baeza and M.I. Icaza, *On Humbert-Minkowski's constant for a number field*. Proc. Amer. Math. Soc. 125 (1997), 195-3202.

[Bl48] H. Blaney, *Indefinite quadratic forms in n variables*. J. London Math. Soc. 23 (1948), 153-160.

[BrRe51] A. Brauer and R.L. Reynolds, *On a theorem of Aubry-Thue*. Canadian J. Math. 3 (1951), 367-374.

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

[CA] P.L. Clark, *Commutative algebra*, `http://math.uga.edu/∼pete/integral.pdf`.

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

[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.

[ClLF1] P.L. Clark, *Lecture notes on valuation theory.* Availabe at `http://math.uga.edu/∼pete/8410Chapter1.pdf`

[Cl11] P.L. Clark, *Thue-Vinogradov and integers of the form $x^2 + Dy^2$*, submitted.

[Co87] T. Cochrane, *Small solutions of congruences over algebraic number fields*. Illinois J. Math. 31 (1987), 618-625.

[Coh] H. Cohen, *A course in computational algebraic number theory*. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[Con] J. H. Conway, *The sensual (quadratic) form*, Carus Math. Monographs 26, 1997.

[De02] J.I. Deutsch, *Geometry of numbers proof of Götzky's four-squares theorem*. J. Number Theory 96 (2002), 417-431.

[FID] P.L. Clark, *Factorization in integral domains*, 2010 preprint.

[Ge73] L.J. Gerstein, *A new proof of a theorem of Cassels and Pfister*. Proc. Amer. Math. Soc. 41 (1973), 327-328.

[Ge79] L.J. Gerstein, *Unimodular quadratic forms over global function fields*. J. Number Theory 11 (1979), 529–541.

[Ge03] L.J. Gerstein, *Definite quadratic forms over $\mathbb{F}_q[t]$*. J. Algebra 268 (2003), 252-263.

[GoN0] P.L. Clark, *Thue-Vinogradov and Idoneal Quadratic Forms*, submitted for publication.

[GoN1] P.L. Clark and H. Parshall, *GoNI: Primes represented by binary quadratic forms*, in preparation.

[GoN2] P.L. Clark, J. Hicks, K. Thompson and N. Walters, *GoNII: Universal quaternary quadratic forms*, submitted for publication.

[Ic97] M.I. Icaza, *Hermite constant and extreme forms for algebraic number fields*. J. London Math. Soc. (2) 55 (1997), 11-22.

[IR] K. Ireland and M. Rosen, *A classical introduction to modern number theory*. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[L] T.Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

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

[Le95] F. Lemmermeyer, *The Euclidean Algorithm in Algebraic Number Fields*. Exposition. Math. 13 (1995), 385-416.

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

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

[PW09] M.E. Pohst and M. Wagner, *On the computation of Hermite-Humbert constants: the algorithm of Cohn revisited*. J. Algebra 322 (2009), 936-947.

[Sa71] P. Samuel, *About Euclidean rings*. J. Algebra 19 (1971), 282-301.

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

[Si] C.L. Siegel, *Lectures on the geometry of numbers*. Springer-Verlag, Berlin, 1989.