MATH. SCAND. 59 (1986), 71–92

THE WITT GROUP OF QUADRATIC CHARACTERS

RAINER WEISSAUER

Introduction.

In [7], A. Weil introduced the notion of a character of second degree on a locally compact abelian group (what is called a quadratic character in this paper). These quadratic characters behave similar to quadratic forms on vector spaces over a given groundfield k. In analogy to the construction of the Witt group $W(k)$ of the field k we define a Witt group W using quadratic characters on locally compact abelian groups. The main result of this paper is that this Witt group W is isomorphic to the complex unit circle as an abelian group (Corollary 5.4).

1. The Witt group.

In the following let G and H be abelian groups carrying a locally compact topology. For every such group G, the character group $\hat{G}$ is the group of all continuous homomorphisms of G into the complex unit circle $\boldsymbol{T}$. The character group $\hat{G}$ is an abelian group and the compact-open topology on $\hat{G}$ is locally compact. We call G self dual if there exists a homomorphism $\varphi: G \to \hat{G}$, which is an algebraic and topological isomorphism. The product of two self dual groups is again self dual.

1.1. DEFINITION. A continuous function f on G with values in $\boldsymbol{T}$ is a quadratic character, if $B(x,y)=f(x+y)\overline{f}(x)\overline{f}(y)$ is bilinear.

It is obvious from the definition that $B(x,y)$ is symmetric. The form $B(x,y)$ defines a homomorphism

$$b: G \to \hat{G}$$

given by $b(x)(y)=B(x,y)$. It is easy to check that the map b is a continuous homomorphism.

1.2. DEFINITION. The quadratic character f is nondegenerate if the map $b: G \to \hat{G}$ is an algebraic and topological isomorphism.

Received November 11, 1984; in revised form June 28, 1985.

For the rest of the paper we are only interested in nondegenerate quadratic characters. We call a pair (G, f), where G is a locally compact abelian group and f a nondegenerate character on G, a quadratic space or Q-space. A quadratic space is *hyperbolic* if there exists a subgroup N of G such that

(1) $f(N) = 1$

(2) $N^{\perp} = N$.

$N^{\perp}$ is the annulator of N with respect to f. It is given by

$$N^{\perp} = \{x \in G : B(x,y) = 1 \text{ for all } y \in N\} .$$

The two quadratic spaces (G, f) and (H, g) are isomorphic if there exists an algebraic and topological isomorphism $s: G \to H$ such that $f = g \circ s$. The sum of quadratic spaces $(G, f) \oplus (H, g)$ is given by the quadratic space whose underlying group is $G \times H$ and whose quadratic character is given by $h(x,y) = f(x)g(y)$ for $(x,y) \in G \times H$. The Q-spaces (G, f) and (H, g) are called similar

$$(G, f) \sim (H, g)$$

if there exist hyperbolic spaces (S, h) and (S', h') such that

$$(G, f) \oplus (S, h) \cong (H, g) \oplus (S', h') .$$

It can be checked easily that this defines an equivalence relation.

1.3. LEMMA. *The equivalence classes of Q-spaces associated to the relation $\sim$ define an abelian group with respect to $\oplus$.*

PROOF. The equivalence classes define a set (Theorem 1.7). Addition is well-defined because the sum of two hyperbolic spaces is again hyperbolic. It remains to show that the inverse elements exist. The class of all hyperbolic elements is the neutral element. If (G, f) is a representative of a class, then $(G, \bar{f})$ is a representative of the inverse class. For this it is enough that $(G, f) \oplus (G, \bar{f})$ is hyperbolic. Let N be the diagonal of $G \times G$, then $f \oplus \bar{f}(N) = 1$ and

$$\begin{aligned} N^{\perp} &= \{(u,v) \in G \times G : B \oplus \bar{B}((u,v),(x,x)) = 1 \text{ for all } x \in G\} \\ &= \{(u,v) \in G \times G : B(u-v,x) = 1 \text{ for all } x \in G\} \\ &= N . \end{aligned}$$

This is a consequence of the fact that f is nondegenerate.

The group so obtained is called the Witt group W. Its definition is similar to the definition of the well-known Witt rings constructed from quadratic forms over rings and fields.

Next we introduce the concept of a reduced Q-space. Suppose (G, f) is a Q-space and N is a closed subgroup of G such that $f(N)=1$. Because $f(N)=1$, we know $N \subseteq N^{\perp}$. The group $N^{\perp}$ is closed by definition and the factor group $N^{\perp}/N$ is again a locally compact abelian group. It is called the reduced group G_{red} (with respect to N). Using

$$f(x+n) = f(x)f(n)B(x,n) \quad \text{for } x \in N^{\perp} \text{ and } n \in N ,$$

one has $f(x+n)=f(x)$. This means that f induces a continuous map from G_{red} to $\boldsymbol{T}$. Cartier showed that the quadratic character on G_{red} induced by f is nondegenerate (see [1]). This defines a Q-space (G_{red}, f). If the Q-space (G, f) has no subgroup $N \neq 1$ such that $f(N)=1$, then (G, f) is called *irreducible*.

1.4. LEMMA. *For every Q-space there exists an irreducible Q-space similar to it.*

PROOF. Apply the Lemma of Zorn to the set of subgroups N of G with property $f(N)=1$. A maximal subgroup N with this property is closed. The reduced space of (G, f) with respect to N is irreducible by construction. Furthermore

$$(G, f) \oplus (G_{\text{red}}, f) \oplus (G_{\text{red}}, \overline{f}) \cong (G_{\text{red}}, f) \oplus (G, f) \oplus (G_{\text{red}}, \overline{f}) .$$

We are done if the right pair of Q-spaces on the right-hand-side has a hyperbolic sum. We have $G_{\text{red}}=N^{\perp}/N$. Let π be the projection of $N^{\perp}$ onto G_{red}. For

$$N' = \{(x, \pi x) \in G \times G_{\text{red}} : x \in N^{\perp}\}$$

we have $f \oplus \overline{f}(N')$ and $(N')^{\perp} = N'$.

A locally compact abelian group is a group with small subgroups if for every neighborhood of the neutral element, there exists a proper subgroup contained in the given neighborhood. If the group does not have this particular property, we say, it is without small subgroups. If H is a closed subgroup of G and G is without small subgroups, then also H and G/H are without small subgroups. The first statement is trivial. A proof of the second statement can be found in [5].

1.5. LEMMA. *If (G, f) is an irreducible Q-space, then the group G is without small subgroups.*

PROOF. Let $B: G \times G \to \boldsymbol{T}$ be the bilinear form of f. The torus $\boldsymbol{T}$ is without small subgroups. Let U be a neighborhood of $\boldsymbol{T}$ without a nontrivial subgroup. Choose neighborhoods U_1 and U_2 of G such that $B(U_1, U_2) \subseteqq U$. If G had small subgroups, there would exist a subgroup H in $U_1 \cap U_2$. Fixing a variable, the image of H would be a subgroup of U. Therefore $B(H,H)=1$ and the restriction of f to H is a character. The same argument applied again shows $f(H)=1$. This contradicts the assumption on the irreducibility of (G,f).

Let G be a locally compact abelian group without little subgroups. Let G^0 be the connected component of G. G^0 is compactly generated. This implies that G^0 is isomorphic to $\mathbb{R}^n \times F$, where F is a compact group. This is the structure theorem for compactly generated groups (see [2]).

1.6. LEMMA. *If F is compact, abelian, connected and without little subgroups, then $F \cong \boldsymbol{T}^m$.*

PROOF. If F is a Lie group, this is well-known. On the other hand, it is a well-known fact from harmonic analysis that the characters separate points of $F - \{0\}$. The intersection of all kernels K_ν of all characters χ_ν of F is therefore $\{1\}$. We choose an open subset U $(1 \in U)$ of F without any proper subgroup. The complement A of U in F is compact

$$\bigcap_\nu K_\nu = \{1\} \Rightarrow \bigcap_\nu (K_\nu \cap A) = \varnothing .$$

By the compactness property there exist finitely many $K_\nu \cap A$ with an empty intersection. As a consequence we have

$$\bigcap_{\nu=1}^{r} K_\nu \subseteqq U, \quad \text{hence} \quad \bigcap_{\nu=1}^{r} K_\nu = 1 .$$

This gives an injective map $F \to \boldsymbol{T}^r$ and F is a Lie group because it is a closed subgroup of $\boldsymbol{T}^r$.

Recalling the above statements, we get the following result. The connected component of a locally compact abelian group without little subgroups is isomorphic to $\mathbb{R}^n \times \boldsymbol{T}^m$

$$G^0 = \mathbb{R}^n \times \boldsymbol{T}^m .$$

The factor group $C = G/G^0$ is totally disconnected. Therefore C has neighborhood basis of 0 consisting of open subgroups. But C is without small subgroups because C is a quotient of G. This implies C to be a

discrete group. But the connected component G^0 is divisible and hence an injective group in the category of abelian groups. The sequence

$$0 \to G^0 \xrightarrow{i} G \underset{\pi}{\overset{s}{\leftrightarrows}} C \to 0$$

splits. Because C is discrete it also splits in the category of topological groups: $G = G^0 \times C$.

If we assume G to be self dual and $G = \mathbf{R}^n \times \boldsymbol{T}^m \times C$, then we get

$$\mathbf{R}^n \times \boldsymbol{T}^m \times C \cong \mathbf{R}^n \times \mathbf{Z}^m \times \hat{C}$$

because $\hat{\mathbf{R}} = \mathbf{R}$ and $\hat{\boldsymbol{T}} = \mathbf{Z}$. We have $\hat{C} = \hat{C}^0 \times E$. As a topological isomorphism respects the connected components, we get $\mathbf{R}^n \times \boldsymbol{T}^m = \mathbf{R}^n \times \hat{C}^0$ and we already know that $\hat{C}^0 = \mathbf{R}^{n'} \times \boldsymbol{T}^{m'}$. As the dual $\hat{C}$ of the discrete group C is compact, we have $n' = 0$. A dimension count gives $m = m'$. E is discrete and compact as a projection of a compact group, meaning E is finite. Putting everything together gives $G = \mathbf{R}^n \times (\boldsymbol{T} \times \mathbf{Z})^m \times E$. The group G is built out of the self dual components $\mathbf{R}$, $\boldsymbol{T} \times \mathbf{Z}$ and E. Thus as a consequence of Lemma 1.4 and 1.5 we get

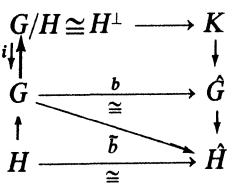
1.7. THEOREM. *Every class in W has a representative Q-space (G, f), where G is isomorphic to $\mathbf{R}^n \times (\boldsymbol{T} \times \mathbf{Z})^m \times E$ and E is finite.*

2. Orthogonal decompositions.

In the previous section, we showed that we can restrict to certain generators (G, f) where G decomposes. We consider now whether the decomposition can be chosen such that it respects the quadratic character.

2.1. THEOREM. *Let H be a subgroup of G and (G, f) be a given Q-space. If the map $\tilde{b}$ (confer to the diagram below) maps H algebraically and topologically isomorphically onto H, then the Q-space (G, f) decomposes: $(G, f) = (H, f) \oplus (H^\perp, f)$.*

PROOF. Consider the diagram



The lower row is by assumption an isomorphism. The commutativity of the lower square defines a retract i of G, that is G splits. The induced isomorphism in the upper row gives $i(G/H)=H^{\perp}$. From $f(x+y)=f(x)f(y)$ for $x \in H$ and $y \in H^{\perp}$ we conclude $(G,f)=(H,f) \oplus (H^{\perp},f)$. It is obvious that both factors have nondegenerate quadratic characters.

The situation of Theorem 2.1 is given whenever G is the direct product of two self dual groups and the lower row of the diagram

$$\begin{array}{ccccc} G_1 \times G_2 & \xrightarrow{b} & (G_1 \times G_1)\hat{} & \xrightarrow{\cong} & \hat{G}_1 \times \hat{G}_2 \\ \uparrow & & & & \downarrow \\ G_1 & & \longrightarrow & & \hat{G}_1 \end{array}$$

is an isomorphism.

Let us now discuss the case $G=G_1 \times G_2 \times G_3$. Here we suppose $G_1=\mathbf{R}^n$, $G_2=(\boldsymbol{T} \times \mathbf{Z})^m$ and $G_3=E$ finite. We identify the groups G_i $(i=1,2,3)$ with their duals. Let us assume that f is a nondegenerate quadratic character on G. The associated map b defines an automorphism of G. We write this map as a block matrix with entries b_{ij} $(1 \leqq i, j \leqq 4)$ according to the decomposition of $G=\mathbf{R}^n \oplus \mathbf{Z}^m \oplus \boldsymbol{T}^m \oplus E$. The map b_{13}: $\boldsymbol{T}^m \to \mathbf{R}^n$ is zero because $\mathbf{R}^n$ hax no compact subgroup. The map b_{23}: $\boldsymbol{T}^m \to \mathbf{Z}^n$ is zero because the image of b_{23} is connected. The map b_{24} is zero because 0 is the only torsion element of $\mathbf{Z}^m$. We know also that the isomorphism maps the connected component isomorphically to the connected component. Because $b_{13}=0$, we conclude that b_{11} and b_{33} are automorphisms of $\mathbf{R}^n$ and $\boldsymbol{T}^m$. As a consequence of the remark following Theorem 2.1, we know that $(\mathbf{R}^n, f)$ splits off as an orthogonal summand. In the orthogonal complement, b_{33} defines an automorphism of $\boldsymbol{T}^m$. As b restricted to the orthocomplement of $\mathbf{R}^n$, which is isomorphic to $\mathbf{Z}^m \oplus \boldsymbol{T}^m \oplus E$, is an automorphism and $b_{23}=0$ and $b_{24}=0$, we see that b_{22} defines an automorphism of $\mathbf{Z}^m$. This shows that b maps the $(\mathbf{Z} \oplus \boldsymbol{T})^m$ block in the orthocomplement of $\mathbf{R}^n$ isomorphically onto itself mod E. Again we conclude that $(\mathbf{Z} \oplus \boldsymbol{T})^m$ splits off as an orthogonal summand. Putting everything together, we see that

$$(G,f) = (G_1,f) \oplus (G_2,f) \oplus (G_3,f)\,.$$

Thus the quadratic character f automatically respects the decomposition $G=G_1 \times G_2 \times G_3$, if the factors G_i are chosen appropriately.

Let us now deal with the three different cases separately:

(1) The case $G=\mathbf{R}^n$. We identify $\mathbf{R}^n$ with $\hat{\mathbf{R}}^n$ using the map $\hat{e}$: $\mathbf{R}^n \to \hat{\mathbf{R}}^n$, $\hat{e}(x)(y)=e(x'y)$ for x and y in $\mathbf{R}^n$. Here $e(\,.\,)$ is an abbreviation for $e^{2\pi i(.)}$.

Given a quadratic character on $\mathbf{R}^n$, we obtain the map b: $\mathbf{R}^n \to \hat{\mathbf{R}}^n$. The composition $\hat{e}^{-1} \circ b$ is a linear map of $\mathbf{R}^n$ to itself because every continuous additive map is R-linear. Call this automorphism S. We have

$$B(x, y) = e(x'S'y)$$

by definition. From $B(x,y)=B(y,x)$ we get $S=S'$. An automorphism U: $\mathbf{R}^n \to \mathbf{R}^n$ changes the matrix S in the usual form: $S \mapsto U'SU$. Now every matrix S can be diagonalized by such a substitution. For the corresponding Q-spaces, this means

$$(\mathbf{R}^n, f) \cong \bigoplus_{i=1}^{m} (\mathbf{R}, f_i)$$

because of Theorem 2.1.

(2) The case of the finite groups. We decompose the group into its p-sylow subgroups. Every linear map from the p-torsion subgroup to its q-sylow subgroup is zero for $p \neq q$ (prime). We can apply Theorem 2.1 as every finite group is self dual. Considering the case of finite Q-spaces, we can now restrict ourselves to the Q-spaces (E_p, f). We use the notion E_p for a finite p-sylow group. We decompose the group E_p into cyclic factors each of the form $\mathbf{Z}/p^n\mathbf{Z}$. Denote A the sum of all copies $\mathbf{Z}/p^n\mathbf{Z}$ with lowest n and B the rest of them. Every automorphism of $E_p \cong A \times B$ is given by a 2×2 matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

according to the decomposition. The existence of an inverse matrix means especially

$$a \circ a' + b \circ c' = \mathrm{id}_A$$

for certain maps c': $A \to B$ and a': $A \to A$. The image of the map c' is contained in pB. Therefore the image of A under $h = b \circ c'$ is contained in pA. We conclude that a high power of the map h is the zero map from A to A. Now $a \circ a' = \mathrm{id}_A - h$ and the right-hand-side is invertible. The map a must be an automorphism of A. Applying Theorem 2.1 we can split off the summand A as an orthogonal summand. The discussion of the Q-spaces with underlying group $G = (\mathbf{Z}/p^n\mathbf{Z})^i$ is similar to the real case. We identify $(\mathbf{Z}/p^n\mathbf{Z})^i$ with its dual. We use the natural ring structure on $\mathbf{Z}/p^n\mathbf{Z}$. We have $e(.) = e^{2\pi i p^{-n}(.)}$ as a standard character on $\mathbf{Z}/p^n\mathbf{Z}$. Analogous to the case $G = \mathbf{R}^i$ we get $B(x,y) = e(x'Sy)$ for a symmetric matrix S with entries in

$\mathbf{Z}/p^n\mathbf{Z}$. We have to distinguish two different cases. The ring $\mathbf{Z}/p^n\mathbf{Z}$ is a local ring. For $p \neq 2$ the element 2 is a unit. In this case there exists an automorphism U such that $\tilde{S} = U'SU$ is a diagonal matrix (see [4]). If $p = 2$, then the situation is more complicated. In this case S is not further decomposable only if $x'Sx \in 2(\mathbf{Z}/p^n\mathbf{Z})$ for all $x \in (\mathbf{Z}/p^n\mathbf{Z})^i$ (see [4]). The matrix S is called an even matrix in this case.

(3) The case $(\boldsymbol{T} \times \mathbf{Z})^m$. For easy notations we identify $\boldsymbol{T}$ and $\mathbf{R}/\mathbf{Z}$.

2.2. LEMMA. *The topological linear maps from* $(\boldsymbol{T} \times \mathbf{Z})^m$ *into itself correspond to the matrices*

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

where a *and* c *are unimodular, integer* $m \times m$*-matrices and* b *is a* $m \times m$*-matrix with elements in* $\mathbf{R}/\mathbf{Z}$.

PROOF. A topological linear map induces an automorphism of the connected component $\boldsymbol{T}^m$. This is a linear map of the universal covering space, mapping the kernel of the exponential map onto itself, hence unimodular. The map from $\boldsymbol{T}^m$ to $\mathbf{Z}^m$ is zero. Therefore c is unimodular.

On $J = \boldsymbol{T} \times \mathbf{Z}$ there is a natural ring structure. Set $(x,n)+(y,m) = (x+y, n+m)$ and $(x,n)\cdot(y,m) = (xm+yn, nm)$ for $x, y \in \boldsymbol{T}$ and $n, m \in \mathbf{Z}$. We choose the following standard character $e(z) = e^{2\pi i x}$ for $z = (x,n)$, $x \in \boldsymbol{T}$ and $n \in \mathbf{Z}$. We identify J with its dual mapping $z \in J$ to the character $e(z \cdot (\,.\,))$ in $\hat{J}$. Now the discussion is similar to the previous cases. There is only one difference. In the previous cases the topological automorphisms were exactly the ring isomorphisms. In the present case there are more topological linear isomorphisms than ring isomorphisms.

2.3. LEMMA. *The map* $s: J^r \times J^r \to \boldsymbol{T}$,

$$s\left[\begin{pmatrix} x \\ n \end{pmatrix}, \begin{pmatrix} y \\ m \end{pmatrix}\right] = \begin{pmatrix} x \\ n \end{pmatrix}' \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} y \\ m \end{pmatrix} \quad \text{for } x, y \in \boldsymbol{T}^r \text{ and } n, m \in \mathbf{Z}^r$$

has the following properties:

(i) $s[z, \tilde{z}] = s[\tilde{z}, z]$.

(ii) $s[z, U\tilde{z}] = s[z, V\tilde{z}]$ *for all* $z, \tilde{z} \in J^r$ *implies* $U = V$ *for matrices* U *and* V *as in Lemma* 2.2.

(iii) $s[Uz, \tilde{z}] = s(z, U^*\tilde{z}]$. *If* U *given as in Lemma* 2.2, *then* U^* *is given by the matrix*

$$\begin{pmatrix} c' & b' \\ 0 & a' \end{pmatrix}.$$

The proof is given by some obvious matrix calculations.

Now suppose f is a quadratic character on J^r. One gets

$$B(z,\tilde{z}) = e\circ s[Sz,\tilde{z}] = e\circ s[\tilde{z},Sz] = e\circ s[z,S^*\tilde{z}]\,.$$

This gives $S=S^*$. The Q-spaces isomorphic to the given one have a matrix $\tilde{S}=U^*SU$. We show that $\tilde{S}$ can be chosen to be the identity. From $S=S^*$ one deduces

$$S = \begin{pmatrix} a & b \\ 0 & a' \end{pmatrix}$$

and $b=b'$. Putting

$$U = \begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -\frac{1}{2}b \\ 0 & 1 \end{pmatrix}$$

we get $U^*SU=\mathrm{id}$. According to Theorem 2.1, the Q-spaces (J^r,f) decomposes into factors (J,f_i), $1\leqq i\leqq r$.

2.4. COROLLARY. *As an abelian group the Witt group W is generated by Q-spaces (G,f), where G ranges over the groups* R, J, $\mathsf{Z}/p^n\mathsf{Z}$ *for* $p\neq 2$ *and* $(\mathsf{Z}/2^n\mathsf{Z})^i$.

3. Relations between the generators.

Observe that a quadratic character is essentially determined by the associated map b. Two quadratic characters f_1 and f_2 with the same associated map b differ by an ordinary character χ. It is therefore reasonable to associate to a given symmetric map b a fixed quadratic character which is called f_0. Here we restrict ourselves to the groups of Corollary 2.4. In the cases $G=\mathsf{R}$ or $G=\mathsf{Z}/p^n\mathsf{Z}$ $(p\neq 2)$ the element 2 is a multiplicative unit. In these cases we put $f_0(x)=b(x)(2^{-1}x)$ using the inverse 2^{-1} of 2. The map f_0 defines a quadratic character whose associated map is b. In the case $G=\boldsymbol{T}\times\mathsf{Z}$ we can assume after applying an automorphism that $B(x,y)=b(x)(y)=e(xy)$ for all x and y in G. It is easy to check that in this case $f_0(x,n)=e^{2\pi inx}$ for $x\in\boldsymbol{T}$ and $n\in\mathsf{Z}$ has the required property. Let us finally look at the case $G=(\mathsf{Z}/2^n\mathsf{Z})^i$. Let $\mathrm{pr}\colon\mathsf{Z}\to\mathsf{Z}/2^n\mathsf{Z}$ be the canonical projection. If we identify G with its dual, the map b corresponds to a symmetric matrix S with coefficients in $\mathsf{Z}/2^n\mathsf{Z}$. We chose representatives of the coefficients in Z and view S as an integer matrix. We set

$$f_0(\mathrm{pr}(x)) = e^{\pi i/2^n \cdot x'Sx}.$$

This is independent of the chosen representative x of $\mathrm{pr}(x)$ and has the required properties. The quadratic characters f_0 should be called *pure* quadratic characters. Now let us return to the simplest case. Let us assume $G=\mathsf{R}$. Up to isomorphism there are only two different pure quadratic characters given by $e^{\pi i x^2}$ and $e^{-\pi i x^2}$.

3.1. DEFINITION. The Q-space (G,f) with $G=\mathsf{R}$ and $f(x)=e^{i\pi x^2+i\pi ax}$ for $a\in\mathsf{R}$ is called (R,a).

3.2. LEMMA.

$$\bigoplus_{i=1}^{n}(\mathsf{R},a_i) \cong \bigoplus_{i=1}^{n-1}(\mathsf{R},0)\oplus\left(\mathsf{R},\left(\sum_{i=1}^{n}a_i^2\right)^{\frac{1}{2}}\right).$$

PROOF. This is obvious. Transformations with orthogonal maps do not change pure quadratic characters, but operate on characters.

3.3. LEMMA.

(i) $(\mathsf{R},2n+1)=0$ *in* W *for all* $n\in\mathsf{Z}$.

(ii) $8(\mathsf{R},0)=0$ *in* W.

(iii) *The map* $s\colon \mathsf{R}/\mathsf{Z}\to W$ *given by* $s(x)=(\mathsf{R},\sqrt{1-8x+8n})$, *where* $n\in\mathsf{Z}$ *is chosen big enough depending on* x, *is a well defined homomorphism from* $\boldsymbol{T}$ *to* W.

PROOF. The subgroup Z of R is its own annihilator $\mathsf{Z}^{\perp}=\mathsf{Z}$ in the Q-space $(\mathsf{R},2n+1)$, $n\in\mathsf{Z}$. This shows that $(\mathsf{R},2n+1)$ is hyperbolic and proves (i). In order to prove (ii) we use Lemma 3.2 to obtain

$$9(\mathsf{R},1) = 8(\mathsf{R},0)\oplus(\mathsf{R},3).$$

According to (i) the spaces $(\mathsf{R},1)$ and $(\mathsf{R},3)$ are hyperbolic. This proves (ii). In order to prove (iii) we choose $n\in\mathsf{Z}$ so that $1-8x+8n\geqq 0$. Let us first show that s is well defined. Given $m>n$ we get for $p=m-n$

$$(\mathsf{R},\sqrt{8p})\oplus(\mathsf{R},\sqrt{1-8x+8n}) \cong (\mathsf{R},0)\oplus(\mathsf{R},\sqrt{1-8x+8m}).$$

Now we have $(\mathsf{R},\sqrt{8p})=(\mathsf{R},0)$ because

$$\begin{aligned}(\mathsf{R},0) &= (\mathsf{R},0)\oplus(8p+1)(\mathsf{R},1)\\ &= 8p(\mathsf{R},0)\oplus(\mathsf{R},\sqrt{8p+1})\oplus(\mathsf{R},0)\\ &= (\mathsf{R},\sqrt{8p})\oplus(\mathsf{R},1)\\ &= (\mathsf{R},\sqrt{8p}).\end{aligned}$$

This shows that $s(x)$ is independent of the number n. In order to prove $s(x+y)=s(x)s(y)$ we put $a=\sqrt{1-8x+8n}$, $b=\sqrt{1-8y+8m}$, and $c=\sqrt{1-8(x+y)+8(m+n)}$. An easy calculation gives $c^2=a^2+b^2-1$. Therefore we have to show

$$(\mathsf{R},a)\oplus(\mathsf{R},b) = (\mathsf{R},\sqrt{a^2+b^2-1})\,.$$

This follows from

$$(\mathsf{R},a)\oplus(\mathsf{R},b) = (\mathsf{R},0)\oplus(\mathsf{R},\sqrt{a^2+b^2})$$

and

$$\begin{aligned}(\mathsf{R},\sqrt{a^2+b^2-1}) &= (\mathsf{R},\sqrt{a^2+b^2-1})\oplus(\mathsf{R},1)\\ &= (\mathsf{R},\sqrt{a^2+b^2})\oplus(\mathsf{R},0)\,.\end{aligned}$$

We will show later that the map s is actually an isomorphism from T onto W. This means that the exact order of $(\mathsf{R},0)$ in W is 8 and that the symmetric even positive unimodular matrices of rank m exists only if m is divisible by 8. One only has to remember that each such lattice defines a hyperbolic structure on the Q-space $m(\mathsf{R},0)$. It should be finally remarked (for computations in the Wittgroup) that every Q-space (R,f) has a representative (R,a) in its class.

3.4. LEMMA. *For every Q-space $(T\times\mathsf{Z},f)$ there exist Q-spaces (R,a) and (E,h), where E is a finite group such that the following identity is true in W:*

$$(T\times\mathsf{Z},f) = (\mathsf{R},a)\oplus(E,h)\,.$$

PROOF. We can restrict to the case

$$f(x,n) = e^{2\pi i(nx+ny+xm)}$$

for x and y in T and n and m in Z. This is shown by decomposing f in f_0 and a character and a modification under an isomorphism. Next we show

$$(\mathsf{R},0)\oplus(T\times\mathsf{Z},f) = (\mathsf{R},\sqrt{8my})\oplus(T\times\mathsf{Z},g)$$

where g is given by

$$g(x,n) = e^{2\pi i(nx+mx)},\quad x\in T,\ n,m\in\mathsf{Z}\,.$$

This isomorphism is given as a matrix $U\colon \mathsf{R}\times T\times\mathsf{Z}\to\mathsf{R}\times T\times\mathsf{Z}$

$$U = \begin{pmatrix} \mathrm{id} & 0 & -c \\ 0 & \mathrm{id} & -\frac{1}{2}c^2 \\ 0 & 0 & \mathrm{id} \end{pmatrix}.$$

This matrix is "orthogonal", i.e. U maps the pure quadratic character onto itself: $h_0 \circ U = h_0$ where

$$h_0(z,x,n) = e^{\pi i(2nx+z^2)}$$

for $z \in \mathsf{R}$, $x \in \boldsymbol{T}$ and $n \in \mathsf{Z}$. On the other hand the characters are changed by U. The above mentioned isomorphism is obtained when $c = \sqrt{2y/m}$. Furthermore $(\boldsymbol{T} \times \mathsf{Z}, g) = 0$ in W because the subgroup $N = 0 \times \mathsf{Z}$ in $\boldsymbol{T} \times \mathsf{Z}$ has the property $g(N) = 1$ and $N = N^{\perp}$. Adding $7(\mathsf{R},0)$ on both sides of the above identity, we get the assertion of the lemma because $(\mathsf{R},0) = (\mathsf{Z}/2\mathsf{Z}, f_0)$. Here the quadratic character has the values $f_0(0) = 1$ and $f_0(1) = i$. It is a reduced Q-space of $(\mathsf{R},0)$.

For the rest of this section, we give some other examples of Q-spaces whose underlying group is a 2-torsion group. As these groups play a distinguished role in further discussions, they are treated now separately.

THE CASE $G = \mathsf{Z}/2\mathsf{Z}$. In this case there are only two quadratic characters

$$f_0(x) = e^{\pi i/2 \cdot x^2} \quad \text{and} \quad f_1(x) = e^{\pi i/2 \cdot (x^2+2x)}.$$

Their values are $f_0(0) = f_1(0) = 1$ and $f_0(1) = -f_1(1) = i$. The classes of (G, f_0) and (G, f_1) are therefore inverses of each other in W.

THE CASE $G = \mathsf{Z}/4\mathsf{Z}$. Here we have two automorphisms of G given by multiplication with 1 and -1. This gives the quadratic characters:

$$\begin{aligned} f_0(x) &= e^{\pi i/4 \cdot x^2} & f_1(x) &= e^{\pi i/4(x^2+2x)} \\ f_2(x) &= e^{\pi i/4(x^2+4x)} & f_3(x) &= e^{\pi i/4(x^2+6x)} \end{aligned}$$

The cases, where the associated map $b = -1$, have the four cases as inverse elements in W. In addition to that $(G, f_1) = (G, f_3) = 0$ in W because they are hyperbolic. The subgroup $2G$ defines a hyperbolic structure for them.

Furthermore, we have the following relations.

3.5. LEMMA.

(i) $(\mathsf{Z}/2\mathsf{Z}, f_0) = (\mathsf{Z}/4\mathsf{Z}, f_0) = (\mathsf{R},0)$ *in* W.

(ii) $(\mathsf{Z}/4\mathsf{Z}, f_2) = 3(\mathsf{Z}/4\mathsf{Z}, f_0)$ *in* W.

PROOF. Assertion (i) is proved by the method of Lemma 1.4. This is done by putting either $N=2\mathbf{Z}$ or $N=\sqrt{2}\cdot\mathbf{Z}$ in $G=\mathbf{R}$ for the Q-space $(\mathbf{R},0)$. This gives a reduced spaces, the spaces in (i). The second assertion is proved by considering the subgroup Γ_4 in $(\mathbf{Z}/4\mathbf{Z})^4$. Γ_4 is the subgroup generated by $(1,1,1,1)$ and

$$U = \left\{(x_1,x_2,x_3,x_4) : x_1 \in 2(\mathbf{Z}/4\mathbf{Z}) \quad \text{and} \quad \sum_{i=1}^{4} x_i = 0\right\}.$$

One checks $f_2(x)=f_0(x)^5$ and f_0 has the values

$$f_0(0) = -f_0(2) = 1 \quad \text{and} \quad f_0(1) = f_0(3) = e^{\pi i/4}.$$

Γ_4 is annulated by $f=f_2\oplus 3f_0$ and $\Gamma_4=\Gamma_4^{\perp}$. The space is therefore hyperbolic and equal to zero in W.

3.6. THEOREM. *Let (G,f) be an irreducible Q-space whose underlying group G is a 2-sylow group. If (G,f) is not decomposable into nontrivial factors, then either $G=\mathbf{Z}/2^n\mathbf{Z}$ or $G=(\mathbf{Z}/2\mathbf{Z})^2$.*

PROOF. According to Theorem 1.7, the group G is finite. Let $p=2$. Suppose $G=\mathbf{Z}/p^n\mathbf{Z}$, then we are done. Because of section 2. we can assume $G=(\mathbf{Z}/p^n\mathbf{Z})^i$ for $i>1$. The map b corresponds to an integer valued symmetric matrix S whose coefficients will also be regarded as coefficients in $\mathbf{Z}/p^n\mathbf{Z}$ by taking projections. Because G is indecomposable, we know that $x'Sx \in 2(\mathbf{Z}/p^n\mathbf{Z})$ for all $x \in (\mathbf{Z}/p^n\mathbf{Z})^i$. This implies for the integer matrix S, that $x'Sx \in 2\mathbf{Z}$ for all $x \in \mathbf{Z}^i$. Remember that f differs from f_0 only by a character, hence

$$f(x) = e^{\pi i/2^n\cdot(x'Sx+2x'Sx_0)}$$

for a certain $x_0 \in \mathbf{Z}^i$.

Let us first assume $n>1$. Then put

$$T = \{x \in (\mathbf{Z}/p^n\mathbf{Z})^i : x'Sx_0 \in 2\mathbf{Z}\}$$

and $N=2^{n-1}T$. The group N is not zero because $T/2G$ is not zero. This can be shown as follows. Suppose $Sx_0=(y_1,\ldots,y_i)$. If one of the coordinates y_r is not even, then $z=(0,\ldots,0,z_r,0,\ldots,0)$ for $z_r=1$ is an element z in T and not in $2G$. If all coordinates y_r are odd, then $z=(1,1,0,\ldots,0)$ is in T and not in $2G$. Remember $i>1$. The subgroup N has the property $f(N)=1$. This is a result of $x'Sx \in (2^{n-1})^2\mathbf{Z}$ for $n \in N$. From the assumption $n>1$, we know that 2^{n+1} divides into 2^{2n-1}. This shows $f(N)=1$ because $x'Sx_0 \in 2^{n-1}\cdot 2\mathbf{Z}$ by definition. The Q-space (G,f) can therefore not be irreducible.

Finally, we have to discuss the case $n=1$. In this case the formula for f shows that f has only the values ± 1. The value $f(0)=1$. Any element $y \neq 0$ with the property $f(y)=1$ defines a subgroup N of order 2 with the property $f(N)=1$. This can not be because we assumed that (G,f) is irreducible. We conclude $f(y)=-1$ for every element $y \neq 0$ in G. If G is $\mathbf{Z}/2\mathbf{Z}$ or $(\mathbf{Z}/2\mathbf{Z})^2$, we are done. We can assume $i \geqq 3$. We set $u=(1,0,\ldots,0)$ and $v=(0,1,0,\ldots,0)$.

Because $i \geqq 3$ there is an element w different from $0, u, v$, and $u+v$. The functional equation for the quadratic character f implies

$$B(u,w) = B(v,w) = B(u+v,w) = -1 .$$

This contradicts the linearity of $B(x,y)$.

The proof of Theorem 3.6 showed that the irreducible and indecomposable Q-space on $G=(\mathbf{Z}/2\mathbf{Z})^2$ is given by the quadratic character $f(0)=1$ and $f(x)=-1$ for $x \neq 0$. Let us take $(\mathbf{Z}/2\mathbf{Z}, f_0)$ of Lemma 3.5. The subgroup N generated by $(1,1,1,1)$ in $(\mathbf{Z}/2\mathbf{Z})^4$ has the property $f_0 \oplus f_0 \oplus f_0 \oplus f_0(N)=1$. The reduced Q-space of $4(\mathbf{Z}/2, f_0)$ with respect to N is the Q-space $((\mathbf{Z}/2\mathbf{Z})^2, f)$.

3.7. COROLLARY. *The Witt group W is generated by the classes (R, a) for $a \in \mathsf{R}$ and the classes $(\mathbf{Z}/p^n\mathbf{Z}, f)$, where p runs over all primes and n over all integers $n \geqq 1$.*

4. The canonical character.

Let G be an arbitrary locally compact abelian group. Let $L^1(G)$ and $A(G)$ denote the space of absolutely integrable functions, respectively the space of absolutely integrable functions whose Fourier transform is in $L^1(\hat{G})$. We assume these functions to be complex valued functions. We write x^* for a character and $\langle x, x^* \rangle$ for its value at the point x. The Fourier transform of a function f is

$$\hat{f}(x^*) = \int_G f(x)\langle x, x^* \rangle \, dx .$$

The Haar measures dx and dx^* on G and $\hat{G}$ are chosen in such a way that the Fourier inversion formulas are given by

$$\hat{f}(x^*) = \int_G f(x)\langle x, x^* \rangle \, dx$$

$$f(x) = \int_{\hat{G}} \hat{f}(x^*)\overline{\langle x, x^* \rangle} \, dx^*$$

for $f \in \Lambda(G)$. We write $\mathscr{L}^1(G)$ for $L^1(G)$ modulo functions almost everywhere zero. $\mathscr{L}^1(G)$ is a commutative involutive Banach algebra, whose product is given by convolution

$$f * g(x) = \int_G f(x-y)g(y)\,dy\,.$$

The Fourier transform maps $\mathscr{L}^1(G)$ to the space $C^b(\hat{G})$, the space of all bounded continuous functions on G vanishing at infinity. $C^b(\hat{G})$ is an involutive Banach algebra with respect to the sup-norm and complex conjugation as involution. Multiplication in $C^b(\hat{G})$ is point-wise multiplication of functions. This being said, the Fourier transform $F\colon \mathscr{L}^1(G) \to C^b(\hat{G})$ can be shown to be a continuous homomorphism of involutive Banach algebras.

Given a quadratic character f on G, we have $B(x,y) = \langle x, b(y)\rangle$ by definition. Because $|f| = 1$, generally, the quadratic character f is not in $L^1(G)$. Remember $f \in L^1(G)$ implies $|f| \in L^1(G)$ and therefore $\int_G dx < \infty$. This is possible only for compact groups. As G is selfdual, this implies G is also discrete, hence finite. Nevertheless, one can define a generalized Fourier transform of f, but we never need this fact. We only use the following theorem (see [1], [7]).

4.1. THEOREM. *For every Q-space (G,f), there are numbers $c \in \mathbf{C}$ with $|c| = 1$ and $r \in \mathbf{R}$ positive such that for all $u \in \Lambda(G)$ the following formula holds:*

$$\int_G f(x)\hat{u}(b(x))\,dx = c(G,f)r(G,f)\int_G \overline{f(x)}u(x)\,dx\,.$$

If (G,f) is hyperbolic, then $c(G,f) = 1$.

4.2. LEMMA. *The map $(G,f) \mapsto c(G,f)$ defines a character of the Witt group.*

PROOF. That this map is additive is obvious. It is an easy application of the Fubini theorem. For $u \in \Lambda(H)$ and $u' \in \Lambda(H')$ the function $u(x)u'(x')$ is again in $\Lambda(H \times H')$. It can be shown that the integral is not zero for such functions. A comparison of coefficients gives $c(H,h)c(H',h') = c(G,f)$ for $(G,f) = (H,h) \oplus (H',h')$. The only thing that remains to be shown is the fact that this map is well-defined. For this, it is enough that isomorphisms do not change the constant c because $c(G,f) = 1$ for hyperbolic spaces by Theorem 4.1. A computation shows that an isomorphism changes the product of the constants c and r by the modulus of that isomorphism. Because this modulus is always a positive real number, the constant c remains uneffected.

4.3. LEMMA. $c(\mathsf{R},a)=e^{(\pi i/4)(1-a^2)}$.

PROOF. The function $u(x)=e^{-\pi x^2}$ is in $\Lambda(\mathsf{R})$. Because $B(x,y)=e^{2\pi ixy}$, we have $\hat{u}(b(x))=\hat{u}(x)=u(x)$ in this special case, if we identify $\hat{\mathsf{R}}$ with its dual R as in the second chapter. We get

$$\int_{\mathsf{R}} f(x)\hat{u}(b(x))\,dx = \int_{\mathsf{R}} e^{\pi i(x^2+ax)}e^{-\pi x^2}\,dx$$

$$= e^{-\pi a^2/(4-4i)}\int_{\mathsf{R}} e^{-\pi(1-i)(x-ia/(2-2i))^2}\,dx\,.$$

We make the substitution $z=x-ia/(2-2i)$. Using Cauchy's theorem, we can shift the line of integration back to the real line. The remaining integral is

$$\int_{\mathsf{R}} e^{-\pi(1-i)z^2}\,dx = 2^{-1/4}e^{\pi i/8}\int_L e^{-\pi w^2}\,dw\,.$$

Shifting again the new contour L back to the real line by Cauchy's theorem, the final result is

$$2^{-1/4}e^{\pi i/8}e^{-\pi a^2/(4-4i)}\,.$$

A similar calculation gives

$$\int_{\mathsf{R}} \bar{f}(x)u(x)\,dx = 2^{-1/4}e^{-\pi i/8}e^{-\pi a^2/(4+4i)}\,.$$

This proves the lemma.

An obvious consequence of Lemma 4.3 is that the character

$$c\colon W \to \boldsymbol{T}$$

is surjective. It is obvious that the map

$$s\colon \boldsymbol{T} \to W$$

defined in Lemma 3.3 in a section of the map c. A consequence is

$$W = \boldsymbol{T}\times \mathrm{Kern}\,(c)\,.$$

In the next section, it will be shown that the kernel of the canonical character c of W is zero. It should be remarked finally, that the constant c attached to a given Q-space (G,f) can be computed rather easily in the case, when G is a finite group. For this reason, we set $\arg(z)=z/|z|$ for $z\in \mathsf{C}^*$ and $|z|=(z\bar{z})^{1/2}$.

4.4. LEMMA. *If (G,f) is a finite Q-space, then*

$$c(G,f) = \arg\left(\int_G f(x)\,dx\right).$$

PROOF. We put $u(x)=1$ for all $x \in G$. Then

$$\hat{u}(b(y)) = \int_G B(x,y)\,dx = B(x_0,y)\int_G B(x,y)\,dx\,.$$

Because $B(x,y)$ is nondegenerate, there exists for $y \neq 0$ a point x_0 such that $B(x_0,y) \neq 1$. We conclude that $\hat{u}(b(y))$ is 0 for $y \neq 0$ and equal to $m(G) = \int_G dx$ for $y=0$. This means

$$m(G) = c(G,f)r(G,f) \times \int \bar{f}(x)\,dx\,.$$

If we multiply by $\int f(x)\,dx$, we get the desired result.

According to Lemma 4.4, the constant $c(G,f)$ is in the case of finite Q-spaces the "sign" of a Gaussian sum. It should be finally remarked, that in the case of finite groups it is very easy to show, that $c=1$ for hyperbolic spaces. If N is a subgroup of G with the properties $N^{\perp}=N$ and $f(N)=1$, then for finite groups G we have

$$\begin{aligned}\int_G f(x)\,dx &= \int_{G/N}\int_N f(x+y)\,dx\,dy \\ &= \int_{G/N} f(y)\left(\int_N B(x,y)\,dx\right)dy \\ &= m(N)\int_{G/N} f(y)\delta(y)\,dy \\ &= m(N)f(0)\,.\end{aligned}$$

The last term is a positive real number. Lemma 4.4 implies $c(G,f)=1$.

5. Connections with classical Witt rings and final computations.

In the previous section we showed $W = \boldsymbol{T} \times \operatorname{Kern}(c)$. In order to determine the kernel $\operatorname{Kern}(c)$ of the canonical character, we compute orders of generators of W.

5.1. LEMMA. *Let (G,f) be an irreducible Q-space with an underlying group $G=\mathbf{Z}/p^n\mathbf{Z}$.*

(i) *If $p \neq 2$ and $n > 1$, then the order of $c(G, f)$ in $\mathbf{T}$ is equal to mp^n, where m is a divisor of 4.*
(ii) *If $p = 2$ and $n > 2$, then the order of $c(G, f)$ in $\mathbf{T}$ is 2^{n+1}.*
(iii) *In the remaining cases, the order of $c(G, f)$ in $\mathbf{T}$ is a divisor of $4p$.*

PROOF. We write the quadratic character f in the form $f(x) = f_0(x)B(x, x_0)$, where f_0 is the associated pure quadratic character to the bilinear form $B(x, y)$ of f. As f and f_0 have the same bilinear form $B(x, y)$ and because f is nondegenerate, we can always find an element x_0 with the above property. Let us first remark that in the cases (i) and (ii) the element x_0 must be a unit. Otherwise the group $N = p^{n-1}G$ has the property $f(N) = 1$. This is impossible because we made the assumption that (G, f) is irreducible. The same argument shows that (G, f_0) is always reducible in the cases (i) and (ii). Furthermore, we have the following general fact:

$$\begin{aligned} c(G, f) &= \arg\left(\int_G f(x)\,dx\right) \\ &= \overline{f_0(x_0)} \arg\left(\int_G f_0(x + x_0)\,dx\right) \\ &= \overline{f_0(x_0)} c(G, f_0)\,. \end{aligned}$$

With this formula, we can show (i) and (ii) by induction under the assumption of (iii). It is easy to check that in cases (i) and (ii) the order of $f_0(x_0)$ is exactly p^n and 2^{n+1}. As (G, f_0) is reducible in these cases, the order of $c(G, f_0)$ is the order of some $(G_{\text{red}}, f_{0,\text{red}})$ and therefore by induction smaller than the order of $f_0(x_0)$. Now it is enough to show (iii). In the case $p = 2$ this is done case by case. A complete list of the cases is given at the end of section 3. In the case $p \neq 2$ one first reduces the problem to the case that $f(x)$ is a pure quadratic character. This gives a contribution of order p in the worst case. For the pure character, the computation of the "signs" of Gaussian sums is classical. For $p \neq 2$ there are only the possibilities $1, -1, i, -i$. These are elements of order 4. Therefore the order is a divisor of $4p$.

5.2. LEMMA. *The Q-space (R, a) is similar to a finite Q-space if and only if the element $c(\mathsf{R}, a)$ is of finite order in W.*

PROOF. The considerations leading to Corollary 3.7 show that every finite Q-space is similar to a sum of Q-spaces $(\mathbf{Z}/p^n\mathbf{Z}, f)$. By Lemma 5.1 the order $c(G, f)$ of a finite Q-space is finite. It is therefore a necessary condition that $c(\mathsf{R}, a)$ is of finite order. Now let us show that this is

sufficient too. If the order of $c(\mathsf{R}, a)$ is finite, Lemma 4.3 implies $a^2 \in \mathsf{Q}$. We set m equal to twice the denominator of a^2. We have $m \in \mathsf{Z}$ and define N to be the sublattice in R generated by ma. It can be shown that $N^{\perp}/N$ is finite and that the Q-space (R, a) is similar to the reduced space $G_{\text{red}} = N^{\perp}/N$.

5.3. LEMMA. Kern (c) *is generated by the* Q*-spaces* $(\mathsf{Z}/p\mathsf{Z}, f_0)$, *where* f_0 *is a pure quadratic character.*

PROOF. According to Lemma 3.2, 3.5, and Corollary 3.7, every class in W has a representative which is a sum of one copy (R, a) and a sum of copies $(\mathsf{Z}/p^n, f)$. Lemma 5.2 implies that a class in the kernel of c has a summand (R, a), which is similar to a finite Q-space. Hence our first conclusion is that an element in Kern (c) can be represented by a finite sum of spaces $(\mathsf{Z}/p^n, f)$. The crucial point is that we can rewrite this sum such that every pair (p, n) has at most one copy $(\mathsf{Z}/p^n, f)$ occurring in the sum. There will be only one exception. Factors $(\mathsf{Z}/p\mathsf{Z}, f_0)$ with a pure quadratic character may occur arbitrarily often. This is done by the following reduction. Suppose first $(\mathsf{Z}/p^n\mathsf{Z}, f)$ is not irreducible. In that case this factor is replaced by the reduced factor. Suppose there are two irreducible factors $(\mathsf{Z}/p^n\mathsf{Z}, f)$ and $(\mathsf{Z}/p^n\mathsf{Z}, f')$ in the sum. We suppose, furthermore, $n > 1$ for $p \neq 2$ and $n > 2$ for $p = 2$. The quadratic characters are $f = f_0 \cdot \chi_1$ and $f' = f'_0 \cdot \chi_2$. Under the above assumption $N = p^{n-1}M$ for

$$M = \{(x, y) \in (\mathsf{Z}/p^n\mathsf{Z})^2 : \chi_1(x) = \chi_2(y)^{-1}\}$$

is a nontrivial subgroup of $(\mathsf{Z}/p^n\mathsf{Z})^2$. Recall that χ_1 and χ_2 correspond to units in $(\mathsf{Z}/p\mathsf{Z})$, when $(\mathsf{Z}/p\mathsf{Z})$ is identified with its dual since both Q-spaces were assumed to be irreducible. The sum of these two spaces will now be replaced by its reduced spaced $N^{\perp}/N = G_{\text{red}}$. Every element in G_{red} has order less than p^n and the number of elements in G_{red} is less p^{2n-1}. In the decomposition of the reduced quaxratic space, at most, one factor $(\mathsf{Z}/p^n\mathsf{Z})$ can occur.

Furthermore, recall that all Q-spaces $(\mathsf{Z}/p^2, f)$ for $p = 2$ can be written as multiplies of $(\mathsf{Z}/2\mathsf{Z}, f_0)$ in W according to section 3. Now we apply Lemma 5.1. As the constant c for the whole sum is 1, no factor of $(\mathsf{Z}/p^n\mathsf{Z}, f)$ with $n > 1$ can occur. What we finally have to show is that all of the remaining factors $(\mathsf{Z}/p\mathsf{Z}, f)$ can be eliminated whenever f is not a pure quadratic character. For this reason, $p \neq 2$ case is the only case that needs to be discussed.

$$(G, f) = \bigoplus_{p} \bigoplus_{i=1}^{r_p} (\mathsf{Z}/p\mathsf{Z}, f_{i,p}) .$$

Every $f_{i,p}$ can be written as

$$f_{i,p}(x) = B_{i,p}(x, t_p x + x_{i,p}) = f_{0,i,p}(x) B_{i,p}(x, x_{i,p})$$

for $t_p \in \mathbf{Z}$ and $2t_p = 1 \bmod p$. Now it is easy to check that $c(G,f)=1$ implies

$$\prod_{i=1}^{r_p} f_{0,i,p}(x_{i,p}) = 1 .$$

First of all, this number is a pth root of unity, since it can be expressed purely in terms of values of $B_{i,p}(x,y)$. On the other hand, by Lemma 5.1 and its proof, this product gives the whole p-power torsion part of $c(G,f)$ and must be 1 for this reason. Looking at the cyclic subgroup generated by the element $z=(x_{1,p},\ldots,x_{r_p,p})$ in $(\mathbf{Z}/p^{\mathbf{Z}})^{r_p}$, we have

$$\begin{aligned}\left(\bigoplus_i f_{i,p}\right)(nz) &= \prod_{i=1}^{r_p} B_{i,p}(nx_{i,p}, nt_p x_{i,p} + x_{i,p}) \\ &= \prod_{i=1}^{r_p} B_{i,p}(x_{i,p}, t_p x_{i,p})^{2n+n^2} \\ &= \prod_{i=1}^{r_p} f_{0,i,p}(x_{i,p})^{2n+n^2} \\ &= 1 .\end{aligned}$$

By further reductions, we can assume $z=0$. This proves the lemma.

Finally, let us discuss the relation of W with some classical Witt rings. Let k be a locally compact self dual field of characteristic different from 2, a local field or a finite field. For each nontrivial character χ of k, one gets a map j from the Witt ring $W(k)$ of that field k (see [3]) to W. This map is linear and is given by

$$\begin{aligned} W(k) &\xrightarrow{j} W \\ (k^n, q) &\mapsto (k^n, \chi \circ q) . \end{aligned}$$

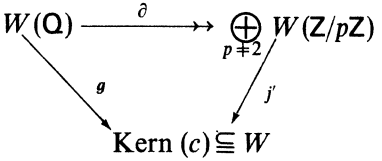
For $k=\mathbf{Z}/p\mathbf{Z}$ or $k=\mathbf{R}$ and $k=\mathbf{Q}_p$, we choose some standard characters. In the first cases we use $e(.)$ defined in section 2. In the second case we use $e^{2\pi i h_p(.)}$, where h_p is the p-adic principal part

$$h_p\left(\sum_i r_i p^i\right) = \sum_{i<0} r_i p^i .$$

Here the r_i are chosen from a representative system $R \subseteq \mathbf{Z}$ of the residue class field. Assume V is a vector space over a number field K and q is a quadratic form on V. Let V_A be the adelic extension of V and q_A the extension of q on V_A. The space V_A is locally compact. We set $\chi = \prod \chi_p$ (product of standard characters) if $K = \mathbf{Q}$. We get a homomorphism of the Witt group $W(K)$ of K into W

$$W(K) \xrightarrow{g} W$$
$$(V, q) \mapsto (V_A, \chi \circ q_A) .$$

This map is the zeromap. It is well-known and easy to check that V defines a hyperbolic structure on $(V_A, \chi \circ q_A)$ (see [7]). On the other hand, this map factors for $K = \mathbf{Q}$ in the following way



To show this we can diagonalize the quadratic form q on V and assume therefore that V is one dimensional. Without restriction $q(x) = ax^2$ for $a \in \mathbf{Z}$ square free. Let N be $\prod \mathbf{Z}_p$ (product over all finite places). Then $f(N) = 1$ and $N^{\perp}/N$ decomposes as a product. The factors correspond to the places of $\mathbf{Q}$.

The factor corresponding to $p = \infty$ is given by $(\mathbf{R}, e(q(x))$ and its class in W is sign $(a)(\mathbf{R}, 0)$. For $p = 2$ the factor is given by (G, f) for $G = \mathbf{Z}/4\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z}$ according whether 2 divides a or not. The discussion preceding Lemma 3.5 therefore shows that its class in W can be written as a sum of copies $(\mathbf{R}, 0)$. For the remaining primes $p \neq 2$ a calculation shows that the class of the factor corresponding to p is given by $j_p \circ \partial_p(V, q)$ where

$$j_p : W(\mathbf{Z}/p\mathbf{Z}) \to W \quad (p \neq 2)$$

is the homomorphism defined above for the finite field $\mathbf{Z}/p\mathbf{Z}$ and ∂_p is the second residue homomorphism

$$\partial_p : W(\mathbf{Q}) \to W(\mathbf{Z}/p\mathbf{Z})$$

defined in [4]. Especially almost all $j_p \circ \partial_p(V, q)$ are zero in W. Hence $g = j' \circ \partial$ for $\partial = \oplus_{p \neq 2} \partial_p$, where j' is defined on the image of ∂ by

$$j'(x) = \sum_{p \neq 2} j_p(x_p) + n(x) \cdot (\mathbf{R}, 0) \quad \text{for } x = \bigoplus_{p \neq 2} x_p, \; x_p \in W(\mathbf{Z}/p\mathbf{Z}) .$$

Here $n(x)\cdot(\mathbf{R},0)$ is the contribution of $p=2,\infty$ and $n(x)$ is the unique integer mod 8 such that $c\circ j'(x)=1$.

Now we can give the final conclusion. Both maps ∂ and j' are surjective. The first fact follows from [4] and the second fact from Lemma 5.3. This implies Kern $(c)=0$.

5.4. COROLLARY. *The Witt group W is canonically isomorphic to the complex unit circle as an additive group. The isomorphism is given by the canonical character c.*

REFERENCES

1. P. Cartier, *Über einige Integralformeln in der Theorie der quadratischen Formen*, Math. Z. 84 (1964), 93–100.
2. E. Hewitt and K. A. Ross, *Abstract harmonic analysis* I, II, (Grundlehren Math. Wiss. 115, 152), Springer-Verlag, Berlin - Heidelberg - New York, 1963, 1970.
3. F. Lorenz, *Quadratische Formen über Körpern* (Lecture Notes in Math. 130), Springer-Verlag, Berlin - Heidelberg - New York, 1970.
4. J. W. Milnor and D. Husemoller, *Symmetric bilinear forms* (Ergeb. Math. Grenzgeb. 73), Springer-Verlag, Berlin - Heidelberg - New York, 1973.
5. M. Moskowitz, *Homological algebra in locally compact abelian groups*, Trans. Amer. Math. Soc. 127 (1967), 361–404.
6. O. T. O'Meara, *Introduction to quadratic forms* (Grundlehren Math. Wiss. 117), Springer-Verlag, Berlin - Heidelberg - New York, 1963.
7. A. Weil, *Sur certain groupes d'operateurs unitaires*, Acta Math. 111 (1964), 143–211.
8. A. Weil, *Basic number theory* (Grundlehren Math. Wiss. 144), Springer-Verlag, Berlin - Heidelberg - New York, 1967.

MATHEMATISCHES INSTITUT
UNIVERSITÄT HEIDELBERG
IM NEUENHEIMER FELD 288
6900 HEIDELBERG 1
WEST GERMANY