EUCLIDEAN QUADRATIC FORMS AND ADC-FORMS: I

PETE L. CLARK

Contents

Partially supported by National Science Foundation grant DMS-0701771.

Notation: Throughout this article R denotes a commutative, unital integral domain and K its fraction field. We write $R^\bullet$ for $R \setminus \{0\}$ and Σ_R for the set of height one prime ideals of R. R is **dyadic** if it possesses a prime ideal $\mathfrak{p}$ such that $R/\mathfrak{p}$ has characteristic 2 and is otherwise **nondyadic**.

Introduction

The goal of this work is to set up the foundations and begin the systematic arithmetic study of certain classes of (mostly) quadratic forms over a fairly general class of integral domains. Much of our work is concentrated around that of two definitions, that of **Euclidean form** and **ADC form**.

These definitions have a classical flavor, and various special cases of them can be found (sometimes implicitly) in the literature. Our work was particularly motivated by the similarities between two classical theorems.

Theorem 1. *(Aubry, Davenport-Cassels) Let $A = (a_{ij})$ be a symmetric $n \times n$ matrix with $\mathbb{Z}$ coefficients, and let $q(x) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$ be a positive definite integral quadratic form. Suppose that for all $x \in \mathbb{Q}^n$, there exists $y \in \mathbb{Z}^n$ such that $q(x-y) < 1$. Then if $d \in \mathbb{Z}$ is such that there exists $x \in \mathbb{Q}^n$ with $q(x) = d$, there exists $y \in \mathbb{Z}^n$ such that $q(y) = d$.*

Let us consider the form $q(x) = x_1^2 + x_2^2 + x_3^2$. It satisfies the hypotheses of the theorem: approximating a vector $x \in \mathbb{Q}^3$ by a vector $y \in \mathbb{Z}^3$ of nearest integer entries, we get

$$(x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2 \le \frac{3}{4} < 1.$$

Thus Theorem 1 shows that every integer which is the sum of three *rational* squares is also the sum of three *integral* squares. Thanks to the Hasse-Minkowski theory the rational representation problem is routine: a rational number d is $\mathbb{Q}$-represented by q iff it is $\mathbb{R}$-represented by q and $\mathbb{Q}_p$-represented by q for all primes p. Of course q $\mathbb{R}$-represents precisely the non-negative rational numbers. For odd p the quadratic form is smooth over $\mathbb{Z}_p$ and hence isotropic: it $\mathbb{Q}_p$-represents all rational numbers. Finally, for $a \in \mathbb{N}$ there are no primitive $\mathbb{Z}_2$-adic representations of $4^a \cdot 7$, so q does not $\mathbb{Q}_2$-adically represent 7, whereas the other 7 classes in $\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2}$ are all $\mathbb{Q}_2$-represented by q. We conclude:

Corollary 2. *(Gauss-Legendre Three Squares Theorem) An integer n is a sum of three integer squares iff $n \ge 0$ and n is* not *of the form $4^a(8k+7)$.*

One may similarly derive Fermat's Theorem on sums of two integer squares. The argument *does not* directly apply to sums of four or more squares since the hypothesis is not satisfied: if $q_n(x) = x_1^2 + \ldots + x_n^2$ and we take $x = (\frac{1}{2}, \ldots, \frac{1}{2})$, the best we can do is to take y to have all coordinates either 0 or 1 which gives $q(x-y) = \frac{n}{4}$.[1]

This proof of Corollary 2 is essentially due to L. Aubry [Aub12], but was long

[1]On the other hand, one can easily deduce Lagrange's Four Squares Theorem from the Three Squares Theorem and Euler's Four Squares Identity.

forgotten until it was rediscovered by Davenport and Cassels in the 1960s. They did not publish their result, but J.-P. Serre included it in his influential text [Se73], and it is by now quite a famous and beloved proof.

On the other hand there is the following theorem.

Theorem 3. *(Pfister* [Pf65]*) Let F be a field of characteristic different from 2, let $q(x)$ be a quadratic form over F, and view it by "base extension" as a quadratic form over the polynomial ring $F[t]$. Suppose that for $d \in F[t]$, there exists $x = (x_1, \ldots, x_n) \in F(t)^n$ such that $q(x) = d$. Then there exists $y = (y_1, \ldots, y_n) \in F[t]^n$ such that $q(y) = d$.*

Corollary 4. *(Cassels* [Ca64]*) Fix $n \in \mathbb{Z}^+$. A polynomial $d \in F[t]$ is a sum of squares of n rational functions iff it is a sum of squares of n polynomials.*

Theorems 1 and 3 each concern certain quadratic forms q over a domain R with fraction field K, and the common conclusion is that for all $d \in R$, q R-represents d iff it K-represents d. This is a natural and useful property for a quadratic form R over an integral domain to have, and we call such a form an **ADC form**.

The relationship between the hypotheses of the Aubry-Davenport-Cassels and Cassels-Pfister theorems is not as immediate. In the former theorem, the hypothesis on q is reminiscent of the Euclidean algorithm. To generalize this to quadratic forms over an arbitrary domain we need some way of measuring the size of $q(x-y)$. We do this by introducing the notion of a **norm function** $|\ |: R \to \mathbb{N}$ on an integral domain. Then we define an anisotropic quadratic form $q(x) = q(x_1, \ldots, x_n)$ over $(R, |\ |)$ to be **Euclidean with respect to the norm** if for all $x \in K^n$, there exists $y \in R^n$ such that $|q(x-y)| < 1$. That this notion is a reasonable one is justified by our carrying over the proof of the Aubry-Davenport-Cassels theorem to this context: we show that for any normed ring $(R, |\ |)$, a Euclidean quadratic form $q_{/R}$ is an ADC form. This suggests a strategy of proof of the Cassels-Pfister theorem, as follows: first, find a natural norm on the domain $R = F[t]$, and second show that any "constant" quadratic form over R is Euclidean with respect to this norm. This strategy is carried out in Section 2.5 to give a proof of the Cassels-Pfister Theorem: in fact, the proof gives a slightly more general result.[2]

After establishing that every Euclidean form is an ADC form, the natural question is to identify all Euclidean forms and ADC forms over (normed) rings of arithmetic interest. The intuition here is that Euclideanness is a sort of geometry of numbers sufficient condition for the more purely algebraic ADC condition, so that the latter class should be significantly wider than the former. In fact, one of the goals of this work is to introduce "geometry of numbers" as a topic of interest over a general normed integral domain and to see how the geometry is influenced by the commutative-algebraic properties of R. Let us single out one result in this direction: let (R, v) be a complete discrete valuation ring $(R, v,)$ endowed with the norm $x \mapsto |x| = 2^{v(x)}$. Then a quadratic form $q_{/R}$ is Euclidean for the norm iff the corresponding quadratic lattice is maximal (Theorem 42).

[2]One may say that this is really a repackaging of the standard proof of the Cassels-Pfister theorem, and we do not disagree, but we think the repackaging is suggestive and useful.

For us the most interesting class of domains are the **Hasse domains**, i.e., S-integer rings in a global field. Here it is interesting to compare notions of Euclidean and ADC form with more standard properties like class number one forms and regular forms. By doing so we get a new perspective on some classical theorems and also bring up new problems, only some of which we are able to solve here. Perhaps the most interesting unsolved question is the following: let R be a Hasse domain endowed with its canonical norm. Must a Euclidean quadratic form $q_{/R}$ have class number one?

Acknowlegements: It is a pleasure to thank F. Lemmermeyer, J.P. Hanke, D. Krashen and W.C. Jagy, who each contributed valuable insights.

1. Norms and Ideal Norms

1.1. **Normed rings.**

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

Remark: Let $\mathrm{Prin}(R)$ be the multiplicative monoid of nonzero principal ideals of R. Then a norm on R determines, and is determined by, a homomorphism of monoids $N : \mathrm{Prin}(R) \to \mathbb{Z}^+$ which is nondegenerate in the sense that the only element which maps under N to the identity of $\mathbb{Z}^+$ is the identity of $\mathrm{Prin}(R)$.

A norm $|\ |$ is **non-Archimedean** (resp. **metric**) if for all $x, y \in R$, $|x + y| \leq \max(|x|, |y|)$ (resp. $|x + y| \leq |x| + |y|$).

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

Example 1.1.1: The usual absolute value $|\ |_\infty$ (inherited from $\mathbb{R}$) is a norm on $\mathbb{Z}$. It is easy to see that $|\ |_\infty$ is the unique metric norm on $\mathbb{Z}$.

Example 1.1.2: 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 $|\ |_a$ on R. When k is finite, it is most natural to take $a = \#k$. Otherwise, we may as well take $a = 2$.

Example 1.1.3: Let R be a discrete valuation ring (DVR) with valuation $v : K^\times \to \mathbb{Z}$ and residue field k. Choosing an integer $a \geq 2$ we can define a norm $|\ |_a : R^\bullet \to \mathbb{Z}^+$ by $|x|_a = a^{v(x)}$.

Example 1.1.4: Let R be a UFD. Then $\mathrm{Prin}(R)$ is a free commutative monoid on the set Σ_R of height one prime ideals of R. 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 $(\pi) = (\pi')$, $n_\pi = n_{\pi'}$. One simple choice is to fix $a \in \mathbb{Z}^{\geq 2}$ and put

$|\pi| = a$ for all prime elements π. For instance, if R is a DVR this agrees with the norm $|\ |_a$ of Example 2.

1.2. **Ideal norms.**

If M and N are monoids (written multiplicatively, with identity element 1), a monoid homomorphism $f : M \to N$ is **nondegenerate** if $f(x) = 1 \iff x = 1$.[3]

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 $|\ | : \mathcal{I}^+(R) \to (\mathbb{Z}^+, \cdot)$. We extend the norm to the zero ideal by putting $|(0)| = 0$.

More generally, let $\mathcal{M}$ be a submonoid of $\mathcal{I}^+(R)$. Then an **$\mathcal{M}$-ideal norm** is a nondegenerate homomorphism of monoids from $\mathcal{M}$ to $\mathbb{Z}^+$. Such a homomorphism induces a homomorphism on Grothendieck groups $G(\mathcal{M}) \to G(\mathbb{Z}^+) = \mathbb{Q}^+$.

Let $\mathrm{Prin}(R)$ be the submonoid of principal ideals. Then a $\mathrm{Prin}(R)$-ideal norm is nothing else than a norm function on R in the sense of the previous section. The Grothendieck group of $\mathrm{Prin}(R)$ is the group $\mathrm{PFrac}(R)$ of principal fractional ideals. R is a UFD iff $\mathrm{Prin}(R)$ is a free commutative monoid (on the nonzero principal prime ideals). Thus every UFD admits a norm and all norms on UFDs arise as in Example 4 above.

Let $\mathrm{Inv}^+(R)$ be the submonoid of invertible ideals. The Grothendieck group of $\mathrm{Inv}^+(R)$ is the group $\mathrm{Inv}(R)$ of invertible fractional ideals. R is a Dedekind domain iff $\mathrm{Inv}^+(R) = \mathcal{I}(R)$ iff $\mathcal{I}(R)$ is a free commutative monoid (on the nonzero prime ideals). Thus every Dedekind domain admits an ideal norm and all norms on Dedekind domains arise as follows. . .. For an ideal R in a Dedekind domain, let $\ell(I)$ be the length of R/I as an R-module. Equivalently, if $I = \prod \mathfrak{p}_i^{r_i}$, then $\ell(I) = \sum_i r_i$. Then the map $\ell : \mathcal{I}^+(R) \to (\mathbb{N}, +)$ is a nondegenerate homomorphism of monoids, so for any $a \in \mathbb{Z}^{\geq 2}$, the function $|\ |_a : \mathcal{I}(R) \to \mathbb{Z}^+$, $|I|_a = 2^{\ell(I)}$ is an ideal norm on R. The following result has an immediate proof.

Lemma 5. *If a domain R admits an $\mathcal{M}$-ideal norm, then the ideals in $\mathcal{M}$ satisfy the ascending chain condition. In particular, a domain which admits a $\mathrm{Prin}(R)$-ideal norm is an ACCP domain (i.e., satisfies ACC on principal ideals), and a domain which admits a $\mathcal{I}^+(R)$-ideal norm is Noetherian.*

1.3. **Divisorial norms.**

For a domain R and a fractional R-ideal I, put $(R : I) = \{x \in K \mid xI \subset R\}$. A fractional ideal is **divisorial** if it is the intersection of all the principal fractional ideals in which it is contained. For any fractional ideal I, the minimal divisorial ideal contianing I is $\overline{I} = (R : (R : I))$. In particular all invertible ideals – and hence all principal ideals – are divisorial.

[3]Note that, unlike the case of groups, a nondegenerate homomorphism need not be injective.

The set $\mathrm{Div}(R)$ of divisorial fractional ideals forms a lattice-ordered monoid under the operation $I \cdot J := \overline{IJ}$. The divisorial principal ideals form a submonoid $\mathrm{Div}^+(R)$. The monoid $\mathrm{Div}(R)$ is a group iff R is completely integrally closed, in which case it is the Grothendieck group of its submonoid $\mathrm{Div}^+(R)$.

A domain R is a Krull domain if: for every height one prime $\mathfrak{p} \in \Sigma_R$, the localization $R_{\mathfrak{p}}$ is a DVR, $R = \bigcap_{\mathfrak{p} \in \Sigma_R} R_{\mathfrak{p}}$ and every $x \in R^\bullet$ lies in only finitely many height one primes. Equivalently, R is a Krull domain iff it is completely integrally closed and satisfies the ascending chain condition on divisorial ideals. In a Krull domain, every height one prime $\mathfrak{p}$ induces a map $v_{\mathfrak{p}} : \mathrm{Frac}(R) \to \mathbb{Z}$: for a fractional ideal I, the pushforward $IR_{\mathfrak{p}}$ is a fractional ideal of the DVR $R_{\mathfrak{p}}$ and thus of the form $(\mathfrak{p}R_{\mathfrak{p}})^n$, and we set $v_{\mathfrak{p}}(I) = n$. Restricting to divisorial ideals induces an isomorphism of groups

$$\mathrm{Div}\, R \xrightarrow{\sim} \bigoplus_{\mathfrak{p} \in \Sigma_R} \mathbb{Z}.$$

All this is to motivate the following definition: a **divisorial norm** on a domain R is a nondegenerate homomorphism $\mathrm{Div}^+(R) \to \mathbb{Z}^+$. When R is a Krull domain, just as above such homomorphisms correspond to assigning to each height one prime $\mathfrak{p}$ a number $n_{\mathfrak{p}} \geq 2$ and passing to Grothendieck groups gives a homomorphism $\mathrm{Div}(R) \to \mathbb{Q}^+$.

Remark 1.3.1: In general a divisorial norm need not be an instance of the $\mathfrak{M}$-ideal construction of the previous construction because in a Krull domain the product of two divisorial ideals need not be divisorial. However, the notion of a divisorial norm directly generalizes both that of an element-wise norm on a UFD and an ideal norm on a Dedekind domain.

For later use we record two results on Krull domains.

Proposition 6. *Let R be a Krull domain.*
a) For divisorial fractional ideals I and J of R, TFAE:
(i) $I \subset J$,
(ii) $v_{\mathfrak{p}}(I) \geq v_{\mathfrak{p}}(J)$ for all $\mathfrak{p} \in \Sigma_R$.
b) (Krull Approximation Theorem) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be a finite set of height one prime ideals of R and $n_1, \ldots, n_r \in \mathbb{Z}$. Then there exists $x \in R$ such that
- *For all $1 \leq i \leq r$, $v_{\mathfrak{p}_i}(x) = n_i$, and*
- *for all other height one primes $\mathfrak{p}$, $v_{\mathfrak{p}}(x) \geq 0$.*

Proof. a) This is [LM71, Prop. 8.10]. b) This is [Bou98, Prop. VII.9]. □

1.4. **Abstract number rings.**

A commutative ring R has the property of **finite norms** (FN) if for all nonzero ideals I of R, R/I is a finite ring [BW66], [CL70], [LM72].

Obviously any finite ring satisfies (FN). On the other hand, it can be shown that any infinite ring satisfying property (FN) is necessarily a domain. We define an **abstract number ring** to be an infinite integral domain satisfying (FN) which is not a field. An abstract number ring is a Noetherian domain of Krull dimension

one, hence it is a Dedekind domain iff it is integrally closed.

Example 1.4.1: The rings $\mathbb{Z}$ and $\mathbb{F}_p[t]$ are abstract number rings. From these many other examples may be derived using the following result.

Proposition 7. *Let R be an abstract number ring 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 an abstract number ring.
b) The integral closure $\tilde{R}$ of R in K is a Dedekind abstract number ring.
c) The completion of an abstract number ring at a maximal ideal is an abstract number ring.

Proof. Part a) is [LM72, Thm. 2.3]. In particular, it follows from part a) that $\tilde{R}$ is an abstract number ring. 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 an abstract number ring. For a nonzero ideal I of R, we define $|I| = \#R/I$. In light of the previous sections, it is natural to ask whether $I \mapsto |I|$ gives an ideal norm on R.

Proposition 8. *Let I and J be nonzero ideals of the abstract number ring R.*
a) If I and J are comaximal – i.e., $I + J = R$ – then $|IJ| = |I||J|$.
b) If I is invertible, then $|IJ| = |I||J|$.

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 abstract number ring $R_{\mathfrak{p}}$. 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. □

Thus $I \mapsto |I|$ is an $\mathrm{Inv}^+(R)$-ideal norm. When R is integrally closed (hence Dedekind), every ideal is invertible so this is an ideal norm. Conversely, if $I \mapsto |I|$ is an ideal norm then R is a Dedekind domain [BW66, Thm. 2].

1.5. **Euclidean norms.** A norm $|\ |$ on R is **Euclidean** if for all $x \in K$, there is $y \in R$ such that $|x - y| < 1$. More generally, let $\mathcal{M}$ be a submonoid of $\mathcal{I}(R)$ and $|\ | : \mathcal{M} \to \mathbb{Z}^+$ be an $\mathcal{M}$-ideal norm. Then $I \in \mathcal{M}$ is a **Euclidean ideal for** $|\ |$ if for all $x \in K$, there exists $y \in I$ with $|x - y| < |I|$.

Remark 1.5.1: The norm $|\ |$ on R is Euclidean iff the improper ideal $I = R$ is a Euclidean ideal.

Remark 1.5.2: The definition that $|\ |$ is Euclidean agrees with the classical one that $|\ |$ be a Euclidean function on R.[4]

Remark 1.5.3: The definition of Euclidean ideal is modelled on that of [Le79].

The norm $|\ |_\infty$ on $\mathbb{Z}$ is Euclidean. The norms $|\ |_a$ on $k[t]$ are Euclidean. For a DVR, the norms $|\ |_a$ (c.f. Example 4) are Euclidean: indeed, for $x \in K^\bullet$, $x \in K \setminus R \iff v(x) < 0 \iff |x|_a = a^{v(x)} < 1$, so we may take $y = 0$. In a similar way, to any semilocal PID R one can attach a natural family of Euclidean norms (including the canonical norm if R is an abstract number ring).

Example 1.5.1: $S = \mathbb{Z}_K$ is the ring of integers in a number field K. Then it is a classical problem to determine whether R is Euclidean for the canonical norm: such fields are called norm-Euclidean. Note that any norm-Eucliean number field has class number one. Remarkably, conditional on GRH it is known that every number field of class number one except $\mathbb{Q} = K(\sqrt{-D})$ for $D = 19, 43, 67, 163$ is Euclidean for some crazy (and possibly non-multiplicative, though this seems to be poorly understood) norm. This is to be contrasted with the fact the standard conjecture that there are infinitely many class number one real quadratic fields but only finitely many *norm-Euclidean* real quadratic fields. The classification of such fields was completed by Barnes and Swinnerton-Dyer [BSD52] and appears below.

2. Euclidean quadratic forms and ADC forms

2.1. Euclidean quadratic forms.

Let $(R, |\ |)$ be a normed ring of characteristic not 2. A **quadratic form** over R, is a polynomial $q \in R[x] = R[x_1, \ldots, x_n]$ which is homogeneous of degree 2. Throughout this note we only consider quadratic forms which are non-degenerate over the fraction field K of R. A nondegenerate quadratic form $q_{/R}$ is **isotropic** if there exists $a = (a_1, \ldots, a_n) \in R^n \setminus \{(0, \ldots, 0)\}$ such that $q(a) = 0$; otherwise q is **anisotropic**. A form q is anisotropic over R iff it is anisotropic over K. A quadratic form $q_{/R}$ is **universal** if for all $d \in R$, there exists $x \in R^n$ such that $q(x) = d$.

A quadratic form q on a normed ring $(R, |\ |)$ is **Euclidean** if for all $x \in K^n \setminus R^n$, there exists $y \in R^n$ such $0 < |q(x-y)| < 1$. We say that q is **boundary-Euclidean** if for all $x \in K^n \setminus R^n$, there exists $y \in R^n$ such that $0 < |q(x - y)| \leq 1$.

[4]Classically, one often encounters a more general definition of Euclidean function in which the multiplicativity is weakened to $|a| \leq |ab|$, but this does not concern us here. In fact, as far as I know it is an open problem whether a domain which admits a Euclidean function must necssarily admit one which is multiplicative.

Remark 2.1.1: An anisotropic quadratic form q is Euclidean (resp. boundary-Euclidean) iff for all $x \in K^n$ there exists $y \in R^n$ such that $|q(x-y)| < 1$ (resp. $|q(x-y)| \leq 1$).

Proposition 9. *The norm $|\ |$ on R is a Euclidean norm iff the quadratic form $q(x) = x^2$ is a Euclidean quadratic form.*

Proof. Noting that q is an anisotropic quadratic form, this comes down to:

$$\forall x, y \in K,\ |x-y| < 1 \iff |q(x-y)| = |(x-y)^2| = |x-y|^2 < 1.$$

□

Remark 2.1.1: Also $(R, |\ |)$ is Euclidean iff the hyperbolic plane $\mathbb{H} = x_1 x_2$ is Euclidean.

Example 2.1.1: Let $n, a_1, \ldots, a_n \in \mathbb{Z}^+$. Then the integral quadratic form $q(x) = a_1 x_1^2 + \ldots + a_n x_n^2$ is Euclidean iff $\sum_i a_i < 4$.

2.2. **Euclideanity.** For a quadratic form q over a normed ring $(R, |\ |)$ with fraction field K, define for $x \in K^n$,

$$E(q, x) = \inf_{y \in R^n} |q(x-y)|$$

and

$$E(q) = \sup_{x \in K^n} E(q, x).$$

Let us call $E(q)$ the **Euclideanity** of q. Thus an anisotropic form q is Euclidean if $E(q) < 1$ and is not Euclidean when $E(q) > 1$. The case $E(q) = 1$ is ambiguous: the form q is *not* Euclidean iff the supremum in the definition of $E(q)$ is attained, i.e., iff there exists $x \in K^n$ such that $E(q, x) = 1$.

Let us also definite the Euclideanity $E(R)$ of R itself to be the Euclideanity of $q(x) = x^2$.

Remark 2.2.1: If we change a norm within its equivalence class, the Euclideanity of a quadratic form changes, but its place in the trichotomy $E(q) < 1$, $E(q) = 1$, $E(q) > 1$ does not change. Moreover, passage to an equivalent norm does not disturb the class of Euclidean quadratic forms.

The following results have immediate proofs.

Lemma 10. *Let q be a quadratic form over R and $a \in R^\bullet$. Then*

$$E(a \cdot q, x) = |a| E(q, x)$$

and

$$E(a \cdot q) = |a| E(q).$$

Lemma 11. *Let $|\ |$ be a metric norm on the domain R, and let q_1 and q_2 be quadratic forms over R. Denote the orthogonal direct sum of q_1 and q_2 by $q_1 \oplus q_2$.*
a) We have $E(q_1 \oplus q_2) \leq E(q_1) + E(q_2)$.
b) If $(R, |\ |) = (\mathbb{Z}, |\ |_\infty)$, and q_1 and q_2 are both positive definite, then

$$E(q_1 \oplus q_2) = E(q_1) + E(q_2).$$

Example 2.2.1: Let $(R, |\ |) = (\mathbb{Z}, |\ |_\infty)$, $q_1 = x_1^2$, $q_2 = -2x^2$. Then $E(q_1) = \frac{1}{4}$, $E(q_2) = \frac{1}{2}$, whereas $E(q_1 \oplus q_2) = E(x_1^2 - 2x_2^2) \leq \frac{1}{2} < E(q_1) + E(q_2)$.

Two quadratic forms q, q' over a domain R are **unit-equivalent** if there exists $a \in R^\times$ such that $q' \cong a \cdot q$.

Lemma 12. *Let q, q' be two unit-equivalent quadratic forms over a domain R.*
a) q is an ADC form iff q' is an ADC form.
b) Let $|\ |$ be any norm on R. Then $E(q) = E(q')$, and q is Euclidean iff q' is Euclidean.

Proof. a) It is enough to show: if $q' = a \cdot q$ for some $a \in R^\times$ and q is an ADC form, then so is q'. Indeed, let $d \in R$ be such that there exists $x \in K^n$ such that $aq(x) = d$. Then the element $a^{-1}d$ of R is K-represented by q; since q is ADC, there exists $y \in R^n$ such that $q(y) = a^{-1}d$, and thus $aq(y) = d$.
This is immediate from Lemma 10. □

In view of Lemma 12, we may simplify matters by only considering quadratic forms up to unit equivalence. For instance, when $R = \mathbb{Z}$ this amounts to identifying q with $-q$: we speak of "definite" quadratic forms rather than positive and negative definite quadratic forms. (Note that when q is indefinite, q and $-q$ may or may not aleady be isometric over $\mathbb{Z}$. E.g, for forms $x^2 - Dy^2$, this depends on whether the fundamental unit of the ring of integers of $\mathbb{Q}(\sqrt{D})$ has positive or negative norm.)

2.3. **ADC-forms.**

A quadratic form $q(x) = q(x_1, \ldots, x_n)$ over R is an **ADC-form** if for all $d \in R$, if there exists $x \in K^n$ such that $q(x) = d$, then there exists $y \in R^n$ such that $q(y) = d$.

Example 2.3.1: Any universal quadratic form is an ADC-form. If $R = \mathbb{Z}$ and q is positive definite and **positive universal** – i.e., represents all positive integers – then q is an ADC-form. Thus for each $n \geq 5$ there are infinitely many positive definite ADC-forms, e.g. $x_1^2 + \ldots + x_{n-1}^2 + dx_n^2$ for $d \in \mathbb{Z}^+$.

Example 2.3.2: Let $\tilde{R}$ be the integral closure of R in K. Then $q(x) = x^2$ is *not* an ADC-form iff there exists $a \in \tilde{R} \setminus R$ such that $a^2 \in R$. In particular x^2 is an ADC-form if R is integrally closed.

Example 2.3.3: Let R be a UFD and $a \in R^\bullet$. Then $q(x) = ax^2$ is an ADC-form iff a is squarefree. (Further discussion of unary forms is given in §5 below.)

Example 2.3.4: Suppose R is an algebra over a field k, and let $q_{/k}$ be isotropic. Then the base extension of q to R is universal. Indeed, since q is isotropic over k, it contains the hyperbolic plane as a subform. That is, after a k-linear change of variables, we may assume $q = x_1x_2 + q'(x_3, \ldots, x_n)$, and the conclusion is now clear.

Example 2.3.5: The isotropic form $q(x, y) = x^2 - y^2$ is not an ADC-form over $\mathbb{Z}$: indeed it is universal over $\mathbb{Q}$ but not over $\mathbb{Z}$.

2.4. **The Main Theorem.**

Theorem 13. *Let $(R, |\ |)$ be a normed ring not of characteristic 2 and $q_{/R}$ a Euclidean quadratic form. Then q is an ADC form.*

Proof. For $x, y \in K^n$, put $x \cdot y := \frac{1}{2}(q(x+y) - q(x) - q(x))$. Then $(x, y) \mapsto x \cdot y$ is bilinear and $x \cdot x = q(x)$. Note that for $x, y \in R^n$, we need not have $x \cdot y \in R$, but certainly we have $2(x \cdot y) \in R$.

Let $d \in R$, and suppose there exists $x \in K^n$ such that $q(x) = d$. Equivalently, there exists $t \in R$ and $x' \in R^n$ such that $t^2 d = x' \cdot x'$. Choose x' and t such that $|t|$ is minimal. It is enough to show that $|t| = 1$, for then by (N1) $t \in R^\times$.

Apply the Euclidean hypothesis with $x = \frac{x'}{t}$: there is $y \in R$ such that if $z = x - y$,

$$0 < |q(z)| < 1.$$

Now put

$$a = y \cdot y - d,\ b = 2dt - 2(x' \cdot y),\ T = at + b,\ X = ax' + by.$$

Then $a, b, T \in R$, and $X \in R^n$.
Claim: $X \cdot X = T^2 d$.
Indeed,

$$X \cdot X = a^2(x' \cdot x') + ab(2x' \cdot y) = b^2(y \cdot y) = a^2 t^2 d + ab(2dt - b) + b^2(d + a)$$

$$= d(a^2 t^2 + 2abt + b^2) = T^2 d.$$

Claim: $T = t(z \cdot z)$.
Indeed,

$$tT = at^2 + bt = t^2(y \cdot y) - dt^2 + 2dt^2 - t(2x' \cdot y)$$

$$= t^2(y \cdot y) - t(2x' \cdot y) + x' \cdot x' = (ty - x') \cdot (ty - x') = (-tz) \cdot (-tz) = t^2(z \cdot z).$$

Since $0 < |z \cdot z| < 1$, we have $0 < |T| < |t|$, contradicting the minimality of $|t|$. □

Remark 2.4.1: This proof is modelled on that of [Se73, pp. 46-47].

2.5. **The Generalized Cassels-Pfister Theorem.**

Lemma 14. *Let q be an anisotropic quadratic form over a field k. Then q remains anisotropic over the rational function field $k(t)$.*

Proof. If there exists a nonzero vector $x \in k(t)^n$ such that $q(x) = 0$, then (since $k[t]$ is a UFD) there exists $y = (y_1, \ldots, y_n)$ such that $y \in R^n$, $\gcd(y_1, \ldots, y_n) = 1$ and $q(y) = 0$. The polynomials $y_1, \ldots, y_n$ do not all vanish at 0, so $(y_1(0), \ldots, y_n(0)) \in k^n \setminus (0, \ldots, 0)$ is such that $q(y_1(0), \ldots, y_n(0)) = 0$, i.e., q is isotropic over k. □

Remark 2.5.1: The argument of Lemma 14 actually shows that a projective variety $V_{/k}$ has a k-rational point iff it has a $k(t)$-rational point.

Theorem 15. *(Generalized Cassels-Pfister Theorem) Let F be a field of characteristic not 2, $R = F[t]$, and $K = F(t)$. Let $q = \sum_{i,j} a_{ij}(t) x_i x_j$ be a quadratic form over R. We suppose that* either*:*
(i) q is anisotropic and each a_{ij} has degree 0 or 1, or
(ii) Each a_{ij} has degree 0, i.e., q is the extension of a quadratic form over k.
Then q is an ADC form.

Proof. Suppose first that q is isotropic over K and extended from a quadratic form q over k. By Lemma 14, $q_{/k}$ is isotropic. Then by Example 2.3.4, $q_{/R}$ is universal.

Now suppose that q is anisotropic over K and that each a_{ij} has degree 0 or 1. By Theorem 13, it suffices to show that as a quadratic form over $R = k[t]$ endowed with the norm $|\ | = |\ |_2$ of Example 1.1.2, q is Euclidean.

Given an element $x = (\frac{f_1(t)}{g_1(t)}, \ldots, \frac{f_n(t)}{g_n(t)}) \in K^n$, by polynomial division we may write $\frac{f_i}{g_i} = y_i + \frac{r_i}{g_i}$ with $y_i, r_i \in k[t]$ and $\deg(r_i) < \deg(g_i)$. Putting $y = (y_1, \ldots, y_n)$ and using the non-Archimedean property of $|\ |$, we find

$$|q(x-y)| = |\sum_{i,j} a_{i,j}(\frac{r_i}{g_i})(\frac{r_j}{g_j})| \leq \left(\max_{i,j} |a_{i,j}|\right)\left(\max_i |\frac{r_i}{g_i}|\right)^2 < 1. \tag{1}$$

□

Remark 2.5.2: Example 2.3.3 shows that extension of Theorem 15 to all forms with $\max_{i,j} \deg(a_{ij}) \leq 2$ is not possible.

2.6. **Maximal Lattices.**

When studying quadratic forms over integral domains it is often convenient to use the terminology of lattices in quadratic spaces. Let R be a domain with fraction field K, let V be a finite-dimensional vector space, and let $q : V \to K$ be a quadratic form. An **R-lattice** Λ in V is a finitely generated R-submodule of V such that $\Lambda \otimes_R K = V$. A **quadratic R-lattice** is an R-lattice Λ in the quadratic space (V, q) such that $q(\Lambda) \subset R$.

In particular, if $q : R^n \to R$ is a quadratic form, then tensoring from R to K gives a quadratic form $q : K^n \to K$ and taking $V = K^n$, $\Lambda = R^n$ gives a quadratic R-lattice. Conversely, a quadratic lattice Λ in R^n which is *free* as an R-module may be identified with a quadratic form over R.

A quadratic R-lattice Λ is said to be **maximal** if it is not strictly contained in another quadratic R-lattice.[5] If R is Noetherian, then discriminant considerations show that every quadratic R-lattice is contained in a maximal quadratic R-lattice.

Proposition 16. *Let $(R, |\ |)$ be a normed ring and $q_{/R}$ a Euclidean quadratic form. Then the associated quadratic R-lattice $\Lambda = R^n$ is maximal.*

Proof. For if not, there exists a strictly larger quadratic R-lattice Λ'. Choose $x \in \Lambda' \backslash \Lambda$, so $x \in K^n \backslash R^n$. For all $y \in \Lambda = R^n$, $x - y \in \Lambda'$, so $|q(x-y)| \in |R| = \mathbb{N}$. □

Example 13: Let $(R, |\ |) = (\mathbb{Z}, |\ |_\infty)$, and let $a \in \mathbb{Z}^\bullet$. Then:
a) The form ax^2 is maximal iff a is squarefree.
b) The form $x^2 + ay^2$ is maximal iff a is squarefree and $a \equiv 1, 2 \pmod 4$. In particular the boundary-Euclidean form $x^2 + 3y^2$ is not maximal.

3. Localization

In this section we collect results about the effect of localization and completion on the Euclidean and ADC-properties.

[5]For the sake of brevity, we will sometimes simply say that the quadratic form q is maximal if its associated free quadratic lattice is maximal.

3.1. **Localization and Euclideanity.**

Suppose first that $(R, |\ |)$ is a normed UFD, and S is a saturated multiplicatively closed subset. We shall define a **localized norm** $|\ |_S$ on the localization $S^{-1}R$. To do so, recall that $S^{-1}R$ is again a UFD and its principal prime ideals (π) are precisely those for which $\pi \cap S = \varnothing$. Therefore we may view the monoid $\mathrm{Prin}(S^{-1}R)$ as a submonoid of $\mathrm{Prin}(R)$ by taking it to be the direct sum over all the height one prime ideals (π) of R with $(\pi) \cap S = \varnothing$: let ι be this embedding of monoids. We define the localized norm $|\ |_S : \mathrm{Prin}(S^{-1}R) \to \mathbb{Z}^+$ by $|x|_S := |\iota(x)|$.

Remark 3.3.1: Here are two easy and useful properties of the localized norm:

• Any $x \in R^\bullet$ may be written as $s_x x'$ with $s_x \in S$ and x' prime to S, and we have

$$|x|_S = |s_x x'|_S = |x'|_S = |x'|.$$

• For any $x \in R^\bullet$, $|x|_S \leq |x|$.

Theorem 17. *Let $(R, |\ |)$ be a UFD with fraction field K, let $S \subset R^\bullet$ be a saturated multiplicatively closed subset, and let R_S be the localization of R at S. 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 $y_S \in R_S^n$ such that $|q(x - y_S)|_S \leq E$.*

Proof. Let $x \in K^n$. We must find $Y \in R_S^n$ such that $|q(x-Y)|_S \leq E$. Writing $x = \frac{a}{b}$ with $a \in R^n$ and $b \in R^\bullet$ and clearing denominators, it suffices to find $y_S \in R_S^n$ such that

$$|q(a - by_S)|_S \leq E|b|_S^2.$$

As above, we may factor b as $s_b b'$ with $s_b \in S$ and b' prime to S, so $|b'|_S = |b'|$. Applying our hypothesis to the element $\frac{a}{b'}$ of K^n we may choose $y \in R^n$ such that $|q(a - b'y)| \leq E|b'|^2$. Now put $y_S = \frac{y}{s_b}$, so

$$|q(a - by_S)|_S = |q(a - b'y)|_S \leq |q(a - b'y)| \leq E|b'|^2 = E|b'|_S^2 = E|b|_S^2.$$

□

Corollary 18. *Retain the notation of Theorem 17 and write q_S for q viewed as a quadratic form on the normed ring $(R_S, |\ |_S)$. Then:*
a) $E(q_S) \leq E(q)$.
b) If q is Euclidean, so is q_S.

Proof. a) By definition of the Euclideanity, for all $\epsilon > 0$ and all $x \in K^n$, there exists $y \in R^n$ such that $|q(x-y)| \leq E(q) + \epsilon$. Therefore Theorem 17 applies with $E = E(q) + \epsilon$ to show that for all $x \in K$, there exists $y_S \in R_S$ with $|q(x - y_S)|_S \leq E(q) + \epsilon$, i.e., $E(q_S) \leq E(q) + \epsilon$. Since ϵ was arbitrary, we conclude $E(q_S) \leq E(q)$.
b) If in the statement of Theorem 17 we take $E = 1$ and replace all the inequalities with strict inequalities, the proof goes through verbatim. □

The rings of most interest to us are Hasse domains, which of course need not be UFDs but are always Dedekind domains. Thus it will be useful to have Dedekind domain analogues of the previous discussion.

Let R be a Dedekind domain endowed with an ideal norm $|\ |$. 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 [LM71, 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** $|\ |_W$ on R_W as the composite map $\mathcal{I}(R_W) \to \mathcal{I}(R) \stackrel{|\ |}{\to} \mathbb{Z}^+$.

Remark 3.1.2.: As above, we single out the following properties of $|\ |_W$:

• 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 19. *Let R be a Dedekind domain with fraction field K, $|\ |$ 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 $|q(x - y_W)|_W \leq E$.*

Proof. The argument is similar to that of Theorem 17. The only point which requires additional attention is the existence of a decomposition of $b \in R^\bullet$ as $b = w_b b'$ with w_b divisible only prime ideals in W and b' prime to W. But this follows by weak approximation (or the Chinese Remainder Theorem) applied to the finite set of prime ideals $\mathfrak{p} \in W$ which appear in the prime factorization of (b). □

Also as before, we deduce the following result.

Corollary 20. *Retain the notation of Theorem 19 and write q_W for q viewed as a quadratic form on the ideal normed ring $(R_W, |\ |_W)$. Then:*
a) $E(q_W) \leq E(q)$.
b) If q is Euclidean, so is q_W.

Remark 3.1.3: There is another analogue of Theorem 17 for overrings of a Krull domain endowed with a divisorial norm. The statement and proof are left to the interested reader.

3.2. **Localization and Completion of ADC-forms.**

Theorem 21. *Let R be a domain, $S \subset R^\bullet$ a saturated multiplicatively closed subset and $R_S = S^{-1}R$ the localized domain. If a quadratic form $q(x) \in R[x]$ is ADC, then q viewed as a quadratic form over R_S is ADC.*

Proof. Let $d \in R_S^\bullet$ be K-represented by q_S, i.e., there exists $x \in K^n$ such that $q(x) = d$. We may write $d = \frac{a}{s}$ with $s \in S$. If $x = (x_1, \ldots, x_n)$, then by sx we mean $(sx_1, \ldots, sx_n)$. Thus $q(sx) = s^2 q(x) = sa \in R$. Since q is ADC over R, there exists $y \in R^n$ such that $q(y) = sa$. But then $s^{-1}y \in R_S^n$ and $q(s^{-1}y) = \frac{a}{s}$. □

Corollary 22. *Let R be a Dedekind domain with fraction field K, let $v : K^\bullet \to \mathbb{Z}$ be a nontrivial discrete valuation which is "R-regular" in the sense that R is contained in the valuation ring $v^{-1}(\mathbb{N}) \cup \{0\}$. Let K_v be the completion of K with respect to v and R_v its valuation ring. Suppose $q \in R[x]$ is an ADC form. Then the base extension of q to R_v is an ADC-form.*

Proof. Under the hypotheses of the theorem, $v = v_\mathfrak{p}$ for a nonzero prime ideal $\mathfrak{p}$ of R. Let $S = R \setminus \mathfrak{p}$, and put $R_S = S^{-1}R$. By the previous theorem, the extension of q to R_S is an ADC form. Now suppose $D \in R_v^\bullet$ is such that there exists $X \in K_v^n$ with $q(X) = D$. We may choose $x \in K^n$ which is sufficiently v-adically close to X so that $q(x) = d \in R_S$ and $\frac{D}{d} = u_d^2$ for some $u_d \in R_v^\times$. (This is possible because: R_S^n is dense in R_v^n, q, being a polynomial function, is continuous for the v-adic topology, and $R_v^{\times 2}$ is an open subgroup of $R_v^\bullet$: e.g. [Ge08, Thm 3.39].) Since q is ADC over R_S, there exists $y \in R_S^n$ such that $q(y) = d$. Thus $q(u_d y) = u_d^2 d = D$, showing that D is R_v-represented by q. □

4. Imprimitive forms

Let R be a domain and $x = (x_1, \ldots, x_N) \in R^N$. We say that the vector x is **imprimitive** if there exists $d \in R^\bullet \setminus R^\times$ such that $d \mid x_i$ for all i. Equivalently, the ideal $\langle x \rangle := \langle x_1, \ldots, x_n \rangle$ generated by the coordinates of x is contained in some proper principal ideal (d). (In particular the zero vector is imprimitive.) Otherwise we say that x is **primitive**.

If R is a GCD-domain (recall PID $\implies$ UFD $\implies$ GCD-domain), then for any nonzero vector $x \in R^N$, we may put $d = \gcd(x_1, \ldots, x_n)$ and then the vector $x' = \frac{1}{d}x$ is primitive: that is, every nonzero vector is a scalar multiple of a primitive vector. In general (and even when R is the ring of integers of a number field of class number greater than one) this sort of factorization is not possible.

In this section we analyze the following question: let $q'_{/R}$ be an ADC form. For which $d \in R^\bullet$ is $q = d \cdot q'$ ADC? Of course the answer depends only on q up to unit equivalence, i.e., on the class of $d \mod R^\times$.

By looking at some basic examples, one swiftly acquires the sense that a key issue is whether d is "squarefree". In an arbitrary domain R, there are however several reasonable ways to define a squarefree element. We list them as separate conditions on an element $x \in R^\bullet$, as follows:

(SF1) For no $d \in R^\bullet \setminus R^\times$ do we have $d^2 \mid x$.
(SF2) There does not exist a nontrivial discrete valuation v on R and elements $a, b \in R^\bullet$ such that $x = a^2 b$, $v(a) \geq 1$ and $v(b) \leq 1$.
(SF3) There do not exist $a, b, p \in R^\bullet$ with $p \notin R^\times$, $x = a^2 b$, $p \mid a$ and $p^2 \nmid b$.

Remark: It is clear that (SF1) implies both (SF2) and (SF3).

Example: Suppose R is a domain which is not a field and which does not admit a nontrivial discrete valuation,[6] and let $x \in R^\bullet \setminus R^\times$. Then x^2 satisfies (SF2)

[6]For instance, take $R = \overline{\mathbb{Z}}$ to be the ring of all algebraic integers.

but not (SF1).

I believe (SF3) does not imply (SF1) but I don't currently have an example.

Proposition 23. *Let R be a Krull domain. Then each element of $R^\bullet$ satisfies (SF1) iff it satisfies (SF2) iff it satisfies (SF3).*

Proof. By the above remark, it is enough to show that if $x \in R^\bullet$ does not satisfy (SF1), then it does not satisfy (SF2) or (SF3). Let $d \in R^\bullet \setminus R^\times$ be such that $d^2 \mid x$. Since d is not a unit, the set of height one primes $\mathfrak{p}$ of R containing d is finite and nonempty; choose one such prime $\mathfrak{p}$. By the Krull Approximation Theorem, there exists $p \in R^\bullet$ such that $v_\mathfrak{p}(p) = 1$ and $v_\mathfrak{q}(p) = 0$ for all other height one primes $\mathfrak{q}$ containing x. Then, putting $k = v_\mathfrak{p}(x)$, we may write $x = p^k x'$ with $x' \in R^\bullet$ and $\mathrm{ord}_\mathfrak{p}(x') = 0$. Moreover $k \geq 2$, so we may write $k = 2\ell + \epsilon$ with $\ell \in \mathbb{Z}^+$ and $\epsilon \in \{0, 1\}$ and then

$$x = (p^\ell)^2 p^\epsilon x'.$$

Taking $a = p^\ell$ and $b = p^\epsilon x'$ shows that x does not satisfy (SF3), while the same choice of a and b and $v = v_\mathfrak{p}$ shows that x does not satisfy (SF2). □

In view of this result, we may say that an element of a Krull domain is **squarefree** if it satisfies any of the equivalent conditions (SF1), (SF2), (SF3).

(Should also show equivalence of (SF4): for all $\mathfrak{p} \in \Sigma_R$, $v_\mathfrak{p}(x) \leq 1$.)

Lemma 24. *Let $q(x)$ be a primitive quadratic form over a Krull domain R. Then, for every height one prime $\mathfrak{p}$ of R, there exists $x_0 \in R^n$ such that $v_\mathfrak{p}(x_0) = 0$.*

Proof. This is a souped up version of Exercise 2.18 in D.A. Cox's book on binary forms. (Details to be filled in!) □

Theorem 25. *Let R be a Krull domain, $d \in R^\bullet$ and let $q'(X)_{/R}$ be a primitive quadratic form. If $q(X) = dq'(X)$ is an ADC form, then d is squarefree.*

Proof. We prove the contrapositive: suppose d is not squarefree, so there exists a height one prime $\mathfrak{p}$ of R and elements $a, b \in R^\bullet$ with $d = a^2 b$, $v_\mathfrak{p}(a) \geq 1$, $v_\mathfrak{p}(b) \leq 1$. By Lemma 24, choose $x_0 \in R^n$ such that $v_\mathfrak{p}(q(x_0)) = 0$. Then q R-represents $a^2 b q'(x_0)$, so being an ADC form it also R-represents $bq'(x_0)$. But this is an obvious contradiction: for all $x \in R^n$, $v_\mathfrak{p}(q(x)) = v_\mathfrak{p}(a^2 b) + v_\mathfrak{p}(q'(x)) \geq 2$, whereas $v_\mathfrak{p}(bq(x_0)) \leq 1$. □

For $q_{/R}$, let $D^\bullet(q)$ be the set of nonzero values R-represented by q.

Theorem 26. *Let R be a Krull domain, $q'_{/R}$ a quadratic form, and let $d \in D^\bullet(q') \setminus R^\times$. Then for all $a \in R^\bullet$, $q = (ad)q'$ is not an ADC-form.*

Proof. Seeking a contradiction, suppose q is an ADC form. By Krull Approximation we may choose a height one prime $\mathfrak{p}$ containing d and choose an element p which has $\mathfrak{p}$-adic valuation 1 and $\mathfrak{q}$-adic valuation 0 at all other height one primes containing d and a. If $v_\mathfrak{p}(a) \geq 1$, then $v_\mathfrak{p}(ad) \geq 2$, so ad is not squarefree and we are reduced to the previous result. Otherwise, choose $x_0 \in R^n$ such that $q'(x_0) = d$. Then q R-represents ad^2, so being an ADC form it also R-represents a, because all elements represented by q have positive $\mathfrak{p}$-adic valuation. □

Example: Let $R = \mathbb{Z}$ and $q'(x,y) = x^2 + y^2$, so q' is Euclidean and thus ADC. Let $d \in \mathbb{Z}^+$ and consider $q(x,y) = d(x^2+y^2)$. By the previous results, if q is ADC then d is squarefree and not divisible by any $n > 1$ which is a sum of two squares. (Since q' is principal, in this case the second condition implies the first.) In other words, d must be of the form $\prod_{i=1}^r p_i$, where the p_i's are distinct primes congruent to 3 modulo 4. Conversely, we claim that for all such values of d, q *is* an ADC-form. The key fact here is that each prime p_i which is 3 mod 4 is anisotropic for q', and it follows that for any $x \in \mathbb{Z}^2$, $\mathrm{ord}_{p_i}(q'(x))$ is even (CITE). So suppose that q $\mathbb{Z}$-represents an integer of the form $a^2 b$, i.e., there exist $(x,y) \in \mathbb{Z}^2$ such that $p_1 \cdots p_r(x^2+y^2) = a^2 b$. Then for any i, ord_{p_i} of the LHS is odd, hence $\mathrm{ord}_{p_i}(a^2 b)$ is odd, so p_i divides b. Since the p_i's are pairwise coprime $p_1 \cdots p_r \mid b$, so we get that the ADC form q' $\mathbb{Z}$-represents $a^2 \left(\frac{b}{p_1 \cdots p_r}\right)$, so q' $\mathbb{Z}$-represents $\frac{b}{p_1 \cdots p_r}$, so q $\mathbb{Z}$-represents b.

Note: This argument should generalize to the case of any principal binary form q over a Krull domain R so that the corresponding quadratic R-order is a UFD. (More on this when time permits.)

4.1. **Unary forms.**

Theorem 27. *Let R be a Krull domain, and $a \in R^\bullet$. Then $q(x) = ax^2$ is an ADC form iff a is squarefree, i.e., for each height one prime ideal $\mathfrak{p}$ of R, we have $\mathrm{ord}_{\mathfrak{p}}(a) \leq 1$.*

Proof. Step 1: R is a UFD, so all the ideals $\mathfrak{p}$ are principal.

Suppose that a is not squarefree. Then there exists a prime element p, $k \in \mathbb{Z}^+$, $\ell \in \{0,1\}$ and $a' \in R$ such that $a = p^{2k} p^\ell a'$ with $\gcd(a', p) = 1$. Thus q R-represents $p^{2k} p^\ell a'$, hence it K-represents the element $d' = p^\ell a'$, with $\mathrm{ord}_p(d) \leq 1$. However, clearly any element d R-represented by q, has $\mathrm{ord}_p(d) \geq 2$, so q is not ADC.

Suppose that a is squarefree and write it as $a = p_1 \cdots p_r u$ where the p_i are mutually nonassociate prime elements of R and $u \in R^\times$. By passing to the unit-equivalent form $u^{-1}q$, we may assume without loss of generality that $u = 1$. Suppose that $d \in R^\bullet$ is K-represented by q, i.e., there exist $x, y \in R^\bullet$ such that $a\left(\frac{x}{y}\right)^2 = d$. Clearing denominators gives

$$p_1 \cdots p_r x^2 = dy^2. \tag{2}$$

For any $1 \leq i \leq r$, we have $\mathrm{ord}_{p_i}(p_1 \cdots p_r x^2) = 2\,\mathrm{ord}_{p_i}(x) + 1$ is odd, whereas $\mathrm{ord}_{p_i}(dy^2) = 2\,\mathrm{ord}_p(y) + \mathrm{ord}_p(d)$. Thus $\mathrm{ord}_{p_i}(d)$ is odd, and in particular $p_i \mid d$. Since the p_i's are pairwise coprime, $p_1 \cdots p_r \mid d$ and thus

$$\left(\frac{x}{y}\right)^2 = \left(\frac{d}{p_1 \cdots p_r}\right).$$

Thus $\frac{x}{y} \in K$ is integral over R. Since R is integrally closed, we have $y \mid x$ and thus $a\left(\frac{x}{y}\right)^2 = d$ is an R-representation of d.

Step 2: R is a Krull Domain.

Suppose that a is not squarefree, i.e., there exists a height one prime ideal $\mathfrak{p}$ such that $\mathrm{ord}_{\mathfrak{p}}(a) \geq 2$. By the Krull Approximation Theorem, there exist elements $\pi_a, a' \in R$, a positive integer k and $\ell \in \{0,1\}$ such that $\mathrm{ord}_{\mathfrak{p}}(\pi_a) = 1$, $\mathrm{ord}_{\mathfrak{p}}(a') = 0$ and $a = \pi_a^{2k} \pi_a^\ell a'$. The argument that q is not ADC then proceeds as above.

Finally, suppose that a is squarefree, and $d \in R^\bullet$ is K-represented by q, i.e., there exist $x, y \in R^\bullet$ such that $a\left(\frac{x}{y}\right)^2 = d$. As above, we wish to prove that $y \mid x$. But since $R = \bigcap_{\mathfrak{p} \in \Sigma_R} R_{\mathfrak{p}}$, it is enough to check this divisibility locally, i.e., in the localization $R_{\mathfrak{p}}$ at each height one prime ideal $\mathfrak{p}$. However, $R_{\mathfrak{p}}$ is a DVR, in particular a UFD, so we are reduced to Step 1. □

5. Euclidean Algebras, Ideals and Modules

5.1. **Normed division algebras over a field.**

Let K be a field. Let $A_{/K}$ be a not necessarily associative K-algebra which is finite-dimensional over K, has a multiplicative identity 1, and such that $K = K \cdot 1$ lies in both the center and the nucleus of A: i.e., elements of K commute with all elements of A and associate with all pairs of elements of K. We put $A^\bullet = A \setminus \{0\}$ as usual. We say that A is a right (resp. left) division algebra if for every $x \in A^\bullet$ there exists $y \in A^\bullet$ such that $xy = 1$ (resp. $yx = 1$). A is a division algebra if it both a right and left division algebra.

Let us say that the algebra A is **1-associative** if every subalgebra generated by a single element is associative (this is more commonly known as power-associative) and **2-associative** if every subalgebra generated by two elements is associative. By a theorem of Artin, every alternative algebra – and in particular every composition algebra – is 2-associative [Sch66].

A **norm** on such a K-algebra A is a homogeneous polynomial map $N : A \to K$ such that $N(1) = 1$ and for all $x, y \in A$, $N(xy) = N(x)N(y)$. We speak of a pair (A, N) as a **normed K-algebra**.

Lemma 28. *Let (A, N) be a normed K-algebra.*
a) If A is a right (or left) division algebra, then N is anisotropic.
b) If N is anisotropic and A is 1-associative, then A is a division algebra.

Proof. a) Suppose A is a right division algebra, and $0 \neq x \in A$. Since A is a division algebra, there exists $y \in A$ such that $xy = 1$, and then $1 = N(1) = N(xy) = N(x)N(y)$, so $N(x) \neq 0$. The case of a left division algebra is similar (or work in the opposite algebra).
b) Suppose N is anisotropic and $x \in A^\bullet$. Then x is neither a left nor a right divisor of zero. Indeed, if say $xy = 0$, then $N(x)N(y) = 0$, contradicting the anisotropy of N. Now since A is finite-dimensional over K, there exists a least $n \in \mathbb{Z}^+$ such that x^n is a K-linear combination of $1, x, \ldots, x^{n-1}$ (here we use the 1-associativity to speak unambiguously of x^k). Thus there exist $a_0, \ldots, a_{n-1} \in K$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

or

$$x(x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) = (x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1)x = -a_0.$$

Since x is not a zero divisor, $a_0 \neq 0$, and thus $\frac{x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1}{-a_0}$ is both a left and right inverse to x. □

Henceforth we restrict ourselves to the case of division algebras, so N is anisotropic.

Example 4.1.1 (Field extensions): Let A/K is a commutative field extension of degree d. Then we may take $N = N_{A/K}$ to be the norm map in the sense of field theory: it is homogeneous of degree d. In particular, from a quadratic field extension we get a binary norm form.

Example 4.1.2 (Associative division algebras) Let A be an associative K-algebra. Put $L = Z(A)$, so that L/K is a field extension of degree a (say). Then A is a central division L-algebra; put $[A : L] = b^2$. Let $n : A \to L$ be the reduced norm, which is homogeneous of degree b, and let $N_{L/K}$ be the field norm. Then $N = N_{L/K} \circ n$ is a degree ab norm form on A.

An important special case is $a = 1,\ b = 2$: A/K is a **quaternion algebra**.

Example 4.1.3 (Octonion algebras): An octonion algebra is a normed algebra (A, N) with $\dim A = 8$ and $\deg N = 2$. Such algebras arise from a quaternion algebra by applying the Cayley-Dickson-Albert construction.

If (A, N) is a normed division algebra and N is a quadratic form, then A is (by definition) a division composition algebra. By a theorem of Hurwitz, $\dim_K A \in \{1, 2, 4, 8\}$, and A is either a quadratic, quaternion or octonion algebra.

Example 4.1.4 (Albert algebras): Let $A_{/K}$ be an Albert algebra, a certain kind of 27-dimensional commutative Jordan algebra. The norm is a cubic form on A.

5.2. **Orders in a normed division algebra.**

Let $\mathcal{O}$ be a unital, but not necessarily associative, $\mathbb{Z}$-algebra. We put $\mathcal{O}^\bullet = \mathcal{O} \setminus \{0\}$: this is a unital magma. A norm function on R is a homomorphism of unital magmas $|| \ || : \mathcal{O}^\bullet \to \mathbb{Z}^+$ which is nondegenerate in the (usual) sense that $||x|| = 1 \iff x = 1$. We are not so much interested in this sort of structure for its own sake but rather the special case which arises via the following construction.

Namely, let $(R, |\ |)$ be a normed domain, and let (A, N) be an n-dimensional normed division K-algebra.

A **free R-order** $\mathcal{O}$ in A is a unital R-subalgebra of A possessing an R-module basis $e_1, \ldots, e_n$ which is also a K-module basis for A. We make the following integrality assumption on the norm form N: $N(\mathcal{O}) \subset R$.

In such a situation, we may endow $\mathcal{O}$ with the structure of a normed $\mathbb{Z}$-algebra via the **composite norm** $|| \ || : \mathcal{O} \to \mathbb{N}$ defined by $||x|| = |N(x)|$.

The normed algebra $(\mathcal{O}, || \ ||)$ is **Euclidean** with respect to the norm if for all $x \in A$, there exists $y \in \mathcal{O}$ such that $||x - y|| < 1$.

Proposition 29. *With notation as above, let $\mathcal{O}$ be a free R-order in the n-dimensional normed division algebra (A, N) which is Euclidean with respect to the composite norm $|| \ ||$. Let $(e_1, \ldots, e_n)$ be an R-basis of $\mathcal{O}$. Then pulling back N under the induced isomorphism $\mathcal{O} \cong R^n$ gives rise to an n-ary Euclidean form of degree* $\deg(N)$.

Proof. In fact this is a direct consequence of the definitions. □

Proposition 30. *Let (A, N) be a 2-associative normed division algebra. If $(\mathcal{O}, || \, ||)$ is a normed algebra, every left (or right) ideal of $\mathcal{O}$ is principal.*

Proof. Let I be a nonzero left $\mathcal{O}$-ideal, and choose $a \in I$ of minimal nonzero norm. We claim that $I = aR$. Indeed, let $b \in I$. Let b^{-1} be the (left = right, since the hypothesis on A implies that it is power-associative) inverse of b. Our hypothesis on associativity implies that $b(b^{-1}a) = (bb^{-1})a = a$. Applying the Euclidean hypothesis to $x = ba^{-1}$, there exists $y \in \mathcal{O}$ such that $||ba^{-1} - y|| < 1$. Multiplying on the right by a gives $||b - ya|| < ||a||$. Since $b - ya$ is an element of I of smaller norm than that of a, we must have $b = ya$, qed. The case of a right ideal is very similar. □

Corollary 31. *With notation as as above, if $\mathcal{O}$ is Euclidean with respect to the norm, $\mathcal{O}$ is a maximal R-order in A.*

Proof. This follows from Proposition 16. □

5.3. **Euclidean ideal classes.**

Let R be a domain with fraction field K, $A_{/K}$ a finite-dimensional associative unital division algebra and $\mathcal{O}$ a free R-order in A. The two-sided $\mathcal{O}$-ideals (resp. two-sided fractional $\mathcal{O}$-ideals) form a monoid under multiplication, which we denote by $\mathcal{I}^+(\mathcal{O})$ (resp. $\mathcal{I}(\mathcal{O})$.

Theorem 32. *If R is a Dedekind domain, then $\mathcal{I}(\mathcal{O})$ (resp. $\mathcal{I}^+(\mathcal{O})$) is a free commutative monoid (resp. free commutative group) with basis the two-sided prime ideals.*

Proof. See [Vi80, Thm. I.4.5]. □

In the general case we write $\mathrm{Inv}^+(\mathcal{O})$ (resp. $\mathrm{Inv}(\mathcal{O})$) for the monoid of invertible two-sided $\mathcal{O}$-ideals (resp. the group of invertible two-sided $\mathcal{O}$-ideals). We define $\mathrm{Pic}(\mathcal{O})$ to be the quotient of $\mathrm{Inv}^+(\mathcal{O})$ by the normal subgroup of principal two-sided fractional ideals.

We now come down to earth and restrict our attention to the case in which case R is a Hasse domain with its canonical norm. In this case, for any R-lattice I in A, we define $||I||$ to be the fractional R-ideal generated by the reduced norms $n(x)$ of the elements x of I. It is not difficult to see that the function $|| \, ||$ gives a nondegenerate homomorphism of monoids from the monoid $\mathrm{Inv}^+(\mathcal{O}) = \mathcal{I}(\mathcal{O})$ of two-sided integral $\mathcal{O}$-ideals to $\mathbb{Z}^+$. However (as usual in this subject) we are more interested in one-sided $\mathcal{O}$-ideals (even though they are more complicated). We need the following result.

Lemma 33. *Let I be a proper right $\mathcal{O}$-ideal, J a proper left $\mathcal{O}$-ideal, let M be an R-lattice in A, and let $x \in A^\bullet$. Then:*
a) $||IJ|| = ||I||||J||$.
b) $||xM|| = ||Mx|| = |n(x)|||M||$.

Proof. See Exercise 2.12 on p. 51 of John Voight's book! □

Definition: Let $\mathcal{O}$ be a free R-order in the associative K-division algebra A, and let $||\ ||$ be an $\mathrm{Inv}^+(\mathcal{O})$-norm on $\mathcal{O}$. A two-sided fractional $\mathcal{O}$-ideal E is **Euclidean** for $||\ ||$ if for all $x \in A$ there exists $y \in E$ such that

$$||x - y|| < ||I||. \tag{3}$$

Remark 4.3.1: When $E = \mathcal{O}$, we recover the notion of a norm Euclidean order.

Remark 4.3.2: If the fractional ideal E is Euclidean, so are xE and Ex for all $x \in A^\bullet$. Thus it makes sense to speak of Euclidean ideal classes $[E]_\ell$ and $[E]_r$.

From the perspective of our study of Euclidean forms, the motivation for this construction is the following result.

♣ For the following Prop, it seems associativity is not used.

Proposition 34. *Let E be a Euclidean ideal of $\mathcal{O}$ which is free as an R-module. Let $n : A \to K$ be the norm map. For $x \in E$, put $f(x) = \frac{n(x)}{||E||}$. Then upon choosing an isomorphism $I \cong R^{\dim_K A}$, f defines a Euclidean form on R of degree equal to that of n in $\dim_K A$ variables. In particular, if $A_{/K}$ is a quadratic field extension (resp. a quaternion algebra), f is a binary (resp. quaternary) quadratic form.*

On the other hand, the existence of Euclidean ideals is of some interest in its own right, because it places restrictions on the ideal theory of $\mathcal{O}$. This observation was made in the commutative case by H.W. Lenstra [Le79]. In the next two results we extend Lenstra's work to the non-commutative case.

Theorem 35. *Let E be a Euclidean fractional ideal in $(\mathcal{O}, ||\ ||)$. For every proper right fractional $\mathcal{O}$-ideal I, there exists $n \in \mathbb{Z}^+$ such that $[IE^n]_\ell = [\mathcal{O}]_\ell$.*

Proof. If $[E]_\ell = [\mathcal{O}]_\ell$, then by Remark 4.3.2 $\mathcal{O}$ is itself Euclidean and Proposition 30 implies that every right $\mathcal{O}$-ideal is principal: a much stronger conclusion! So we may assume that E is *not* of the form $\mathcal{O}x$ for $x \in A$. For similar reasons we may assume that E is an integral $\mathcal{O}$-ideal.

Following Lenstra we introduce the quantity $\Psi(I) := ||I||^{-1}$. Again because the conclusion depends only on the left classes of the ideals involved, it is no loss of generality to assume that $I \supset \mathcal{O}$. Thus $\Psi(I) \in \mathbb{Z}^+$ and we will prove result by induction on $\Psi(I)$, the case $\Psi(I) = 1$ again being trivial.

To perform the induction step, choose $x \in IE \setminus E$. By the Euclidean condition, there exists $y \in E$ such that $||x - y|| < ||E||$. Put $z := x - y$. Then $\Psi(z^{-1}E) \leq 1$. In fact equality here is equivalent to $E = z\mathcal{O}$, a case which we have already ruled out, so in fact $\Psi(z^{-1}E) < 1$. Using Lemma 33 we get

$$\Psi(z^{-1}IE) = |n(z)|^{-1}\Psi(IE) = |n(z)|^{-1}\Psi(I)\Psi(E) = \Psi(z^{-1}E)\Psi(I) < \Psi(I).$$

Since $z \in IE$, $\Psi(z^{-1}IE) \in \mathbb{Z}^+$; moreover the right order of $z^{-1}IE$ is $\mathcal{O}$. Therefore by induction there exists m with

$$[\mathcal{O}]_\ell = [(z^{-1}IE)E^m]_\ell = [IE^{m+1}]_\ell.$$

□

Remark 4.3.3: Of course there is an analogue of Theorem 35 for left ideals.

Theorem 36. *Suppose $A_{/K}$ is a central division algebra and $\mathcal{O}$ is a maximal R-order in A. Moreover, suppose that there exists $N \in \mathbb{Z}^+$ such that $\mathrm{Pic}(R) = \mathrm{Pic}(R)[N]$, and let $A_{/K}$ be a central division algebra with $\dim_K A = P^2$. Then if $\mathcal{O}$ admits a Euclidean ideal E, we have*

$$\#\,\mathrm{Pic}_\ell(\mathcal{O}) = \#\,\mathrm{Pic}_r(\mathcal{O}) \leq NP.$$

Proof. Since the center of $\mathcal{O}$ is equal to R, the Picard group $\mathrm{Pic}(\mathcal{O})$ of $\mathcal{O}$ is canonically isomorphic to the *central Picard group* $\mathrm{Picent}(\mathcal{O})$ [Re75, Thm. 37.18]. We have a short exact sequence

$$1 \to \mathrm{Pic}(R) \to \mathrm{Picent}(\mathcal{O}) \to \prod_{\mathfrak{p}} \mathbb{Z}/e_{\mathfrak{p}}\mathbb{Z} \to 1,$$

where the product extends over all $\mathfrak{p} \in \Sigma_R$ which ramify in $\mathcal{O}$, and $e_{\mathfrak{p}}$ is the ramification index of A at $\mathfrak{p}$. By [Re75, Thm. 13.17], for all $\mathfrak{p} \in \Sigma_R$ one has $e_{\mathfrak{p}} \mid P$. It follows that $\mathrm{Pic}(\mathcal{O}) = \mathrm{Pic}(\mathcal{O})[NP]$ is an NP-torsion abelian group.

Applying this to the class $[E]$ of E in $\mathrm{Pic}(\mathcal{O})$ we get that for all $n \in \mathbb{Z}^+$, there exists $1 \leq i \leq NP$ such that $E^{-n} = x_n E^i$ for some $x_n \in A^\bullet$ (in fact such that $x\mathcal{O} = \mathcal{O}x$, but this is not needed). Using Theorem 35, for any projective left $\mathcal{O}$-ideal I we have $IE^n = x_I\mathcal{O}$ for some $x_I \in A^\bullet$. Multiplying on the right by E^{-n} gives $I = x_i E^{-n} = x_i x_n E^i$, so $[I]_\ell = [E^i]_\ell$ for some $1 \leq i \leq NP$. This gives the conclusion for $\mathrm{Pic}_\ell(\mathcal{O})$. It works the same way for $\mathrm{Pic}_r(\mathcal{O})$; alternatively, the map $I \mapsto I^{-1}$ (always) induces a bijection between the left and right Picard sets. □

♣ Try to squeeze the following out of the proof:

♣ 1. Uniqueness (in some sense!) of the Euclidean ideal class E

♣ 2. Does the existence of E imply that $\mathcal{O}$ is hereditary?

We immediately derive the following quaternionic analogue of a result of Lenstra on Euclidean ideal classes in the ring of integers of a quadratic number field.

Corollary 37. *Let $(R, |\ |)$ be a normed PID with fraction field K, $B_{/K}$ a division quaternion algebra. If there exists a maximal order $\mathcal{O}$ and a Euclidean $\mathcal{O}$-ideal class, then the class number of B – i.e., the number of either left or right ideal classes for any maximal R-order in B – is either 1 or 2.*

5.4. **Binary forms associated to Euclidean quadratic orders and ideals. Rewrite this to be a special case of the above construction!**

Let $(R, |\ |)$ be a PID with fraction field K (of characteristic not 2, as usual). As in §1, since R is a PID, the given norm may equally well be viewed as an ideal norm, and we shall do so.

Let $L = K(\sqrt{D})$ be a quadratic extension of K and let S be a quadratic R-order of L, i.e., an R-subalgebra of L which is free of rank 2 as an R-module and such that $S \otimes_R K = L$. Let $\alpha \mapsto \overline{\alpha}$ be the nontrivial element of $\mathrm{Aut}(L/K)$: we assume that $\overline{S} = S$ and $S^{\mathrm{Aut}(L/K)} = R$, so that $\alpha \mapsto |\alpha\overline{\alpha}|$ is a norm on S. This allows us to define a norm on ideals of S, $|\mathfrak{c}|_S := |\mathfrak{c}\overline{\mathfrak{c}}|$.

Example 13: take R to be a PID satisfying the condition (FN) and $|\ |$ the canonical

norm. Let L be a quadratic extension of K (the fraction field of R) and let S be the integral closure of R in L. Then S satisfies the above hypotheses, and moreover, for a nonzero ideal $\mathfrak{c}$ of S, $|\mathfrak{c}| = \#S/\mathfrak{c}$. (In particular, we may take $R = \mathbb{Z}$!)

Let $\mathfrak{c}$ be an invertible integral ideal of S. To the ideal $\mathfrak{c}$ we will assign a quadratic form $q_{\mathfrak{c}}$, which up to multiplication by a unit of R, is well-defined and depends only on the class of $\mathfrak{c}$ in $\mathrm{Pic}(S)$.

Since $\mathfrak{c}$ is invertible, it is a rank 1 locally free S-module and thus a rank 2 locally free R-module. Since R is a PID, $\mathfrak{c}$ is in fact free of rank 2 as an R-module, i.e., we may choose $\alpha, \beta \in \mathfrak{c}$ such that $\mathfrak{c} \cong_R R\alpha \oplus R\beta$. Moreover $\mathfrak{c}\overline{\mathfrak{c}}$ is a nonzero ideal of the PID R; let c be a generator of this ideal. (Note that c is uniquely determined up to an element of $R^\times$ and it is here that the unit ambiguity arises in our construction.) We define

$$q_{\mathfrak{c}}(x_1, x_2) = \frac{(x_1\alpha + x_2\beta)\overline{((x_1\alpha + x_2\beta)}}{c}.$$

The numerator of q is $(\alpha\overline{\alpha})x_1^2 + (\alpha\overline{\beta} + \overline{\alpha}\beta)x_1x_2 + (\beta\overline{\beta})x_2^2$; clearly each of $\alpha\overline{\alpha}, \alpha\overline{\beta}, \overline{\alpha}\beta, \beta\overline{\beta}$ lie in $\mathfrak{c}\overline{\mathfrak{c}} = cR$ hence are all divisible by c, so that indeed $q_{\mathfrak{c}} \in R[x_1, x_2]$. It is easy to see that $q_{\mathfrak{c}}$ is anisotropic.

Remark 7: The ideal $\mathfrak{c}$ is principal iff the quadratic form $q_{\mathfrak{c}}$ is (up to a unit) principal, i.e., represents 1 so can be put in the form $x_1^2 + bx_1x_2 + cx_2^2$.

The binary form $q_{\mathfrak{c}}$ is Euclidean (with respect to the fixed norm $|\ |$ on R) iff for all $x = (x_1, x_2) \in K^2$, there exists $y = (y_1, y_2) \in R^2$ such that

$$|q_{\mathfrak{c}}(x - y)| < 1,$$

i.e., iff

$$|(x_1 - y_1)\alpha + (x_2 - y_2)\beta|_S < |\mathfrak{c}|.$$

Putting $X = x_1\alpha + x_2\beta$ and $Y = x_1\alpha + y_2\beta$, the conditions are equivalent to: for all $X \in L$ and $Y \in \mathfrak{c}$, $|X - Y|_S < |\mathfrak{c}|_S$. This is precisely the condition for the ideal class $\mathfrak{c}$ of the normed ring $(S, |\ |_S)$ to be Euclidean in the sense of [Le79].

We may therefore make use of Lenstra's results, as follows:

Theorem 38. *(Lenstra) Suppose that the binary quadratic form $q_{\mathfrak{c}}$ is Euclidean. Then S is a Dedekind domain,* $\mathrm{Pic}(S) = \langle[\mathfrak{c}]\rangle$, *and* $\#\,\mathrm{Pic}(S) \leq 2$.

Theorem 39. *(Lenstra) Let $R = \mathbb{Z}$ with its canonical norm, $L = \mathbb{Q}(\sqrt{D})$ be a quadratic field, and let $S = \mathbb{Z}_L$ be the ring of integers of L. Then S admits a non-principal ideal class iff $D \in \{-20, -15, 40, 60, 85\}$.*

The corresponding nonprincipal Euclidean binary quadratic forms are:

$$2x_1^2 + 2x_1x_2 + 3x_2^2,\ 2x_1^2 + x_1x_2 + 2x_2^2,\ 2x_1^2 - 5x_2^2,\ 3x_1^2 - 5x_2^2,\ 3x_1^2 - 7x_1x_2 - 3x_2^2.$$

Theorem 40. *Let $D < 0$ be a fundamental discriminant, and let q_D be the norm form of the imaginary quadratic order of discriminant D. Then:*
a) If $D \equiv 0 \pmod 4$, $E(q_D) = \frac{|D|+4}{16}$.
b) If $D \equiv 1 \pmod 4$, $E(q_D) = \frac{(|D|+1)^2}{16|D|}$.

Thus the complete list of principal positive definite Euclidean forms is as follows:

- $q_{-3}(x,y) = x^2 + xy + y^2$, $E(q_{-3}) = \frac{1}{3}$.
- $q_{-4}(x,y) = x^2 + y^2$, $E(q_{-4}) = \frac{1}{2}$.
- $q_{-7}(x,y) = x^2 + xy + 2y^2$, $E(q_{-7}) = \frac{4}{7}$.
- $q_{-11}(x,y) = x^2 + xy + 3y^2$, $E(q_{-11}) = \frac{9}{11}$.

By the work of Lenstra, the remaining primitive, positive definite binary Euclidean forms over $\mathbb{Z}$ are

$$q_{-15} = 2x^2 + xy + 2y^2, \ E(q_{-15}) = \frac{4}{5},$$

$$q_{-20} = 2x^2 + 2xy + 3y^2, E(q_{-20}) = \frac{9}{10}.$$

the nonprincipal forms of discriminants -15 and -20, respectively.

5.5. **Quaternary forms attached to Euclidean quaternion orders and ideals.**

Let $(R, |\ |)$ be a Hasse domain, $A_{/K}$ a division quaternion algebra, and let $\mathcal{O}$ be a maximal, free R-order in A, and suppose that $\mathcal{O}$ admits a two-sided Euclidean ideal E. By Corollary 37, the class number of $\mathcal{O}$ – and thus of A itself, since all maximal orders have the same class number – is either 1 or 2.

Let us consider the case of definite quaternion algebras over $R = \mathbb{Z}$. In this case, there is the following well-known formula for the class number $h(A)$ of A in terms of its reduced discriminant D due to Eichler:

$$h(A) = \frac{1}{12} \prod_{p \mid D} (p-1) + \frac{1}{4} \prod_{p \mid D} \left(1 - (\frac{-4}{p})\right) + \frac{1}{3} \prod_{p \mid D} \left(1 - (\frac{-3}{p})\right).$$

From this one easily computes

$$h(A) = 1 \iff D \in \{2,3,5,7,13\},$$

$$h(A) = 2 \iff D \in \{11,17,19,30,42,70,78\}.$$

As a check on the accuracy of this calculation, we note that it agrees with the results of [**?**], who enumerate all Eichler $\mathbb{Z}_F$-orders in totally definite quaternion algebras over all totally real number fields F of class number at most 2.

Now using the MAGMA programming language it is a short, straightforward computation to determine which of these quaternion algebras give rise to two-sided Euclidean ideals for some maximal $\mathbb{Z}$-order $\mathcal{O}$.

Consider first the case in which $h(A) = 1$. Since the type number is always less than or equal to the class number, this implies that the type number is one – i.e., there is up to conjugacy a unique maximal order. The MAGMA command `MaximalOrder` automatically supplies one maximal order $\mathcal{O}$ in a given quaternion algebra over a number field. If $B = e_1, \ldots, e_4$ is a $\mathbb{Z}$-basis for $\mathcal{O}$, then the Hessian matrix of the quadratic norm form has (i,j) entry `Trace(B[i]*Conjugate(B[j]))` . Dividing by 2 yields the Gram matrix, say M, and the MAGMA command `CoveringRadius(LatticeWithGram(M))` computes the Euclideanity of the norm

form. The results are as follows:

$E(q_2) = \frac{1}{2}$.
$E(q_3) = \frac{2}{3}$.
$E(q_5) = \frac{4}{5}$.
$E(q_7) = \frac{8}{7}$.
$E(q_{13}) = \frac{20}{13}$.

Thus there are precisely three norm-Euclidean definite quaternion orders over $\mathbb{Z}$. The corresponding quadratic forms are:

$q_2 : x_1^2 + x_1x_2 + x_1x_3 + x_1x_4 + x_2^2 + x_2x_4 + x_3^2 + x_3x_4 + x_4^2$
$q_3 : x_1^2 + x_1x_2 + x_2^2 + x_3^2 + x_3x_4 + x_4^2$
$q_5 : x_1^2 + x_1x_2 + x_1x_3 + x_1x_4 + x_2^2 + x_2x_3 + 2x_3^2 + 2x_3x_4 + 2x_4^2$.

This same classification has recently been done by R.W. Fitzgerald [Fi10] by other means.[7]

Let us now consider the cases of class number 2. These naturally subdivide into $D = 11, 17, 19$ (prime discriminant) and $D = 30, 42, 70, 78$.

When $D = 11, 17, 19$, the type number of A is equal to 2: that is, there are precisely two nonconjugate maximal orders, say $\mathcal{O}_1$ and $\mathcal{O}_2$. We can compute this in MAGMA by starting with one maximal order `O1 := MaximalOrderQuaternionAlgebra(D)`, computing a set of representatives for the left-ideal classes of $\mathcal{O}_1$
`LL1 := LeftIdealClasses(O1)` and comparing the corresponding right orders
`IsIsomorphic(RightOrder(LL1[1]),RightOrder(LLL1[2])` .

We find in all three cases that these right-orders are not isomorphic. Let I to be the unique class of ideal with right-order $\mathcal{O}_1$ and nonconjugate right order $\mathcal{O}_2$. In particular, there are no nonprincipal two-sided $\mathcal{O}_1$-ideals, hence, since the class number is greater than 1, no two-sided Euclidean $\mathcal{O}_1$-ideals. Doing the same for the maximal order $\mathcal{O}_2$, we find again that the unique class of nonprincipal left $\mathcal{O}_2$-ideals is represented by a one-sided ideal. Of course this should not be a surprise, since $[\overline{I}] = [I^{-1}]$ represents that class. In summary, the **Brandt groupoid** has the following structure in this case: it may be viewed as a graph with two vertices, corresponding to $\mathcal{O}_1$ and $\mathcal{O}_2$. Each of these vertices has a single loop, corresponding to the two-sided ideal $\mathcal{O}_i$. Moreover, there is one oriented edge running from $\mathcal{O}_1$ to $\mathcal{O}_2$ corresponding to I and one oriented edge running from $\mathcal{O}_2$ to $\mathcal{O}_1$ corresponding to I^{-1}. It is easy to see that the norm form on the ideal class $[I^{-1}] = [\overline{I}]$ is the same as that on I, so altogether we get 3 nonisomorphic quadratic forms, q_1, q_2, q_3 which give a full set of representatives for the genus of any one of them. In particular, each q_i had class number 3, as one confirms using the MAGMA command
`# GenusRepresentatives(L)` on each of the quadratic lattices L.

When $D = 30, 42, 70, 78$, the Brandt groupoid has a different and simpler structure

[7]His work was done first, and we acknowledge it as a motivation for developing the present theory.

(the same in all four cases): in all four cases the type number is one, i.e., there is a unique (up to conjugacy) maximal order $\mathcal{O}$. Since the class number is 2, it follows that there is a unique nonprincipal two-sided ideal I. This is an auspicious sign for the existence of Euclidean ideals, but it turns out that nevertheless in all all four cases the ideal is not Euclidean. Indeed the Euclideanities of norm forms associated to $\mathcal{O}$ and I are as follows:

$$D = 30: \ E(\mathcal{O}) = \frac{11}{3}, \ E(I) = \frac{7}{3}.$$
$$D = 42: \ E(\mathcal{O}) = \frac{11}{2}, \ E(I) = \frac{5}{2}.$$
$$D = 70: \ E(\mathcal{O}) = \frac{243}{35}, \ E(I) = \frac{27}{7}.$$
$$D = 78: \ E(\mathcal{O}) = \frac{161}{26}, \ E(I) = \frac{119}{26}.$$

The maximal order $\mathcal{O}$ in the rational quaternion algebra of discriminant 2 is none other than the Hurwitz order $\mathbb{Z}[1, i, j, k, \frac{1+i+j+k}{2}]$. This perhaps the most famous of all non-commutative Euclidean rings, and its Euclidean property is used in one of the well-known proofs of the Four Squares Theorem. From our perspective, it is immediate from our theory that the form q_2 is positive universal. On the other hand, the four squares form corresponds to the nonmaximal order $\mathbb{Z}[1, i, j, k]$. Thus some argument is necessary in order to pass from the universality of q_2 to that of the Four Squares Theorem: this is due to Hurwitz. Extensions of this argument to show that certain other nonmaximal diagonal quaternary forms are Euclidean are considered in [Fi10].

5.6. **A Euclidean octonion order.**

There is a unique division octonion algebra $A_{/\mathbb{Q}}$, whose norm form is the sum of eight squares form. Moreover, there are precisely 7 maximal $\mathbb{Z}$-orders $\mathcal{O}$ in A. These 7 orders are isomorphic as algebras and also give rise to a unique (up to isomorphism) quadratic $\mathbb{Z}$-lattice q: namely the E_8-root lattice scaled by a factor of $\frac{1}{2}$. The Euclideanities of all of the root lattices are classically known (see e.g. [CSl99]) and in particular one has $E(q) = \frac{1}{2}$. It follows that the octonion order $\mathcal{O}$ is norm Euclidean!

These facts are given a stylish presentation in [CSm03, Ch. 9]. They also explore the ideal theory of $\mathcal{O}$, which is surprisingly meager: it turns out that the only (left-, right- or two-sided ideals) in $\mathcal{O}$ are $n\mathcal{O}$ for $n \in \mathbb{Z}^+$. In particular there is no hope of deriving further Euclidean forms from the ideals of $\mathcal{O}$.

6. Maximal Lattices, Hasse Domains and Complete DVRs

6.1. **CDVRs and Hasse Domains.**

Let (R, v) be a discrete valuation ring (DVR) with fraction field K and residue field k. As usual, we require that the characteristic of K be different from 2; however, although it is invariably more troublesome, we certainly must admit the case in which k has characteristic 2: such DVRs are called **dyadic**. We will be especially interested in the case in which R is complete, a **CDVR**.

A **Hasse domain** is the ring of S-integers in a number field K (where S is some finite set of places of K including all of the Archimedean place) or the coordinate ring of a regular, integral algebraic curve over a finite field $k = \mathbb{F}_q$. (The terminology is taken from [OM00].) In particular, a Hasse domain is a Dedekind abstract number ring.

Let Σ_K denote the set of all places of K, including Archimedean ones in the number field case. Let $\Sigma_R = \Sigma_K \setminus S$ denote the subset of Σ_K consisting of places which correspond to maximal ideals of R; these places will be called *finite*. The completion R_v of a Hasse domain R at $v \in \Sigma_R$ is a CDVR with finite residue field.

If R is a Hasse domain and Λ is a quadratic R-lattice in the quadratic space (V, q), then to each $v \in \Sigma_R$ we may attach the local lattice $\Lambda_v = \Lambda \otimes_R R_v$. Being a finitely generated torsion-free module over the PID R_v, Λ_v is necesssarily free. In particular, we may define δ_v, the valuation of the discriminant over R_v and then the global discriminant may be defined as the ideal $\Delta(\Lambda) = \prod_{v \in \Sigma_R} \mathfrak{p}_v^{\delta_v}$.

Lemma 41.
a) The R-lattice Λ is maximal iff Λ_v is a maximal R_v-lattice for all $v \in \Sigma_R$.
b) For any nondyadic *place v such that $\delta_v(\Lambda) \leq 1$, the lattice Λ_v is R_v-maximal.*

6.2. **Classification of Euclidean forms over CDVRs.**

In this section R is a CDVR with fraction field K of characteristic different from 2, endowed with the norm $|\ |_a$ (for some $a \geq 2$) of Example 3. In this setting we can give a very clean characterization of Euclidean forms.

Theorem 42. *A quadratic form over a complete discrete valuation domain is Euclidean for the canonical norm iff the corresponding quadratic lattice is maximal.*

For the proof we require the following preliminary results.

Theorem 43. *(Eichler's Maximal Lattice Theorem) Let q be an anisotropic quadratic form over a complete discrete valuation field K with valuation ring R. Then there is a unique maximal R-lattice for q, namely*

$$\Lambda = \{x \in K^n \mid q(x) \in R\}.$$

Proof. See [Ei52] or [Ge08, Thm. 8.8]. □

Theorem 44. *Let (V, q) be a finite-dimensional quadratic space over K and $\Lambda \subset V$ a maximal quadratic R-lattice. Then there exists a decomposition*

$$V = \bigoplus_{i=1}^{r} \mathbb{H}_K \oplus V'$$

with $q|_{V'}$ anisotropic such that

$$\Lambda = \bigoplus_{i=1}^{r} \mathbb{H}_R \oplus \Lambda',$$

where $\Lambda' = \Lambda \cap V'$.

Proof. See [Sh10, Lemma 29.8], wherein the result is stated for complete discrete valuation rings with finite residue field. However, it is easy to see that the finiteness of the residue field is not used in the proof. □

Proof of Theorem 42: According to Proposition 16, a Euclidean form over any normed ring is maximal, so it is enough to suppose that q is maximal and deduce that it is Euclidean.

Suppose first that q is anisotropic over R. In this case, the Euclideanness of q follows immediately from Eichler's Maximal Lattice Theorem: indeed, we have $R^n = \{x \in K^n \mid |q(x)|_a \geq 1\}$, where $|x|_a = a^{v(x)}$ is the norm of Example 4. Therefore, $x \in K^n \setminus R^n \iff |q(x)|_a = |q(x-0)|_a < 1$.
We now deal with the general case. By Theorem 44, we may write $\Lambda = \bigoplus_{i=1}^r \mathbb{H}_R \oplus \Lambda'$ with Λ' anisotropic. With respect to a suitable R-basis of Λ, q takes the form

$$q(X) = q(x, x') = x_1x_2 + \ldots + x_{2r-1}x_{2r} + q'(x'),$$

where $x' = (x_{2r+1}, \ldots, x_n)$ and q' is anisotropic. Let $X = (x, x') \in K^n \setminus R^n$. We must find $Y = (y, y') \in R^n$ such that $v(q(X - Y))) < 0$. By symmetry, we may assume that $v(x_1x_2) \geq \ldots \geq v(x_{2r-1}x_{2r})$ and $v(x_{2r}) \leq v(x_{2r-1})$.
Case 1: $v(x_{2r}) \geq 0$. Then $x = (x_1, \ldots, x_{2r}) \in R^{2r}$ so that we must have $x' \in K^{n-2r} \setminus R^{n-2r}$. Put $Y = (y, y') = 0$. Then $v(x_1x_2 + \ldots + x_{2r-1}x_{2r}) \geq 0$, whereas by Eichler's Maximal Lattice Theorem, $v(q'(x')) < 0$, so

$$v(q(X)) = v(x_1x_2 + \ldots + x_{2r-1}x_{2r} + q'(x')) < 0.$$

Case 2: $v(x_{2r}) < 0$. We choose $y' = 0$ and $y_1 = \ldots = y_{2r-2} = 0$. Also define

$$\alpha = q_2(x'),\ \beta = x_1x_2 + \ldots + x_{2r-3}x_{2r-2}.$$

If $v(\alpha + \beta + x_{2r-1}x_{2r}) \leq v(x_{2r})$, then since $v(x_{2r}) < 0$, we may take $y = 0$, getting

$$v(q(X)) = v(\alpha + \beta + x_{2r-1}x_{2r}) < 0.$$

If $v(\alpha + \beta + x_{2r-1}x_{2r-2}) > v(x_{2r})$, we may take $y_{2r-1} = 1$, $y_{2r} = 0$, getting

$$v(q(X - Y)) = v(\alpha + \beta + x_{2r-1}x_{2r} - x_{2r}) = v(x_{2r}) < 0.$$

Corollary 45. *Let R be a Hasse domain and $q_{/R}$ a quadratic form. Then q is locally Euclidean iff the corresponding lattice Λ_q is maximal.*

Proof. This is an immediate consequence of Theorem 42 and Lemma 41. □

6.3. **ADC forms over Hasse domains.**

Let $q_{/R}$ be a nondegenerate quadratic form. We define the **genus** $\mathfrak{g}(q)$ as follows: it is the set of R-isometry classes of quadratic forms q' such that: for each $v \in S$, $q \cong_{K_v} q'$, and for each $v \in \Sigma_R$, $q \cong_{R_v} q'$.

Theorem 46. *For any nondegenerate quadratic form q over a Hasse domain R, the genus $\mathfrak{g}(q)$ of q is finite.*

Proof. See e.g. [OM00, Thm. 103:4]. □

This allows us to define the **class number** $h(q)$ of a quadratic form q as $\#\mathfrak{g}(q)$. Of particular interest are forms of class number one, i.e., for which q is (up to isometry) the only form in its genus.

A quadratic form $q_{/R}$ is **regular** if it R-represents every element of R which is represented by its genus. In other words, q is regular if for all $d \in R$, if there is $q' \in \mathfrak{g}(q)$ and $x \in R^n$ such that $q'(x) = d$, then there is $y \in R^n$ such that $q(y) = d$.

Theorem 47. *Let $q_{/R}$ be a nondegenerate quadratic form over a Hasse domain, and let $d \in R$. Suppose that for all $v \in S$, q K_v-represents d and for all $v \in \Sigma_R$, q R_v-represents d. Then there exists $q' \in \mathfrak{g}(q)$ such that q' R-represents d.*

Proof. [OM00]. □

Theorem 48. *For a quadratic form q over a Hasse domain R, TFAE:*
(i) q is an ADC form.
(ii) q is regular and "locally ADC": for all $\mathfrak{p} \in \Sigma(R)$, q is ADC over $\mathfrak{p}$.

Proof. (i) $\implies$ (ii): Suppose q is ADC. By our theorems on localization, q is locally ADC. Now let $d \in R$ be represented by the genus of q: i.e., there exists $q' \in \mathfrak{g}(q)$ such that q' R-represents d. Since for all $v \in \Sigma_K$, $q' \cong_{K_v} q$, it follows that q K_v-represents d for all v. By Hasse-Minkowski, q K-represents d, and since q is an ADC-form, q R-represents d.
(ii) $\implies$ (i): Suppose q is regular and locally ADC, and let $d \in R$ be K-rationally represented by q. Then for all $v \in \Sigma(R)$, d is K_v-represented by q, hence using the local ADC hypothesis, is R_v-represented. Moreover, for all places $v \in \Sigma(K) \setminus \Sigma(R)$, d is K_v-represented by q. By Theorem 47, there exists $q' \in \mathfrak{g}(q)$ which R-represents d, and then by definition of regular, q R-represents d. □

A quadratic form q over a Hasse domain R is **sign-universal** if for all $d \in R$, if q K_v-represents d for all real places $v \in \Sigma_K$, then q R-represents d.

Proposition 49. *Let $n \geq 4$, and let $q(x_1, \ldots, x_n)$ be a nondegenerate quadratic form over a Hasse domain R. Then q is ADC iff it is sign-universal.*

Proof. Indeed, by the Hasse-Minkowski theory of quadratic forms over global fields, any nondegenerate quadratic form in at least four variables over the fraction field K is sign-universal. The result follows immediately from this. □

6.4. **Definite quadratic forms over $\mathbb{Z}$.**

In the case of $R = \mathbb{Z}$, Conjecture 59 is related to some classical problems and work in the geometry of numbers. Especially, the classification of definite Euclidean forms $q_{/\mathbb{Z}}$ can be rephrased as the classification of all integral lattices in Euclidean space with **covering radius** strictly less than 1. This problem has been essentially solved by G. Nebe [Ne03]: in particular, her paper contains 69 Euclidean lattices.

W.C. Jagy and I had been independently searching for Euclidean lattices before we learned of Nebe's work. When we compared our list (not claimed to be complete) to hers, we found that she lists several lattices we had not found. However, one of our Euclidean lattices does not appear on Nebe's list, namely

$$q(x_1, x_2, x_3, x_4, x_5) = x_1^2 + x_1x_4 + x_2^2 + x_2x_5 + x_3^2 + x_3x_5 + x_4^2 + x_4x_5 + 2x_5^2.$$

We are of the opinion that the method behind the classification – namely a clever exploitation of root sublattices – is sound and the error is one of tabulation only. Needless to say, it seems worthwhile to revisit this classification and check whether

there are indeed only $70 = 69 + 1$ Euclidean lattices over $\mathbb{Z}$, and Jagy and I plan to do this in a future joint paper.

Each of these $69 + 1$ Euclidean lattices has class number one. Therefore verifying Nebe's work will probably show that Conjecture 60 holds for definite quadratic forms over $\mathbb{Z}$. The case of indefinite forms seems much more difficult, for instance because the indefinite forms of class number one are believed to be infinite in number.

Let us turn now to definite ADC forms over $\mathbb{Z}$.

Unary forms: A unary form $q_a(x) = ax^2$ is ADC iff a is squarefree. In particular there are infinitely many definite unary forms over $\mathbb{Z}$.

Binary forms: The classical genus theory shows that a regular binary form $q(x, y) = ax^2 + bxy + cy^2$ has class number one in the above sense. Alternately, if $\Delta = b^2 - 4ac$ is the discriminant of q, q is regular iff the Picard group of the quadratic order of discriminant Δ has exponent dividing 2. The disccriminants $\Delta \equiv 0 \pmod 4$ in question are precisely Euler's idoneal numbers. This set is known to be finite but its explicit computation is known only conditionally on the Generalized Riemann Hypothesis (GRH). Assuming GRH, it becomes a finite problem to determine all ADC forms, and we will address this in a future work.

Ternary forms: Again there are only finitely many definite regular ternary forms.

Theorem 50. *(Jagy-Kaplansky-Schiemann* [JKS97]*) There are at most* 913 *primitive positive definite regular forms* $q(x_1, x_2, x_3)_{/\mathbb{Z}}$.

More precisely, in [JKS97] the authors write down an explicit list of 913 definite ternary forms such that any regular form must be equivalent to some form in their list. Further they prove regularity of 891 of the forms in their list, whereas the regularity of the remaining 22 forms is conjectured but not proven.

Fortunately, all 22 of the forms whose regularity was not shown by Jagy-Kaplansky-Schiemann are seen *not* to be ADC by the easy method of finding integers a and b such that the form represents a^2b but not b. Indeed, Jagy has found such "non-ADC certificates" for most of the regular ternary forms: this process leads to a list of 104 definite ternary regular forms which are probably ADC. By Theorem 48, it suffices to decide whether each of these forms are locally ADC over $\mathbb{Z}_p$ for all primes p. These local calculations are certainly doable but somewhat intricate and are deferred to a later work.

$n = 4$: A quadratic form $q_{/\mathbb{Z}}$ in at least four variables is ADC iff it is sign-universal. Thus the following result solves the problem for us when $n = 4$.

Theorem 51. *(Bhargava-Hanke* [BH05]*) There are precisely* 6436 *positive definite sign-universal forms* $q(x_1, x_2, x_3, x_4)_{/\mathbb{Z}}$.

So there are precisely 6436 positive definite quaternary ADC forms over $\mathbb{Z}$.

$n \geq 5$: It seems hopeless to classify positive definite sign-universal forms in 5

or more variables. Certainly there are infinitely many such primitive forms, e.g. $x_1^2 + \ldots + x_{n-1}^2 + Dx_n^2$. More generally, any form with a sign-universal subform is obviously sign-universal, and this makes the problem difficult. However, there is the following relevant result.

Theorem 52. *(Bhargava-Hanke* [BH05]*) For $n \geq 4$, a positive definite quadratic form $q(x_1, \ldots, x_n)_{/\mathbb{Z}}$ is sign-universal iff it $\mathbb{Z}$-represents all of the following integers:*

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290.$$

Thus a definite integral form $q(x_1, \ldots, x_n)$, $n \geq 4$, is ADC iff it represents all the integers in the above list. So this is a sort of classification result for definite ADC forms in at least five variables, perhaps the best that can reasonably be hoped for.

6.5. **Some preliminary results over $\mathbb{Z}$.**

Lemma 53. *Let R be a nondyadic integrally closed local domain. Let $q(x)$ be a unimodular binary form over R. If q is isotropic, then it is hyperbolic, and in particular ADC.*

Proof. It is known that any form q over such a ring can be diagonalized [Ba78], so we may assume $q(x, y) = ax^2 + by^2$ with $a, b \in R^\times$. Moreover $q = a(x^2 + \frac{b}{a}y^2) \sim a(x^2 + aby^2)$ is isotropic iff $-ab$ is a square in the fraction field iff $-ab \in R^{\times 2}$ (since R is integrally closed). Therefore $q \sim a(x^2 - y^2) \sim axy$. The change of variables $(x, y) \mapsto (a^{-1}x, y)$ shows that $q \sim xy$, the hyperbolic plane. Thus q R-represents every element of R and is ADC. □

Theorem 54. *Let $a, b \in \mathbb{Z}^\bullet$ be relatively prime, and put $q(x, y) = ax^2 + by^2$.*
a) If $a, b \in \mathbb{Z}^+$ and $q(x, y)$ is ADC over $\mathbb{Z}$, then ab is squarefree.
a) Suppose ab is squarefree. Then q is an ADC form over $\mathbb{Z}$ iff it is regular and $ab \not\equiv -1 \pmod 8$.

Proof. a) Since a and b are coprime, ab is squarefree iff both a and b are squarefree. By symmetry, it is enough to show that a is squarefree. Suppose not: then there exists a prime p, $k, a' \in \mathbb{Z}^+$ and $\epsilon \in \{0, 1\}$ such that $a = p^{2k}p^\epsilon a'$ with $\gcd(a', p) = 1$. Now $q(1, 0) = a = (p^k)^2 p^\epsilon a'$, so since q is ADC, it $\mathbb{Z}$-represents $p^\epsilon a'$.
Case 1: $\epsilon = 1$. Then $1 < p^\epsilon a' < a$, so if $q(x, y) = p^\epsilon a' = pa'$, then $x = 0$, i.e., $by^2 = pa'$. Since $(p, b) = 1$, $\mathrm{ord}_p(by^2)$ is even, whereas $\mathrm{ord}_p(pa') = 1$, contradiction.
Case 2: Suppose $\epsilon = 0$. Then $a' < a$, so if $q(x, y) = p^\epsilon a' = a'$, then $x = 0$ and $by^2 = a'$, so $b \mid a'$. Since $\gcd(b, a') = 1$, this forces $b = 1$ and $a' = A^2$ i.e., $q(x, y) = p^{2k}A^2x^2 + y^2$. Thus q is $\mathbb{Q}$-equivalent to $x^2 + y^2$ so $\mathbb{Q}$-represents 2, but it clearly does not $\mathbb{Z}$-represent 2, contradiction.
b) Suppose $ab \equiv -1 \pmod 8$. Then q is $\mathbb{Z}_2$-equivalent to $a(x^2 - y^2)$. Note that the form $q' = x^2 - y^2$ over $\mathbb{Z}_2$ is isotropic but not hyperbolic: indeed it is does not represent any $d \in \mathbb{Z}_2$ with $\mathrm{ord}_2(d) = 1$. Since $a \in \mathbb{Z}_2^\times$, the same holds for $q \sim a(x^2 - y^2)$. So q is *not* ADC over $\mathbb{Z}_2$; by Corollary 22 it is *a fortiori* not ADC over $\mathbb{Z}$.

Now we assume that q is regular, ab is squarefree and $ab \not\equiv -1 \pmod 8$. We want to show that q is ADC: for this, by Theorem 48, it suffices to show that for all primes p, q is ADC as a form over $\mathbb{Z}_p$.
Case 1: $p \neq 2$, $\gcd(p, ab) = 1$.
We suppose first that $q(x, y)$ is isotropic, i.e., $-ab \in \mathbb{Z}_p^{\times 2}$. By Lemma 53 q is

hyerbolic, hence ADC. Otherwise $(\frac{-ab}{p}) = -1$ and q is anisotropic over $\mathbb{Z}_p$. Because $\mathrm{ord}_p(\mathrm{disc}(q)) = 1$, it is a *maximal* lattice in an anisotropic quadratic space. Using Theorem 6 and Corollary 7 of [**?**], such a form is necessarily Euclidean and thus ADC over $\mathbb{Z}_p$.
Case 2: $p \neq 2$, $\gcd(p, ab) = p$. Since $v_p(-\mathrm{disc}(q)) = 1$, q is again anisotropic over $\mathbb{Z}_p$ and gives a maximal lattice in its quadratic space, so it is once again ADC over $\mathbb{Z}_p$.
Case 3: $p = 2$. As above, q is isotropic over $\mathbb{Z}_2$ iff $-ab \in \mathbb{Q}_2^{\times 2}$ iff $ab \equiv 7 \pmod 8$. Since we are excluding this caes, q is anisotropic. If $ab \not\equiv 3 \pmod 4$, then again the lattice is maximal and arguing as before we deduce that q is ADC over $\mathbb{Z}_2$. The remaining case is $ab \equiv 3 \pmod 8$, when the lattice is *not* $\mathbb{Z}_2$-maximal. In this case q is $\mathbb{Z}_2$-equivalent to $a(x^2 + 3y^2)$. Since $a \in \mathbb{Z}_2^\times$ and ADC only matters up to unit equivalence, it comes down to showing that $x^2 + 3y^2$ is ADC over $\mathbb{Z}_2$. But indeed, as is well-known, it is ADC over $\mathbb{Z}$. One way to see this is as follows: the corresponding $\mathbb{Z}$-maximal lattice is $x^2 + xy + y^2$, which is Euclidean, hence ADC, and an elementary argument shows that every integer which is represented by $x^2 + xy + y^2$ is also represented by $x^2 + y^2$. (Or see [**?**, Cor. 18] in which in an elementary manner all integers represented by $x^2 + 3y^2$ are determined.) □

This result allows us to write down (conditionally on GRH) all primitive diagonal positive definite integral binary forms $q(x, y) = ax^2 + by^2$ which are ADC. The precise tabulation, together with the non-diagonal case, is left for a later work.

6.6. **Some preliminary results over $\mathbb{F}_p[t]$.**

Let $\mathbb{F}$ be a finite field of odd order, $\delta \in \mathbb{F}^\times \setminus \mathbb{F}^{\times 2}$,$R = \mathbb{F}[t]$ be endowed with its canonical norm, $K = \mathbb{F}(t)$, and ∞ be the infinite place of K (corresponding to the valuation $v_\infty(\frac{f}{g}) = \deg(g) - \deg(f)$), so that $K_\infty = K((\frac{1}{t}))$.

Recall that K has u-invariant 4: i.e., the maximum dimension of an anisotropic quadratic form over R is 4. We call a quadratic form $q_{/R}$ **definite** if q is anisotropic as a quadratic form over K_∞: in particular, such forms are aniostropic.

The following recent result is a significant departure from the number field case.

Theorem 55. *(Bureau* [Bu07]*) Suppose that $\#F > 3$. Then every regular definite form $q_{/\mathbb{F}[t]}$ has class number one.*

It is known that there are only finitely many definite quadratic forms over $\mathbb{F}[t]$ of any given class number. So it follows Conjectures 59 and 60 hold for definite quadratic forms over $\mathbb{F}[t]$ (except possibly when $\mathbb{F} = \mathbb{F}_3$).

In general the function field situation seems to be a bit more tractable than the number field case. Again we hope to give a complete classification of Euclidean and ADC forms over $\mathbb{F}_q[t]$ in a future work. However by making use of other recent work we can give some preliminary results.

Theorem 56. *For a definite quaternary quadratic form q over $\mathbb{F}[t]$, TFAE:*
(i) q is ADC.
(ii) q is universal.
(iii) The discriminant of q has degree 2.

Proof. (i) $\iff$ (ii) is a case of Proposition 49.
(ii) $\iff$ (iii): this is a result of W.K. Chan and J. Daniels [CD05, Cor. 4.3]. □

Theorem 57. *For a* diagonal *definite quaternary quadratic form q over $\mathbb{F}[t]$, TFAE:*
(i) q is Euclidean.
(ii) q is universal.
(iii) The discriminant of q has degree 2*.*

Proof.
(i) $\implies$ (ii) follows from Theorem 13 and Proposition 49.
(ii) $\implies$ (iii) is immediate from the previous result.
(iii) $\implies$ (i): Suppose

$$q = p_1x_1^2 + p_2x_2^2 + p_3x_3^2 + p_4x_4^2$$

with Without loss of generality, we may assume that $\deg(p_1) \leq \deg(p_2) \leq \deg(p_3) \leq deg(p_4)$. If $\deg(p_3) = 0$, then q contains a 3-dimensional constant subform and is thus isotropic. Since $\sum_i \deg(p_i) = 2$, the only other possibility is $\deg(p_1) = \deg(p_2) = 0$, $\deg(p_3) = \deg(p_4) = 1$, and now the fact that q is Euclidean follows from the Generalized Cassels-Pfister Theorem. □

Theorem 58. *If q is a* diagonal *definite ternary form over $\mathbb{F}[t]$ with $\deg(\Delta(q)) \leq 2$, then q is ADC.*

Proof. By [CD05, Thm. 3.5] any definite ternary form over $\mathbb{F}[t]$ with $\deg(\Delta(q)) \leq 2$ has class number one, hence is regular. Therefore, by Theorem 48 it is sufficient to show that q is locally ADC.

If $\deg(\Delta(q)) \leq 1$, then since R is nondyadic, the corresponding lattice is maximal, hence locally ADC by Theorem 48 and Corollary 45.

Suppose $\deg(\Delta(q)) = 2$ and write $q = p_1(t)x_1^2 + p_2(t)x_2^2 + p_3(t)x_3^2$ with $\deg(p_1) \leq \deg(p_2) \leq \deg(p_3)$. If $\deg(p_3) = 1$, then by the Generalized Cassels-Pfister Theorem q is Euclidean. Otherwise $\deg(p_1) = \deg(p_2) = 0$ and $\deg(p_3) = 2$. If p_3 is squarefree then so is $\Delta(q)$, hence q is maximal and thus locally ADC. Otherwise there exist $a \in \mathbb{F}^\times$, $b \in \mathbb{F}$ such that $p_3 = a(t-b)^2$, but then q is equivalent over K to the constant form $p_1x_1^2 + p_2x_2^2 + ax_3^2$ and is therefore isotropic, a contradiction. □

7. Conjectures and Open Problems

7.1. **Conjectures On Euclidean Forms.**

Conjecture 59. *For any Hasse domain R, there are only finitely many isomorphism classes of anisotropic Euclidean forms $q_{/R}$.*

Conjecture 60. *Let q be an anisotropic Euclidean quadratic form over a Hasse domain R. Then q has class number one.*

Conjecture 60 has a striking consequence. Consider the set $\mathcal{S}_1$ of all class number one totally definite quadratic forms defined over the ring of integers of some totally real number field. Work of Siegel shows that $\mathcal{S}_1$ is a finite set. Thus Conjecture 60 implies the following result, which we also state as a conjecture.

Conjecture 61. *As R ranges through all rings of integers of totally real number fields, there are only finitely many totally definite Euclidean quadratic forms $q_{/R}$.*

References

[Aub12] L. Aubry, Sphinx-Œdipe 7 (1912), 81-84.

[Ba78] R. Baeza, *Quadratic forms over semilocal rings*. Lecture Notes in Mathematics, Vol. 655. Springer-Verlag, Berlin-New York, 1978.

[BCC09] E. Bayer-Fluckiger, J.-P. Cerri, and J. Chaubert, *Euclidean minima and central division algebras*. Int. J. Number Theory 5 (2009), no. 7, 1155-1168.

[BH05] M. Bhargava and J.P. Hanke, *Universal quadratic forms and the 290-theorem*, to appear in Invent. Math.

[BSD52] E.S. Barnes and H.P.F. Swinnerton-Dyer, *The inhomogeneous minima of binary quadratic forms. I.* Acta Math. 87 (1952), 259–323.

[Bou98] N. Bourbaki, *Commutative algebra. Chapters 17*. Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998.

[Bu07] J. Bureau, *Definite $\mathbb{F}[t]$-Lattices with Class Number One*, preprint, 2007.

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

[CB54] S. Chowla and W. Briggs, *On discriminants of binary quadratic forms with a single class in each genus*. Can. J. Math. 6 (1954), 463-470.

[Ca64] J.W.S. Cassels, *On the representation of rational functions as sums of squares*. Acta Arith. 9 (1964), 79–82.

[CD05] W.K. Chan and J. Daniels, *Definite regular quadratic forms over $\mathbb{F}_q[T]$*. Proc. Amer. Math. Soc. 133 (2005), no. 11, 3121-313.

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

[CSl99] J.H. Conway and N.J.A. Sloane, *Sphere packings, lattices and groups*. Third edition. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 290. Springer-Verlag, New York, 1999.

[CSm03] J.H. Conway and D.A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*. A K Peters, Ltd., Natick, MA, 2003.

[Co93] H. Cohen, *A course in computational algebraic number theory*. Graduate Texts in Mathematics, 138. Springer-Verlag, Berlin, 1993.

[Co07] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*. Graduate Texts in Mathematics, 239. Springer, New York, 2007.

[Ei52] M. Eichler, *Martin Quadratische Formen und orthogonale Gruppen*. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete. Band LXIII. Springer-Verlag, 1952.

[Fi10] R.W. Fitzgerald, *Norm Euclidean Quaternionic Orders*, preprint, 2010.

[Ge08] L.J. Gerstein, *Basic quadratic forms*. Graduate Studies in Mathematics, 90. American Mathematical Society, Providence, RI, 2008.

[JKS97] W.C. Jagy, I. Kaplansky and A. Schiemann, *There are 913 regular ternary forms*. Mathematika 44 (1997), no. 2, 332-341.

[KV10] M. Kirschmer and J. Voight, *Algorithmic enumeration of ideal classes for quaternion orders*. SIAM J. Comput. 39 (2010), no. 5, 1714-1747.

[La05] T.Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[LM71] M.D. Larsen and P.J. McCarthy, *Multiplicative theory of ideals*. Pure and Applied Mathematics, Vol. 43. Academic Press, New York-London, 1971.

[Le79] H.W. Lenstra, Jr., *Euclidean ideal classes*. Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978), pp. 121–131,

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

[Ne03] G. Nebe, *Even lattices with covering radius $< \sqrt{2}$*. Beiträge Algebra Geom. 44 (2003), no. 1, 229-234.

[OM00] O.T. O'Meara, *Introduction to quadratic forms*. Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[Pf65] A. Pfister, *Multiplikative quadratische Formen*. Arch. Math. (Basel) 16 (1965), 363–370.

[Pf95] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*. London Math. Society Lecture Note Series, 217. Cambridge University Press, Cambridge, 1995.
[Ra02] A.M. Rahimi, *Euclidean modules*. Libertas Math. 22 (2002), 123-126.
[Re75] I. Reiner, *Maximal orders*. London Mathematical Society Monographs, No. 5. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975.
[Sch66] R.D. Schafer, *An introduction to nonassociative algebras*. Pure and Applied Mathematics, Vol. 22 Academic Press, New York-London 1966
[Se73] J.-P. Serre, *A course in arithmetic*. Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.
[SeMO] J.-.P. Serre communicated to B. Poonen communicated to MathOverflow.net: `mathoverflow.net/questions/3269`
[Sh10] G. Shimura, *Arithmetic of quadratic forms*. Springer Monographs in Mathematics. Springer, New York, 2010.
[Vi80] M.-F. Vignéras, *Arithmétique des algbres de quaternions*. Lecture Notes in Mathematics, 800. Springer, Berlin, 1980.
[Vo11] J. Voight, *Characterizing quaternion rings over an arbitrary base*, to appear.
[We84] A. Weil, *Number theory. An approach through history from Hammurapi to Legendre*. Reprint of the 1984 edition. Modern Birkhäuser Classics, Boston, MA, 2007.

Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602-7403, USA
E-mail address: `pete@math.uga.edu`