ACTA ARITHMETICA
173.4 (2016)

Sums of squares in rings of integers with 2 inverted

by

Gaël Collinet (Strasbourg)

Introduction. Let K be a number field with ring of integers $\mathcal{O}_K$. In this paper, an element x of K will be said to be *totally positive* if $\sigma(x) > 0$ for any embedding $\sigma : K \to \mathbb{R}$.

Let A be a subring of K containing $\mathcal{O}_K$. An A-quadratic module $\mathrm{L} = (L, q)$ is the datum of a projective A-module of finite rank together with a quadratic form $q : L \to A$ such that the K-quadratic space $\mathrm{L} \otimes_A K$ is non-degenerate. Such a quadratic module is said to be *totally positive definite* if $q(x)$ is totally positive for any *non-trivial* x in L.

A totally positive quadratic module $\mathrm{L} = (L, q)$ over A is said to be *absolutely universal* if any totally positive element $a \in A$ is *represented by* L, i.e. $a = q(x)$ for some $x \in L$.

Examples. For any natural number n, let us denote by I_n the $\mathbb{Z}$-quadratic module $\mathbb{Z}^n$ together with its standard euclidean quadratic form

$$x \mapsto x_1^2 + \cdots + x_n^2.$$

For any subring A as above, $\mathrm{I}_n \otimes A$ is totally positive definite and

(1) as is well known, a theorem of Lagrange says that I_4 is absolutely universal;
(2) a theorem of Niven [4] says that if m is a prime congruent to 3 modulo 4, and if K is the number field $\mathbb{Q}[i\sqrt{m}]$, then $\mathrm{I}_3 \otimes \mathcal{O}_K$ is absolutely universal (here, the positiveness conditions are empty).

So (1) above says that any natural integer is a sum of four squares, and (2) says that any integer in the quadratic field $\mathbb{Q}[i\sqrt{m}]$ (with $m \equiv 3 \bmod 4$) is a sum of three such integers squared.

2010 *Mathematics Subject Classification*: Primary 11E25; Secondary 11P05.
Key words and phrases: sums of squares, rings of (S)-integers, universal forms.
Received 25 November 2015; revised 23 February 2016.
Published online 18 May 2016.

In a recent work [3], V. Kala, pursuing work with Blomer [2], shows that such phenomena cannot be expected for the case of integers in real quadratic fields:

(3) for any natural number M, there exist infinitely many quadratic number fields K such that no totally positive definite quadratic $\mathcal{O}_K$-module of rank M can be absolutely universal.

In this note, we shall prove the following:

THEOREM.

(i) *For any number field K, and any subring A of K containing $\mathcal{O}_K[1/2]$, the quadratic module $\mathrm{I}_5 \otimes A$ is absolutely universal.*
(ii) *There exist number fields K such that, for $A := \mathcal{O}_K[1/2]$, there exist totally positive elements in A that are not represented by $\mathrm{I}_4 \otimes A$.*

In Section 1, we will prove (i). The method extends and allows us to prove that under the same hypothesis on A, any totally positive integral quadratic A-module of rank k is represented by $\mathrm{I}_{k+4} \otimes A$ (we say a module A is *represented* by a module B if there exists an injective isometry $A \to B$). In Section 2, we will prove (ii) by analyzing what appear to be the smallest counter-examples.

The choice of inverting 2 is not arbitrary. It makes $\mathrm{I}_n \otimes A$ maximal among the integral A-lattices on $\mathrm{I}_n \otimes K$, an important remark in our argument. We could similarly prove that $\mathrm{E}_8 \otimes A$ is absolutely universal whenever either A strictly contains $\mathcal{O}_K$, or K has a complex place (here E_8 is the unique unimodular positive definite $\mathbb{Z}$-quadratic module of rank 8).

1. Constructing universal modules

1.1. (S)-arithmetic rings. Let K be a number field, let $\mathcal{O}_K$ be its ring of integers, and let $\mathcal{V}_K$ be the set of equivalence classes of valuations (i.e. the set of places) on K.

Ostrowski's theorem tells us that $\mathcal{V}_K$ is made up of three parts:

$\mathcal{V}_\mathbb{R}$: the finite set of real archimedean places, corresponding to embeddings $K \to \mathbb{R}$,
$\mathcal{V}_\mathbb{C}$: the finite set of complex archimedean places, corresponding to embeddings $K \to \mathbb{C}$ whose image does not lie in $\mathbb{R}$,
$\mathcal{V}_f$: the infinite set of non-archimedean places, consisting of one place for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the equivalence class of the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$.

The union of $\mathcal{V}_\mathbb{R}$ and $\mathcal{V}_\mathbb{C}$ is written $\mathcal{V}_\infty$.

Let S be a subset of $\mathcal{V}_f$. The ring of (S)-integers in K is

$$A = \{x \in K : v_\mathfrak{p}(x) \geq 0 \ \forall \mathfrak{p} \in \mathcal{V}_f - S\}.$$

The completion of A at an ideal $\mathfrak{p}$ will be denoted by $A_{\mathfrak{p}}$. Its fraction field $K \otimes A_{\mathfrak{p}}$ will be denoted by $K_{\mathfrak{p}}$. This notation is extended to the case of archimedean valuations by allowing $\mathfrak{p}$ to denote an embedding $K \to \mathbb{C}$. In that case, $A_{\mathfrak{p}}$ and $K_{\mathfrak{p}}$ both denote the completion of $\mathfrak{p}(K)$ (thus either $\mathbb{R}$ or $\mathbb{C}$).

1.2. A-lattices on quadratic spaces. Let $\mathrm{V} = (V, q)$ be a quadratic space on K. We denote by

$$(x, y) \mapsto x.y := q(x + y) - q(x) - q(y)$$

the associated bilinear form (thus we have $x.x = 2q(x)$ for $x \in V$).

An *A-lattice* on V is a finitely generated A-submodule of V whose K-span is V.

Let L be an A-lattice on V. Its dual lattice is defined by

$$L^{\sharp} := \{v \in \mathrm{V} : \forall x \in L,\, v.x \in A\}.$$

The lattice L is said to be *integral* when $q(L)$ is contained in A. This implies that L is contained in $L^{\sharp}$.

The set of integral lattices containing a given integral lattice L is finite, since there is a bijection between those lattices and the submodules of the finitely generated torsion module $L^{\sharp}/L$ that are isotropic for the inherited quadratic form $L^{\sharp}/L \to K/A$. We note that, in particular:

- any integral lattice L on V is contained in a maximal integral lattice,
- a lattice is maximal integral if and only if $L \otimes A_{\mathfrak{p}}$ is a maximal $A_{\mathfrak{p}}$-lattice on $V \otimes K_{\mathfrak{p}}$ at each place $\mathfrak{p} \in S$.

LEMMA 1.1. *Let $a \in A$ be represented by the quadratic space* V. *Then a is represented by a maximal A-lattice on V.*

Proof. The case $a = 0$ is obvious: if V is isotropic then so is any lattice on V. If $a \neq 0$, let $v_1 \in V$ be such that $q(v_1) = a$. Let $(v_1, v_2, \ldots, v_n)$ be any orthogonal basis of V. Up to rescaling, we may assume $q(v_2), \ldots, q(v_n)$ are elements of A. The A-lattice generated by this basis is integral, and thus is contained in a maximal integral lattice. ∎

1.3. Genera and spinor genera of A-lattices on V. Two lattices L_1 and L_2 on V are said to be *in the same genus* if at any place $\mathfrak{p}$ there exists an isometry $\sigma_{\mathfrak{p}} \in \mathrm{O}(\mathrm{V}_{\mathfrak{p}})$ sending $L_1 \otimes A_{\mathfrak{p}}$ onto $L_2 \otimes A_{\mathfrak{p}}$. Note that for all but finitely many $\mathfrak{p}$ one has $L_1 \otimes A_{\mathfrak{p}} = L_2 \otimes A_{\mathfrak{p}}$.

The following result shows that when σ_p exists, one can assume without loss of generality that it is a rotation:

PROPOSITION R1 ([5, 91.4]). *Let $L_{\mathfrak{p}}$ be a lattice on* $\mathrm{V}_{\mathfrak{p}}$. *Then* $\mathrm{O}(L_{\mathfrak{p}})$ *contains a reflection.*

The next observation indicates that maximal integral lattices on V form a single genus:

Proposition R2 ([5, 91.2]). *Two maximal lattices on* $\mathrm{V}_{\mathfrak{p}}$ *are isometric.*

A genus splits in spinor genera. Let us recall that there exists a unique morphism $\mathrm{Sp} : \mathrm{O}(\mathrm{V}) \to K^{\times}/K^{\times 2}$ taking the value $q(x)$ on the reflection

$$\tau_x : y \mapsto y - \frac{\langle x, y\rangle}{q(x)} x.$$

This morphism is called the *spinor norm* and its kernel on $\mathrm{SO}(\mathrm{V})$ is written $\mathrm{SO}'(\mathrm{V})$. Two lattices lying in the same genus are said to lie in the same *spinor genus* if the isometries $\sigma_{\mathfrak{p}}$ can be chosen in $\mathrm{SO}'(\mathrm{V}_{\mathfrak{p}})$. The following elementary result will be crucial.

Lemma 1.2. *Let* L *be an* A*-lattice on* V. *Let* U *be a non-degenerate subspace of* V. *Let* W *be the orthogonal complement of* U *in* V. *Write* $D := L \cap U$. *If* $\mathrm{W}_{\mathfrak{p}}$ *is universal at each finite place* $\mathfrak{p} \in S$, *then for any spinor genus* $\mathcal{S}$ *in the genus of* L *there exists a lattice* $L' \in \mathcal{S}$ *containing* D.

Proof. Let M be a representative of a spinor genus in the genus of L. Let T be the set of places $\mathfrak{p}$ where $L_{\mathfrak{p}}$ and $M_{\mathfrak{p}}$ differ. The set T is finite and its intersection with $\mathcal{V}_{\infty} \cup S$ is empty. At any place $\mathfrak{p} \in T$ we have an isometry $\sigma_{\mathfrak{p}} : M_{\mathfrak{p}} \to L_{\mathfrak{p}}$. Choose any rotation $\rho_{\mathfrak{p}}$ of $W_{\mathfrak{p}}$ such that $\mathrm{Sp}(\rho_{\mathfrak{p}})$ and $\mathrm{Sp}(\sigma_{\mathfrak{p}})$ coincide, and extend it by the identity on $U_{\mathfrak{p}}$ to obtain a rotation $\theta_{\mathfrak{p}}$ of $V_{\mathfrak{p}}$. Finally, write $L'_{\mathfrak{p}} := \theta_{\mathfrak{p}}(L_{\mathfrak{p}})$. Then $L'_{\mathfrak{p}}$ contains $D_{\mathfrak{p}}$, and $\mathrm{Sp}(\theta_{\mathfrak{p}} \circ \sigma_{\mathfrak{p}})$ is trivial. Putting all these together, we obtain an element L' containing D in the same spinor genus as M. ∎

Being members of a common spinor genus is a strong requirement, as the following result, known as Kneser's Strong Approximation Theorem, demonstrates

Proposition R3 ([5, 104.5]). *Let* L_1 *and* L_2 *be lattices on* V *lying in the same spinor genus. Assume*

- V *is at least* 3*-dimensional,*
- *there exists a place* $\mathfrak{p} \in \mathcal{V}_K - S$ *such that* $\mathrm{V} \otimes K_{\mathfrak{p}}$ *is isotropic.*

Then L_1 *and* L_2 *are isometric.*

1.4. The proof of (i). If a module D is represented by $\mathrm{I}_n \otimes A$, then $\mathrm{D} \otimes K$ is represented by $\mathrm{I}_n \otimes K$. Let us first establish a representation result for spaces.

Lemma 1.3. *Let* P *be a totally positive* K*-space of dimension* k. *Then* P *is represented by* $\mathrm{I}_{k+3} \otimes K$.

Proof. First we note that any totally positive quadratic space of dimension $r \geq 4$ decomposes as a sum $\mathrm{I}_{r-3} \otimes K \perp \mathrm{W}$ for some space W. This follows from Witt's Cancellation Theorem and the fact that totally positive spaces of rank 4 are absolutely universal (a well known result, a consequence of the theorem of Hasse–Minkowski [5, 66.4] and the fact that a 4-dimensional space is universal at each ultrametric place $\mathfrak{p}$ [5, 63.18]).

The result is then a consequence of the remark that for any totally positive k-dimensional quadratic module Q, the quadratic spaces $(\mathrm{Q})^{\perp 4}$ and I_{4k} are isomorphic (one easily sees that $(\mathrm{L})^{\perp 4}$ is isomorphic to $\mathrm{I}_4 \otimes K$ for any totally positive quadratic line L over K). ∎

REMARK 1.4. Thus any totally positive quadratic A-module is represented by a maximal lattice on $\mathrm{I}_{k+3} \otimes K$. When 2 is invertible in A, these maximal modules form the genus of $\mathrm{I}_{k+3} \otimes A$.

LEMMA 1.5. *Assume A contains $1/2$ and P is a totally positive A-quadratic module of rank k. Then P is represented by $\mathrm{I}_{k+4} \otimes A$.*

Proof. By Remark 1.4, P is represented by an element in the genus of $\mathrm{I}_{k+4} \otimes A$. Since for any finite place $\mathfrak{p}$ the K-space $P^{\perp}$ is non-degenerate and 4-dimensional, it is universal, so Lemma 1.2 applies and P is represented by an element in the spinor genus of $\mathrm{I}_{k+4} \otimes A$, say M. Finally, since $\mathrm{I}_{k+4} \otimes K_{\mathfrak{p}}$ is at least 5-dimensional, it is isotropic at any finite place $\mathfrak{p}$, in particular at dyadic places, so Proposition R3 applies and M is isometric to $\mathrm{I}_{k+4} \otimes A$. ∎

REMARK 1.6. This in particular implies (i). Nevertheless, when P has rank 1, we can do better.

LEMMA 1.7. *Assume A contains $1/2$ and a is a totally positive element of A. Then a is represented by a maximal lattice on $\mathrm{I}_4 \otimes K$ that belongs to the same spinor genus as $\mathrm{I}_4 \otimes A$.*

Proof. By Lemma 1.2 it is enough to prove that, for any vector v in $\mathrm{V} := \mathrm{I}_4 \otimes K$, the orthogonal P of v in V is universal at any non-dyadic place $\mathfrak{p}$. Now at such a place, V is a sum of two hyperbolic planes. Thus P is non-degenerate and isotropic. ∎

In order to derive a universality result for I_4, we need to use the Strong Approximation Theorem. If K has complex places, all the conditions required are satisfied, and this will also be the case if $\mathrm{I}_4 \otimes K_{\mathfrak{p}}$ is isotropic at some ultrametric place outside of S.

DEFINITION 1.8. Let A be the ring of (S)-integers in a number field K. We say that A is a *bad* ring if the following conditions are satisfied:

- S is the union of the archimedean and the dyadic places (thus $A = \mathcal{O}_K[1/2]$),

- K is totally real,
- for any dyadic prime $\mathfrak{p}$, the extension $K_{\mathfrak{p}}/\mathbb{Q}_2$ has odd degree.

We say A is a *good* ring if it contains $\mathcal{O}_K[1/2]$ but is not bad.

LEMMA 1.9. *If A is a good ring, then any totally positive element of A is represented by* $\mathrm{I}_4 \otimes A$.

Proof. We are just left with verifying that when K is totally real and $A = \mathcal{O}_K[1/2]$, and at least one of the extensions $K_{\mathfrak{p}}/\mathbb{Q}_2$ has even degree, strong approximation applies. But at a dyadic place, $\mathrm{I}_3 \otimes K_{\mathfrak{p}}$ is isotropic if and only if the Hilbert symbol $\left(\frac{-1,-1}{\mathfrak{p}}\right)$ is trivial. A theorem of Bender [1] says that this happens exactly when the degree $[K_{\mathfrak{p}} : \mathbb{Q}_2]$ is even. ∎

2. Examples of rings A such that $\mathrm{I}_4 \otimes A$ is not universal. By Lemma 1.9 we have to look for such counterexamples among bad rings.

PROPOSITION R4 ([5, 91.1]). *Let K be a field such that $\mathcal{O}_K[1/2]$ is a bad ring. Let L be a maximal A-lattice on $\mathrm{V} := \mathrm{I}_4 \otimes K$. Then the subset $L_{\mathcal{O}_K}$ of vectors x in L that satisfy $q(x) \in \mathcal{O}_K$ is a (maximal integral) $\mathcal{O}_K$-lattice on* V.

The simplest bad ring is $A = \mathbb{Z}[1/2]$. Thus let us consider the case when V is the space $\mathrm{I}_4 \otimes \mathbb{Q}$, whose canonical basis is denoted by $\underline{e} = (e_1, e_2, e_3, e_4)$, and L is the A-lattice with basis $\underline{e}$. The $\mathbb{Z}$-lattice $L_{\mathbb{Z}}$ is known as the *Hurwitz lattice H*; setting $u := \frac{1}{2}(e_1 + e_2 + e_3 + e_4)$, we see it has (e_1, e_2, e_3, u) as a basis, in which the Gram matrix of q has the form

$$\begin{pmatrix} 1 & 0 & 0 & 1/2 \\ 0 & 1 & 0 & 1/2 \\ 0 & 0 & 1 & 1/2 \\ 1/2 & 1/2 & 1/2 & 1 \end{pmatrix}.$$

In other words, the $\mathbb{Z}$-quadratic module $\mathrm{H} := (H, q|_H)$ is isometric to $(\mathbb{Z}^4, q')$ with

$$q'(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + (x_1x_4 + x_2x_4 + x_3x_4).$$

This module is absolutely universal: it contains the standard lattice I_4, which is absolutely universal by Lagrange's theorem.

Therefore let us study the case when $A = \mathbb{Z}[1/2, \sqrt{p}]$ where p is a prime. This ring is bad if p is a square in $\mathbb{Q}_2$, i.e. if p is congruent to 1 modulo 8. In the following, we assume that p can be written in the form $p = (2m+1)^2 - 8$, and we write $\omega = (1 + \sqrt{p})/2$, so that $\mathcal{O}_K = \mathbb{Z}[\omega]$. Here are the first few such primes:

$$p = 17, 41, 73, 113, 281, 353, 433, 521, 617, 953, 1217, 1361, 2017, \ldots.$$

A special case of a conjecture of Bunyakovskiĭ says that there should exist infinitely many such primes.

We write $x \mapsto \bar{x}$ for the Galois automorphism of K. Let $\pi = m + \omega$. We see that π is a totally positive integer whose norm equals 2 and whose trace equals $2m+1$ (and we have a factorization $(2) = (\pi)(\bar{\pi})$ in the monoid of ideals of $\mathcal{O}_K$).

Lemma 2.1. *The integer π cannot be written as the sum of two totally positive elements of $\mathcal{O}_K$.*

Proof. Assume we can write $\pi = x + y$ with x and y totally positive in $\mathcal{O}_K$. We would have the inequalities $x < \pi$ and $\bar{x} < \pi$, and hence we would get

$$N(x) < N(\pi) = 2, \qquad \mathrm{Tr}(x) < \mathrm{Tr}(\pi) = 2m + 1 = \sqrt{p+8}.$$

If we write $x = (a + b\sqrt{p})/2$, with a and b rational, these inequalities translate into

$$a^2 = 4 + pb^2, \qquad a^2 < p + 8.$$

Thus b is an element of $\{0, \pm 1\}$. The case $b = 0$ cannot occur: we would have $x = 1$, and $\pi - 1$ would be totally positive, which it is not, since $\bar{\pi} - 1 = \frac{\sqrt{p+8}-\sqrt{p}-2}{2} < 0$ (recall that $p \geq 17$). The case $b = 1$ cannot occur, since it would imply that y is a rational integer. Finally the case $b = -1$ would imply $\bar{\pi} \geq 1$. ∎

Now let us assume there exists an $x \in \mathrm{H} \otimes \mathcal{O}_K$ such that $q'(x) = \pi$. Then the identity

$$q'(x) = \left(x_1 + \tfrac{1}{2}x_4\right)^2 + \left(x_2 + \tfrac{1}{2}x_4\right)^2 + \left(x_3 + \tfrac{1}{2}x_4\right)^2 + \tfrac{1}{4}x_4^2$$

shows that, up to reindexing, $(x_1 + x_4/2)^2 \leq \pi/3$. We also have $(\overline{x_1 + x_4/2})^2 \leq \bar{\pi}$. Thus, writing $y = 2x_1 + x_4$, we obtain

$$(*) \qquad \mathrm{Tr}(y^2) \leq \tfrac{4}{3}(\pi + 3\bar{\pi}) \quad \text{and} \quad N(y)^2 \leq \tfrac{16}{3}N(\pi).$$

Setting $y = \frac{a+b\sqrt{p}}{2}$, with a and b rational integers of the same parity, we can rewrite the first part of $(*)$ as

$$(1) \qquad a^2 + pb^2 \leq \tfrac{16}{3}(\sqrt{p+8} - \sqrt{p}).$$

Since $p \geq 17$, this implies $b = 0$. So a is even and y is a rational integer whose fourth power, by the second part of $(*)$, cannot exceed 10. So y is either 0 or ± 1. For $p \geq 73$, it cannot be ± 1, since this would imply that $\pi - 1/4$ is a sum of squares, so $\bar{\pi} - 1/4$ is positive, which is not the case. We deduce that y is zero, x_4 is a multiple of 2, and finally π is a sum of four squares in $\mathcal{O}_K$. By Lemma 2.1, this cannot happen.

Thus, for $p \geq 73$, the equation $q'(x) = \pi$ has no solution. For $p = 17$ and $p = 41$, a computer assisted calculation shows that the same holds. In conclusion, we have the following result.

THEOREM 2.2. *Let p be a prime of the form $p = (2m+1)^2 - 8$. Let A be the ring $\mathbb{Z}[1/2, \sqrt{p}]$. Then $\mathrm{I}_4 \otimes A$ does not represent the totally positive integer $(2m+1+\sqrt{p})/2$.*

Acknowledgements. The author wishes to thank Pete L. Clark for pointing out references [3] and [4], and the referee for valuable remarks.

References

[1] E. A. Bender, *A lifting formula for the Hilbert symbol*, Proc. Amer. Math. Soc. 40 (1973), 63–65.

[2] V. Blomer and V. Kala, *Number fields without n-ary universal quadratic forms*, Math. Proc. Cambridge Philos. Soc. 159 (2015), 239–252.

[3] V. Kala, *Universal quadratic forms and elements of small norm in real quadratic fields*, Bull. Austral. Math. Soc., to appear; arXiv:1507.04237.

[4] I. Niven, *Integers of quadratic fields as sums of squares*, Trans. Amer. Math. Soc. 48 (1940), 405–417.

[5] O. T. O'Meara, *Introduction to Quadratic Forms*, Classics Math., Springer, Berlin, 2000.

Gaël Collinet
IRMA, Université de Strasbourg et CNRS
7 rue René Descartes
67084 Strasbourg, France
E-mail: collinet@math.unistra.fr