Pacific Journal of Mathematics

DIAGONALIZATION UP TO WITT

MAX WARSHAUER

Vol. 98, No. 2 April 1982

PACIFIC JOURNAL OF MATHEMATICS
Vol. 98, No. 2, 1982

DIAGONALIZATION UP TO WITT

MAX WARSHAUER

In this paper we construct an additive system of generators for the Witt group of u-Hermitian inner product spaces.

The idea to do this was suggested by Conner, who should be thanked for his help on this and other matters. The reader should note that the additive system of generators obtained is for $H_u(K)$, where K is a fractional ideal in an algebraic number field. In this setting there are in general no rank one forms. This contrasts sharply with the case of $H_1(O(K))$ for the Dedekind ring of integers $O(K)$ in an algebraic number field which has been studied and understood [1].

The case of a fractional ideal arises in [3], for example, where the group $H_{\pm 1}(\mathscr{D}^{-1}(E/Q))$ for $K = \mathscr{D}^{-1}(E/Q)$ the inverse different is computed. However, no method for constructing representatives of the Witt classes is discussed in [3].

In [2], the group $H_{-1}(Z(\lambda))$, where $\lambda = \exp 2\pi i/p$ a pth root of unity, p an odd prime, was studied. Here rank 2 forms were constructed by *ad hoc* considerations. We return to this example later, as it is a special case of the general result we obtain.

We now begin by describing the setting in which we work. Let E be an algebraic number field together with an involution —. The fixed field of — is F. We denote by $O(E)$ and $O(F)$ the Dedekind rings of integers in E and F respectively. Let K be a — invariant fractional $O(E)$-ideal. We fix u a unit in E of norm 1, i.e., $u\bar{u} = 1$.

DEFINITION 1. A K-valued inner product space is a pair (M, B) satisfying:

(1) M is a finitely generated torsion free $O(E)$-module.

(2) B: $M \times M \to K$ is a non-singular K-valued u-Hermitian inner product defined on M.

The non-singularity condition is that the adjoint map $Ad_R B$: $M \to \mathrm{Hom}_{O(E)}(M, K)$ defined by $m \to B(-, m)$ is an isomorphism. Further, B is u-Hermitian, meaning

(a) $B(x, y) = u\overline{B(y, x)}$ for x, y in M.

(b) $B(\lambda x, y) = B(x, \bar{\lambda} y) = \lambda B(x, y)$ for λ in $O(E)$.

Note that when $u = +1$, this is the usual notion of Hermitian. When $u = -1$, we have skew-Hermitian. The generalization to u-

Hermitian arises naturally in studying asymmetric inner product spaces [4], where no assumption about symmetry is made.

An inner product space (M, B) is metabolic or Witt equivalent to zero if there is a subspace $N \subset M$ which is equal to its own orthogonal complement $N^{\perp}$. This means $N = N^{\perp} = \{v \in M: B(v, n) = 0 \text{ for all } n \in N\}$. If such an N exists, it is called a metabolizer.

DEFINITION 2. Two Hermitian inner product spaces (M_1, B_1) and (M_2, B_2) are Witt equivalent if $(M_1 \oplus M_2, B_1 \oplus -B_2)$ is metabolic.

The notion of Witt equivalence is an equivalence relation and there results the usual Witt group $H_u(K)$ of Witt equivalence classes of u-Hermitian K-valued inner product spaces. The reader is referred to [1] where this group is discussed in detail. The intimate relation of this group to topology is examined in [3] and [2].

We begin our study of the general case by introducing the group $\mathrm{Iso}\,(E/F)$. The purpose of this group is to restrict out attention to various equivalence classes of $H_u(K)$ which are canonically isomorphic. Following [1], we consider pairs (u, K) satisfying:

(1) $u\bar{u} = 1$. K is a — invariant fractional $O(E)$-ideal.

(2) (u, K) is equivalent to (u_1, K_1), written $(u, K) \sim (u_1, K_1)$, provided there exists a fractional $O(E)$-ideal A, and $x \in E$, satisfying

(a) $xA\bar{A}K = K_1$

(b) $x\bar{x}^{-1}u = u_1$

The group of equivalence classes of pairs (u, K) satisfying (1) and (2) is called $\mathrm{Iso}\,(E/F)$. The following theorem results.

THEOREM 3. *$(u, K) \sim (u_1, K_1)$ implies $H_u(K)$ is canonically isomorphic to $H_{u_1}(K_1)$.* [1, p. 29]

This theorem implies that to give an additive system of generators for $H_u(K)$ it suffices to consider the equivalence class $|u, K|$ of (u, K) in $\mathrm{Iso}\,(E/F)$.

In fact, we can compute $\mathrm{Iso}\,(E/F)$ as follows. Let R denote the collection of prime ideals $\mathfrak{P}$ in $O(E)$ which lie over prime ideals P in $O(F)$ which ramify in E over F.

Now suppose $E = F(\sqrt{\sigma})$. Let $\tau: F \to \boldsymbol{C}$ be an embedding. We say τ is a real infinite prime if $\tau: F \to \boldsymbol{R}$, and in this case τ induces an ordering on F. If $\sigma < 0$ with respect to this ordering, meaning $\tau(\sigma) < 0$, then τ is said to be an infinite ramified prime as opposed to the (finite) ramified prime ideals described above.

Each infinite ramified prime gives rise to a signature $\mathrm{sgn}\,[M, B]$

for $[M, B]$ in $H_u(K)$. The signature is obtained by letting $X^+ = \{x \in M: B(x, x) > 0\}$, and $X^- = \{x \in M: B(x, x) < 0\}$. Then $\operatorname{sgn}[M, B] =$ dimension X^+-dimension X^-.

Associated to a finite prime ideal $\mathfrak{P}$ in $O(E)$ is the $\mathfrak{P}$-adic valuation $v_{\mathfrak{P}}$ on E. If K is a fractional ideal, $v_{\mathfrak{P}}(K)$ is the exponent to which $\mathfrak{P}$ appears in the factorization of K. If $x \in E$, $v_{\mathfrak{P}}(x) = v_{\mathfrak{P}}(xO(E))$.

We now define a map f: $\operatorname{Iso}(E/F) \to R/R^2$ by:

$$|u, K| \longrightarrow \prod_{\substack{\mathfrak{P}=\bar{\mathfrak{P}} \\ \mathfrak{P} \text{ over ramified}}} \mathfrak{P}^{v_{\mathfrak{P}}(z)+v_{\mathfrak{P}}(K)},$$

where $z\bar{z}^{-1} = u$ is given by Hilbert's Theorem 90.

THEOREM 4. *If at least one prime, finite or infinite, is ramified, then f above is an isomorphism. If no primes ramify,* $\operatorname{Iso}(E/F)$ *is isomorphic to C_2, the finite group with 2 elements.* [1, p. 82]

The final preliminary step needed is to recall the computation of $H_u(K)$. This is done in terms of an exact sequence

$$0 \longrightarrow H_u(K) \longrightarrow H_u(E) \xrightarrow{\partial} H_u(E/K).$$

$H_u(K)$ is then the kernel of the ∂ map, which is computed in [1, p. 89].

At each prime $\mathfrak{P}$, there is the local boundary

$$\partial(\mathfrak{P})\colon H_u(E) \longrightarrow H_u(E/K(\mathfrak{P})) \approx H(O(E)/\mathfrak{P}).$$

We will implicitly use this calculation in what follows. The important observation is this. Choose $x \in E$ with $x\bar{x}^{-1} = u$. Then ramified primes are divided into two classes

(a) $\operatorname{cl}(\mathfrak{P}) = 0$ if $v_{\mathfrak{P}}(K) \equiv v_{\mathfrak{P}}(x) \bmod 2$.

(b) $\operatorname{cl}(\mathfrak{P}) = 1$ if $v_{\mathfrak{P}}(K) \equiv v_{\mathfrak{P}}(x) + 1 \bmod 2$.

$\partial(\mathfrak{P}) = 0$ at ramified primes of class 0, and $\partial(\mathfrak{P})$ preserves rank at ramified primes of class 1 [1, p. 94]. Thus we see that in order for a rank 1 form to exist it is necessary that there be no class 1 ramified primes.

We now proceed to give an additive system of generators for $H_u(K)$. By Theorem 3, it suffices to consider $|u, K|$ in $\operatorname{Iso}(E/F)$.

Case 1. If no prime, finite or infinite, is ramified, then

$$|u, K| = \text{(a) } |1, O(E)| \text{ or}$$
$$\text{(b) } |1, \mathfrak{P}| \ \mathfrak{P} \text{ inert.}$$

This is discussed in [4]. In case (a), $H_1(O(E))$ is generated by the 1-dimensional form $[O(E), 1]$. In case (b), $H_1(\mathscr{P}) = 0$.

Case 2. Some prime, finite or infinite, is ramified. By Theorems 3 and 4, we may without loss of generality write $K = \mathscr{P}_1 \cdots \mathscr{P}_s$, where $\mathscr{P}_i$ are ramified, and choose $u = 1$.

(a) If $s = 0$, $K = O(E)$. In this case there are no class 1 ramified primes and a rank 1 form exists. A complete description of the additive generators is given in [1, p. 102]

(b) If $s > 0$, then all ramified primes $\mathscr{P}_i$ which divide K are class 1, so no rank 1 forms can exist. The object now is to build up rank 2 forms which generate $H_1(K)$.

Before continuing, we introduce the Hilbert symbol $(y, \sigma)_P$, where $y \in F$, and $E = F(\sqrt{\sigma})$. This symbol is $+1$ if y is a norm from the completion of E at $\mathscr{P}$, and -1 otherwise. We shall need the following lemma.

LEMMA 5. *For P tamely ramified, (characteristic of $O(F)/P$ not equal to 2), a local unit u is a local norm,* i.e. $(u, \sigma)_P = +1$, *if and only if the image of u in the residue field $O(F)/P$ is a square.* [1, p. 10]

Now let d be a discriminant for a form $[M, B]$ in $H_1(K)$. The following conditions follow from the boundary sequence.

(1) $(d, \sigma)_P = +1$ at P inert.

(2) $(d, \sigma)_P = +1$ at all class 1 ramified primes. This is because $[M, B]$ is even rank, and the Hilbert symbol determines $\partial(P)$.

The following lemma is not difficult to show.

LEMMA 6. *If d is the discriminant of (M, B), then there is a fractional $O(E)$-ideal A with $dA\bar{A} = O(E)$. In fact, we may take $A = \Lambda^n M$, the nth exterior power of M.*

Now let L: $E \oplus E \to E \oplus E$ have matrix $\begin{pmatrix} \alpha & \beta \\ \bar{\beta} & \gamma \end{pmatrix}$. Identify elements in $E \oplus E$ as column vectors $\begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$. Then L defines an E-valued Hermitian inner product L^* on $E \oplus E$ as follows. Let $x = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ any $y = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ be elements in $E \oplus E$. Then $L^*(x, y) = (\bar{b}_1 \bar{b}_2)\begin{pmatrix} \alpha & \beta \\ \bar{\beta} & \gamma \end{pmatrix}\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \bar{y}^t L x$.

We shall now show that L can be chosen with the following properties:

(1) L: $O(E) \oplus AK \to K \oplus dA$

(2) L^{-1}: $K \oplus dA \to O(E) \oplus AK$

(3) $\alpha\gamma - \beta\bar{\beta} = -d$, so L^* has discriminant d.

The following lemmas follow.

LEMMA 7. *L^* satisfying* (1), (2) *and* (3) *above defines a K-valued Hermitian inner product on $O(E) \oplus AK$.*

LEMMA 8. *If L satisfies condition* (3), *and $\alpha \in K$, $\beta \in d\bar{A} = A^{-1}$, and $\gamma \in dK^{-1}$, then L will also satisfy conditions* (1) *and* (2).

We now make an observation. By the Strong Approximation Theorem, we can find $w \in E$ satisfying $wA \subset O(E)$, and wA and K are relatively prime ideals. Notice now that if $dA\bar{A} = O(E)$, then $(d/w\bar{w})(wA)(\bar{w}\bar{A}) = O(E)$. We may now rechoose d as $d/w\bar{w}$ and A as wA. This does not affect the norm class of d, so without loss of generality $A \subset O(E)$, and A and K are relatively prime $O(E)$-ideals.

We now show how to choose α, β, γ satisfying $\alpha\gamma - \beta\bar{\beta} = -d$. Thus, we must solve $\alpha\gamma + d = \beta\bar{\beta}$, or

$$(*) \qquad \alpha(\gamma d^{-1}) + 1 = d^{-1}(\beta\bar{\beta})$$

To begin with, let $\gamma = d$. Then $\gamma \in dO(E) \subset dK^{-1}$. Consider the above equation modulo $\mathfrak{P}_i$ where $\mathfrak{P}_i$ divides K.

We claim that there exists β_i' in $O(E)/\mathfrak{P}_i$ such that $1 = d^{-1}(\beta_i'\bar{\beta}_i')$. ($\beta_i' = \bar{\beta}_i'$ since $\mathfrak{P}_i$ is ramified). In order to see this, recall that $dA\bar{A} = O(E)$, so $d^{-1} \in A\bar{A} \subset O(E)$. By choice A and K are relatively prime ideals, so d^{-1} is a local unit at all $\mathfrak{P}_i$ dividing K. But all $\mathfrak{P}_i$ dividing K are class 1 ramified primes, so by the boundary sequence $(d, \sigma)_P = +1$ at all such $\mathfrak{P}_i$. Thus, by Lemma 5, d^{-1} is a square in the residue field at all tamely ramified primes dividing K. At all wildly ramified primes dividing K, d^{-1} is also clearly a square in the residue field since in this case the residue field has characteristic 2 and everything is a square. Thus, for all primes $\mathfrak{P}_i$ dividing K, we can find β_i' in $O(E)/\mathfrak{P}_i$ such that

$$1 = d^{-1}(\beta_i'\beta_i') \ .$$

Let β_i be a lift of β_i' to $O(E)$.

Notice that if $\mathfrak{P}_i$ and $\mathfrak{P}_2$ are relatively prime ideals dividing K, then we can find r_1, s_2 in $\mathfrak{P}_1$ and $\mathfrak{P}_2$ with $r_1 + s_2 = 1$. Now consider $\beta_2 r_1 + \beta_1 s_2$. It follows that $(\beta_2 r_1 + \beta_1 s_2)^2 d^{-1} = 1$ in $O(E)/\mathfrak{P}_1$ and $O(E)/\mathfrak{P}_2$. Thus $(\beta_2 r_1 + \beta_1 s_2)^2 d^{-1} = 1$ in $O(E)/\mathfrak{P}_1\mathfrak{P}_2$. It follows inductively that we can find $\beta \in O(E) \subset A^{-1}$ such that $\beta^2 d^{-1} = \beta\bar{\beta}d^{-1} = 1$ in $O(E)/K$. Thus there exists $\alpha \in K$ with $(\beta\bar{\beta})d^{-1} = 1 + \alpha = 1 + \alpha(\gamma d^{-1})$ as desired.

So given d a discriminant of any form in $H_1(K)$, we have pro-

duced a two dimensional form $\begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix}$ with discriminant d. The question is whether these two-dimensional forms generate $H_1(K)$.

A. If there are no infinite ramified primes, so no signatures, then the answer is yes. In this case, $H_1(E)$ is determined by rank mod 2 and discriminant, and we have realized all possible discriminants.

B. Suppose there are 2 or more infinite ramified primes. Then arguing as above we may produce a two-dimensional form $M = O(E) \oplus AK$, $B = \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix}$, with discriminant d satisfying:

$(d, \sigma)_P = +1$ at all primes, finite or infinite, except for τ_1 and τ_2, two specified infinite primes.

$(d, \sigma)_{\tau_1} = (d, \sigma)_{\tau_2} = -1$.

Note that $(d, \sigma)_{\tau_1} = -1$ implies $[M, B]$ has signature ± 2 at τ_1. By tensoring with an appropriate 1-dimensional form from $H_1(O(E))$ if necessary, we can produce two 2-dimensional forms in $H_1(K)$ with the following properties.

$[M_1, B_1]$ has signature $+2$ at τ_1 and τ_2 .
$[M_2, B_2]$ has signature $+2$ at τ_1 and -2 at τ_2 .

These forms still have discriminant d since tensoring an even rank form with a 1-dimensional form from $H(O(E))$ does not change the discriminant. Hence $[M_1, B_1] \oplus [M_2, B_2]$ has signature $+4$ at τ_1, and 0 at τ_2. In this manner, we have shown that J^2, the square of the fundamental ideal of even rank forms, is additively generated by the 2-dimensional forms described above. However, the collection of 2-dimensional forms given clearly generates $H_1(K)/J^2$ which is determined by rank mod 2 and discriminant.

C. There is exactly one infinite ramified prime τ. If there are any class 0 ramified primes, meaning any $\mathfrak{P}_i$ which ramify but do not divide K, we can produce a 2-dimensional form with discriminant d having $(d, \sigma)_\tau = -1$ by realization of Hilbert symbols and the above construction. We use the class 0 ramified prime $\mathfrak{P}_i$ to let $(d, \sigma)_{P_i} = -1$ and satisfy Hilbert reciprocity. This 2-dimensional form has signature ± 2. Adding this form to itself, it is clear that we obtain a form with signature ± 4, and trivial discriminant. Hence J^2 is additively generated by this 2-dimensional form, and we finish as before.

The above also works if there are any dyadic ramified primes. However, if there are no class 0 ramified primes and all ramified primes are non-dyadic, then every form $[M, B]$ in $H_1(K)$ has even rank and discriminant d satisfying $(d, \sigma)_P = +1$ at all primes except possibly τ, the one infinite ramified prime. But then Hilbert reciprocity implies $(d, \sigma)_\tau = +1$ also. Thus, there are no non-zero 2-dimensional forms. $H_1(K)$ is then generated by 4-dimensional form with signature $+4$ at τ, but it is unclear how to explicitly produce this form.

We have thus shown in all cases except the above how to explicitly construct a collection of 2-dimensional forms additively generating $H_1(K)$. In this one exceptional case, $H_1(K)$ has no non-zero 2-dimensional forms, and is additively generated by a 4-dimensional form with signature $+4$.

To illustrate these results, again consider $H_{-1}(Z(\lambda))$. In Iso (E/F), $|-1, Z(\lambda)| = |1, \mathscr{P}|$, where $\mathscr{P} = \bar{\mathscr{P}}$ is the prime in $Z(\lambda)$ over $p \in Z$. In fact, letting $\Delta = \lambda^{(p-1)/2} - \lambda^{(p+1)/2} = \lambda^{(p-1)/2}(1 - \lambda)$ we see that Δ generates $\mathscr{P}$. However $\bar{\Delta} = -\Delta$, so $\Delta\bar{\Delta}^{-1} = -1$, and we use the isomorphism f preceding Theorem 4.

All $(p - 1)/2$ infinite primes in $Q(\lambda + \lambda^{-1}) = F$ ramify, and $\mathscr{P} = \bar{\mathscr{P}} = (\Delta)$ is the only finite prime over ramified. Our discussion applies perfectly. When $p = 3$, we obtain the exceptional case described above. In this case only one real infinite prime ramifies, and only one finite non-dyadic prime ramifies.

References

1. P. E. Conner, *Notes on the Witt Classification of Innerproduct Spaces over a Ring of Algebraic Integers*, University of Texas Press, Austin, Texas (1979).
2. P. E. Conner, J. P. Alexander, and G. C. Hamrick, *Odd Order Group Actions and Witt Classification of Innerproducts*, Lecture Notes in Mathematics 625, Springer-Verlag, Heidelberg, Germany, (1977).
3. N. W. Stoltzfus, *Unravelling the integral knot concordance group*, Mem. Amer. Math. Soc., Prov., R. I. (1977).
4. M. L. Warshauer, *Witt Classification of Inner Product Spaces*, Dissertation, L.S.U., Baton Rouge, La. (1979).

Received February 22, 1980.

Southwest Texas State University
San Marcos, TX 78666

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

DONALD BABBITT (Managing Editor)
University of California
Los Angeles, CA 90024

HUGO ROSSI
University of Utah
Salt Lake City, UT 84112

C. C. MOORE and ANDREW OGG
University of California
Berkeley, CA 94720

J. DUGUNDJI
Department of Mathematics
University of Southern California
Los Angeles, CA 90007

R. FINN and J. MILGRAM
Stanford University
Stanford, CA 94305

ASSOCIATE EDITORS

R. ARENS E. F. BECKENBACH B. H. NEUMANN F. WOLF K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF ARIZONA
UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA, RENO
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF HAWAII
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of the manuscript. However, you may use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Please propose a heading for the odd numbered pages of less than 35 characters. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. Supply name and address of author to whom proofs should be sent. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

50 reprints to each author are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: $102.00 a year (6 Vols., 12 issues). Special rate: $51.00 a year to individual members of supporting institutions.

Subscriptions, orders for numbers issued in the last three calendar years, and changes of address shoud be sent to Pacific Journal of Mathematics, P.O. Box 969, Carmel Valley, CA 93924, U.S.A. Old back numbers obtainable from Kraus Periodicals Co., Route 100, Millwood, NY 10546.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION
Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.).
8-8, 3-chome, Takadanobaba, Shinjuku-ku, Tokyo 160, Japan.

Pacific Journal of Mathematics
Vol. 98, No. 2 April, 1982

Thomas E. Armstrong, Barycentric simplicial subdivision of infinite-dimensional simplexes and octahedra 251
Hom Nath Bhattarai and James William Fernandez, Joins of double coset spaces 271
Alexandru Buium, Ritt schemes and torsion theory 281
Jacob Burbea, Operator-valued Pick's conditions and holomorphicity 295
Su-Shing Chen, Duality condition and property (S) 313
Ky Fan, Evenly distributed subsets of S^n and a combinatorial application . . . 323
Leslie Foged, On g-metrizability 327
John Groves Heywood, An error estimate uniform in time for spectral Galerkin approximations of the Navier-Stokes problem 333
Aggie Ho, The Kreĭn-Milman property and complemented bushes in Banach spaces 347
David R. Jackett, Rings on certain mixed abelian groups 365
Shoji Kyuno, Prime ideals in gamma rings 375
George Lucius O'Brien, Zero-inducing functions on finite abelian groups 381
P. Robba, Sur les équations différentielles linéaires p-adiques. II 393
Wolfgang Ruess, [Weakly] compact operators and DF spaces 419
Claude Schochet, Topological methods for C^*-algebras. II. Geometry resolutions and the Künneth formula 443
Harry F. Smith, Jr., Equivalent nilpotencies in certain generalized right alternative rings 459
Max Warshauer, Diagonalization up to Witt 469
Hugh C. Williams, A class of primality tests for trinomials which includes the Lucas-Lehmer test 477