

MINKOWSKI'S EMBEDDING

MAURICE CRAIG

1. INTRODUCTION

In [3] I constructed certain quadratic forms, in low dimension, as an application of Minkowski's method for embedding a number field K in Euclidean space. The emphasis differed somewhat from the treatment in [1, p 94–99]. Rather than focus attention on the real and imaginary parts of the conjugates ξ^g of $\xi \in K$, I invoked (but omitted to name) the expression

$$\sum |\xi^g|^2. \quad (1)$$

In their account of this work, Conway and Sloane [2] start instead from the “trace norm”

$$\sum |\xi|^{2g}. \quad (2)$$

It's a catchy term, but let us beware of mistaking a slogan for an argument! Dissatisfied with several features of [2, p. 224–225], I attempt here belatedly to restore the original train of thought. Fighting fire with fire, I coin a new term of my own, calling the expression (1) the “total norm” of ξ . Though chosen in reference to the summation involved, the name is happily consistent with the terminology for totally real or totally complex fields.

My specific reservations concerning the trace norm run as follows.

(a) Restricting it to the case when K is Galois ([1, p. 224]) seems wholly gratuitous. Both expressions (1), (2) are meaningful for every number field K . Henceforth, I disregard this restriction.

(b) “The two most interesting cases for our purposes occur when K is either *totally real* ... or *totally complex* ...” ([1, p. 225]). No justification is offered for this assertion, which I consider misleading.

(c) The trace norm, while always rational, is not necessarily positive, so may fail to define a geometric embedding. The total norm, though not necessarily rational, is always positive definite.

(d) Equation (55b) of [2, p. 225], asserting the equality of the two norms when K is totally complex, is not true generally, even for Galois fields.

In numerous cases of arithmetic interest, the expressions (1), (2) agree, yielding then a positive, rational-valued quadratic form. The importance of rationality

for lattice packings of space by equal spheres is that, by a classical theorem [6, p. 248–251], the (locally and hence also globally) densest packings arise from forms with commensurate coefficients. (In technical language: “Every extreme form is perfect”.)

To state the simplest sufficient condition for agreement, let L be the rootfield for ξ and let c denote the restriction, to L , of complex conjugation. Writing

$$\text{total norm} = \sum \xi^{g(1+c)}; \quad \text{trace norm} = \sum \xi^{(1+c)g},$$

we see that the two quadratic forms concur whenever c falls in the *centre* of the Galois group $\text{Aut}(L/\mathbb{Q})$.

It is this subtler condition that should stand in place of the preference (b) expressed for totally real or totally complex fields. It holds in the special case when K is totally real, because c is then the identity map. When K is totally imaginary, it may be either valid or invalid, whence totally complex fields are in no sense distinguished as especially simple.

Section 3, the heart of the paper, elaborates two examples (mentioned already in [3]) that illustrate the capricious behaviour of such fields. However, I interpose a section aimed at clarifying the reason for preferring the total norm to the componentwise treatment in [1].

2. LATTICES AND THEIR QUADRATIC FORMS

Minkowski’s construction associates spatial coordinates with an assigned algebraic number ξ . The resulting picture, of a point suspended in Euclidean space, is scarcely illuminating *per se*. What brings life to the representation is that the points representing a subring of $\mathbb{Q}(\xi)$, such as the ring of integers, comprise a point–lattice. This fact opens a world of creative possibilities. For example, we can imagine multiply periodic functions of several real or complex variables.

A lattice can be specified by giving the coordinates for a set of basic vectors. Thus, the densest latticed–centred packing of equal spheres can be taken as having, for the lattice basis, the columns of the matrix

$$M = \begin{bmatrix} \sqrt{2} & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & \sqrt{3}/\sqrt{2} & 1/\sqrt{6} \\ 0 & 0 & 2/\sqrt{3} \end{bmatrix}. \quad (3)$$

The squared length of a typical lattice vector $\mathbf{y} = M\mathbf{x}$, $\mathbf{x} \in \mathbb{Z}^3$, is $\mathbf{y}^T\mathbf{y} = \mathbf{x}^T H\mathbf{x}$, where

$$H = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}. \quad (4)$$

It needs no explaining which matrix is the more malleable and memorable. Some information is lost, in passing from the lattice–basis matrix (3) to the quadratic form matrix (4). Namely, $H = N^T N$ also for $N = WM$, with arbitrary orthogonal W . However, the loss is slight, for $N^T N = M^T M$ implies conversely that

$N = WM$, with W orthogonal. Thus, the lattice $N\mathbb{Z}^3$ is the image of $M\mathbb{Z}^3$ under an orthogonal transformation. Reflection in the origin allows us to suppose $\det(W) > 0$, and hence that W is a mere rotation about the origin.

Minkowski's procedure [1, p. 94–99], by directing attention to coordinates, arrives at a description of the type (3), the kind just criticised for its lack of simplicity and convenience. The remedy is passage instead to the corresponding quadratic form, which is none other than the total norm. For example, if $\alpha = 2^{1/3}$, the field $K = \mathbb{Q}(\alpha)$ has an integral basis $1, \alpha, \alpha^2$. The conjugates of an integer $\xi \in K$ take the form

$$\begin{aligned}\xi &= a + b\alpha + c\alpha^2, \\ \eta &= a + b\alpha\omega + c\alpha^2\omega^2, \\ \zeta &= a + b\alpha\omega^2 + c\alpha^2\omega,\end{aligned}$$

where $a, b, c \in \mathbb{Z}$ and $\omega^2 + \omega + 1 = 0$. Thence we easily compute

$$\begin{aligned}\text{Total norm} &= \xi^2 + 2\eta\zeta = 3(a^2 + b^2\alpha^2 + c^2\alpha^4), \\ \text{Trace norm} &= \xi^2 + \eta^2 + \zeta^2 = 3(a^2 + 4bc).\end{aligned}$$

Here, the total norm is irrational but positive, able to supply an embedding in Euclidean 3-space. Its matrix factors as $3N^T N$, with $N = \text{diag}(1, \alpha, \alpha^2)$, to produce a (rectangular) point-lattice, the columns of $N\sqrt{3}$ serving as basis vectors. The trace norm, though rational, is indefinite, so fails this requirement.

The conditions for rationality of the total norm being somewhat cryptic, I noted in [3, p. 47] a pair of quartic fields, superficially similar, but with opposite behavior. They are the dihedral quartic fields determined by roots of the positive definite polynomials $x^4 + 3x^2 + 5, x^4 + 5x^2 + 3$. Unfortunately their passing mention makes little impression on the mind. Lest the intended point continue to elude notice, the section below elaborates these contrasting examples. In particular it will be seen that, to ensure rationality of the total norm, and positivity of the trace norm, it is not enough for K to be totally complex.

3. TWO QUARTIC FIELDS

The centre of the octic group $D = \langle (1234), (24) \rangle$ comprises the even permutations, whence $(13)(24)$ is central but (24) is not. The examples treat fields where c , restricted to the normal closure, is one of these two elements. Write $i = \sqrt{-1}$.

(a) Discordant Norms

Let $\alpha = \sqrt{2\sqrt{5}-3}, \beta = \sqrt{2\sqrt{5}+3}$, both positive. The polynomial with roots $(x_1, x_2, x_3, x_4) = (\alpha, i\beta, -\alpha, -i\beta)$ is $x^4 + 6x^2 - 11$. Its rootfield $L = \mathbb{Q}(\alpha, i\beta)$ has Galois group $G \cong D$, permuting the roots by its action on the subscripts. For, c clearly acts as (24) . Thence G cannot contain (1243) because $(1243)(24) = (123)$ is a 3-cycle. Likewise we may exclude (1324) and the inverses of these disallowed 4-cycles, meaning that D is the required group.

Let $\gamma = (\alpha + i\beta)/2$. The elements $\pm\gamma, \pm\gamma^c$ are the roots of $x^4 + 3x^2 + 5$. The non-normal quartic subfields of L are $\mathbb{Q}(\alpha), \mathbb{Q}(i\beta)$, intersecting in $\mathbb{Q}(\sqrt{5})$, and $\mathbb{Q}(\gamma), \mathbb{Q}(\gamma^c)$, with common subfield $\mathbb{Q}(\sqrt{-11})$. The composite of these two quadratic fields is the normal quartic field $\mathbb{Q}(\sqrt{5}, \sqrt{-11})$, containing also $\mathbb{Q}(\sqrt{-55})$.

To compute the two quadratic norms relative to the powers of γ , write $\xi = p + q\gamma + r\gamma^2 + s\gamma^3$, with $p, q, r, s \in \mathbb{Z}$. Now $\gamma + \gamma^c = \alpha$, $\gamma^{1+c} = \sqrt{5}$, whence ξ^{1+c} lies in $\mathbb{Q}(\alpha)$. Explicitly, we have

$$\begin{aligned} \xi^{1+c} = & p^2 - 3pr + 5r^2 + (q^2 - 3qs + 5s^2)\sqrt{5} \\ & + [pq - 3ps + 5rs + (qr - ps)\sqrt{5}]\alpha. \end{aligned} \quad (3)$$

The conjugate ξ^h of ξ obtained by reversing the sign of α gives a similar result, only with the signs of q, s reversed. Adding the results and doubling to account for ξ^c, ξ^{ch} , we obtain

$$\sum \xi^{g(1+c)}/2 = \xi^{1+c} + \xi^{h(1+c)} = 2(p^2 - 3pr + 5r^2) + 2(q^2 - 3qs + 5s^2)\sqrt{5}. \quad (4)$$

The total norm is thus a definite quaternary form of determinant $2^4 \cdot 5 \cdot 11^2$.

To compute the trace of ξ^{1+c} we sum the four equations obtained from (3) by conjugation. The pair for $\pm\alpha$ reproduce the right side of equation (4). For $\pm i\beta$, observe that $\sqrt{5} = (3 + \alpha^2)/2$ reverses sign. Consequently

$$\sum \xi^{(1+c)g} = 4(p^2 - 3pr + 5r^2), \quad (5)$$

a semi-definite quaternary form, albeit definite as a binary form. The equation $\gamma^{1+c} = \sqrt{5}$ gave forewarning, as this non-zero element has trace zero.

(b) Concordant Norms

The second calculation is similar but easier. Let $\alpha = \sqrt{5 - 2\sqrt{3}}, \beta = \sqrt{5 + 2\sqrt{3}}$, both positive. The polynomial with roots $(x_1, x_2, x_3, x_4) = (i\alpha, i\beta, -i\alpha, -i\beta)$ is $x^4 + 10x^2 + 13$. Its rootfield $L = \mathbb{Q}(i\alpha, i\beta)$ has Galois group $G \cong D$. This time $c = (13)(24)$. Now, $(1324)(13)(24) = (12)$ is not an automorphism, because $x_1 \mapsto x_2$ necessarily entails also $x_3 \mapsto x_4$. Hence (1324) and its inverse are excluded, and $(1243), (1342)$ likewise. But $(1234), (1432)$ and the permutations conjugate to c are admissible.

With $2u = i\alpha, 2v = i\beta$, the elements $\pm u \pm v$ are the roots of $x^4 + 5x^2 + 3$. The non-normal quartic subfields of L are $\mathbb{Q}(i\alpha), \mathbb{Q}(i\beta)$, intersecting in $\mathbb{Q}(\sqrt{3})$, and $\mathbb{Q}(u+v), \mathbb{Q}(u-v)$, both containing $\mathbb{Q}(\sqrt{13})$. The quadratic fields unite in $\mathbb{Q}(\sqrt{3}, \sqrt{13})$, with the further subfield $\mathbb{Q}(\sqrt{39})$.

The element $\gamma = u+v$ has different $2^6 u^2 v^2 (u^2 - v^2) = \alpha^2 \beta^2 (\beta^2 - \alpha^2) = 2^2 \cdot 13 \sqrt{3}$, so its powers form a basis with discriminant $2^4 \cdot 3 \cdot 13^2$. As before, write $\xi = p + q\gamma + r\gamma^2 + s\gamma^3$, with $p, q, r, s \in \mathbb{Z}$. Reversing signs for q, s gives ξ^c , whence

$$\xi^{1+c} = p^2 + 6qs - 3r^2 - 15s^2 + (2pr + 10qs - q^2 - 5r^2 - 22s^2)\gamma^2.$$

The only distinct conjugate of $\gamma^2 = (u + v)^2$ is $(u - v)^2$. The sum of these roots of $x^2 + 5x + 3$ is -5 . So the common value of the total and trace norms is

$$\sum \xi^{g(1+c)} = 2(2p^2 - 10pr + 19r^2) + 2(5q^2 - 38qs + 80s^2), \quad (6)$$

a positive quaternary form of determinant $2^4 \cdot 3 \cdot 13^2$.

These two quartic fields are not themselves Galois. However, the conclusions extend to their normal closures (complex, self-conjugate, and hence again totally complex). For example, the trace norm cannot be positive on an octic field if not so on some quartic subfield.

Finally, the discriminant of γ in both examples coincides with the field discriminant of $\mathbb{Q}(\gamma)$, as given by [4, Theorem 1, p. 89]. Hence the γ -power bases are actually \mathbb{Z} -bases for their respective quartic fields. The equalities of determinants with discriminants thus accords with [3, Lemma 1, p. 44].

REFERENCES

- [1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*. Academic Press, New York, 1966, 453 pp.
- [2] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*. Springer, New York, 1988, 663 pp.
- [3] M. Craig, *Extreme forms and cyclotomy*. *Mathematika* **25** (1978), 44–56.
- [4] J. G. Huard, B. K. Spearman and K. S. Williams, *Integral bases for quartic fields with quadratic subfields*. *J. Number Theory* **53** (1995), 87–102.
- [5] L.-C. Kappe and B. Warren, *An elementary test for the Galois group of a quartic polynomial*. *Amer. Math. Monthly* **96** (1989), 133–137.
- [6] A. Korkine and G. Zolotareff, *Sur les formes quadratiques positives*. *Math. Ann.* **11** (1877), 242–292.
- [7] C. E. van der Ploeg, *Duality in non-normal quartic fields*. *Amer. Math. Monthly* **94** (1989), 279–284. (On p. 281 a superscript 2 is missing.)