EUCLIDEAN QUADRATIC FORMS AND ADC-EXTENSIONS

PETE L. CLARK

Abstract. A classical result, often called the Davenport-Cassels Theorem, gives a sufficient condition for an integral quadratic form to integrally represent every integer that it rationally represents. We present a version of this result which allows one to pass from rational to integral representations for certain quadratic forms over a *normed ring*. Applying our theorem to the ring $k[t]$ we recover the Cassels-Pfister theorem. This motivates a closer study of both the class of forms which satisfy the hypothesis of our theorem ("Euclidean forms") and its conclusion ("Aubry-Davenport-Cassels forms"). We give a very preliminary analysis of these classes, mainly concentating on formulating some natural conjectures and questions concerning their classification.

1. Euclidean Forms and ADC-Extensions

1.1. **Normed rings.**

Let R be a commutative, unital ring. We write $R^\bullet$ for $R \setminus \{0\}$.

A **norm** on R is a function $| \ | : R^\bullet \rightarrow \mathbb{Z}^+$ such that
(N1) $\forall x \in R$, $x \in R^\times \iff |x| = 1$, and
(N2) $\forall x, y \in R$, $|xy| = |x||y|$.

When convenient, we extend $| \ |$ to R by putting $|0| = 0$.

In other words, a norm on R is a homomorphism of multiplicative monoids $(R^\bullet, \cdot) \rightarrow (\mathbb{Z}^+, \cdot)$ satisfying the additional condition that nonunits map to nonunits.

A norm $| \ |$ is **non-Archimedean** if for all $x, y \in R$, $|x + y| \leq \max(|x|, |y|)$.[1]

By a **normed ring**, we shall mean (here) a pair $(R, | \ |)$ where $| \ |$ is a norm on R. Note that a normed ring is necessarily an integral domain. We denote the fraction field by K. The norm extends uniquely to a homomorphism of groups $(K^\times, \cdot) \rightarrow (\mathbb{Q}^{>0}, \cdot)$ via $|\frac{x}{y}| = \frac{|x|}{|y|}$, and the induced norm on K is non-Archimedean iff the norm on R is non-Archimedean.

Example 1: Let $R = \mathbb{Z}$. The usual Euclidean absolute value is a norm on R.

Example 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,

Partially supported by National Science Foundation grant DMS-0701771.

[1] Note that we do not require that a general norm satisfy the triangle inequality.

it is most natural to take $a = \#k$ (see below). Otherwise, we may as well take $a = 2$.

Example 3: Let R be an infinite integral domain with property (FN): for every nonzero ideal I of R, R/I is finite. (In particular, R may be an order in a number field, the ring of regular functions on an affine algebraic curve over a finite field, or any localization or completion thereof.) Then the map $x \in R^\bullet \mapsto \#R/(x)$ gives a norm on R [Cl10, Prop. 5], which we will call the **canonical norm** on R. The given norm $| \ |$ on $\mathbb{Z}$ is the canonical norm, as is the norm $| \ |_q$ on the polynomial ring $\mathbb{F}_q[t]$.

Example 4: Let R be a discrete valuation ring (DVR) with valuation $v : K^\times \rightarrow \mathbb{Z}$ and residue field k. If k has characteristic 2, we say R is **dyadic**, and otherwise that R is **non-dyadic**. As above, choosing an integer $a \geq 2$ we can define a norm $| \ |_a : R^\bullet \rightarrow \mathbb{Z}^+$ by $|x|_a = a^{v(x)}$. Note that R has property (FN) iff the residue field k is finite, and in this case the norm $| \ |_{\#k}$ is the canonical norm. When k is infinite we may as well take $a = 2$.

Note well that the norm $| \ |_a$ is not quite the usual norm $x \mapsto a^{-v(x)}$ associated to a DVR: rather, it is the reciprocal of the usual norm. Especially, *beware*: the norm $| \ |_a$ is *not* non-Archimedean: e.g. let π be an element of R with $v(\pi) = 1$; then $a = |\pi|_a = |(\pi - 1) + 1|_a > \max(|\pi - 1|_a, |1|_a) = 1$.

A norm $| \ |$ on a ring R is **Euclidean** if for all $x \in K \setminus R$, there exists $y \in R$ such that $|x - y| < 1$. A domain which admits a Euclidean norm is a principal ideal domain (PID). It is known that the converse is not true, both in the sense that a given norm on a PID need not be Euclidean and in the stronger sense that there are PIDs which do not admit any Euclidean norm. However, for our purposes we wish to consider the norm as part of the given structure on R, so when we say "R is Euclidean", we really mean "the given norm $| \ |$ on R is a Euclidean norm".

Example 5: The standard norm on $\mathbb{Z}$ is a Euclidean norm. For any field k and any $a \geq 2$, the norm $| \ |_a$ on $k[t]$ (c.f. Example 2) is a Euclidean norm. Indeed, by usual polynomial division, for $n, d \in k[t]$, $\deg(d) > 1$, we may write $\frac{n}{d} = q + \frac{r}{d}$, with $q, r \in k[t]$ and $\deg(r) < \deg(d)$, and then $|\frac{n}{d} - q|_a < 1$. If (R, v) is discrete valuation ring, then the norm $| \ |_a$ (c.f. Example 4) is a Euclidean norm: indeed, for $x \in K^\bullet$, $x \in K \setminus R \iff v(x) < 0 \iff |x|_a = a^{v(x)} < 1$. Thus in this case the Euclidean condition holds with $y = 0$!

1.2. **Euclidean quadratic forms.**

Let $(R, | \ |)$ be a normed ring of characteristic different from 2. By a **quadratic form** over R, we mean a polynomial $q \in R[x] = R[x_1, \ldots, x_n]$ which is homogeneous of degree 2. Recall that a 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**. It is easy to see that q is anistropic as a quadratic form over R iff it is anisotropic over the fraction field K.

Now for the first of two fundamental definitions of this paper.

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 $0 < |q(x - y)| < 1$.

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

Proposition 1. *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:

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

□

Example 6: The sum of n-squares form $x_1^2 + \ldots + x_n^2$ is Euclidean over $\mathbb{Z}$ iff $n \leq 3$. Indeed, a moment's thought shows that for a given $x \in \mathbb{Q}^n$, the quantity $|q(x-y)|$ is minimized by choosing each y_i to be a nearest integer to x_i, thus $|x_i - y_i| \leq \frac{1}{2}$ for all i, and these inequalities are sharp. So the optimal estimate is $|q(x-y)| \leq \frac{n}{4}$.

1.3. **ADC-extensions and ADC-forms.**

Now for the other key definitions of this paper.

Let $R \hookrightarrow S$ be an extension of domains, and let $q_{/R}$ be a quadratic form. We say that S/R is an **ADC-extension**[2] for q if: for all $d \in R$, if there exists $x \in S^n$ such that $q(x) = d$, there exists $y \in R^n$ such that $q(y) = d$. If R is a domain with fraction field K, we say that q is an **ADC-form** if the extension K/R is an ADC-extension for q.

Example 7: If R is integrally closed, then $q(x) = x^2$ is an ADC-form. Indeed, $a \in R^\bullet$ is K-represented by q iff the monic polynomial $t^2 - a$ has a K-rational root. An explicit example of a domain R for which x^2 is *not* an ADC-form is $R = \mathbb{Z}[\sqrt{-4}]$, in which q represents -1 over the fraction field but not over R.

Example 8: Let k be a field (of characteristic different from 2), and let q be an isotropic quadratic form over k. Then any extension S/k is an ADC-extension for q. Indeed, since q is isotropic over k, it contains the hyperbolic plane xy as a subform. More precisely, after a k-linear change of variables, we may assume $q = x_1x_2 + q'(x_3, \ldots, x_n)$. It is then clear that for any ring extension S of k and any $s \in S$, q S-represents s: take $x_1 = s$, $x_2 = 1$, $x_3 = \cdots = x_n = 0$.

Example 9: If $q(x_1, \ldots, x_n)$ is a quadratic form over $\mathbb{Q}$ with $n \geq 4$, then $\mathbb{R}/\mathbb{Q}$ is an ADC-extension for $\mathbb{Q}$, i.e., q rationally represents all rational numbers permitted by sign considerations. (This was first shown by A. Meyer [Me84] and is nowadays viewed as a consequence of the Hasse-Minkowski theory.)

The ADC-condition can be made quite concrete, as follows. Suppose $a \in R$ and the R-quadratic form q K-represents a. Then there exist $x_1, \ldots, x_n \in R$ and $d \in R^\bullet$ such that $q(\frac{x_1}{d}, \ldots, \frac{x_n}{d}) = a$, and thus $q(x_1, \ldots, x_n) = d^2a$; and conversely. In other words, for any $a \in R$, we can "rationally" represent a iff we can "integrally"

[2] ADC stands for **A**ubry-**D**avenport-**C**assels. The reasons for this nomenclature will become clear shortly.

represent some nonzero square times a, and thus the ADC-condition can be viewed as a *desquaring property.* It is thus a natural and useful property to have when trying to understand integral representations in terms of rational representations: e.g. in the case $R = \mathbb{Z}$ it reduces $\mathbb{Z}$-representation of arbirary elements of $\mathbb{Z}$ to $\mathbb{Z}$-representation of *squarefree* integers.

Example 10: The form $q(x, y) = x^2 - y^2$ is isotropic over $\mathbb{Z}$ but is not an ADC-form. Indeed, over the field $\mathbb{Q}$ the isotropic form q is isomorphic to the hyperbolic plane and thus represents every number: concretely, $a = (\frac{a+1}{2})^2 - (\frac{a-1}{2})^2$. However, reducing modulo 4 shows that q does not $\mathbb{Z}$-represent any $a \equiv 2 \pmod 4$.

Example 11: In 1912, the amateur mathematician L. Aubry showed that $q(x) = x_1^2 + x_2^2 + x_3^2$ is an ADC-form [Aub12]. This leads to an elegant and conceptual proof of the Legendre-Gauss Three Squares Theorem, since already by Aubry's day the theory of rational quadratic forms had been systematically understood by H. Minkowski.

We observed in Example 6 that q is Euclidean. Indeed, Aubry's proof exploits the Euclidean property. However, his argument seems to have been forgotten for many years, and circa 1960 Davenport and Cassels (unpublished) rediscovered Aubry's argument. The result which is generally attributed to Davenport and Cassels may be stated in our terminology as follows.

Theorem 2. *(Aubry-Davenport-Cassels-Serre-Weil)*
Every Euclidean quadratic form q over $\mathbb{Z}$ is an ADC-form.

Remark 2: As mentioned above, in the special case of the three squares form this result goes back to L. Aubry. The work of Davenport and Cassels was unpublished, so I don't know exactly what they proved. In his widely read text [Se73], Serre states and proves this theorem with the additional hypotheses that q be positive-definite and classically integral: i.e., that the bilinear form $\frac{1}{2}(q(x+y) - q(x) - q(y))$ be $\mathbb{Z}$-valued (and attributes it to Davenport and Cassels). The first statement of Theorem 2 in full generality seems to have been given by A. Weil in [We84, p. 294]. He states this result rather casually, so one has to read carefully to find it (and indeed, until recently it does not seem to have been well-known). Finally, in late December of 2009, Serre communicated a new proof to Bjorn Poonen. Poonen posted Serre's proof on the website MathOverflow.net on December 31, 2009 [SeMO]. This argument proves a slightly more general result, namely q in Theorem 2 can be a quadratic polynomial instead of a quadratic form.

ADC-forms also appear in the literature via the following result.

Theorem 3. *(Cassels-Pfister* [Ca64] [Pf65]*) Let k be a field of characteristic different from* 2*. Let $q_{/k}$ be a quadratic form, and consider q as a quadratic form over the polynomial ring $R = k[t]$. Then $q_{/R}$ is an ADC-form: that is, every polynomial $p \in k[t]$ which is represented by q over the field $k(t)$ of rational functions is also represented by q over the ring $k[t]$ of polynomial runctions.*

The standard proofs of Theorems 2 and 3 have a classical flavor as well as a marked resemblance to each other. As above, the matter of it is to assume that, for $d \in R$, we have $x \in R^n$ such that $q(x) = t^2 d$ for some $t \in R^\bullet$ and deduce an R-representation of d. This is done by a process of **descent**: taking a $y \in R^n$ such that $|q(x-y)| < 1$, we intersect the line ℓ joining x and y with the surface $q = d$. One of the two points of intersection is x, so the associated quadratic equation has another rational root x', and then – and this is the magical part! – a straightforward computation shows that $q(x') = (t')^2 a$, with $|t'| < |t|$. Repeating this process yields an R-representation.

1.4. **The Main Theorem.**

We are now ready to state and prove the main result of this note, a generalization of Theorem 2 which yields Theorem 3 as a corollary.

Theorem 4. *Let $(R, | \, |)$ be a normed ring not characteristic 2 and $q_{/R}$ a Euclidean quadratic form. Then q is an ADC-form.*

Proof. We will make use of the well-known correspondence between quadratic forms and bilinear forms outside of characteristic 2. Namely, 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 $2(x \cdot y) \in R$. Our computations below are parenthesized so as to emphasize this integrality property. Let $d \in R$, and suppose that there exists $x \in K^n$ such that $q(x) = d$. Equivalently, there exists $t \in R$ and $x' \in R^n$ such that $t^2 d = x' \cdot x'$. We choose x' and t such that $|t|$ is minimal, and it is enough to show that $|t| = 1$, for then by (N1) $t \in R^\times$.

Applying the Euclidean hypothesis with $x = \frac{x'}{d}$, there exists a $y \in R$ such that if $z = x - y$ we have

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

Now put

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

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 3: This proof is modelled on that of [Se73]. The modifications were made in two steps. First, circa 2008, I realized that the hypotheses of positive-definiteness and classical integrality in Serre's proof can be removed (by taking absolute values and noting that the necessary factors of 2 appear in all the formulas, respectively). This writeup appears in my Math 4400/6400 course notes (CITE). Once I realized (in early September, 2010) the statement could be generalized to replace $\mathbb{Z}$ by a normed ring, the modifications in my proof were immediate: indeed, what is presented above is word-for-word identical to the proof in *loc. cit.* except for replacing $\mathbb{Z}$ by R and $\mathbb{Q}$ by K!

1.5. **Deducing the Cassels-Pfister Theorem.**

We now deduce Theorem 3 as a corollary of Theorem 4.

Lemma 5. *Let q be an anisotropic quadratic form over a field k. Then q remains anisotropic over $k(t)$.*

Proof. Arguing contrapositively, suppose that there exists a nonzero $x \in k(t)$ such that $q(x) = 0$. Clearing denominators, there exists $y = (y_1, \ldots, y_n)$ such that $y \in R^n \backslash (0, \ldots, 0)$, $\gcd(y_1, \ldots, y_n) = 1$ and $q(y) = 0$.[3] In particular, the polynomials $y_1, \ldots, y_n$ do not all vanish at 0, for otherwise t would be a common factor, 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 4: The proof of Lemma 5 has nothing to do with quadratic forms. Really it shows that a variety $V_{/k}$ has a k-rational point iff it has a $k(t)$-rational point.

Proof of Theorem 3: let $q = \sum_{i,j} a_{ij} x_i x_j$ be a quadratic form over k. We view q as a quadratic form over $R = k[t]$ via base extension. If q is isotropic over k, then by Example 8, q R-represents every element of R.
So suppose q is anisotropic over k, hence also, by Lemma 5, over $k(t)$. By Theorem 4, it suffices to show that as a quadratic form over $R = k[t]$ endowed with the norm $| \ | = | \ |_2$ of Example 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

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

Remark 5: Suppose that $q = \sum_{i,j} a_{i,j} x_i x_j$ is an anisotropic quadratic form over $k[t]$ such that each polynomial $a_{i,j}$ has degree at most one. Then $\max_{i,j} |a_{i,j}| \leq 2$ while $\max_i |\frac{r_i}{g_i}|^2 \leq \frac{1}{4}$, so (1) still holds in this case and shows that q is Euclidean. This known result is sometimes called the *Generalized* Cassels-Pfister Theorem: c.f. [Pf95, Remark 1.2.3]. As Pfister remarks, in this case the anisotropy hypothesis is needed for the result to be true.

2. Classification of Euclidean forms

Let $(R, | \ |)$ be a normed ring. It seems to be the case that there are relatively few anisotropic Euclidean forms and ADC-forms over R. This raises the prospect of classfying all such forms, and in particular understanding how much stronger the Euclidean property is than the ADC-property.

[3] Here we use the fact that $k(t)$ is the fraction field of the UFD $k[t]$.

2.1. **Binary Euclidean forms over a PID.**

An earlier draft of this paper contained the remark that under the classical correspondence between principal binary quadratic forms and quadratic orders, the Euclidean forms correspond to the Euclidean quadratic orders. Thus a special class of Euclidean forms is related to a classical problem in number theory. Franz Lemmermeyer saw this remark and immediately saw the following generalization: under the classical correspondence between binary quadratic forms and ideal classes in a quadratic order, Euclidean quadratic forms in the sense of this paper correspond to Euclidean ideal classes in the sense of H. Lenstra. In this section we give an exegesis of Lemmermeyer's observation.

We will perform our construction in the following setup: let $(R, |\ |)$ be a PID with fraction field K (of characteristic not 2, as usual). Since R is a PID, the given norm may equally well be viewed as a norm map on ideals: for any ideal $\mathfrak{a}$ of R, we may define $|\mathfrak{a}|$ to be the norm of any generator of $\mathfrak{a}$.

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 $\operatorname{Aut}(L/K)$: we assume that $\overline{S} = S$ and $S^{\operatorname{Aut}(L/K)} = R$, 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 12: 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 $\operatorname{Pic}(S)$.

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

Theorem 7. *(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. Suppose that S admits a non-principal Euclidean ideal class. Then $D \in \{-20, -15, 40, 60, 85\}$.*

The corresponding nonprincipal Euclidean binary quadratic forms are:

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

2.2. **Euclidean forms over $\mathbb{Z}$.**

Problem 1. *Show that there are only finitely many anisotropic Euclidean forms over $\mathbb{Z}$, and give a complete list of them.*

As we saw, the positive definite Euclidean forms over $\mathbb{Z}$ certainly include:

$$x^2, x^2 + y^2, x^2 + y^2 + z^2.$$

Calculations done by J. Houriet and reported in [Co07, §5.4.2] give the following further example:[4]

$$x^2 + 2y^2 + 2yz + 2z^2.$$

In the case $R = \mathbb{Z}$, our work in the previous section specializes to give one direction of the classical correspondence between primitive anisotropic binary quadratic forms over $\mathbb{Z}$ of discriminant Δ and invertible ideal classes in the quadratic order of discriminant Δ (see e.g. [Co93, §5.2]). As we saw, under this correspondence primitive Euclidean binary quadratic forms over $\mathbb{Z}$ correspond to Euclidean ideal classes in the ring of integers of real and imaginary quadratic fields. The two positive definite nonprincipal Euclidean forms we get in this way are:

$$2x^2 + 2xy + 3y^2, 2x^2 + xy + 2y^2.$$

It is well known that the ring of integers of the imaginary quadratic field of discriminant Δ is norm-Euclidean precisely for $\Delta = -3, -4, -7, -8, -11$. The corresponding quadratic forms are

$$x^2 + xy + y^2, x^2 + y^2, x^2 + xy + 2y^2, x^2 + xy + 3y^2.$$

These forms are all primitive. If for some integer $n > 1$ we find that the Euclidean maximum $\max_{x \in \mathbb{Q}^n,\ y \in \mathbb{Z}^n} |q(x - y)| < \frac{1}{n}$, then also the imprimitive form $n \cdot q$ is Euclidean – and conversely. This gives

$$2x^2, 3x^2, 2x^2 + 2xy + 2y^2, 2x^2 + 2y^2.$$

[4] Cohen uses the name "strongly Euclidean" for these forms. To the best of my knowledge, he is the first to explicitly identify the hypothesis of the Davenport-Cassels theorem as being a sort of Euclidean property.

Noting that the form $x^2 + y^2$ has appeared twice on our list, altogether this shows that there are at least 13 positive definite Euclidean quadratic forms over $\mathbb{Z}$. We have not attempted to check whether this list is complete, although that seems to be a tractable and appealing computational problem.[5]

The case of indefinite Euclidean forms is more involved. Indeed, as above the classification of principal indefinite binary Euclidean forms amounts to the classification of norm-Euclidean real quadratic fields, a solved – but nontrivial! – problem in the geometry of numbers.

Theorem 8. *The real quadratic fields for which the maximal order is norm-Euclidean are as follows:*

$$\mathbb{Q}(\sqrt{a}) \text{ for } a \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}.$$

Proof. This represents the work of several mathematicians over the first half of the 20th century, culminating in a 1952 work of Barnes and Swinnerton-Dyer [BSD52]. □

2.3. Euclidean forms over other rings.

The theory of quadratic forms over $\mathbb{F}_q[t]$ (with q odd) is known to be analogous in many respects to the theory of integral quadratic forms. In particular, most of the questions of the previous section apply. Note that, although any quadratic form q which is base-changed from $\mathbb{F}_q$ is Euclidean, there are only finitely many such *anisotropic* forms, so it remains plausible that there are only finitely many anisotropic Euclidean forms over $\mathbb{F}_q[t]$.

It seems interesting to look also at Euclidean forms over localizations of $\mathbb{Z}$, since by Theorem 4 these yield quadratic forms which have the ADC-property "away from certain primes". The case of $\mathbb{Z}[\frac{1}{2}]$ seems especially relevant.

Similarly, one can try to find Euclidean forms over the ring of integers $\mathbb{Z}_K$ of a number field K. In this regard, the following is relevant.

Problem 2. *Let $(R, |\ |)$ be a normed domain which admits some (nonzero!) Euclidean quadratic form. Is $(R, |\ |)$ then necessarily a Euclidean domain?*

By Proposition 1, an equivalent restatement of this question is: if there are any Euclidean forms over R, is $q(x) = x^2$ then necessarily a Euclidean form?

Apart from the situation of the Cassels-Pfister theorem, I know of only one other systematic means for constructing Euclidean quadratic forms. It goes as follows.

Let R be a complete discrete valuation ring with fraction field K. Let $q : R^n \to R$ be a quadratic form on R. By tensoring to K, we may view q as being a quadratic form on K^n and R^n as an R-lattice $\Lambda \subset K^n$. The quadratic form q satisfies the integrality property $q(\Lambda) \subset R$. We say that q is **maximal** if there does not exist

[5] Indeed I have this in mind as a possible research project for an undergraduate or early career graduate student. Of course, you – whoever you are – are welcome to do the computation yourself, but I would appreciate it if you would contact me if you start (or finish!) working on this problem.

an R-lattice Λ' strictly containing Λ such that $q(\Lambda') \subset R$. It is easy to see that every lattice is contained in at least one maximal lattice [Ge08, Remark 6.33].

Theorem 9. *(Eichler's Maximal Lattice Theorem) Let K be a complete, discretely valued field (not of characteristic 2) with valuation ring R. Let $q_{/K}$ be a regular quadratic form.*
a) Any two maximal R-lattices for q are isometric.
b) If q is anisotropic, 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]. □

Corollary 10. *Let R be a complete, discretely valued ring (not of characteristic 2), with fraction field K. Then, for each anisotropic quadratic form $q_{/K}$, restricting to the unique maximal R-lattice Λ defines a Euclidean quadratic form over R.*

Proof. The proof is immediate from the fact that $R^n = \{x \in K^n \mid q(x) \in R\}$. Indeed, this is equivalent to $R^n = \{x \in K^n \mid |q(x)|_a \geq 1\}$, where $|x|_a = a^{v(x)}$ is the norm of Example 4. Therefore, $x \in K^n \setminus R^n \iff |q(x)|_a < 1$, so the Euclidean condition is met by taking $y = 0$![6] □

3. Classification of ADC-forms

Proposition 11. *Let q be an ADC-form over $\mathbb{Z}$. Then q is* **regular***: it $\mathbb{Z}$-represents every integer that is represented by its genus.*

Proof. Let $d \in \mathbb{Z}$. To say that the genus of q represents d is equivalent to saying that for all $p \leq \infty$, q represents d over $\mathbb{Z}_p$. It follows that q represents d over $\mathbb{Q}_p$ for all $p \leq \infty$. Thus q $\mathbb{Q}$-represents d by Hasse-Minkowski and thus $\mathbb{Z}$-represents d by the hypothesis that it is an ADC-form. □

This is significant because regular quadratic forms are known to be quite rare, at least in the positive definite case in a small number of variables. Would that I were more qualified even to survey known results here. We will have to content ourselves for now with the following remarks.

Example 13: A primitive, positive definite binary quadratic form q is regular iff every genus has a single class, iff the class group of $\mathbb{Q}(\sqrt{\Delta(q)})$ is 2-torsion. It is known that there are only finitely many such forms and there is suggested classification, but this is currently known to be complete only conditionally on the Generalized Riemann Hypothesis [CB54].

Example 13: Work of Jagy and Kaplansky shows that the number N_3 of regular positive-definite ternary quadratic forms satisfies $891 \leq N_3 \leq 913$. In 2008, Byeong-Kweon Oh announced that $N_3 \geq 899$.[7]

Example 14: Work of Watson shows that there are infinitely many regular positive-definite quaternary quadratic forms, only finitely many of which are diagonalizable over $\mathbb{Z}$.

[6] Note that this argument directly generalizes Example 5, in which $q(x) = x^2$.

[7] c.f. `http://www.mathnet.or.kr/real/2008/1/Byeong-Kweon_Oh.pdf`

Question 3. *What can be said about the set of ADC-forms over $\mathbb{Z}$? Are there, for instance, only finitely many positive-definite such forms in at most* 4 *variables?*

Problem 4. *Classify all ADC-forms over a complete DVR with finite residue field.*

Acknowledgements I thank Keith Conrad, Jonathan P. Hanke and William C. Jagy for close readings and helpful comments. Thanks especially to Franz Lemmermeyer.

References

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

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

[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.

[Cl10] P.L. Clark, *Factorization in Integral Domains*, `http://math.uga.edu/~pete/factorization2010.pdf`

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

[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.* (German) Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen mit besonderer Bercksichtigung der Anwendungsgebiete. Band LXIII. Springer-Verlag, Berlin-Gttingen-Heidelberg, 1952.

[Ge08] L.J. Gerstein, *Basic quadratic forms.* Graduate Studies in Mathematics, 90. American Mathematical Society, Providence, RI, 2008. xiv+255 pp.

[Le79] H.W. Lenstra, Jr., *Euclidean ideal classes.* Journées Arithmétiques de Luminy (Colloq. Internat. CNRS, Centre Univ. Luminy, Luminy, 1978), pp. 121–131, Astrisque, 61, Soc. Math. France, Paris, 1979.

[Me84] A. Meyer, Mathematische Mittheilungen, Vierteljahrschrift der Naturforschenden Gesellschaft in Zrich, 29 (1884), 209222.

[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 Mathematical Society Lecture Note Series, 217. Cambridge University Press, Cambridge, 1995.

[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`

[We84] A. Weil, Weil, *Number theory. An approach through history from Hammurapi to Legendre.* Reprint of the 1984 edition. Modern Birkhuser Classics. Birkhuser Boston, Inc., 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`