Total positivity and algebraic Witt classes.

Comment. Math. Helvetici 60 (1985) 284-290 0010-2571/85/020284-07$01.50 + 0.20/0

Total positivity and algebraic Witt classes

DENNIS R. ESTES, JURGEN HURRELBRINK, and ROBERT PERLIS

This paper is in three parts. In the first part we give a criterion for an element of an algebraic number field F to be totally positive. Part two contains simple reformulations of this criterion in terms of Brauer groups, the Milnor K-*Group* $K_2(F)$, and sums of squares. Part three contains an application, due to P. E. Conner. It characterizes the totally positive elements of F as those elements α for which the rank one quadratic form αX^2 is Witt equivalent to the trace form of some finite extension E of F. As a corollary, it is proved that every Witt class in the Witt ring $W(F)$ is represented by a trace form when the base field F is purely imaginary.

We take this opportunity to acknowledge the generous contribution of P. E. Conner, and we thank him for many discussions.

I. The Norm Theorem

Let F be an algebraic number field. An element α in F^* is said to be *totally positive* (relative to F) if α is positive in every possible ordering of F. In particular, if F has no real embeddings, then every element of F^* is totally positive.

NORM THEOREM. *Let $\alpha \neq 0$ be an element of an algebraic number field F. Then there is a positive rational number q such that $-q$ is a norm from $F(\sqrt{\alpha})/F$ if and only if α is totally positive. Moreover, the existence of one positive rational number q with $-q$ a norm from $F(\sqrt{\alpha})/F$ is equivalent with the existence of infinitely many rational primes q with $-q$ a norm from $F(\sqrt{\alpha})/F$.*

Proof. We may replace α by αt^2 with $t \neq 0$ in $\mathbb{Z}$ without affecting the statement of the theorem, and therefore we can assume that α is an algebraic integer. Suppose that α is totally positive, and set $m = 8 \cdot N_{F/\mathbb{Q}}(\alpha)$. Then m is a positive integer. Let ζ_m be a primitive m-th root of unity, and let N be the normal closure over $\mathbb{Q}$ of $F(\sqrt{\alpha}, \zeta_m)$. Fix an embedding of N into the field of complex numbers, so we can talk about complex conjugation acting on N. By Čebotarev's Density

Theorem, there are infinitely many prime numbers q, unramified in N, having a prime factor Q in N whose Frobenius automorphism is complex conjugation. Of these infinitely many q take any one which is relatively prime to m. We claim that $-q$ is a norm from $F(\sqrt{\alpha})/F$.

This can be checked locally. Let P denote a prime of F. If P is infinite, then $F_P(\sqrt{\alpha}) = F_P$; this is obvious if P is complex, while if P is real this follows from the fact that α, being totally positive, is positive in the real embedding of F associated with P. In either case, we see that $-q$ is a norm from the trivial local extension. Now consider finite primes P of F. There are several cases. If P does not divide mq, then $-q$ is a unit in the local unramified extension $F_P(\sqrt{\alpha})/F_P$ and therefore $-q$ is a local norm (see [Lang], Lemma 4, p. 188). It remains to consider finite primes P dividing mq.

First, we claim that $-q \equiv 1 \pmod{m}$. For this let Q, from above, be the prime of N lying over q whose Frobenius automorphism Φ_Q is complex conjugation. Then we have

$$(\zeta_m)^{-1} = \Phi_Q(\zeta_m) \equiv (\zeta_m)^q \pmod{Q}.$$

Since $(q, m) = 1$, the m-th roots of unity are distinct mod Q, and it follows that $\zeta_m^{-1} = \zeta_m^q$ in F; that is, $-q \equiv 1 \pmod{m}$.

Now suppose that the prime P of F divides mq. If P divides m and is nondyadic, then the fact $-q \equiv 1 \pmod{P}$ implies that $-q$ is a square in F_P, and is therefore a norm from $F_P(\sqrt{\alpha})/F_P$. If P is a dyadic prime dividing m, then $-q \equiv 1 \pmod{m}$ implies $-q \equiv 1 \pmod{8}$ by the definition of m, so $-q$ is already a square in the subfield $\mathbb{Q}_2$ of F_P, and therefore $-q$ is a norm from $F_P(\sqrt{\alpha})/F_P$. Finally, suppose that P divides q. Again, let Q be the chosen factor of q in N whose Frobenius automorphism equals complex conjugation, and let $\Phi_{Q'}$ be the Frobenius automorphism of a prime factor Q' of P in N. Then $\Phi_{Q'} = \sigma^{-1}\Phi_Q\sigma$ for some σ in $\mathrm{Gal}(N/\mathbb{Q})$. We claim that the extension $F_P(\sqrt{\alpha})/F_P$ is trivial. Now this extension is sandwiched in the quadratic extension $N_{Q'}/\mathbb{Q}_q$. Note that the Galois group of this latter extension is generated by $\Phi_{Q'}$.

Therefore $F_P(\sqrt{\alpha}) = F_P$ if and only if $\Phi_{Q'}$ has the same restriction to both of these fields. But this is detected in the dense subfields $F(\sqrt{\alpha})$ and F. If $\Phi_{Q'}$ acts non-trivially on F then there is nothing to show, so we may assume that $\Phi_{Q'}$ is trivial on F. Then for each x in F we see that $\sigma(x)$ is fixed by complex conjugation, so σ is a real embedding of F. Since α is totally positive, $\sigma(\sqrt{\alpha})$ is real, and it follows that $\Phi_{Q'}$ is also trivial on $F(\sqrt{\alpha})$. Hence $F_P(\sqrt{\alpha}) = F_P$, so $-q$ is a norm from $F_P(\sqrt{\alpha})/F_P$. This being true for every P, Hasse's Norm Theorem implies that $-q$ is a norm from $F(\sqrt{\alpha})/F$.

Conversely, if α is not totally positive then α is not a square in F. If q is a positive rational number and $-q$ is a norm from $F(\sqrt{\alpha})/F$ then $-q = x^2 - \alpha y^2$ for appropriate x and y in F. But then for some real embedding of F we would have $x^2 - \alpha y^2$ to be positive, while $-q$ is negative. Hence $-q$ is not a norm.

We finish this first part with a small remark. While we started it for algebraic number fields, the Norm Theorem can be interpreted for any field F of characteristic 0. It is easy to see that the Norm Theorem remains true when F is any p-adic field. However, for $F = \mathbb{R}(X_1, X_2, X_3, X_4)(\sqrt{-d})$ with $d = X_1^2 + X_2^2 + X_3^2 + X_4^2$ one can show that the Norm Theorem is false for the choice $\alpha = d$.

II. Reformulations

Since $-q$ is represented over F by the binary quadratic form $\langle 1, -\alpha\rangle$ if and only if α is represented over F by $\langle 1, q\rangle$, the Norm Theorem can be restated as

REFORMULATION 1. *Let F be a number field and α in F^*. Then there exists a positive q in $\mathbb{Z}$ such that α is represented over F by the form $\langle 1, q\rangle$ if and only if α is totally positive.*

Recall that an element of F^* is totally positive if and only if it is a sum of squares of elements in F^*. Hence even for sums of squares in F which require more than two squares (i.e. three or four in the number field case) we obtain

REFORMULATION 2. *Let α be an element in a number field F. Then α is a sum of squares in F if and only if α is a single square plus a sum of equal squares of elements of F, i.e. $\alpha = x^2 + y^2 + \cdots + y^2$ for certain elements x, y in F.*

Since $-q$ is a norm from $F(\sqrt{\alpha})/F$ if and only if the quaternion algebra $\left(\frac{\alpha, -q}{F}\right)$ is isomorphic to a full matrix algebra $M_2(F)$, if and only if the class of $\left(\frac{\alpha, -q}{F}\right)$ is trivial in the Brauer group $Br(F)$, we have

REFORMULATION 3. *Let F be a number field and α in F^*. Then there exists a rational prime q such that $\left(\frac{\alpha, -q}{F}\right) = 1$ in $Br(F)$ if and only if α is totally positive.*

Now consider the quadratic norm residue homomorphism from the Milnor

K-group $K_2(F)$ to $Br(F)$, which maps every Steinberg symbol $\{a, b\}$ in $K_2(F)$ to the class of $\left(\frac{a, b}{F}\right)$ in $Br(F)$. The kernel of this map is the subgroup of squares in $K_2(F)$ (see [Tate], Theorem 2, p. 207 for number fields F, or [Mer] for arbitrary fields F). Thus we see

REFORMULATION 4. *Let F be a number field and α in F^*. Then there exists a rational prime q such that $\{\alpha, -q\}$ is a square in $K_2(F)$ if and only if α is totally positive.*

III. Algebraic Witt classes

We will use the results of [C–P] to obtain another characterization of total positivity. Let E be a finite extension of the algebraic number field F. The *trace form* of the extension E/F is the quadratic form $tr_{E/F}(X^2)$, and the Witt class of this form in the Witt ring $W(F)$ is denoted $\langle E\rangle$. The Witt classes in $W(F)$ arising in this way from algebraic extensions E/F are said to be *algebraic* classes. For an element α of F^*, the Witt class of the rank one form αX^2 is denoted $\langle\alpha\rangle$.

COROLLARY 1. *The element α in F^* is totally positive if and only if the Witt class $\langle\alpha\rangle$ in $W(F)$ is algebraic.*

We use three lemmas from [C–P].

LEMMA 1. *Let $f(t) = t^m + at + b$ be an irreducible polynomial in $F[t]$, with odd degree $m \geqslant 3$. Let $E = F[t]/(f(t))$ be the associated extension of F, and let $d = \operatorname{dis}\langle E\rangle$ be the discriminant of the Witt class $\langle E\rangle$. Then in $W(F)$*

$$\langle E\rangle = \langle d\rangle + (\langle d\rangle - \langle 1\rangle)(\langle 1-m\rangle - \langle 1\rangle).$$

This is proved in [C–P], Theorem VI.2.1 for the field $F = \mathbb{Q}$, but the proof is valid for any field F of characteristic 0.

LEMMA 2. *For any odd $m \geqslant 3$ and for any α in F^* there is an irreducible trinomial $f(t) = t^m + at + b$ in $F[t]$ for which the resulting extension E has* $\operatorname{dis}\langle E\rangle =$ *α, modulo squares in F^*.*

This was shown in [C–P], Theorem VI.2.8, again for the field $F = \mathbb{Q}$. However, the argument is entirely local in character, and extends at once to any algebraic number field F.

LEMMA 3. *Let E be a finite extension of the algebraic number field F. Then in any ordering of F the corresponding signature of the Witt class $\langle E\rangle$ equals the number of extensions of that ordering to an ordering of E. Hence if X is an algebraic Witt class in $W(F)$, then every signature of X is non-negative.*

This is proved in [C–P], Theorem I.5.2 when $F=\mathbb{Q}$, and again the proof remains true without change when F is an algebraic number field.

Proof of Corollary 1. Take α in F^* and assume that $\langle\alpha\rangle$ is algebraic. By Lemma 3, every signature of $\langle\alpha\rangle$ is non-negative, so α is non-negative and hence positive in every ordering of F. So α is totally positive.

Conversely, suppose α is totally positive. By the Norm Theorem we can find a positive rational integer whose negative is a relative norm from $F(\sqrt{\alpha})/F$. Multiplying by the square 4, which is clearly a relative norm, we may assume our rational integer to be even, say $2n$. Take $m=2n+1$. Then using Lemmas 1 and 2 we find an extension E/F of degree m for which

$$\langle E\rangle=\langle\alpha\rangle+X$$

with $X=(\langle\alpha\rangle-\langle 1\rangle)(\langle -2n\rangle-\langle 1\rangle)$ in $W(F)$. We contend that $X=0$. For this it suffices to show that the invariants of X equal the corresponding invariants of the 0 class in $W(F)$, namely: $\operatorname{rank}(0)\equiv 0 \pmod 2$; $\operatorname{sgn}(0)=0$ in any ordering, $\operatorname{dis}(0)\equiv 1$ modulo squares in F^*, and every Hasse–Witt symbol $c_p(0)=1$. Clearly $\operatorname{rank}(X)\equiv 0 \pmod 2$. Since α is totally positive, the presence of the factor $\langle\alpha\rangle-\langle 1\rangle$ guarantees that every signature of X is 0. Being the product of two classes of even rank, $\operatorname{dis}(X)$ is a square in F^* (see [C–P], p. 12), so $\operatorname{dis}(X)\equiv 1$ modulo squares. Finally we compute the Hasse–Witt symbols $c_p(X)$. By multiplying the factors in X and adding two copies of the trivial class $\langle 1,-1\rangle$ we obtain the rank 8 representative $\langle -2\alpha, -\alpha, 2n, 1, 1, -1, 1, -1\rangle$ of X. Then the Hasse–Witt symbol $c_p(X)$ is just the Hasse symbol of this rank 8 representative, and using the definition (see [C–P], p. 15) we see at once that $c_p(X)=(-2n,\alpha)_p$. But since $-2n$ is a relative norm from $F(\sqrt{\alpha})/F$ this latter symbol is 1, as desired. So $X=0$, and $\langle\alpha\rangle=\langle E\rangle$ is an algebraic class, proving Corollary 1.

In the extreme case when the number field F is totally complex there are no orderings at all, so every element α in F^* is totally positive, and the Witt class $\langle\alpha\rangle$ of every rank one form αX^2 is algebraic. In fact we can show more.

COROLLARY 2. *If the algebraic number field F is totally complex then every Witt class in $W(F)$ is algebraic.*

Proof. Take X in $W(F)$ and suppose first that X has even rank. Since F has no orderings, it follows that X is algebraic by [C–P], Theorem II.9.5. So we must consider classes of odd rank.

Since F is an algebraic number field with no orderings, any quadratic form over F of rank exceeding four is isotropic. Hence the odd-rank Witt class X is represented by a rank three form, which may still be isotropic. The matrix of this form, after diagonalizing, is a non-singular 3×3 diagonal matrix over F. Then Lemmas III.5.4 and III.5.2 of [C–P] show the existence of a cubic extension L of F and an element α in L^* such that X can be written

$$X = T_{L/F}\langle\alpha\rangle_L$$

as the Scharlau Transfer of the Witt class $\langle\alpha\rangle_L$ in $W(L)$. (Since we will deal with several fields, we have appended a subscript on the Witt classes). Now the field L is also totally complex, so we can apply Corollary 1 to $\langle\alpha\rangle_L$ in $W(L)$ to find an extension E/L for which $\langle E\rangle_L = \langle\alpha\rangle_L$ in $W(L)$. Note that the class $\langle E\rangle_L$ in $W(L)$ is just the image under the Scharlau Transfer $T_{E/L}$ of the class $\langle 1\rangle_E$ in $W(E)$. If we then transfer this class all the way down to $W(F)$ we obtain

$$\langle E\rangle_F = T_{E/F}\langle 1\rangle_E = T_{L/F}\langle\alpha\rangle_L = X,$$

so X is algebraic. This proves Corollary 2.

In general it is a difficult problem to determine the algebraic classes in the Witt ring of an algebraic number field F. By Lemma 3, any algebraic class necessarily has non-negative signature in every possible ordering of F. When $F=\mathbb{Q}$ is the field of rational numbers, it is proved in [C–P] that non-negative signature is not only a necessary but also a sufficient condition for a Witt class in $W(\mathbb{Q})$ to be algebraic. This result together with Corollary 2 makes it reasonable to ask:

Question. Let F be an algebraic number field. Is it true that a Witt class X in W(F) is algebraic if and only if the signature of X with respect to every ordering of F is non-negative?

REFERENCE

[Lang] S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass. (1970).

[Lam] T. Y. Lam, *The algebraic theory of quadratic forms*, W. A. Benjamin, Reading, Mass. (1973).

[C–P] P. E. Conner and R. Perlis, *A survey of trace forms of algebraic number fields*, Lecture Notes on Pure Math. 2, World Scientific, Singapore (1984).

[Mer] A. S. MERKURJEV, *On the norm residue symbol of degree 2*, Dokl. Akad. Nauk. SSSR, *261*, 542–547, (1981).

[Tate] J. TATE, *Symbols in arithmetic*, Proc. ICM Nice 1970, vol. 1, 201–211, (1971).

Department of Mathematics
University of Southern California
Los Angeles, CA 90089–1113

Department of Mathematics
Louisiana State University
Baton Rouge, LA 70803

Department of Mathematics
Louisiana State University
Baton Rouge, LA 70803

Received August 6, 1984