Andrew Ranicki

BONNER MATHEMATISCHE SCHRIFTEN

Herausgeber:

E. BRIESKORN, J. FREHSE, ST. HILDEBRANDT
F. HIRZEBRUCH, W. KLINGENBERG, R. LEIS,
I. LIEB, E. PESCHL, H. UNGER, W. VOGEL

Nr. 100

W. D. Neumann

Equivariant Witt Rings

BONN 1977

Als Manuskript gedruckt im
Mathematischen Institut der Universität
Bonn, Wegelerstraße 10

§1. Introduction

The Witt theory of bilinear representations of a group G has arisen as the natural domain for certain interesting invariants in the topology of manifolds. For this reason it has recently been studied for finite G by various people, especially P. Conner and his students, by A. Bak [B], and by A. Dress [D], and for arbitrary G by the author [N1]. The theory is still very tractable for infinite G, as I hope this paper shows. This is an expanded version of the first chapter of the unpublished notes [N1]. The expansion is by some material of chapter 3 of those notes and by the extension of many results from cyclic to arbitrary abelian groups.

A bilinear representation of a group G over a field F is a representation $G \to \mathrm{Aut}(V,b)$ into the automorphism group of a non-singular bilinear space over F. This representation is called hyperbolic if a G-invariant subspace $K \subset V$ exists which is its own orthogonal complement. The semigroup with respect to orthogonal sum of all symmetric or antisymmetric bilinear representations of G modulo the ideal of hyperbolic ones is a group $W_+(G;F)$ respectively $W_-(G;F)$. Similarly, one defines a Witt group $WU(G;F)$ of hermitian representations over a field F with involution, and these groups can also be defined over a ring rather than a field.

Sections 2 and 3 introduce the basic tools - the main one being that Witt rings over fields are generated by irreducible representations with invariant bilinear or hermitian forms. In section 4 we calculate the Witt ring $WU(G) = WU(G;\mathbb{C})$ of hermitian representations over $\mathbb{C}$. This is a very pleasant functor of G. It is always free as a group and for compact Lie groups it is the usual representation ring. It satisfies the Künneth formula $WU(G\times H) = WU(G) \otimes WU(H)$, a fact which has useful topological implications [N2]. This formula hinges on the fact that an irreducible representation over $\mathbb{C}$ of $G\times H$ splits as a tensor product of irreducible representations of G and H and vice versa, a fact which is well known for finite groups, for which it is usually proved using character theory. The proof we give seems more natural. The same results hold on replacing by any algebraically closed field E with non-trivial involution. This is a less general statement than may appear at first sight, since by Artin-Schreier, E is then the algebraic closure of its fixed field K which is real closed, and it is well known that such fields behave almost exactly like $\mathbb{R}$ and .

In section 5 we calculate $W_{\pm}(G;\mathbb{R})$. Again the results hold true for any real closed field. The main result is that the natural ring homomorphism $W_{*}(G;\mathbb{R}) \longrightarrow WU(G)$ $(W_{*} = W_{+} \oplus W_{-})$ is a modulo 2 isomorphism; more precisely, its kernel and cokernel have exponent 2 and are described quite explicitly.

$WU(G)$ and $W_{\pm}(G;\mathbb{R})$ are calculated completely for abelian G, for instance $WU(G)$ is the group ring $\mathbb{Z}[\hat{G}]$ of the Pontryagin dual of G.

The next section discusses $W_{\pm}(G;A)$ for a dedekind domain A. This is defined using non-singular bilinear representations in projective A-modules, and is difficult to handle since it is no longer generated by irreducible representations. The larger

group $W_{\pm}^{n.d.}(G;A)$, defined using non-degenerate forms, is much easier - it <u>is</u> generated by irreducible representations and is a natural direct summand of $W_{\pm}(G;F)$ where F is the quotient field of A. We prove an equivariant version of an exact sequence of Knebusch [Kn] and Milnor [MH]:

$$0 \longrightarrow W_{\pm}(G;A) \longrightarrow W_{\pm}^{n.d.}(G;A) \longrightarrow \coprod_{\mathfrak{p}} W_{\pm}(G;A/\mathfrak{p}) \quad ,$$

which relates $W_{\pm}(G;A)$ to easier groups. For finite G this has also been proved by Dress [D]; in this case $W_{\pm}^{n.d.}(G;A) = W_{\pm}(G;F)$.

In sections 7 and 8 we restrict G to be abelian and show how to reduce the theory to the Witt theory of hermitian forms (no group acting) over suitable fields. This enables us to obtain "complete" results over finite fields and complete results modulo torsion over algebraic number fields and their dedekind domains. We also say something about torsion in the latter case - it is always 2-primary of exponent ≤ 8 (≤ 4 in the antisymmetric and hermitian cases) and we obtain upper and lower bounds on the amount of torsion. For instance there is always infinite torsion if G has an infinite cyclic quotient, an example of importance in topology (see Appendix) is

$$W_{\pm}(\mathbb{Z};\mathbb{Z}) = \mathbb{Z}^{\infty} \oplus (\mathbb{Z}/4)^{\infty} \oplus (\mathbb{Z}/2)^{\infty} \quad .$$

On the other hand Alexander et al. [ACHV] have shown that $W_{+}(\mathbb{Z}/p;\mathbb{Z})$ is torsion free if p is an odd prime. One can deduce that $W_{+}(G;\mathbb{Z})$ is torsion free for any abelian p-group G, finite or not, so infiniteness of G is not sufficient to imply infinite torsion.

An interesting consequence of these calculations is that the Künneth formula ($A = \mathbb{Z}$ or $\mathbb{Q}$, $R = \mathbb{Z}[\frac{1}{2}]$)

$$W_*(G\times H;A)\otimes R = W_*(G;A)\otimes W_*(H;A)\otimes R$$

holds for abelian G and H . The same holds true for finite G and H by Dress [D] . I do not know if this holds in general. A positive answer would be of topological interest.

In section 9 we generalize the definition of character of a representation to give a ring homomorphism

$$\chi : WU(G) \longrightarrow \mathbb{C}^G \quad .$$

If G is a compact Lie group, so as already mentioned $WU(G)$ is isomorphic to the representation ring, this is the usual character and is hence injective. It is also injective for abelian G , but fails to be so for the free group of rank 2 .

In section 10 we describe the behavior of Witt rings for direct limits of groups.

An appendix describes briefly some directions of topological application.

There is some relationship between the theory discussed here and the algebraic L-theory built up in the series of papers of C.T.C. Wall ([W2] and the literature therein quoted). The major difference is that L-theory uses G-modules which are projective over the group ring. All the same, there are intimate connections between the theories, particularly for finite G , and therefore inevitably also some intersection with Wall's results. We have not gone into these connections, see Wall (loc. cit.) or Dress [D].

I would like to express my appreciation to the various people, especially M. Kreck and F. Raymond, who by their interest and otherwise convinced me of the desirability of rewriting these results for a wider audience, and also to the many people who in conversations or by their comments on the original version have contributed to this paper.

I am grateful to the referee for pointing out that the following important reference had eluded my attention:

A. Fröhlich, Orthogonal and symplectic representations of groups, Proc. London Math. Soc. 24(1972), 470-506.

This reference includes, among other things, some of the results of §§2-6.

As the referee also points out, in §7 the result (7.2) (where Witt groups are tensored with $R = \mathbb{Z}[1/2]$) is relatively easy to prove, while results given less prominence lie deeper. Indeed (7.2) follows from (7.14), and (7.14) on tensoring with R reduces to the simple statement $WU(E)\otimes R = WU(E\otimes R)\otimes R$, which also holds in the nonabelian case, see for instance [W2] and the papers leading up to it.

2. Witt rings of bilinear representations over fields

In this section we discuss the general theory of the Witt ring of bilinear representations of an arbitrary group over a field. In the next sections we shall show how these results extend to Dedekind domains and to sesquilinear representations.

If F is a field and $\epsilon = \pm 1$, an ϵ-bilinear space V over F is a finitely generated vector space V over F together with a non-singular F-valued ϵ-symmetric bilinear form $\langle u,v\rangle$ on V. Non-singular (or non-degenerate) means that the correlation

$$b\colon V \to V^* = \mathrm{Hom}(V,F)$$

defined by $b(v)(w) = \langle v,w\rangle$ is an isomorphism, and ϵ-symmetric is equivalent to saying that $b^*\colon V^{**} \to V^*$ equals ϵb after identifying V^{**} with V in the usual way. The group of isometries of V (that is, F-linear automorphisms t of V satisfying $\langle tu,tv\rangle = \langle u,v\rangle$, or equivalently $t^*bt = b$) will be denoted by $\mathrm{Aut}(V,b)$. If F has a topology then $\mathrm{Aut}(V,b)$ will inherit a topology.

If G is an arbitrary (not necessarily finite, not necessarily discrete) group, let $R_\epsilon(G;F)$ be the Grothendieck group of isomorphism classes of representations of G in ϵ-bilinear spaces over F, with orthogonal sum giving the group structure. $R_{-1}(G;F) \oplus R_{+1}(G;F)$ is actually a $(\mathbb{Z}/2)$-graded ring with product

$$R_{\epsilon_1}(G;F) \otimes R_{\epsilon_2}(G;F) \longrightarrow R_{\epsilon_1\epsilon_2}(G;F)$$

induced by tensor product of representatives (for reasons that are clear later one actually takes the negative of this map when $\epsilon_1 = \epsilon_2 = -1$).

are clear later, one actually takes the negative of this map when $\epsilon_1 = \epsilon_2 = -1$).

Terminology. We shall use the bilinear form $\langle\,,\rangle$ and its correlation b interchangeably, writing $b(v,w)$ instead of $\langle v,w\rangle$. G-representation module, G-module, G-space, etc. always mean a vector space V with a G-action given by a representation $G \to GL(V)$. G-maps are linear maps compatible with G-actions. The adjective "invariant" always means G-invariant. We abbreviate the subscripts $+1$ and -1 to $+$ and $-$, writing for instance $R_+(G;F)$ instead of $R_{+1}(G;F)$.

When we talk of irreducible or indecomposable representations, it is always forgetting bilinear forms. Thus irreducible means having no non-trivial proper subrepresentation and indecomposable means not decomposable as a non-trivial direct sum (not necessarily orthogonal sum). Although we allow G to be infinite, the usual theorems about uniqueness up to isomorphism of the irreducible constituents and indecomposable components of a representation still hold, since they are just special cases of the Jordan-Hölder theorem and the Remak-Krull-Schmidt theorem for groups with operators and involve no restrictions on the size of the set of operators. However, it is not true in general that indecomposable representations are irreducible, even for bilinear representations; an example is the representation $\rho\colon \mathbb{Z} \to Sp(\mathbb{R}^2)$ given by $\rho(1) = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in Sp(\mathbb{R}^2)$. This causes difficulties in the study of $R_\epsilon(G;F)$, however we shall see that modulo hyperbolic representations these difficulties vanish and the theory becomes quite tractable.

A bilinear representation $G \to \mathrm{Aut}(V,b)$ is called <u>hyperbolic</u> if V contains an <u>invariant kernel</u>, that is a subspace K with $K = K^{\perp}$ and $GK = K$. Since for any subspace $K \subset V$ one has $\dim K + \dim K^{\perp} = \dim V$, it is sufficient to require $K \subset K^{\perp}$ and $2(\dim K) = \dim V$. The hyperbolic representations generate a subgroup $I_{\epsilon} \subset R_{\epsilon}(G;F)$ and we define the Witt group as

$$W_{\epsilon}(G;F) := R_{\epsilon}(G;F)/I_{\epsilon} \quad .$$

In fact $I_{+} \oplus I_{-}$ is clearly an ideal in $R_{+}(G;F) \oplus R_{-}(G;F)$, so $W_{+}(G;F) \oplus W_{-}(G;F)$ inherits an $(\mathbb{Z}/2)$-graded ring structure.

<u>Remark</u>. If $\rho: G \to \mathrm{Aut}(V,b)$ is a bilinear representation, then the representation obtained by reversing the sign of b represents the negative element in $W_{\epsilon}(G;F)$, since $\{(v,v) \mid v \in V\} \subset (V,b) \oplus (V,-b)$ is an invariant kernel. We will therefore denote this representation by $-\rho$. It follows that every element of $W_{\epsilon}(G;F)$ is represented by an actual representation, rather than a difference of representations.

<u>Lemma 2.1</u>. <u>If a bilinear representation</u> $\rho: G \to \mathrm{Aut}(V,b)$ <u>represents zero in</u> $W_{\epsilon}(G;F)$, <u>then</u> ρ <u>is hyperbolic</u>.

<u>Proof</u>. By definition of $W_{\epsilon}(G;F)$ there exists a hyperbolic representation $\tau: G \to \mathrm{Aut}(W,b')$ such that $\rho \oplus \tau$ is hyperbolic. Let $L \subset W$ and $H \subset V \oplus W$ be invariant kernels for τ and $\rho \oplus \tau$; we claim that $K = p_1((V \oplus L) \cap H) \subset V$ is an invariant kernel for ρ. We can write K in the form

$$K = \{v \in V \mid \exists w \in L \text{ such that } (v,w) \in H\} \quad ,$$

which makes it clear that $K \subset K^{\perp}$. Thus we must only show that $\dim K = (\dim V)/2$. Let $\dim V = 2r$ and $\dim W = 2s$. Since the kernel of $p_1: (V \oplus L) \cap H \to K$ is $(\{0\} \oplus L) \cap H$, we have

$$\dim K = \dim((V \oplus L) \cap H) - \dim((\{0\} \oplus L) \cap H) \quad .$$

On the other hand, $((V \oplus L) \cap H)^{\perp} = (V \oplus L)^{\perp} + H^{\perp} = (\{0\} \oplus L) + H$, so

$$\dim(V \oplus L) \cap H = 2(r+s) - \dim((\{0\} \oplus L) + H) \quad ,$$

and inserting in the first equation gives

$$\begin{aligned} \dim K &= 2(r+s) - (\dim((\{0\} \oplus L) + H) + \dim((\{0\} \oplus L) \cap H)) \\ &= 2(r+s) - (\dim(\{0\} \oplus L) + \dim H) \\ &= 2(r+s) - (s+r+s) = r \quad , \end{aligned}$$

as was to be shown.

Recall that for a degenerate form $b(,)$ on V, the <u>radical</u> is the subspace $\{v \in V \mid b(v,w) = 0 \text{ for all } w \in V\}$. We formulate the next lemma so that it holds for more general rings (see section 6).

<u>Lemma 2.2</u>. <u>Given a bilinear representation</u> $\rho: G \to \mathrm{Aut}(V,b)$ <u>and an invariant subspace</u> $L \subset V$ <u>with</u> $L \subset L^{\perp}$, <u>then the bilinear form on</u> V <u>restricts to a degenerate form on</u> $L^{\perp}$ <u>with radical</u> $L^{\perp\perp}$ <u>(of course in our present situation</u> $L^{\perp\perp} = L$) <u>and thus</u> b <u>induces a non-singular form on</u> $V' = L^{\perp}/L^{\perp\perp}$. <u>Let</u> $\rho': G \to \mathrm{Aut}(V',b')$ <u>be the representation induced by</u> ρ. <u>Then</u> $[\rho] = [\rho']$ <u>in</u> $W(G;F)$.

<u>Proof</u>. Let $-V'$ be V' with the negative form and $\pi: L^{\perp} \to V'$ the projection. The orthogonal sum $V \oplus (-V')$ has an invariant subspace $K = \{(x, \pi(x)) \mid x \in L^{\perp}\}$ which certainly

satisfies $K \subset K^{\perp}$. But $\dim K = \frac{1}{2}\dim(V \oplus (-V'))$, so in $W_\epsilon(G;F)$ we have $[\rho] + [-\rho'] = 0$, as was to be proved.

Corollary 2.3. $W_\epsilon(G;F)$ *is generated by irreducible representations.*

Proof. If $\rho : G \to \mathrm{Aut}(V,b)$ is any representation, we wish to write it, modulo the equivalence relation in $W_\epsilon(G;F)$, as an orthogonal sum of irreducible representations. Let $W \subset V$ be an irreducible G-subspace. If the form on W is degenerate it is actually zero (as otherwise the radical would be a proper non-trivial G-subspace, contradicting irreducibility), so by Lemma 2.2 we can replace V by $W^{\perp}/W$. If the form on W is non-degenerate then V splits orthogonally as $V = W \oplus W^{\perp}$ (this uses that F is a field). Thus the corollary follows by induction on dimension.

Now for any irreducible representation $\rho : G \to GL(V)$ (no bilinear form) let

$$W_\epsilon(G;F,\rho) = \{[\tau] \in W_\epsilon(G;F) \mid \text{every irreducible constituent of } \tau \text{ is isomorphic to } \rho \text{ after forgetting bilinear form}\}.$$

Theorem 2.4. $W_\epsilon(G;F) = \bigoplus_\rho W_\epsilon(G;F,\rho)$ *as a group, sum over all isomorphism classes of finite dimensional representations of* G. $W_\epsilon(G;F,\rho) \neq 0$ *if and only if* ρ *admits a non-trivial invariant* ϵ-*symmetric form.*

Proof. By corollary 2.3 we know that $W_\epsilon(G;F) = \sum_\rho W(G;F,\rho)$, so we must just show this sum is direct. Suppose we have an

irreducible representation $\mu : G \to GL(V_o)$, and $x \in W_\epsilon(G;F,\mu) \cap (\sum_{\rho \neq u} W_\epsilon(G;F,\rho))$. We must show that $x = 0$. Now x can be represented by a representation

$$\mu \oplus \ldots \oplus \mu : G \to GL(V_o \oplus \ldots \oplus V_o) = GL(V_o^n)$$

together with a bilinear form b_o on $U_o = V_o^n$ and also by some representation

$$\rho_1 \oplus \ldots \oplus \rho_m : G \to GL(V_1 \oplus \ldots \oplus V_m)\ ,\ (\rho_i \neq \mu,\ \rho_i \text{ irred.})$$

together with some bilinear form b_1 on $U_1 = V_1 \oplus \ldots \oplus V_m$. The G-module $U = U_o \oplus U_1$ with form $(b_o,-b_1)$ represents $x-x = 0$ in $W_\epsilon(G;F)$, so it is hyperbolic by Lemma 2.1. Let $K \subset U$ be an invariant kernel, and put $K_o = K \cap (U_o \oplus 0)$, $K_1 = K \cap (\{0\} \oplus U_1)$. Now $K_o \oplus K_1 \subset K$ and $K/(K_o \oplus K_1)$ maps injectively into both U_o/K_o and U_1/K_1 by the maps $K/(K_o \oplus K_1) \to (U_o + U_1)/(K_o + K_1) \to U_j/K_j$, $j = 0,1$. Thus any irreducible constituent of $K/(K_o \oplus K_1)$ must be simultaneously of type μ and of type ρ_i for some i, which is impossible. Thus $K/(K_o \oplus K_1) = 0$, so $K = K_o \oplus K_1$. It follows that K_j is an invariant kernel in U_j for $j = 0,1$, so $K = 0$ as was to be shown.

It remains to show that $W_\epsilon(G;F,\rho) \neq 0$ if and only if admits a non-trivial ϵ-symmetric invariant form. The "only if" is trivial by corollary 2.3, and the "if" is clear by observing that ρ together with such a form must represent a nonzero element of $W_\epsilon(G;F)$, by Lemma 2.1 and irreducibility of ρ.

3. Witt rings of hermitian representations

Given a field F together with an involutory automorphism $x \to \bar{x}$ on F, then for $\epsilon = \pm 1$ an ϵ-hermitian space over F is a finitely generated vector space V over F plus a non-singular F-valued ϵ-hermitian form $b(u,v)$ on V. That is, $b(u,v)$ is linear in the first variable and satisfies the identity $b(v,u) = \epsilon \overline{b(u,v)}$. Non-singular means as usual that the correlation (also denoted by b)

$$b : V \longrightarrow \bar{V}^* = \mathrm{Hom}(\bar{V},F)$$

(where $\bar{V}$ is V with conjugate F-structure), defined by $b(v)(w) = b(v,w)$, is an isomorphism, and ϵ-hermitian is equivalent to saying that $\bar{b}^* : V^{**} \longrightarrow \bar{V}^*$ equals ϵb after identifying V^{**} with V.

The Grothendieck group $RU_\epsilon(G;F)$ and Witt group $WU_\epsilon(G;F)$ of ϵ-hermitian representations of a group G are defined precisely as in the bilinear case (which is the special case that the involution is trivial). Now suppose the involution is non-trivial. Then it has at least one eigenvalue -1 (as a linear mapping over the fixed field $K \subset F$), so there exists $\lambda \in F$ with $\bar{\lambda} = -\lambda$. Then any ϵ-hermitian form $b_\epsilon(u,v)$ determines a $(-\epsilon)$-hermitian form $b_{-\epsilon}(u,v)$ by $b_{-\epsilon}(u,v) = b_\epsilon(\lambda u,v)$. Hence we get natural isomorphisms (after choosing λ):

$$RU_+(G;F) \cong RU_-(G;F) \quad ,$$

$$WU_+(G;F) \cong WU_-(G;F) \quad ,$$

so we shall drop the index and only consider the groups

$$RU(G;F) \quad , \quad WU(G;F)$$

of hermitian representations of G.

The discussion of the previous section extends without change to the hermitian case, so in particular we get (with the obvious definitions):

Theorem 3.1. $WU(G;F) = \bigoplus_\rho WU(G;F,\rho)$ *as a group, sum over all isomorphism classes of irreducible finite dimensional representations* ρ *of* G. $WU(G;F,\rho) \neq 0$ *if and only if* ρ *admits an invariant non-trivial hermitian form.*

§4. Hermitian representations over algebraically closed fields

Until further notice our field is always $\mathbb{C}$ with conjugation as involution. We abbreviate $WU(G;\mathbb{C})$ by $WU(G)$. We intend to prove the following results; in remark 4.8 we describe how they generalize to arbitrary algebraically closed fields.

Theorem 4.1. *If $\rho : G \to GL(V)$ is any irreducible representation over $\mathbb{C}$ then $WU(G;\rho) = \mathbb{Z}$ if ρ admits an invariant hermitian form (which is then unique up to sign, modulo G-isomorphism) and $WU(G;\rho) = 0$ otherwise.*

With Theorem 3.1 this gives immediately

Corollary 4.2. $WU(G)$ *is a free abelian group, with one generator to each isomorphism class of irreducible representations $\rho : G \to GL(V)$ which admits an invariant hermitian form.*

Since any representation of a compact Lie group admits a hermitian metric, we get:

Corollary 4.3. *For a compact Lie group $WU(G)$ is canonically isomorphic to the usual representation ring $R(G)$.*

We shall also prove the following result.

Theorem 4.4. *For any two groups G and H the natural map*

$$WU(G) \otimes WU(H) \longrightarrow WU(G\times H) \quad ,$$

induced by tensor product of representations, is a ring isomorphism

The most important tool will be the classical Schur lemma,

which is well-known for compact G but still holds for any G:

Lemma 4.5. (*Schur's lemma*) *Let $G \to GL(V)$ and $G \to GL(W)$ be irreducible complex representations. Then*

$$\mathrm{Hom}_G(V,W) = 0 \quad \text{if} \quad V \not\cong W \quad \text{as G-spaces,}$$
$$= \mathbb{C} \quad \text{if} \quad V \cong W \quad \text{as G-spaces.}$$

Proof. Any non-trivial linear G-map $U \to W$ must have kernel zero and image W by irreducibility of V and W and is hence an isomorphism. If $V \cong W$, without loss of generality $V = W$, and for any isomorphism $\varphi: V \to V$ and any eigenvalue λ of φ the G-map $\varphi - \lambda(\mathrm{id})$ is a non-isomorphism, hence zero, so $\varphi = \lambda(\mathrm{id})$, proving that $\mathrm{Hom}_G(V,V) \cong \mathbb{C}$.

Proposition 4.6. *Let $\rho: G \to GL(V)$ be any irreducible representation over $\mathbb{C}$. Then V admits an invariant non-singular hermitian form $b(,)$ if and only if $V \cong \overline{V}^*$ (as G-representation modules). In this case the form is unique up to multiplication by non-zero reals and there are exactly the two forms $\pm b$ up to G-isomorphism.*

Proof. The "only if" is clear since the correlation $b: V \to \overline{V}^*$ gives an isomorphism. Conversely suppose $V \cong \overline{V}^*$ as G-modules and let $c: V \to \overline{V}^*$ be an isomorphism. Then $\overline{c}^*: V \to \overline{V}^*$ is also an isomorphism, so by Schur's lemma $\overline{c}^* = \lambda c$ for some $\lambda \in \mathbb{C}$. Conjugate dual of this equation gives $c = \overline{\lambda}\overline{c}^*$, so $\lambda\overline{\lambda} = 1$ Any other G-isomorphism $b: V \to \overline{V}^*$ is of the form $b = \mu c$, and the condition that b defines a hermitian form, namely $b = \overline{b}^*$, can be written $\mu c = \overline{\mu}\lambda c$, which is equivalent to $(\mu/|\mu|)^2 = \lambda$, which can be solved for μ since $|\lambda| = 1$. Furthermore the solution μ and hence also the hermitian form is unique up to multiplication by nonzero reals. Finally G-automorphisms of V multiply the form by positive reals (since such an automorphism is $\alpha\cdot\mathrm{id}$ with $\alpha \in \mathbb{C} - \{0\}$ and $b(\alpha v, \alpha w) = \alpha\bar{\alpha}\, b(v,w)$, so there are exactly the two forms $\pm b$ up to G-isomorphism.

Proof of 4.1. To prove Theorem 4.1. it only remains to prove that if $\rho: G \to \mathrm{Aut}(V,b)$ is an irreducible hermitian representation, then $[\rho]$ has infinite order in WU(G). Suppose we have a finite orthogonal sum $W = V \oplus \ldots \oplus V = nV$ which is hyperbolic, say $K \subset W$ is an invariant kernel. Now the complex vector space $W' = \mathrm{Hom}_G(V,W)$ has dimension n by Schur's lemma; in fact the n natural inclusions $i_k: V \to W = nV$, $k = 1,\ldots,n$, form a $\mathbb{C}$-basis. W' has a hermitian form b' as follows: choose a $v \in V$ with $b(v,v) \neq 0$, say $b(v,v) = \lambda$, and for $f,g \in W'$ put $b'(f,g) = \lambda^{-1} b_W(f(v),g(v))$. This is independent of the choice of v, in fact with respect to the above basis of W' this form has matrix

$$\begin{pmatrix} 1 & & 0 \\ & 1 & \\ 0 & & \ddots & \\ & & & 1 \end{pmatrix}$$

and is thus definite. On the other hand $K' = \mathrm{Hom}_G(V,K) \subset W'$ is a nontrivial subspace on which the form is identically zero, which is a contradiction which proves the theorem.

To prove theorem 4.4 we shall need the following proposition, which again is well-known for finite groups, but still holds in our present situation.

Proposition 4.7. Any irreducible representation $\rho: G\times H \to GL(V)$ of $G\times H$ is isomorphic to the tensor product $\tau \otimes \tau'$ of unique (up to isomorphism) irreducible representations $\tau: G \to GL(W)$, $\tau': H \to GL(W')$. If ρ admits a hermitian form, then so do τ and τ' and $\rho = \pm\tau\otimes\tau'$ as hermitian representations.

Proof. Consider V as a G-representation module by restricting ρ, and let $W \subset V$ be any irreducible G-subspace. We show first that V splits as a G-space as the sum $V = W_1 \oplus \ldots \oplus W_s$ of isomorphic copies of W. For suppose we have already $W_1 \oplus \ldots \oplus W_k \subset V$. Either this is an equality and we are done, or by irreducibility of ρ there exists an $h \in H$ with $hW \not\subset W_1 \oplus \ldots \oplus W_k$ and then by irreducibility of the G-module $W \cong hW$ it follows that $(W_1 \oplus \ldots \oplus W_k) \cap hW = 0$, so $W_1 \oplus \ldots \oplus W_k \oplus hW \subset V$. We can then put $hW = W_{k+1}$ and continue inductively.

Define $W' = \mathrm{Hom}_G(W,V)$. This space inherits an H-structure from V and Schur's lemma shows it has dimension s. The evaluation map

$$W \otimes \mathrm{Hom}_G(W,V) \longrightarrow V$$

is obviously epimorphic, hence isomorphic, since the dimensions of both sides are equal. It hus gives the required tensor product representation of ρ, and it follows that $W' = \mathrm{Hom}_G(W,V)$ must be irreducible, as otherwise ρ would not be. In fact W' is an irreducible H-constituent of V, and V clearly splits as an H-module into isomorphic copies of W'. Thus τ and τ' are uniquely determined up to isomorphism.

Now suppose V has a $(G\times H)$-invariant hermitian form f. Then $V \cong \bar{V}^*$ as $(G\times H)$-modules, so certainly $V \cong \bar{V}^*$ as G-modules. Thus the irreducible G-constituent $\bar{W}^*$ of $\bar{V}^*$ is isomorphic to some irreducible G-constituent of V, hence isomorphic to W, so W admits an invariant hermitian form b by proposition 4.6. Similarly W' admits an invariant hermitian form b' and by the uniqueness statement of 4.6 we can adjust b' by a non-zero factor so that $f = b \otimes b'$.

Proof of theorem 4.4. The surjectivity of the map $WU(G) \otimes WU(H) \longrightarrow WU(G\times H)$ is immediate from proposition 4.7 and theorem 3.1, and injectivity follows too if we show that a tensor product $\tau\otimes\tau' : G\times H \longrightarrow GL(W\otimes W')$ of irreducible representations τ and τ' is irreducible. But suppose we have an irreducible constituent of $\tau\otimes\tau'$. By proposition 4.7 it has the form $\gamma\otimes\gamma'$ for some irreducible representations γ and γ' of G and H. By comparing the irreducible constituents of $\gamma\otimes\gamma'|G$ and $\tau\otimes\tau'|G$ we see that $\gamma \cong \tau$. Similarly $\gamma' \cong \tau'$, so $\gamma\otimes\gamma' = \tau\otimes\tau'$.

Remark 4.8. The above results extend as follows to any algebraically closed field E with non-trivial involution. Let K be the fixed field of the involution. Then $[E:K] = 2$, so by Artin-Schreier (see for instance [J]) K is real closed, $E = K(\sqrt{-1})$ and the involution is $\sqrt{-1} \mapsto -\sqrt{-1}$. All the above proofs thus go through with absolutely no change.

Theorem. All the results of this section hold as stated if $\mathbb{C}$ is replaced by an arbitrary algebraically closed field with non-trivial involution.

Example: G abelian. Then any irreducible representation of G is 1-dimensional, that is, it is a homomorphism

$$G \longrightarrow GL(1,E) = E^* \quad .$$

A hermitian form b on E has the form $b(x,y) = \lambda x\bar{y}$ for some λ in the fixed field K of the involution, and a linear map $\mu \in GL(1,E) = E^*$ preserves this form if and only if $\lambda(\mu x)(\overline{\mu y}) = \lambda x\bar{y}$ for all x and y, that is $\mu\bar{\mu} = 1$. Thus the set of all irreducible representations of G which preserve some hermitian form is precisely

$$\hat{G} = Hom(G,U(1,E)) \subset Hom(G,GL(1,E)) \quad ,$$

where

$$U(1,E) = \{ \mu \in E^* \mid \mu\bar{\mu} = 1 \} \quad .$$

Hence, by the above theorem,

Theorem 4.9. If G is abelian and E is as above, then

$$WU(G;E) = \mathbb{Z}[\hat{G}] \quad ,$$

where the right side means the group ring of $\hat{G}$. This is a ring isomorphism.

In the special case $E = \mathbb{C}$, we have $U(1,E) = S^1$, the circle group, and $\hat{G}$ is the usual Pontryagin dual of G. For example for $G = \mathbb{Z}$, $\hat{G} = S^1$, so

$$WU(\mathbb{Z}) = \mathbb{Z}[S^1] \quad .$$

§5. $W_{\pm}(G)$: Bilinear representations over $\mathbb{R}$

We shall abbreviate $W_{\pm}(G;\mathbb{R})$ by $W_{\pm}(G)$ in this section. Given a (± 1)-symmetric bilinear real G-module V, we can extend the form to a (± 1)-hermitian form on $V \times \mathbb{C}$ and then in the non-hermitian case multiply the form by $+i$ to make it hermitian. This defines a map

$$\phi : W_+(G) \oplus W_-(G) \longrightarrow WU(G)$$

(which is a ring homomorphism if one takes the sign convention of the footnote on page 2).

__Theorem 5.1__. ϕ __is an isomorphism modulo torsion of exponent__ 2 (__that is__ $\mathrm{Ker}\,\phi$ __and__ $\mathrm{Cok}\,\phi$ __are torsion groups of exponent__ 2).

This theorem follows easily from the detailed calculations of $W_{\pm}(G)$ below (see corollary 5.5), however it can be deduced with much less work as follows. We just sketch the proof.

__Proof__. There are maps $\psi_{\pm}: WU(G) \to W_{\pm}(G)$ by forgetting complex structure on a hermitian G-module and taking real or imaginary part of the hermitian form. If we write $\psi = \psi_+ - \psi_-$: $WU(G) \to W_+(G) \oplus W_-(G)$, then the following facts are clear (at least up to sign, but the signs are easily checked):

a) $\psi\phi =$ multiplication by 2 ;

b) $\phi\psi_+(x) = \bar{x} + x$ for all $x \in WU(G)$;

c) $\phi\psi_-(x) = \bar{x} - x$ for all $x \in WU(G)$.

a) implies that the kernel of ϕ and the cokernel of ψ have exponent 2, and b) and c) imply that $\phi\psi$ is also multiplication by 2, so the cokernel of ϕ and the kernel of ψ have exponent 2.

Since $WU(G)$ is free as an abelian group, theorem 5.1 implies that $W_+(G)$ and $W_-(G)$ only have torsion of exponent 2. To obtain a more detailed description of these groups, we need the real versions of Schur's lemma and proposition 4.6. These are as follows.

Lemma 5.2 (Schur's lemma). If $G \to GL(V)$ and $G \to GL(W)$ are irreducible representations over $\mathbb{R}$ then $\mathrm{Hom}_G(V,W) = 0$ if $V \not\cong W$. If $V \cong W$ (without loss of generality $V = W$), one of the following three cases occurs, where U always denotes an irreducible G-module over $\mathbb{C}$:

I. $\mathrm{End}_G(V) \cong \mathbb{R}$ and $V \otimes_{\mathbb{R}} \mathbb{C} \cong U$;

II. $\mathrm{End}_G(V) \cong \mathbb{C}$ and $V \otimes_{\mathbb{R}} \mathbb{C} = U \oplus \bar{U}$, $U \not\cong \bar{U}$;

III. $\mathrm{End}_G(V) \cong \mathbb{H}$ and $V \otimes_{\mathbb{R}} \mathbb{C} = U \oplus \bar{U}$, $U \cong \bar{U}$.

Proof. Any G-map $V \to W$ must be an isomorphism or zero by irreducibility of V and W, proving the first statement and showing that $\mathrm{End}_G(V)$ must be a division algebra over $\mathbb{R}$. Now it is easy to see that one of the following three possibilities holds: $V\otimes\mathbb{C}$ irreducible, $V\otimes\mathbb{C} \cong U \oplus \bar{U}$ with $U \not\cong \bar{U}$, $V\otimes\mathbb{C} \cong U \oplus \bar{U}$ with $U \cong \bar{U}$, where U is irreducible over $\mathbb{C}$. Using that $\mathrm{End}_G(V) \otimes \mathbb{C} = \mathrm{End}_G(V\otimes\mathbb{C})$, it follows that $\mathrm{End}_G(V)$ is respectively 1, 2 or 4 dimensional over $\mathbb{R}$, and hence must be respectively $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Proposition 4.6 must be replaced by:

Proposition 5.3. Let $\rho : G \to GL(V)$ be any irreducible representation over $\mathbb{R}$. Then V admits an invariant non-singular bilinear form b if and only if $V \cong V^*$ as G-modules. The possibilities are then given by the following table (roman numbering as in Schur's lemma):

Case	Forms on V: Symmetric	Forms on V: Antisymmetric	Forms on V up to G-isomorphism: Symmetric	Forms on V up to G-isomorphism: Antisymmetric
I a	$(\mathbb{R}-\{0\})$-family	-	$b, -b$	-
I b	-	$(\mathbb{R}-\{0\})$-family	-	$b, -b$
II a	$(\mathbb{R}-\{0\})$-family	$(\mathbb{R}-\{0\})$-family	$b_1, -b_1$	$b_2, -b_2$
II b_+	$(\mathbb{C}-\{0\})$-family	-	$b (\cong -b)$	-
II b_-	-	$(\mathbb{C}-\{0\})$-family	-	$b (\cong -b)$
III a	$(\mathbb{R}-\{0\})$-family	$(\mathbb{R}^3-\{0\})$-family	$b_1, -b_1$	$b_2 (\cong -b_2)$
III b	$(\mathbb{R}^3-\{0\})$-family	$(\mathbb{R}-\{0\})$-family	$b_1 (= -b_1)$	$b_2, -b_2$

Remark. Note that in the (b)-cases any symmetric form which occurs has signature zero (since it is isomorphic to its own negative). In particular these cases do not occur for compact or abelian Lie groups, since V then actually has an invariant positive definite form. It is not hard to find examples for all the (b)-cases with G free of rank 2. As is well known, the cases (a) all occur already for finite groups.

Before proving the above proposition, let us deduce the structure of $W_\pm(G)$. This is described completely by theorem 2.4 together with the following theorem.

Theorem 5.4. Let $\rho : G \to GL(V)$ be an irreducible representation over $\mathbb{R}$. Then with the classification of the previous proposition we have

of type:	Ia	Ib	IIa	IIb_+	IIb_-	IIIa	IIIb
$W_+(G;\rho) =$	$\mathbb{Z}$	0	$\mathbb{Z}$	$\mathbb{Z}/2$	0	$\mathbb{Z}$	$\mathbb{Z}/2$
$W_-(G;\rho) =$	0	$\mathbb{Z}$	$\mathbb{Z}$	0	$\mathbb{Z}/2$	$\mathbb{Z}/2$	$\mathbb{Z}$

Proof. The cases $W_\epsilon(G,\rho) = 0$ or $\mathbb{Z}/2$ are immediate from the previous proposition, so all that remains to be checked is that in the remaining cases ρ together with an invariant ϵ-bilinear form b (which by assumption satisfies $b \not\cong -b$) represents an element of infinite order in $W_\epsilon(G)$. But we have already remarked that the only torsion in $W_\epsilon(G)$ has order 2, and if $\rho \oplus \rho$ were hyperbolic then any invariant kernel $K \subset V \oplus V$ would be the group of an isomorphism $(V,b) \cong (V,-b)$ contradicting the assumption.

Since we shall not need it, we leave to the interested reader the details of the calculation of the map $\phi: W_+(G) \oplus W_-($(WU(G). The result is that it is trivial on torsion, and on the free part it splits according to types I, II, III as a sum of maps of the form:

I. $\mathbb{Z} \to \mathbb{Z}$ with matrix $\pm(1)$

II. $\mathbb{Z} \oplus \mathbb{Z} \to \mathbb{Z} \oplus \mathbb{Z}$ with matrix $\pm\begin{pmatrix} +1 & -1 \\ +1 & +1 \end{pmatrix}$

III. $\mathbb{Z} \to \mathbb{Z}$ with matrix $\pm(2)$.

Corollary 5.5. Ker ϕ = Torsion$(W_+(G) \oplus W_-(G))$ and oker $\phi = \bigoplus_\rho (\mathbb{Z}/2)$, sum over all isomorphism classes of real rreducible representations of type IIa, IIIa, IIIb.

Proof of proposition 5.3. We interpret a bilinear form on as a G-map $b: V \to V^*$. If V is irreducible, b must be n isomorphism or zero, so as a form b is non-singular or ero. Note that if $b \neq 0$ then by replacing b by either $b+b^*$ or $b-b^*$ if necessary (one of which will be non-zero) we can ssume that $b = \epsilon b^*$ with $\epsilon = \pm 1$. We will assume b has een thus chosen.

Consider the map $\varphi: End_G(V) \to End_G(V)$ given by $\varphi(f) = b^{-1}f^*b$. The following properties are easy:

i) φ is an $\mathbb{R}$-algebra anti-isomorphism of $End_G(V) \cong \mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$;

ii) $\varphi^2 = id$;

iii) $(b\lambda)^* = \epsilon(b\lambda)\lambda^{-1}\varphi(\lambda)$, for $\lambda \in End_G(V)-\{0\} = Aut(V)$;

iv) $\mu^*(b\lambda)\mu = b\varphi(\mu)\lambda\mu$ for $\lambda,\mu \in Aut_G(V)$.

Since any invariant bilinear form on V must have the form $b\lambda$ with $\lambda \in Aut_G(V)$, property iii) implies that the set of all ϵ-symmetric, respectively $(-\epsilon)$-symmetric invariant forms on V is

$$\{b\lambda \mid \lambda^{-1}\varphi(\lambda) = 1\} \text{ respec. } \{b\lambda \mid \lambda^{-1}\varphi(\lambda) = -1\},$$

while iv) says that the set of forms equivalent to a given form $b\lambda$ by G-automorphisms of V is

$$\{b\lambda' \mid \lambda' = \varphi(\mu)\lambda\mu \text{ for some } \mu \in Aut_G V\}.$$

<u>Case I</u>: $\mathrm{End}_G(V) \cong \mathbb{R}$. Then $\varphi = \mathrm{id}$. Thus the only forms on V are $b\lambda$, $\lambda \in \mathbb{R} - \{0\}$, and the forms equivalent to a given $b\lambda$ are $b\lambda\mu^2$, $\mu \in \mathbb{R} - \{0\}$. Thus we get Ia or Ib according as b is symmetric or antisymmetric.

<u>Case II</u>: $\mathrm{End}_G(V) \cong \mathbb{C}$. Then φ = conjugation or $\varphi = \mathrm{id}$. If φ = conjugation then by the above the ϵ-symmetric forms are all $b\lambda$ with $\lambda \in \mathbb{R} - \{0\}$ and the $(-\epsilon)$-symmetric forms are all $b\lambda$ with $\lambda \in i\mathbb{R} - \{0\}$. The forms equivalent to a given $b\lambda$ are all $b\lambda\bar{\mu}\mu$ with $\mu \in \mathbb{C} - \{0\}$, that is all $b\lambda r$ with $r \in \mathbb{R}^+$. Thus we get case IIa. If $\varphi = \mathrm{id}$ then every $b\lambda$, $\lambda \in \mathbb{C} - \{0\}$, is ϵ-symmetric, but they are all equivalent to b since $b\lambda = \mu^t b\mu$ with $\mu = \lambda^{1/2}$. Thus we get the two cases IIb according as $\epsilon = +1$ or $\epsilon = -1$.

<u>Case III</u>: $\mathrm{End}_G(V) \cong \mathbb{H}$. There are again two possibilities for φ, namely φ has 3 or 1 eigenvalues equal to -1 (just 2 such eigenvalues cannot occur for an anti-isomorphism). In the first case it is usual conjugation $\varphi(\lambda) = \bar{\lambda}$ and in the second case it is $\varphi(\lambda) = \alpha^{-1}\bar{\lambda}\alpha$ for some $\alpha \in \mathbb{R}(i,j,k) - \{0\}$. In the latter case, replacing b by $b\alpha$ replaces φ by conjugation, so we can assume φ is conjugation. Then

$$\{\epsilon\text{-symmetric forms}\} = \{b\lambda \mid \lambda^{-1}\bar{\lambda} = 1\} = \{b\lambda \mid \lambda \in \mathbb{R} - \{0\}\},$$

$$\{(-\epsilon)\text{-symmetric forms}\} = \{b\lambda \mid \lambda^{-1}\bar{\lambda} = -1\} = \{b\lambda \mid \lambda \in \mathbb{R}(i,j,k) - \{0\}\}.$$

The forms equivalent to b are all $b\bar{\mu}\mu$ with $\mu \in \mathbb{H} - \{0\}$, which is all br with $r \in \mathbb{R}^+$. The forms equivalent to bi are all $b\bar{\mu}i\mu$ with $\mu \in \mathbb{H} - \{0\}$ which is easily checked to be all $b\lambda$ with $\lambda \in \mathbb{R}(i,j,k) - \{0\}$. Thus we get case IIIa or IIIb

according as $\epsilon = +1$ or $\epsilon = -1$.

<u>Example 5.6 :</u> G <u>abelian</u>. The irreducible representations of G are all of dimension ≤ 2. The 1-dimensional ones which admit an invariant form are just the homomorphisms

$$G \longrightarrow \{\pm 1\} \subset \mathbb{R}^* = GL(1,\mathbb{R}) \ .$$

Each of these is of type Ia and thus gives a $\mathbb{Z}$-summand of $W_+(G)$. The two-dimensional representations which admit an invariant form are all obtained by forgetting complex structure from a representation

$$\rho : G \longrightarrow U(1) \subset \mathbb{C}^* = GL(1,\mathbb{C}) \quad \text{with} \quad \rho(G) \not\subset \{\pm 1\}$$

and are all of type IIa. Each thus gives a $\mathbb{Z}$-summand both in $W_+(G)$ and $W_-(G)$. Note that ρ and $\bar{\rho}$ both give the same real representation, so to obtain unique representatives one must choose one representation from each complex conjugate pair. In particular, $W_+(G) \oplus W_-(G)$ is torsion free if G is abelian.

<u>Remark 5.7</u>. The results of this section hold as stated for any real-closed field K. One must replace $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ throughout the proofs by K, its algebraic closure E, and the quaternionic algebra $\mathbb{H}(K)$ over K, see remark 4.8.

§6. Dedekind domains

Let A be any Dedekind domain (for instance $\mathbb{Z}$, which is the example of most interest to us here). An ϵ-bilinear space over A is a finitely generated projective A-module V together with a non-singular ϵ-symmetric bilinear form on V. It is now important to distinguish between non-singular, which means that the correlation $b: V \to V^* = \mathrm{Hom}(V,A)$ is an isomorphism, and non-degenerate, which only means that b is injective. We can define representations of groups in ϵ-bilinear spaces over A in the obvious way and thus again define a Grothendieck group $R_{\pm}(G;A)$ and a Witt group $W_{\pm}(G;A)$. The following lemma is important to extend some of our earlier results.

Lemma 6.1. Let $\rho : G \to \mathrm{Aut}(V,b)$ be an ϵ-bilinear representation, and $K \subset V$ an invariant submodule. The following statements are equivalent, where $V \to K^*$ is the composition $V \to V^* \xrightarrow{i^*} K^*$:

i) $K = K^{\perp}$;

ii) $0 \to K \to V \to K^*$ is exact;

iii) $K = K^{\perp}$ and $K \subset V$ is a direct summand;

iv) $0 \to K \to V \to K^* \to 0$ is exact;

v) $K = L^{\perp}$ where $L \subset V$ has rank $\frac{1}{2}\mathrm{rank}\, V$ and $L \subset L^{\perp}$.

Proof. $\mathrm{Ker}(V \to K^*)$ equals $K^{\perp}$ by definition, so i) ⇒ ii). Now K, as a submodule of a finitely generated projective module over a Dedekind domain, is projective, so K^* is projective, so $\mathrm{Im}(V \to K^*)$ is projective, so the inclusion $K \subset V$ splits, proving ii) ⇒ iii). Certainly iii) ⇒ iv) ⇒ i), so it remains to prove

i) ⇔ v). The direction i) ⇒ v) is trivial, taking $K = L$, and v) ⇒ i) follows by observing that K and $K^{\perp}$ are direct summands of V of equal rank and $K^{\perp} \subset K$, so $K^{\perp} = K$.

It follows that lemmas 2.1 and 2.2 extend without change. To see this for 2.2 we must check that if $L \subset V$ satisfies $L \subset L^{\perp}$, then the induced form on $L^{\perp}/L^{\perp\perp}$ is non-singular. In other words that the last map of the sequence

$$0 \longrightarrow L^{\perp\perp} \longrightarrow L^{\perp} \longrightarrow \mathrm{Hom}(L^{\perp}/L^{\perp\perp},A)$$

is an epimorphism. If $f \in \mathrm{Hom}(L^{\perp}/L^{\perp\perp},A)$, interpret f as a map $L^{\perp} \to A$ vanishing on $L^{\perp\perp}$ and extend it to a map $g: V \to A$ (possible since $L^{\perp} \subset V$ is a direct summand by an argument in the proof of lemma 6.1). Now $g = b(v)$ for some $v \in V$ and since $b(v)$ vanishes on $L^{\perp\perp}$, $v \in L^{\perp\perp\perp} = L^{\perp}$, as was to be shown.

Unfortunately the proofs of 2.3 and hence also of 2.4 do not extend. We shall see later that 2.4 can be replaced in the arithmetic case by the statement:

Proposition 6.2. If F, the field of fractions of A, is an algebraic number field and we sum over any set of representatives of isomorphism classes over F of irreducible representations over A, then the natural map

$$\bigoplus_{\rho} W_{\epsilon}(G;A,\rho) \longrightarrow W_{\epsilon}(G;A)$$

is injective with torsion cokernel of exponent ≤ 4.

More important for the calculation of $W_{\epsilon}(G;A)$ will be the result:

<u>Proposition 6.3. If F is the field of fractions of A, then the natural map $W_\epsilon(G;A) \longrightarrow W_\epsilon(G;F)$ is injective.</u>

<u>Proof</u>. If $x \in W_\epsilon(G;A)$ is represented by the bilinear G-space V over A, then the image $x' \in W_\epsilon(G;F)$ is represented by $V \otimes_A F$. If $x' = 0$ then $V \otimes_A F$ has an invariant kernel K by lemma 2.1 and intersecting this with the lattice $V \subset V \otimes_A F$ gives an invariant kernel in V, so $x = 0$ (see [OM], §81 for a discussion of lattices in F-vector spaces).

The same discussion goes through for the <u>Witt group $W_\epsilon^{n.d.}(G;A)$ of non-degenerate (instead of non-singular) bilinear ϵ-symmetric representations of G over A</u>, so the natural map $W_\epsilon^{n.d.}(G;A) \longrightarrow W_\epsilon(G;F)$ is also injective. In this case the image is easily described. A representation $G \longrightarrow GL(F^n)$ is said to be <u>defined over</u> A if there exists an invariant A-lattice of rank n in F^n. Such representations with invariant bilinear forms generate a subgroup of $W_\epsilon(G;F)$ which we shall call $W_\epsilon(G;F,A)$.

<u>Proposition 6.4.</u> $W_\epsilon(G;F,A)$ <u>is the image of the injection</u> $W_\epsilon^{n.d.}(G;A) \longrightarrow W_\epsilon(G;F)$. <u>As a group</u>

$$W_\epsilon(G;F,A) = \bigoplus_\rho W_\epsilon(G;F,\rho) ,$$

<u>sum over all irreducible representations</u> ρ <u>which are defined over</u> A.

<u>Proof</u>. Suppose $\rho: G \longrightarrow \mathrm{Aut}(F^n,b)$ admits an invariant A-lattice $V \subset F^n$ of rank n. Then $b(V \otimes V) \subset F$ is a finitely generated A-submodule, hence a fractional ideal, so by multiplying

V by a suitable $a \in A$ we can assume that $b(V \otimes V) \subset A$, implying the first statement of the proposition. The second follows from theorem 2.4 and the fact that a subrepresentation of a representation defined over A is again defined over A (by intersecting the invariant A-lattice with the subrepresentation module).

We can now improve the statement of proposition 6.3.

<u>Theorem 6.5. There is an exact sequence</u>

$$0 \longrightarrow W_\epsilon(G;A) \longrightarrow W_\epsilon(G;F,A) \xrightarrow{\partial} \bigoplus_{\mathfrak{p}} W_\epsilon(G;A/\mathfrak{p}) ,$$

<u>sum over all maximal ideals</u> $\mathfrak{p}$ <u>of</u> A.

<u>Proof</u>. The proof is very similar to the case when there is no G (see Knebusch [Kn]; Knebusch and Scharlau [KnS]; Fröhlich [F]; Husemoller and Milnor [MH]), so we just sketch a proof briefly with $A = \mathbb{Z}$ to simplify notation (in this case the map ∂ is natural, but in general it depends on choices of embeddings $A/\mathfrak{p} \subset F/A$).

Given a finitely generated $\mathbb{Z}$-torsion module T (i.e. a finite group), a bilinear form on T is a map $b: T \otimes T \longrightarrow \mathbb{Q}/\mathbb{Z}$, and ϵ-symmetric and non-singular are defined in the natural way. Hyperbolic means there exists a $K \subset T$ (not necessarily a direct summand) with $K = K^\perp$ (equivalently: $K \subset K^\perp$ and $|K| = \frac{1}{2}|T|$). Let $W_\epsilon(G;\mathbb{Z}-\mathrm{tor})$ denote the Witt group of representations of G in non-singular ϵ-symmetric bilinear torsion modules modulo hyperbolic representations.

Lemmas 2.1 and 2.2 and corollary 2.3 carry over to the torsion situation without change using essentially the same proofs.

We first define a map $\partial_o: W_\epsilon(G;\mathbb{Q},\mathbb{Z}) \longrightarrow W_\epsilon(G;\mathbb{Z}\text{-tor})$ as follows: given a bilinear representation $\rho : G \longrightarrow \mathrm{Aut}(\mathbb{Q}^n,b)$ which is defined over $\mathbb{Z}$, choose an invariant $\mathbb{Z}$-lattice $V \subset \mathbb{Q}^n$ of rank n satisfying $b(V \otimes V) \subset \mathbb{Z}$ and put $V' = \{w \in \mathbb{Q}^n \mid b(v,w) \in \mathbb{Z}$ for all $v \in V\}$. Then V' is also an invariant $\mathbb{Z}$-lattice of rank n and $V \subset V'$, so $T = V'/V$ is a torsion module. Furthermore b induces a non-singular G-invariant bilinear form $c: T \otimes T \longrightarrow \mathbb{Q}/\mathbb{Z}$ by $c(\pi(v),\pi(w)) = b(v,w) \bmod \mathbb{Z}$, where $\pi : V' \longrightarrow T$ is the projection. Of course (T,c) depends on the choice of V, but we shall see that its Witt class does not.

First observe that if ρ above is hyperbolic with invariant kernal $K \subset \mathbb{Q}^n$ then $L = \pi(K \cap V') \subset T$ is an invariant kernel in T. Indeed $L \subset L^\perp$ is trivial; to show $L^\perp \subset L$ suppose we have $\pi(x) \in L^\perp$, that is $b(x,v') \in \mathbb{Z}$ for all $v'' \in K \cap V'$. Since $K \cap V'$ is a direct summand in V', the map $b(x,-): K \cap V' \longrightarrow \mathbb{Z}$ extends to a map $V' \longrightarrow \mathbb{Z}$. Since V and V'' are dually paired by b, this latter map has the form $b(x_o,-)$ for some $x_o \in V$. Then $x-x_o \in K \cap V'$ and $\pi(x-x_o) = \pi(x)$, so $\pi(x) \in L$ as was to be shown.

For any ρ and any two bilinear torsion G-modules T_1 and T_2 constructed as above using different choices of V, the difference $T_1 \oplus (-T_2)$ is constructible from $\rho \oplus -\rho$ and is hence hyperbolic. Thus we have obtained a well-defined map

$$\partial_o: W_\epsilon(G;\mathbb{Q},\mathbb{Z}) \longrightarrow W_\epsilon(G;\mathbb{Z}\text{-tor}) .$$

We claim

$$0 \longrightarrow W_\epsilon(G;\mathbb{Z}) \xrightarrow{\ i\ } W_\epsilon(G;\mathbb{Q},\mathbb{Z}) \xrightarrow{\ \partial_o\ } W_\epsilon(G;\mathbb{Z}\text{-tor})$$

is exact. Indeed $\mathrm{Im}\ i \subset \mathrm{Ker}\ \partial_o$. Now suppose $\rho: G \to \mathrm{Aut}(\mathbb{Q}^n,b)$ satisfies $\partial_o[\rho] = 0$. Let $V \subset \mathbb{Q}^n$, V' and $(T = V'/V,c)$ be as above. As mentioned before, lemma 2.1 holds for (T,c), that is we can find an invariant kernel $L \subset T$, say $L = K/V$. Then $K + V$ is self-dual under b, so $(K+V,b)$ represents an element of $W(G,\mathbb{Z})$ whose image is $[\rho]$.

To complete the proof of theorem 6.5 we must show that the natural map

$$\bigoplus_p W_\epsilon(G;\mathbb{Z}/p) \longrightarrow W_\epsilon(G;\mathbb{Z}\text{-tor})$$

is an isomorphism. (For general Dedekind domains this maps depends on a choice of identification of the $\mathfrak{p}$-torsion in F/A, namely $\mathfrak{p}^{-1}/A$, with $A/\mathfrak{p}$, so it is not natural). Injectivity is trivial. Surjectivity follows from corollary 2.3, which we have already remarked to hold in the torsion situation, on observing that an irreducible torsion G-module T is actually a $(\mathbb{Z}/p)$-module for some p, since if we choose p such that $pT \neq T$ then $pT = \{0\}$ by irreducibility of T.

Corollary 6.6. If F is an algebraic number field then $W_\epsilon(G;A) \to W_\epsilon(G;F,A)$ is injective with cokernel of exponent ≤ 4.

Proof. It suffices to show that $W_\epsilon(G;A/\mathfrak{p})$ always has exponent ≤ 4. But $W_\epsilon(G;A/\mathfrak{p})$ is a $W_\epsilon(A/\mathfrak{p})$-module, and $W_\epsilon(A/\mathfrak{p})$ has exponent ≤ 4 since $A/\mathfrak{p}$ is a finite field (see proposition 7.9).

Theorem 6.7. For any irreducible representation ρ of G over A there is an exact sequence

$$0 \longrightarrow W_\epsilon(G;A,\rho) \longrightarrow W_\epsilon(G;F,\rho) \longrightarrow \bigoplus_{\mathcal{Y},\rho'} W_\epsilon(G;A/\mathcal{Y},\rho')$$

where the sum is over all maximal ideals $\mathcal{Y} \subset A$ and irreducible components ρ' of ρ reduced modulo $\mathcal{Y}$.

This is proved exactly as theorem 6.5.

If F is an algebraic number field it follows as in corollary 6.6 that $W_\epsilon(G;A,\rho) \longrightarrow W_\epsilon(G;F,\rho)$ is injective with cokernel of exponent ≤ 4, so combining this with 6.4 proves proposition 6.2.

Remark 6.8. For G finite, $W_\epsilon(G;F,A) = W_\epsilon(G;F)$, so $W_\epsilon(G;A) \longrightarrow W_\epsilon(G;F)$ is a modulo torsion isomorphism for F an algebraic number field. Furthermore, the map

$$W_\epsilon(G;F) \longrightarrow \coprod_i W_\epsilon(G;\mathbb{R}) ,$$

sum over all real embeddings $i: F \longrightarrow \mathbb{R}$, is a modulo torsion isomorphism (Dress [D]).

In the next section we shall extend this remark to arbitrary abelian groups.

§7. Abelian G

Throughout this section we assume G is abelian. We shall reduce the calculation of the Witt groups of G over a field F to the Witt groups of hermitian forms over certain finite extensions of F. The main application of this reduction will be the following results, which describe such Witt groups over finite fields and up to torsion over algebraic number fields and number rings. In the next section we say something about the torsion.

In view of theorems 2.4 and 3.1 , the case of a finite field is completely described by the following theorem.

Theorem 7.1. If G is abelian, F is finite, and ρ is an irreducible representation of G over F which admits an invariant bilinear form, then

$$W_\epsilon(G;F,\rho) = W_\epsilon(F) \quad \text{if } 2(\rho(G)) = (0) ,$$
$$= \mathbb{Z}/2 \quad \text{if } 2(\rho(G)) \neq (0) .$$

$W_\epsilon(F)$ is described in theorem 7.9. If F has a non-trivial involution and ρ is an irreducible representation which admits an invariant hermitian form then

$$WU(G;F, \ ) = \mathbb{Z}/2 .$$

To describe the situation for algebraic number fields we need some notation. Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the field of algebraic numbers and $\overline{\mathbb{Q}}_0 = \overline{\mathbb{Q}} \cap \mathbb{R}$.

Theorem 7.2. Let G be finitely generated abelian, F an algebraic number field, and $R = \mathbb{Z}[\frac{1}{2}]$. Then the natural map

$$W_\epsilon(G;F) \otimes R \longrightarrow \coprod_i W_\epsilon(G;\overline{\mathbb{Q}}_o) \otimes R \quad ,$$

sum over all real embeddings $i: F \longrightarrow \overline{\mathbb{Q}}_o$, is an isomorphism. If F has a non-trivial involution then the natural map

$$WU(G;F) \otimes R \longrightarrow \coprod_i WU(G;\overline{\mathbb{Q}}) \otimes R \quad ,$$

sum over all involution-preserving embeddings $i: F \to \overline{\mathbb{Q}}$, is an isomorphism.

Note that $W_*(G;\overline{\mathbb{Q}}_o)$ and $WU(G;\overline{\mathbb{Q}})$ have been calculated in theorem 4.9 and example 5.6. Let $\hat{G}_{\overline{\mathbb{Q}}} = \mathrm{Hom}(G,S^1 \cap \overline{\mathbb{Q}})$.

Corollary 7.3. If G is finitely generated, then

$$W_*(G;F) \otimes R \cong \coprod_i R[\hat{G}_{\overline{\mathbb{Q}}}] \quad ,$$

$$W_\pm(G;F) \otimes R \cong \{x \pm \bar{x} \mid x \in W_*(G;F) \otimes R\} \quad ,$$

$$WU(G;F) \otimes R \cong \coprod_i R[\hat{G}_{\overline{\mathbb{Q}}}] \quad ,$$

sum over the same i as in 7.2. In particular

$$W_*(G;\mathbb{Q}) \otimes R \cong R[\hat{G}_{\overline{\mathbb{Q}}}] \quad .$$

If $A \subset F$ is a Dedekind domain with quotient field F we can describe the image of the injection $W_*(G;A) \longrightarrow W_*(G;F)$ up to torsion. Let $\hat{G}_{\bar{A}} = \mathrm{Hom}(G,S^1 \cap \bar{A})$, where $\bar{A} \subset \overline{\mathbb{Q}}$ is the integral closure of A. If A is the ring of integers of F, then $\bar{A} = \bar{\mathbb{Z}}$, the ring of algebraic integers.

Corollary 7.4. If A is as above and G is finitely generated then

$$W_*(G;A) \otimes R = \coprod_i R[\hat{G}_{\bar{A}}] \quad ,$$

sum over all real embeddings $i: F \longrightarrow \overline{\mathbb{Q}}_o$. If A has a non-trivial involution, the corresponding result holds for $WU(G;A)$.

We shall describe how the above results generalize to the case of infinitely generated G at the end of this section.

The reduction to hermitian forms.

Let $\rho : G \longrightarrow GL(V)$ be an irreducible representation over the field F. Then $\rho(G)$ generates a subalgebra $F(\rho)$ of $End(V)$ which is commutative since G is commutative and is simple because ρ is irreducible. By the classification of simple algebras over a field (Wedderburn's theorem, see for instance [OM] §52), $F(\rho)$ is a finite extension field of F.

ρ induces a homomorphism

$$\rho : G \longrightarrow F(\rho)$$

into the multiplicative group of $F(\rho)$, and the image generates $F(\rho)$ as an F-vector-space. V can be considered as an $F(\rho)$-vector-space and, as such, it has dimension 1 by irreducibility. More generally, any representation module W of G over F which is G-isomorphic to a sum $V \oplus \ldots \oplus V$ (we shall call such a G-module a ρ-space) is in a natural way an $F(\rho)$-vector-space and any $F(\rho)$-vector-space can be interpreted as a ρ-space.

Theorem 7.5. Suppose ρ above admits an invariant bilinear form and $E = F(\rho)$. Then

a). The involution $\rho(G) \longrightarrow \rho(G)$, $\rho(g) \longmapsto \rho(g)^{-1}$, extends to a unique involution $\bar{\ }: E \longrightarrow E$.

b). There exists a non-trivial F-linear map $\varphi: E \longrightarrow F$ with $\varphi(\bar{x}) = \varphi(x)$ for all $x \in E$.

c). If W is an E-vector-space and $b: W \times W \longrightarrow E$ an ϵ-hermitian form on W, then $b_F: W \times W \longrightarrow F$ defined by

$$b_F(x,y) = \varphi(b(x,y))$$

is a G-invariant ϵ-bilinear form on W considered as a ρ-space. Conversely, every G-invariant ϵ-bilinear form on W arises in this way from a unique b. b_F is non-degenerate if and only if b is, and is hyperbolic if and only if b is.

Theorem 7.6. If ρ admits an invariant bilinear form then

$$\begin{aligned} W_\epsilon(G;F,\rho) &= WU_\epsilon(E), \quad (E = F(\rho)), \\ &= WU(E) \quad \text{if } \rho(G) \text{ does not have exponent } 2, \\ &= W_\epsilon(F) \quad \text{if } \rho(G) \text{ has exponent } 2. \end{aligned}$$

Proofs. We first deduce theorem 7.6 from 7.5. By 2.3, $W_\epsilon(G;F,\rho)$ can be regarded as the Witt group of G-invariant ϵ-bilinear forms on ρ-spaces. Thus the first line of 7.6 follows from 7.5 c). Now if some element of $\rho(G)$ has order > 2, then the involution on E is non-trivial, so we can drop the

subscript ϵ by section 3. If every element of $\rho(G)$ has order ≤ 2 then the involution on E is trivial. Also $E = F$ since $\rho(G)$ generates E and the only elements of order ≤ 2 in E are ± 1 (since $x^2 - 1 = 0$ has at most two solutions in a field).

Proof of 7.5 a). An invariant bilinear form b on V can be thought of as a G-isomorphism

$$b: V \longrightarrow V^*$$

so it induces a map

$$\mathrm{End}(b): \mathrm{End}(V) \longrightarrow \mathrm{End}(V^*), \quad f \longmapsto bfb^{-1}.$$

Let

$$D: \mathrm{End}(V) \longrightarrow \mathrm{End}(V^*)$$

be the multiplicative anti-isomorphism $D(f) = f^*$. We claim that

$$\begin{array}{ccc} \rho(G) & \xrightarrow{\rho(g) \longmapsto \rho(g)^{-1}} & \rho(G) \\ \cap & & \cap \\ \mathrm{End}(V) & \xrightarrow{D^{-1} \circ \mathrm{End}(b)} & \mathrm{End}(V) \end{array}$$

commutes. Indeed commutativity means $D^{-1} \circ \mathrm{End}(b)(\rho(g)) = \rho(g)^{-1}$ which is equivalent to $\mathrm{End}(b)(\rho(g)) = D(\rho(g)^{-1})$, or $b\rho(g)b^{-1} = (\rho(g)^{-1})^*$, or $\rho(g)^* b \rho(g) = b$, which is the equation expressing that b is an invariant form.

$D^{-1} \circ \mathrm{End}(b)|E$ is an anti-isomorphism, hence an automorphism since E is commutative, so it is the required extension. Since $\rho(G)$ generates E it is the only extension.

ad b) : If E/F is a separable extension we can simply take $\varphi = tr_{E/F}$ here. In general we are looking for any non-trivial F-linear $\varphi : E \to F$ with kernel containing $A = \{x-\bar{x} \mid x \in E\}$. It thus suffices to show that A is a proper F-sub-vector-space of E. But A is the image of the F-linear map $E \to E$, $x \mapsto x-\bar{x}$, which has non-trivial kernel, so $\dim_F A < \dim_F E$.

ad c) : If $b: W \times W \to E$ is ϵ-hermitian, then $b_F(x,y) = \varphi b(x,y)$ is clearly F-bilinear and ϵ-symmetric, and it is also G-invariant since $b_F(\rho(g)x, \rho(g)y) = \varphi b(\rho(g)x, \rho(g)y) = \varphi(\rho(g)\overline{\rho(g)}b(x,y)) = \varphi b(x,y) = b_F(x,y)$. To see that b_F is non-degenerate if b is, observe that the F-linear map

$$\varphi_* : Hom_E(W,\bar{E}) \longrightarrow Hom_F(W,F)$$

defined by $\varphi_* f = \varphi f$ is injective, hence an F-isomorphism for dimensional reasons. The diagram

$$\begin{array}{ccc} W & \longrightarrow & Hom_E(W,\bar{E}) \\ \| & & \downarrow \varphi_* \\ W & \longrightarrow & Hom_F(W,F) \end{array}$$

is commutative by definition, so b_F is an isomorphism if b is.

Conversely, suppose b_F is given. Then the above diagram defines a unique F-bilinear $b: W \times W \to E$ which satisfies $b_F(x,y) = \varphi b(x,y)$ and which is $\bar{E}$-linear in the second variable. On the other hand, the fact that $\rho(g)$ is a b_F-isometry implies the identity

$$b_F(ex,y) = b_F(x,\bar{e}y)$$

for any $e \in \rho(G)$, hence for any $e \in E$. The same identity thus holds for b, so since $b(x,y)$ is $\bar{E}$-linear in y, it is E-linear in x. Thus $b'(x,y) = \epsilon\overline{b(y,x)}$ also satisfies the properties which defined b uniquely, so it equals b. Thus b is ϵ-hermitian.

Finally it is clear that a kernel $K \subset W$ for b is an invariant kernel for b_F and vice versa (since by one-one-ness of the correspondence, $b|K$ is trivial if and only if $b_F|K = (b|K)_F$ is), so b is hyperbolic if and only if b_F is.

In exactly the same way one proves

Theorem 7.7. *If F is a field with a non-trivial involution and $\rho: G \to GL(V)$ is an irreducible representation over F which admits an invariant hermitian form, then*

$$WU(G;F,\rho) = WU(G;E) \quad ,$$

where E is the subfield of $End(V)$ generated by $\rho(G)$ together with the unique involution $\bar{\ }: E \to E$ which simultaneously extends the given involution on F and the involution $\rho(g) \longmapsto \rho(g)^{-1}$ on (G).

Thus to calculate the Witt groups of bilinear and hermitian representations of abelian groups we must know the ordinary Witt groups $W_\epsilon(F)$ and $WU(E)$ of bilinear spaces over F and hermitian spaces over finite extensions of F. We first summarize some known results about $W_\epsilon(F)$. Good general references for these are Milnor and Husemoller [MH] or Scharlau's appendix to [HNK] and the literature quoted there.

The standard proof that an anti-symmetric form has a symplectic basis shows:

Theorem 7.8. $W_-(F) = 0$ *if* $char(F) \neq 2$; *clearly* $W_-(F) = W_+(F)$ *if* $char(F) = 2$.

For finite fields we have

Theorem 7.9. *If* F *is finite then*

$$
\begin{aligned}
W_+(F) &\cong \mathbb{Z}/2 \oplus \mathbb{Z}/2 && (\ char(F) \equiv 1 \bmod 4\ ) \\
&\cong \mathbb{Z}/4 && (\ char(F) \equiv 3 \bmod 4\ ) \\
&= \mathbb{Z}/2 && (\ char(F) = 2\ ).
\end{aligned}
$$

See for instance Witt [Wi] or Milnor-Husemoller [MH] .

For algebraic number fields we have the Hasse-Minkowski theorem:

Theorem 7.10. *If* F *is an algebraic number field and* $\mathcal{O}$ *its ring of integers then the natural map*

$$\mathrm{Loc} \ : W_+(F) \longrightarrow \prod_{\mathfrak{p}} W_+(F_{\mathfrak{p}})$$

is injective, where $\mathfrak{p}$ *ranges over all finite and infinite real prime places of* F . *If* $\mathfrak{p}$ *is an infinite real prime, then* $F_{\mathfrak{p}} = \mathbb{R}$, *so* $W_+(F_{\mathfrak{p}}) = \mathbb{Z}$, *given by signature of forms. If* $\mathfrak{p}$ *is a finite prime then*

$$
\begin{aligned}
W_+(F_{\mathfrak{p}}) &= W_+(\mathcal{O}/\mathfrak{p}) \oplus W_+(\mathcal{O}/\mathfrak{p}) && \textit{if}\ \ char(\mathcal{O}/\mathfrak{p}) \neq 2\ , \\
&= (\text{Finite } 2\text{-group of exponent } \leq 8) && \textit{if}\ \ char(\mathcal{O}/\mathfrak{p}) = 2\ .
\end{aligned}
$$

The image of loc *can be determined.* loc *is an isomorphism after tensoring with* $R = \mathbb{Z}[\frac{1}{2}]$.

For $F = \mathbb{Q}$ we can be much more precise.

Theorem 7.11. $W_+(\mathbb{Q}) = \mathbb{Z} \oplus \coprod_{p=2,3,\ldots} W_+(\mathbb{Z}/p)$.

This is a strengthening of theorem 6.5 with $G = \{1\}$, $A = \mathbb{Z}$. The map $W_+(\mathbb{Q}) \longrightarrow \mathbb{Z}$ is signature of forms and the maps $W_+(\mathbb{Q}) \longrightarrow W_+(\mathbb{Z}/p)$ are as in 6.5.

For these last two theorems see the literature already quoted and Knebusch [K].

The Witt theory of hermitian forms is much tidier, as the prime 2 no longer plays a special role.

Any hermitian form over a field E can be diagonalized as $\langle a_1, \ldots, a_n \rangle$ with $a_i \in K$, the fixed field of the involution. Multiplying a basis element of the hermitian space by $e \in E^*$ multiplies the corresponding a_i by $e\bar{e} = N_{E/K}(e)$, so the a_i are just determined up to norms and can be considered as elements of the norm class group $K^*/N_{E/K}(E^*)$. Let us denote the Witt class of a unary form $\langle a \rangle$ by $[a]$. The following simple lemma is useful.

Lemma 7.12. $[a] + [b] = 0$ *in* $WU(E)$ *if and only if* $-ab \in N_{E/K}(E^*)$.

Proof. Since by lemma 2.1 , $[a] + [b] = 0$ if and only if $\langle a,b \rangle$ is hermitian, the proof is a trivial calculation. This lemma in fact gives a sufficient set of relations for the Witt group in terms of the generators $[a]$, $a \in K^*/N_{E/K}(E^*)$, but we will not need this.

Theorem 7.13. If E is a finite field then $WU(E) = \mathbb{Z}/2$.

Proof. Since for finite fields $K \subset E$ the norm map $N_{E/K}: E^* \longrightarrow K^*$ is onto, any hermitian form is equivalent to a diagonal form $\langle 1, \dots, 1\rangle$ and is thus classified by its rank alone. In particular any binary form is hyperbolic, so $WU(E) = \mathbb{Z}/2$, generated by the unary form 1 .

Theorem 7.1 is thus proven by theorems 7.6, 7.7, and 7.13 .

For an algebraic number field the situation is as follows. E is a quadratic extension of the fixed field K of the involution, say $E = K(\sqrt{a})$, and the involution is $\sqrt{a} \mapsto -\sqrt{a}$.

Theorem 7.14. If $E = K(\sqrt{a})$ is as above, then the canonical map

$$loc : WU(E) \longrightarrow \prod_{\mathfrak{p}} WU(E_{\mathfrak{p}})$$

is injective, where $\mathfrak{p}$ ranges over all (infinite and finite) prime places of K for which $\sqrt{a} \notin K_{\mathfrak{p}}$ (and $E_{\mathfrak{p}} := K_{\mathfrak{p}}(\sqrt{a})$).
Furthermore

$$\begin{aligned} WU(E_{\mathfrak{p}}) &= \mathbb{Z} && (\mathfrak{p} \text{ infinite}) ; \\ &= \mathbb{Z}/4 && (\mathfrak{p} \text{ finite}, -1 \notin N_{E_{\mathfrak{p}}/K_{\mathfrak{p}}}(E^*)) ; \\ &= \mathbb{Z}/2 \oplus \mathbb{Z}/2 && (\mathfrak{p} \text{ finite}, -1 \in N_{E_{\mathfrak{p}}/K_{\mathfrak{p}}}(E^*)) , \end{aligned}$$

with generators respectively: $\langle 1\rangle$; $\langle 1\rangle$; $\langle 1\rangle$, $\langle g\rangle$, $g \notin N_{E_{\mathfrak{p}}/K_{\mathfrak{p}}}(E^*)$
There are only a finite even number of primes of the first two types. An element of

$$\mathbb{Z} \times \dots \times \mathbb{Z} \times (\mathbb{Z}/4) \times \dots \times (\mathbb{Z}/4) \times (\mathbb{Z}/2 \oplus \mathbb{Z}/2) \times \dots$$

is in the image of loc if and only if it has the form

$$(s_1, \dots, s_p, t_1, \dots, t_q, (r, l_1), (r, l_2), \dots)$$

with

i) $s_1 \equiv \dots \equiv s_p \equiv t_1 \equiv \dots \equiv t_q \equiv r \pmod 2$;

ii) Only finitely many $l_i \neq 0$;

iii) $\sum_i^{\infty} l_i \equiv r(p+q)/2 + (\sum_i^{p} s_i + \sum_j^{q} t_j)/2 \pmod 2$.

Proof. Let $(V, b(,))$ be a hermitian space of rank r over E . By lemma 2.1 we can assume that V does not represent zero, that is $b(x,x) \neq 0$ whenever $x \neq 0$. Note that $q: V \longrightarrow K$ given by $q(x) = b(x,x)$ is a quadratic form of rank $2r$ over K and is isomorphic to $q' \oplus (-aq')$ for a suitable quadratic form q' over K . At any prime $\mathfrak{p}$ with $\sqrt{a} \in K_{\mathfrak{p}}$, q thus becomes hyperbolic on localizing. Suppose (V,b) , and hence q , is hyperbolic also at every prime $\mathfrak{p}$ with $\sqrt{a} \notin K$. Then q represents zero at every prime, so by [OM] theorem 66.1 , q already represented zero before localization, contradicting the assumption. This proves the injectivity of loc .

The calculation of $WU(E_{\mathfrak{p}})$ is detailed in [Ke]. We need the description to discuss the image of loc . An infinite prime $\mathfrak{p}$ with $\sqrt{a} \notin K_{\mathfrak{p}}$ must clearly be real, so $K_{\mathfrak{p}} = \mathbb{R}$, $E_{\mathfrak{p}} = \mathbb{C}$, and $WU(E_{\mathfrak{p}})$ is the Witt group of hermitian forms over $\mathbb{C}$. This is $\mathbb{Z}$, generated by the unary form $\langle 1\rangle$, with isomorphism given by signature. For a finite prime the norm class group $K_{\mathfrak{p}}^* / N_{E_{\mathfrak{p}}/K_{\mathfrak{p}}}(E^*)$ is $\mathbb{Z}/2$ (a hermitian space V over $E_{\mathfrak{p}}$ is in fact determined up to equivalence by its rank and its determinant $\det(V) \in K^*_{\wp}/N_{E_\wp/K_\wp}(E_\wp)$). Choose $g \in K^*_\wp$ not a norm. Then the unary forms $\langle 1\rangle$ and $\langle g\rangle$ clearly generate $WU(E_\wp)$. By lemma 7.12 one has relations $[1]+[1] = [g]+[g] \neq 0$, $[1]+[g] \neq 0$, if -1 is not a norm, and relations $[1]+[1] = [g]+[g] = 0$, $[1]+[g] \neq 0$, if -1 is a norm. Thus in the first case $WU(E_\wp) = \mathbb{Z}/4$, generated by $[1] = -[g] = -[-1]$, and in the second case $WU(E_\wp) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$, generated by $[1]$ and $[g]$.

Index the primes $\wp$ for which $\sqrt{a} \notin K_\wp$ according to the three cases (real; finite, -1 not a norm; finite, -1 is a norm) as

$$\wp_1, \ldots, \wp_p ; \wp'_1, \ldots, \wp'_q ; \wp''_1, \ldots, \wp''_k, \ldots$$

Note that the primes $\wp_i, \wp'_j$ are just the primes $\wp$ for which -1 is not a norm, so there are a finite even number of them by Hilbert reciprocity (see e.g. O'Meara [OM]). For any hermitian space V over E of rank r , denote by $d_\wp = \pm 1$ the determinant of V at the prime $\wp$, that is

$$d_\wp = \left(\frac{\det V, a}{\wp}\right) ,$$

by definition of the Hilbert symbol. Let $l_\wp \in \{0,1\}$ be

$$l_\wp = (1-d_\wp)/2 \quad , \text{ so } \quad d_\wp = (-1)^{l_\wp} .$$

The above calculation shows that the Witt class of V at $\wp$ is determined by the signature s_i of V at $\wp$ for $\wp = \wp_i$ by $t_j = r + 2l_\wp \pmod 4$ for $\wp = \wp'_j$, and by $r \pmod 2$ and $l_k = l_\wp$ for $\wp = \wp''_k$. The invariants satisfy the necessary conditions:

a) $s_i \equiv r \pmod 2$, $d_\wp = (-1)^{(r-s_i)/2}$ for $\wp = \wp_i$;

b) $t_j \equiv r \pmod 2$, $d_\wp = (-1)^{(r-t_j)/2}$ for $\wp = \wp'_j$;

c) Only finitely many $d_\wp \neq 1$, $\prod_\wp d_\wp = \pm 1$ (Hilbert reciprocit

d) $s_i \leq r$.

By Landherr [La] these conditions also suffice for existence of a hermitian space. In the Witt group d) is irrelevant, since it can always be satisfied by adding hyperbolic forms, and a), b), c easily translate to the conditions in the theorem, completing the proof.

<u>Corollary 7.15</u>. <u>With notation as above,</u>

$$WU(E) \cong \bigoplus_{i=1}^{p} \mathbb{Z} \oplus \bigoplus_{k=1}^{\infty} (\mathbb{Z}/2) \qquad (p \geq 1)$$

$$\cong \mathbb{Z}/4 \oplus \bigoplus_{k=1}^{\infty} (\mathbb{Z}/2) \qquad (p=0,\ -1 \notin N_{E/K}(E^*)\ ) ;$$

$$\cong \bigoplus_{k=1}^{\infty} (\mathbb{Z}/2) \qquad (p=0,\ -1 \in N_{E/K}(E^*)\ ) .$$

<u>Here</u> p <u>is the number of embeddings</u> $K \hookrightarrow \mathbb{R}$ <u>which do not extend to</u> E . <u>Any hermitian space over</u> E <u>of rank</u> $r = 1$ <u>actually represents an element of the maximal order</u> ∞, 4, 2 <u>in each of the above three cases</u>.

<u>Proof</u>. The first statement follows from the theorem by observing that if $p \neq 0$ then condition i) implies that any torsion element is $(\mathbb{Z}/2)$-torsion and if $p = 0$ it implies that

any element which is zero on the first $(\mathbb{Z}/4)$-component of $\prod_{\gamma} WU(E_{\gamma})$ is a $(\mathbb{Z}/2)$-torsion element. Further, if $p = 0$, then $q = 0$ says that -1 is a norm of E/K at every prime, which is equivalent to saying that -1 is a norm of E/K, by the Hasse norm theorem (see [OM], 65:23).

The second statement of the corollary follows directly from statement 7.13 i).

We now come to the proof of theorem 7.2. We shall just consider the case $W_+(G;F)$, the antisymmetric and hermitian cases being completely analogous. We assume until further notice that G is finitely generated.

Let $\rho : G \longrightarrow GL(V)$ be an irreducible representation over F. For each real embedding $i: F \longrightarrow \bar{\mathbb{Q}}_o$, we can consider the induced representation $\rho \otimes_F \mathbb{Q}_o$ over $\bar{\mathbb{Q}}_o$. Denote $\rho^{(i)} = \rho \otimes_F \bar{\mathbb{Q}}_o$ and $V^{(i)} = V \otimes_F \bar{\mathbb{Q}}_o$ and let

$$\left.\begin{array}{l} \rho^{(i)} = \rho_1^{(i)} \oplus \ldots \oplus \rho_{k(i)+l(i)}^{(i)} \\ V^{(i)} = V_1^{(i)} \oplus \ldots \oplus V_{k(i)+l(i)}^{(i)} \end{array}\right\} \begin{array}{ll} \dim V_j^{(i)} = 2 & , j \le k(i) \ , \\ \dim V_j^{(i)} = 1 & , j > k(i) \end{array}$$

be the splitting of this representation into irreducible representations over $\bar{\mathbb{Q}}_o$ ($\rho^{(i)}$ is completely decomposable by lemma 7.17 below). In view of theorem 2.4, theorem 7.2 follows from the following proposition.

<u>Proposition 7.16</u>.

a). <u>For a fixed real embedding</u> i <u>and fixed</u> ρ <u>the representations</u> $\rho_j^{(i)}$ <u>are all distinct</u>.

b). <u>For a fixed real embedding</u> i, <u>every irreducible representation</u> τ <u>of</u> G <u>over</u> $\bar{\mathbb{Q}}_o$ <u>occurs as a</u> $\rho_j^{(i)}$ <u>for some unique</u> ρ <u>and some</u> j.

c). <u>The natural map</u> $(R = \mathbb{Z}[\frac{1}{2}])$

$$W_+(G;F,\rho) \otimes R \longrightarrow \coprod_i \coprod_j W_+(G;\bar{\mathbb{Q}}_o, \rho_j^{(i)}) \otimes R$$

<u>is an isomorphism</u>.

<u>Proof</u>. We first need a preparatory lemma. Let $E = F(\rho)$ and let $\xi \in E$ be a primitive element for the extension E/F. Let $m(t)$ be the minimal polynomial for ξ over F and denote by $m^{(i)}(t)$ the image of $m(t)$ under the real embedding $i: F \longrightarrow \bar{\mathbb{Q}}_o$. Note that we can think of ξ as $\rho(\eta)$ for some η in the group ring $F[G]$.

<u>Lemma 7.17</u>. $m^{(i)}(t)$ <u>splits as follows into a product of irreducible polynomials over</u> $\bar{\mathbb{Q}}_o$:

$$m^{(i)}(t) = m_1^{(i)}(t) \cdot \ldots \cdot m_{k(i)+l(i)}^{(i)}(t) \ ,$$

<u>where</u> $\deg m_j^{(i)}(t) = 2$ <u>or</u> 1 <u>according as</u> $j \le k(i)$ <u>or</u> $j > k(i)$. <u>If</u>

$$V_j^{(i)} = \{x \in V^{(i)} \mid m_j^{(i)}(\xi)\cdot x = 0\}$$

<u>then</u>

$$V^{(i)} = \coprod_j V_j^{(i)}$$

<u>and this gives the splitting of</u> $\rho^{(i)}$ <u>into its irreducible</u>

<u>components. If one writes</u> $m^{(i)}(t) = m_j^{(i)}(t)\cdot q_j^{(i)}(t)$, <u>then</u> $V_j^{(i)}$ <u>is generated as a</u> G-<u>module over</u> $\overline{\mathbb{Q}}_o$ <u>by an element of the form</u> $q_j^{(i)}(\xi)\cdot x$ <u>for some</u> $x \in V^{(i)}$.

<u>Proof</u>. Observe that since $m_j^{(i)}(t)$ and $q_j^{(i)}(t)$ are coprime in $\overline{\mathbb{Q}}_o[t]$, there exist polynomials $a(t)$ and $b(t)$ in $\overline{\mathbb{Q}}_o[t]$ such that $a(t)\cdot m_j^{(i)}(t) + b(t)\cdot q_j^{(i)}(t) = 1$. Let $V_j^{(i)}$ be defined as in the lemma. Observe that

$$V_j^{(i)} \cap \sum_{k \neq j} V_k^{(i)} = (0) ,$$

since if x is in this intersection then x is annihilated both by $m_j^{(i)}(\xi)$ and $q_j^{(i)}(\xi)$ and hence by $a(\xi)\cdot m_j^{(i)}(\xi) + b(\xi)\cdot q_j^{(i)}(\xi) = 1$. Hence

(1) $$\coprod V_j^{(i)} \subset V^{(i)}$$

Next observe that

$$q_j^{(i)}(\xi)\cdot V^{(i)} = V_j^{(i)} \quad ;$$

indeed the inclusion from left to right is trivial, and if $x \in V_j^{(i)}$ then $x = (a(\xi)\cdot m_j^{(i)}(\xi) + b(\xi)\cdot q_j^{(i)}(\xi))x = q_j^{(i)}(\xi)b(\xi)x \in q_j^{(i)}(\xi)\cdot V^{(i)}$. Since, by irreducibility of ρ , $q_j^{(i)}(\xi)\cdot V^{(i)} \neq (0)$,

(2) $$\dim V_j^{(i)} \geqslant 1 \quad .$$

Furthermore, if we tensor V with $\overline{\mathbb{Q}}$ instead of $\overline{\mathbb{Q}}_o$ and split in the same way, then $V_j^{(i)}$ with $j \leqslant k(i)$ splits into two

non-trivial summands, so

$$\dim V_j^{(i)} \geqslant 2 \quad \text{for} \quad j \leqslant k(i) \quad .$$

Comparing dimensions in (1) now shows

$$\dim V_j^{(i)} \begin{cases} = 2 & \text{for } j \leqslant k(i) , \\ = 1 & \text{for } j > k(i) , \end{cases}$$

$$V^{(i)} = \coprod_j V_j^{(i)} \quad .$$

Now think of ξ as $\rho(\eta)$ for some $\eta \in F[G]$, the group ring of G over F . Since the minimal polynomial of $\rho(\eta)$ acting on $V_j^{(i)}$ is $m_j^{(i)}(t)$, of degree equal to the dimension of $V_j^{(i)}$, $V_j^{(i)}$ must be irreducible. In particular $V_j^{(i)}$ is generated as a G-module over $\overline{\mathbb{Q}}_o$ by a single non-trivial element, which by (2) above has the form $q_j^{(i)}(\xi)\cdot x$ for some $x \in V^{(i)}$. This completes the proof of the lemma. It also proves 7.16 a) , namely the representations $\rho_j^{(i)}$ are distinguished, for fixed i and varying j , by the minimal polynomials $m_j^{(i)}(t)$ of the element $\xi = \rho(\eta)$, and are hence distinct.

To prove 7.16 b) , suppose $\tau : G \longrightarrow GL(W)$ is an irreducible representation over $\overline{\mathbb{Q}}_o$. Let E_τ be the subalgebra of $GL(W)$ generated by $\tau(G)$. Then, since E_τ is a finite extension field of $\overline{\mathbb{Q}}_o$, $E_\tau = \overline{\mathbb{Q}}_o$ or $\overline{\mathbb{Q}}$. Let E be the subfield of E_τ generated by $\tau(G)$ and $i(F)$. This is a finite extension of F since G is finitely generated. Let V be E considered as F-vector-space. Since E acts on V , so does G via $\tau : G \longrightarrow E$, so V is a G-module over F and is certainly irreducible. The inclusion $V \cong E \subset E_\tau$ induces a map

$$V \otimes_F \bar{\mathbb{Q}}_0 \longrightarrow E_\tau \cong W$$

which is G-equivariant and hence shows that τ is a component of $V \otimes_F \bar{\mathbb{Q}}_0$. To see uniqueness of this irreducible G-module V over F, observe that applying the construction just given to one of the components $\rho_j^{(i)}$ of $\rho^{(i)}$ in a) just gives ρ back again.

Finally we come to the proof of 7.16 c). First suppose that ρ admits no invariant form, so $W_+(G;F,\rho) = 0$. Then it is easily seen that none of the $\rho_j^{(i)}$ admits an invariant form, so the theorem is trivial. Suppose therefore that ρ admits an invariant form. If $\rho(G)$ has exponent 2, then the result is immediate from theorems 7.6 and 7.10, so assume $\rho(G)$ does not have exponent 2. Thus $E = F(\rho)$ has the non-trivial involution of theorem 7.5. Let K be the fixed field of this involution.

If $\mathfrak{y}$ is a real prime of K with $E_\mathfrak{y} = \mathbb{C}$, then the corresponding embedding

$$i_\mathfrak{y} : E \longrightarrow E_\mathfrak{y} = \mathbb{C}$$

factors as

$$\begin{array}{ccc} E & \xrightarrow{\;i'_\mathfrak{y}\;} & \bar{\mathbb{Q}} \\ & {\searrow}^{i_\mathfrak{y}} & \cap \\ & & \mathbb{C} \end{array}$$

Since the inclusion $\bar{\mathbb{Q}} \subset \mathbb{C}$ induces an isomorphism $WU(\bar{\mathbb{Q}}) \longrightarrow WU(\mathbb{C})$, we may reformulate as much of theorem 7.14 as we need here as follows:

$$WU(E) \otimes R \xrightarrow{\;\sum i'_\mathfrak{y}\;} \coprod_{\mathfrak{y}} WU(\bar{\mathbb{Q}}) \otimes R ,$$

sum over all real primes $\mathfrak{y}$ of K with $E_\mathfrak{y} = \mathbb{C}$, is an isomorphism $(R = \mathbb{Z}[\frac{1}{2}])$.

Observe that the real primes $\mathfrak{y}$ of K with $E_\mathfrak{y} = \mathbb{C}$ are classified as follows by the $m_j^{(i)}(t)$, $j \le k(i)$: the corresponding embedding $i'_\mathfrak{y} : E \to \bar{\mathbb{Q}}$ maps ξ onto a complex root of $m^{(i)}(t)$ where $i = i'_\mathfrak{y} | F$, so $i'_\mathfrak{y}(\xi)$ is a root of one of the $m_j^{(i)}(t)$; conversely, given $m_j^{(i)}(t)$, mapping ξ to a root of this polynomial defines a complex embedding $i'_\mathfrak{y} : E \to \bar{\mathbb{Q}}$ as desired. Denote the $\mathfrak{y}$ corresponding in this way to $m_j^{(i)}(t)$ by $\mathfrak{y}_j^{(i)}$.

Consider the diagram

$$\begin{array}{ccc} WU(E) \otimes R & \xrightarrow{\;\sum i'_\mathfrak{y}\;} & \coprod_{\mathfrak{y}_j^{(i)}} WU(\bar{\mathbb{Q}}) \otimes R \\ \downarrow & & \downarrow \\ W_+(G;F,\rho) \otimes R & \longrightarrow & \coprod_{\rho_j^{(i)}} W_+(G;\bar{\mathbb{Q}}_0, \rho_j^{(i)}) \otimes R \end{array}$$

where we need only sum over the $\rho_j^{(i)}$ with $j \le k(i)$, since the other $\rho_j^{(i)}$ admit no invariant bilinear form (if they did, then $\rho(G)$ would have had exponent 2) and thus give zero summands. Here the vertical arrows are given by theorem 7.6 and are hence isomorphisms. To prove 7.16 c), it suffices therefore to prove commutativity of this diagram.

Suppose we have a hermitian space over E. Without loss of generality assume it is the unary space $\langle k \rangle$ with $k \in K^*$.

By theorem 7.5, the corresponding bilinear G-space over F is given by the F-bilinear form

$$b(x,y) = tr_{E/F}(kx\bar{y})$$

on E . The $\rho_j^{(i)}$ component of $E^{(i)} = E \otimes_F \bar{\mathbb{Q}}_o$ is the subspace generated by $q_j^{(i)}(\xi)x$ for suitable x (lemma 7.17); $x = 1$ leads to a non-zero element and is hence suitable. We must thus calculate $tr(k \cdot q_j^{(i)}(\xi) \cdot \overline{q_j^{(i)}(\xi)})$, where $tr: E^{(i)} \longrightarrow \bar{\mathbb{Q}}_o$ is $tr_{E/F} \otimes id_{\bar{\mathbb{Q}}_o}$. If k is the element $\sum a_s \xi^s \in K$ with $a_s \in F$, then

$$tr(k \cdot q(\xi) \cdot \overline{q(\xi)}) = \sum_{\lambda} \left(\sum a_s \lambda^s\right) \cdot q(\lambda) \cdot q(\bar{\lambda}) \ , \ (q = q_j^{(i)}) \ ,$$

sum over all roots of $m^{(i)}(t)$, by definition of trace. But $q(\lambda) = 0$ unless λ is one of the two roots μ and $\bar{\mu}$ say of $m_j^{(i)}(t)$, so

$$\begin{aligned} tr(k \cdot q(\xi) \cdot \overline{q(\xi)}) &= q(\mu)\overline{q(\mu)}(\sum a_s \mu^s + \sum a_s \bar{\mu}^s) \\ &= q(\mu)\overline{q(\mu)}(i'_\chi(k) + \overline{i'_\chi(k)}) \ , \ (\chi = \chi_j^{(i)}) \\ &= q(\mu)\overline{q(\mu)}(i'_\chi(k) + i'_\chi(k)) \\ &= 2q(\mu)\overline{q(\mu)} i'_\chi(k) \ . \end{aligned}$$

Since $2q(\mu)\overline{q(\mu)} \in \bar{\mathbb{Q}}_o^+$, the corresponding hermitian form over $\bar{\mathbb{Q}}$ is equivalent to $\langle i'_\chi(k) \rangle$, proving commutativity of the diagram and completing the proof of 7.16.

It remains only to prove corollary 7.4. Let A and F be as in that corollary. By corollary 6.6 we know that the inclusion

$$W_*(G;A) \longrightarrow W_*(G;F,A)$$

becomes an isomorphism on tensoring with R . Thus we must determine the image of the injection

$$W_*(G;F,A) \otimes R \longrightarrow W_*(G;F) \otimes R = \coprod_i R[\hat{G}_{\bar{\mathbb{Q}}}] \ .$$

Now from the above analysis it is clear that the image is contained in $\coprod_i R[\hat{G}_{\bar{A}}]$, since if $\rho: G \to GL(V)$ is an irreducible representation which is defined over A , then each element of $\rho(G)$ has monic minimal polynomial in $A[t]$, so the roots are all in $\bar{A}$, but these roots determine the representations into which ρ splits on tensoring with $\bar{\mathbb{Q}}_o$. To see that the image is exactly $\coprod R[\hat{G}_{\bar{A}}]$, observe that, for fixed real embedding i , an element of $R[\hat{G}_{\bar{A}}]$ defines a representation $\tau: G \to GL(W)$ over $\bar{\mathbb{Q}}$, which, under the procedure of the proof of 7.16 b) , leads to a representation which is defined over A .

To close this section we describe how theorem 7.2 and its corollaries must be modified if G is not finitely generated. Define a representation $\rho: G \to GL(V)$ over $\bar{\mathbb{Q}}_o$ or $\bar{\mathbb{Q}}$ to have <u>finite type</u> if the $\mathbb{Q}$-subalgebra of GL(V) generated by $\rho(G)$ is finite dimensional over $\mathbb{Q}$. Denote by

$$W^o(G;\bar{\mathbb{Q}}_o) \quad , \quad WU^o(G;\bar{\mathbb{Q}})$$

the Witt groups of representations of finite type. Similarly if S_X^1 is any subgroup of the circle group $S^1 \subset \mathbb{C}$, define a homomorphism $f: G \to S_X^1$ to have <u>finite type</u> if $f(G)$ generates a finite extension of $\mathbb{Q}$ in $\mathbb{C}$. Define

$$\hat{G}^{o}_{X} := \{f \in \mathrm{Hom}(G,S^{1}_{X}) \mid f \text{ has finite type}\} .$$

Theorem 7.18. Theorem 7.2, corollary 7.3, and corollary 7.4 are correct for any abelian G if we replace $W_{\epsilon}(G;\bar{\mathbb{Q}}_{o})$ by $W^{o}_{\epsilon}(G;\bar{\mathbb{Q}}_{o})$, $WU(G;\bar{\mathbb{Q}})$ by $WU^{o}(G;\bar{\mathbb{Q}})$, $R[\hat{G}_{\bar{\mathbb{Q}}}]$ by $R[\hat{G}^{o}_{\bar{\mathbb{Q}}}]$, and $R[\hat{G}_{\bar{A}}]$ by $R[\hat{G}^{o}_{\bar{A}}]$.

Proof. The finite type condition is precisely what is needed to make 7.16 b) go through, otherwise everything is unchanged.

§8. Torsion in Witt groups of abelian groups

We first summarize the immediate consequences of the analysis of the previous section for torsion in Witt groups of abelian groups over algebraic number fields.

Theorem 8.1. If G is abelian then the Witt groups $W_{\epsilon}(G;F)$, $WU(G;F)$ over algebraic number fields have only 2-primary torsion of exponent ≤ 8.

If $G/2G$ is finitely generated, the 8-torsion is finite. If further G is finite of $\sqrt{-1} \in F$, then respectively only finite or no 4-torsion occurs (if $\epsilon = 1$ we must add the condition $G/2G = 0$).

8-torsion only occurs in the symmetric case, and then only if $W_{+}(F)$ has 8-torsion (e.g. not for $F = \mathbb{Q}$).

Proof. The only way 8-torsion arises is in the summands $W_{+}(G;F,\rho)$ with $2(\rho(G)) = \{0\}$, in which case $W_{+}(G;F,\rho) = W_{+}(F)$ (theorems 7.6, 7.7, 7.8, 7.10, 7.14). This proves the statements on 8-torsion. If G is finite it has only finitely many irreducible representations over F, and each one only gives finite 4-torsion by 7.8, 7.14. If $\sqrt{-1} \in F$, then -1 is a norm of E/K in theorem 7.14, so 4-torsion can only occur in the summands $W_{+}(G;F,\rho)$ with $2(\rho(G)) = \{0\}$.

If G is a non-torsion abelian group, then the groups $W_{\epsilon}(G;A)$ over a Dedekind domain A in an algebraic number field will in general still have infinite torsion. We consider here the case $G = \mathbb{Z}$. Note that if G more generally has a quotient equal to $\mathbb{Z}$, then the induced map $W_\epsilon(\mathbb{Z};A) \longrightarrow W_\epsilon(G;A)$ is injective, so our results extend to such G.

Theorem 8.2. *Let A be a Dedekind domain in an algebraic number field F. If $\sqrt{-1} \notin A$ then $W_\epsilon(\mathbb{Z};A)$ has infinite 2-torsion and infinite 4-torsion. If $\sqrt{-1} \in A$, then $W_\epsilon(\mathbb{Z};A)$ still has infinite 2-torsion (but zero 4- and 8-torsion by 8.1 if $\epsilon = -1$). In particular*

$$W_\epsilon(\mathbb{Z};\mathbb{Z}) = \mathbb{Z}^\infty \oplus (\mathbb{Z}/2)^\infty \oplus (\mathbb{Z}/4)^\infty .$$

Proof. A bilinear representation $\rho: \mathbb{Z} \longrightarrow \mathrm{Aut}(V,b)$ of $\mathbb{Z}$ is determined by the triple $(V,b,\rho(1))$ consisting of the bilinear space (V,b) plus an isometry $\rho(1)$. Such a triple is called an *isometric structure*, and it is convenient to talk in terms of this equivalent notion when considering bilinear representations of $\mathbb{Z}$. If ρ is irreducible and $m(t)$ is the minimal polynomial of $\rho(1)$, then $m(t)$ is irreducible and the field $F(\rho)$ of section 7 is

$$F(\rho) = F[t]/(m(t)) .$$

Lemma 8.3.

(i). *Let $X \in Sp(2,A) = \mathrm{Aut}(A^2, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix})$ and let $[X] \in W_-(\mathbb{Z};A)$ be the class of the bilinear antisymmetric representation of $\mathbb{Z}$ generated by X. Let $s = tr(X)$, $D = s^2-4$. Then the order of $[X]$ is*

1 *if D is a square in F,*

∞ *if it is false that $D \gg 0$,*

2 *if -1 is a norm of $F(\sqrt{D})/F$,*

4 *if $D \gg 0$ and D is not a norm of $F(\sqrt{D})/F$.*

Here $D \gg 0$ means D totally positive, that is $D > 0$ in each real embedding of F.

(ii). *If $s \neq 0$, the same holds for the order of $[X \otimes X] \in W_+(\mathbb{Z};A)$.*

Remark. If $A = \mathbb{Z}$ in the above lemma, then elementary number theory says that -1 is a norm of $Q(\sqrt{D})/Q$, $D = s^2-4 > 0$, if and only if each prime of the form $4k+3$ occurring in $s-2$ or $s+2$ occurs to an even power. Thus $[X]$ has infinite order iff $|s| < 2$, is trivial iff $|s| = 2$, has order 2 iff $|s| = 3,6,7,11,15,18,27,34,38,39,43,47, \ldots$, and has order 4 otherwise.

Proof of lemma. Since $W_\epsilon(\mathbb{Z};A) \longrightarrow W_\epsilon(\mathbb{Z};F)$ is injective, we may work in $W_\epsilon(\mathbb{Z};F)$. To prove (i), observe that the minimal polynomial of X is $m(t) = t^2-st+1$, which has roots $(s\pm\sqrt{D})/2$. Thus the field $F(\rho) = F[t]/(m(t))$ is $F(\sqrt{D})$ if D is not a square, and the lemma follows from the last sentence of corollary 7.15. If D is a square, then $m(t)$ is reducible, so the representation is reducible. Any non-trivial invariant subspace is self-orthogonal, hence an invariant kernel, so $[X] = 0$ in $W_-(\mathbb{Z};F)$.

Statement (ii) of the lemma is now trivial if D is a square in F, so assume this is not the case. Then the characteristic polynomial of $X \otimes X$ is $(t-\mu^2)(t-\bar{\mu}^2)(t-1)^2$, where

$\mu = (s+\sqrt{D})/2$ is a root of $m(t) = t^2-st+1$. Since μ^2 still generates $F(\sqrt{D})$ over F, the factor $m_1(t) = (t-\mu^2)(t-\bar{\mu}^2)$ is irreducible, so it corresponds to a summand C of $X \otimes X$ and we have a splitting (over F) $X \otimes X = C \oplus D$. Thus $[X \otimes X] = [C] + [D]$ in $W_+(\mathbb{Z};F)$, and since $[C]$ and $[D]$ correspond to different minimal polynomials, they are independent in $W_+(\mathbb{Z};F)$ (theorem 2.4). Now $[X \otimes X]$ can have at most the stated order in $W_+(\mathbb{Z};F)$ by part (i), but it has at least this order, since $[C]$ does, by the same argument as in part (i).

Proof of 8.2. To find an element of order 2 in $W_\epsilon(\mathbb{Z};A)$ we can for instance in lemma 8.3 choose $X = \begin{pmatrix} s & 1 \\ -1 & 0 \end{pmatrix} \in Sp(2,A)$ with $s = r^2+2$, $r \in A$. Then $D = r^2(r^2+4)$, which is a non-square for most values of r and is totally positive. Also -1 is a norm of $F(\sqrt{D})/F$, namely $-1 = N(r/2 + \sqrt{D}/2r)$. Thus $[X]$ has order 2 if D is a non-square. The $[X]$ obtained in this way for varying r have different minimal polynomials, so they are independent in $W_\epsilon(\mathbb{Z};A)$.

Now suppose $\sqrt{-1} \notin A$. Then $\sqrt{-1} \notin F$, so -1 is a non-square in F for infinitely many $\mathfrak{p}$ ([OM ; 65:15]). Choose such a $\mathfrak{p}$ which is not dyadic, that is, it does not divide (2), and choose $s \in A$ satisfying

$$s-2 \in \mathfrak{p} - \mathfrak{p}^2 \quad , \quad s-2 \gg 0 \quad .$$

For given $\mathfrak{p}$ one can find infinitely many such s ([OM ; 33:5]). For each such s, $D = s^2-4$ will be in $\mathfrak{p} - \mathfrak{p}^2$ and be totally positive. Also -1 is not a norm of $F(\sqrt{D})$, since if it were,

then we would have $x^2-Dy^2 = -1$ for some $x,y \in F_{\mathfrak{p}}$ and by considering divisibility by $\mathfrak{p}$ we would see that actually $x,y \in A_{\mathfrak{p}}$. Reducing modulo $\mathfrak{p}$ would thus give $x^2 = -1$ in $A_{\mathfrak{p}}/\mathfrak{p} = A/\mathfrak{p}$, contradicting the choice of $\mathfrak{p}$. Thus $X \in Sp(2,A)$ with $tr(X) = s$ as above gives elements of order 4 in $W_\epsilon(\mathbb{Z};A)$ by lemma 8.3. For varying s we again get infinitely many independent elements, since they belong to different minimal polynomials.

The analysis of the last two sections also easily gives finiteness results for torsion in $W_\epsilon(G;A)$.

Theorem 8.4. *If A is a Dedekind domain in an algebraic number field F which is integral at all but finitely many primes of F (e.g. A = ring of integers of F), then for any irreducible representation $\rho : G \longrightarrow GL(V)$ over F which is defined over A, $W_\epsilon(G;A,\rho)$ is finitely generated, hence has finite torsion.*

Proof. Assume first that A is the ring of integers of F. We assume also that $2(\mathrm{Im}(\rho)) \neq (0)$, the proof is analogous if $2(\mathrm{Im}(\rho)) = (0)$.

Let $E = F(\rho)$ and let $A(\rho)$ be the subring of E generated by A and $\mathrm{Im}(\rho)$. V is a 1-dimensional E-vector-space, and any E-linear isomorphism $E \cong V$ identifies $A(\rho)$ as a G-invariant A-lattice in V.

Now $A(\rho) \subset \bar{A}$, the integral closure of A in E, and since $A(\rho)$ and $\bar{A}$ are both A-lattices in E, the index

$[\bar{A}:A(\rho)] = D$ is finite. Let $\mathfrak{p}$ be a prime ideal in A which does not divide D and which is unramified for E/F. Then

$$\bar{A}/\bar{A}_{\mathfrak{p}} = A(\rho)/A(\rho)\mathfrak{p} \quad ,$$

so the decomposition of $\bar{A}/\bar{A}$ as a product of finite fields:

$$\bar{A}/\bar{A}\mathfrak{p} = A/\mathfrak{P}_1 \times \ldots \times A/\mathfrak{P}_s \quad ,$$

corresponding to the decomposition

$$\bar{A}\mathfrak{p} = \mathfrak{P}_1 \mathfrak{P}_2 \cdots \mathfrak{P}_s$$

of $\bar{A}\mathfrak{p}$ into primes in E, can be written as

$$A(\rho)/A(\rho)\mathfrak{p} = (A/\mathfrak{p})(\bar{\rho}_1) \times \ldots \times (A/\mathfrak{p})(\bar{\rho}_s) \quad ,$$

and gives simultaneously the decomposition of the representation $\bar{\rho} = (\rho \bmod \mathfrak{p})$ over $A/\mathfrak{p}$ into its irreducible components

$$\bar{\rho} = \bar{\rho}_1 \oplus \ldots \oplus \bar{\rho}_s \quad .$$

The involution on E induces involutions on everything we have considered, in particular it permutes the $\mathfrak{P}_i$ and the $\bar{\rho}_i$. For each $\mathfrak{P}_i$, let $\mathfrak{P}_i'$ be the unique prime of the fixed field $K \subset E$ lying under $\mathfrak{P}_i$. We must consider three possible cases.

Case 1. If the involution exchanges $\mathfrak{P}_i$ and $\mathfrak{P}_j$ $(i \neq j)$, then it exchanges $(A/\mathfrak{p})(\bar{\rho}_i)$ and $(A/\mathfrak{p})(\bar{\rho}_j)$, so it is not definable of $(A/\mathfrak{p})(\bar{\rho}_i)$ or $(A/\mathfrak{p})(\bar{\rho}_j)$ alone. Thus by theorem 7.5, $\bar{\rho}_i$ and $\bar{\rho}_j$ admit no invariant form, so $W_\epsilon(G;A/\mathfrak{p},\bar{\rho}_i) = W_\epsilon(G;A/\mathfrak{p},\bar{\rho}_j) = \{0\}$. Further $\mathfrak{P}_i' = \mathfrak{P}_j'$, so $\mathfrak{P}_i'$ splits completely in E/K, so $K_{\mathfrak{P}_i'} = E_{\mathfrak{P}_i}$. Note that $E_{\mathfrak{P}_i} = E_{\mathfrak{P}_i'}$ in the notation of theorem 7.14, so this means that these primes are disregarded in that theorem.

Case 2. The involution maps $\mathfrak{P}_i$ onto itself and induces the trivial involution on $\bar{A}/\mathfrak{P}_i = (A/\mathfrak{p})(\bar{\rho}_i)$. This can only happen for finitely many $\mathfrak{p}$ and i.

Case 3. The involution maps $\mathfrak{P}_i$ onto itself and is non-trivial on $\bar{A}/\mathfrak{P}_i = (A/\mathfrak{p})(\bar{\rho}_i)$. Then by corollary 7.6,

$$W_\epsilon(G;A/\mathfrak{p},\bar{\rho}_i) \cong WU((A/\mathfrak{p})(\bar{\rho}_i)) = WU(\bar{A}/\mathfrak{P}_i) \quad .$$

Further $\mathfrak{P}_i$ is the unique prime of E lying over $\mathfrak{P}_i'$ and is by assumption unramified. In this case we can define a map (the "second residue class form")

$$\partial' : WU(E_{\mathfrak{P}_i}) \longrightarrow WU(\bar{A}/\mathfrak{P}_i)$$

exactly as in the bilinear case (theorem 6.5 with $G = \{1\}$). Since $\mathfrak{P}_i/\mathfrak{P}_i'$ is unramified, -1 is a norm of $E_{\mathfrak{P}_i}/K_{\mathfrak{P}_i}$, so $WU(E_{\mathfrak{P}_i}) = \mathbb{Z}/2 \oplus \mathbb{Z}/2$ (theorem 7.14). Also $WU(\bar{A}/\mathfrak{P}_i) = \mathbb{Z}/2$ theorem 7.13) and an easy calculation shows that ∂' is the map $\partial'(r,1) = 1 \in \mathbb{Z}/2$, notation as in 7.14.

Thus by summing over the primes $\mathfrak{p}$ of F considered above and the factors $\mathfrak{P}_i$ of $\mathfrak{p}$ in E of case 3 (respectively the corresponding $\bar{\rho}_i$) we have a commutative diagram

$$\begin{array}{ccc}
W_\epsilon(G;F,\rho) & \xrightarrow{\ \partial\ } & \coprod_{\mathfrak{p}} \coprod_{\bar\rho_i} W_\epsilon(G;\Lambda/\mathfrak{p},\bar\rho_i) \\
\downarrow \cong & & \\
WU(E) & & \downarrow \cong \\
\downarrow \text{loc} & & \\
\prod_{\mathfrak{p}} \prod_{\mathfrak{p}_i} WU(E_{\mathfrak{p}_i}) & \xrightarrow{\ \partial'\ } & \coprod_{\mathfrak{p}} \coprod_{\mathfrak{p}_i} WU(\bar\Lambda/\mathfrak{p}_i)
\end{array}$$

with ∂ and loc as in 6.7 and 7.14. By 7.14 i), ∂' restricted to the image of loc has kernel $\mathbb{Z}/2$, so since we have only disregarded finitely many relevant primes, $\partial' \circ \text{loc}$ has finitely generated kernel. Hence ∂ has finitely generated kernel, but $W_\epsilon(G;A,\rho) \subset \text{Ker}(\partial)$ by theorem 6.7, so the proof is complete in this case.

If A is not the ring of integers of F but is still integral at all but finitely many primes of F, then the same argument goes through, omitting these finitely many additional primes of F.

<u>Corollary 8.5</u>. <u>If</u> A <u>is as in the above theorem and</u> G <u>is finite</u>, <u>then</u> $W_\epsilon(G;A)$ <u>is finitely generated</u>.

A. Bak has informed me that this corollary holds for any finite G; abelianness is not necessary.

<u>Proof</u>. Consider the diagram (theorems 6.2, 6.4, 6.6, 6.7)

$$\begin{array}{ccccccc}
 & & 0 & & & & \\
 & & \downarrow & & & & \\
0 & \longrightarrow & \coprod_{\rho} W(G;A,\rho) & \longrightarrow & \coprod_{\rho} W_\epsilon(G;F,\rho) & \longrightarrow & \coprod_{\rho} \coprod_{\mathfrak{p}} \coprod_{\rho_j^{\mathfrak{p}}} W_\epsilon(G;\Lambda/\mathfrak{p},\rho_j^{\mathfrak{p}}) \\
 & & \downarrow & & & & \downarrow \\
0 & \longrightarrow & W_\epsilon(G;A) & \longrightarrow & W_\epsilon(G;F,A) & \longrightarrow & \coprod_{\mathfrak{p}} \coprod_{\rho^{\mathfrak{p}}} W(G;\Lambda/\mathfrak{p},\rho^{\mathfrak{p}})
\end{array}$$

where the $\rho^{\mathfrak{p}}$ in the bottom line run through all irreducible representations over $A/\mathfrak{p}$, and for each ρ and $\mathfrak{p}$, the $\rho_j^{\mathfrak{p}}$ in the top line run through the irreducible components of (ρ mod $\mathfrak{p}$). The right vertical arrow in general has a kernel, since it may happen that $\rho_j^{\mathfrak{p}} = (\rho')_{j'}^{\mathfrak{p}}$ for $\rho \neq \rho'$. But for any fixed pair ρ, ρ' this can only happen for finitely many $\mathfrak{p}$, and since there are only finitely many ρ and each summand on the right is finite, the kernel of the right vertical map is finite. This hence also holds for the cokernel of the left vertical map, so the corollary follows from the previous theorem.

§9. Characters of hermitian representations

In this section we generalize the usual character of a representation to a Witt ring invariant of hermitian representations. This generalization, though very natural, has some rather unsatisfactory aspects, the main one being that for non-compact non-abelian groups representations are in general no longer distinguished by their characters.

Before we define character in general, we first consider two examples. We only consider hermitian representations over $\mathbb{C}$ for the moment.

Example 9.1. G a compact Lie group. By corollary 4.3 there is a natural isomorphism

$$\varphi : R(G) \xrightarrow{\cong} WU(G)$$

from the complex representation ring, by putting a positive definite hermitian metric on any complex representation. The inverse of φ can be described as follows: given a hermitian representation ρ of G, ρ can be split as the orthogonal sum $\rho^+ \oplus \rho^-$ of a positive and a negative definite representation and we have

$$\varphi^{-1}[\rho] = [\rho^+] - [\rho^-] \in R(G) \quad .$$

For any $[\rho] \in WU(G)$ we can define the character $\chi_\rho : G \to \mathbb{C}$ of ρ to be the character of $\varphi^{-1}[\rho]$, that is, $\chi_\rho(g) =$ trace $\rho^+(g)$ - trace $\rho^-(g)$. To extend the definition of character to arbitrary G we need another example.

Example 9.2. $G = \mathbb{Z}$, cyclic of infinite order. As we saw in theorem 4.9 and subsequent remarks, $WU(\mathbb{Z})$ is isomorphic to the group ring

$$WU(\mathbb{Z}) = \mathbb{Z}[S^1] \quad ,$$

where the isomorphism takes the element $\mu \in S^1 \subset \mathbb{Z}[S^1]$ to the positive definite representation

$$\mathbb{Z} \longrightarrow U(1) = S^1 \quad ; \quad 1 \longmapsto \mu \quad .$$

Observe that any $x \in WU(\mathbb{Z})$ can be written $x = [\rho^+] + [\rho^-]$ where ρ^+ and ρ^- are a positive definite and negative definite representation respectively (this is true for any G all of whose irreducible hermitian representations are definite). We can thus define the character $\chi_x : G \to \mathbb{C}$ as $\chi_{\rho^+} - \chi_{\rho^-}$, that is $\chi_x(g) =$ trace $\rho^+(g)$ - trace $\rho^-(g)$.

More generally for arbitrary G and $x \in WU(G)$ we define the character

$$\chi_x : G \longrightarrow \mathbb{C}$$

by setting $\chi_x(g)$ equal to $\chi_y(g)$ where y is the restriction of x to any cyclic subgroup of G containing g.

Theorem 9.3. As a map from $WU(G)$ to $\mathbb{C}^G$, χ is a ring homomorphism. It is injective for compact Lie groups and for abelian groups, but is not injective for instance for free groups on two or more generators.

Proof. The condition that χ is a ring homomorphism is that $\chi_{x \otimes y}(g) = \chi_x(g)\,\chi_y(g)$. Since this holds for G cyclic it also holds for arbitrary G. The injectivity of χ is standard for compact Lie groups, since then χ can be interpreted as the usual character on $R(G)$ (example 9.1). For $G = \mathbb{Z}$ injectivity follows from the easily checked orthogonality relation

$$\lim_{N} \frac{1}{2N} \sum_{n=-N}^{N} \chi_\rho(n)\, \chi_\tau(n)^{-1} = \begin{cases} 1\,, & \rho = \tau \\ \,, & \rho \neq \tau \end{cases}$$

for any two irreducible hermitian representations ρ and τ of $\mathbb{Z}$. For arbitrary finitely generated abelian groups a similar orthogonality relation holds; alternatively observe that if χ is injective for groups G and H, then it is injective for $G \times H$ by the commutativity of

$$\begin{array}{ccc} WU(G) \otimes WU(H) & \xrightarrow{\chi_G \otimes \chi_H} & \mathbb{C}^G \otimes \mathbb{C}^H \\ \downarrow & & \downarrow \\ WU(G \times H) & \xrightarrow{\chi_{G \times H}} & \mathbb{C}^{G \times H} \end{array}$$

and the injectivity of the right vertical arrow. Finally for arbitrary abelian groups injectivity follows by a direct limit argument; in fact we show in § 10 that for a direct limit of groups G_α the natural map $WU(\varinjlim G_\alpha) \longrightarrow \varprojlim WU(G_\alpha)$ is injective, so if character is injective for each G_α it also is injective for the direct limit.

The following remarks yield any number of irreducible representations $\rho : G \rightarrow U(1,1)$ of free groups G with $\chi_\rho = 0$. Since an irreducible representation is non-zero in $WU(G)$, this shows non-injectivity of χ.

9.4. Direct calculation shows that the character $\chi : U(1,1) \longrightarrow \mathbb{C}$ is given by $\chi(A) = \pm\sqrt{\det A} \cdot \operatorname{Im} \sqrt{|\operatorname{tr} A|^2 - 4}$, so $\chi(A) = 0$ if and only if $|\operatorname{tr} A| \geq 2$.

9.5. The obvious action of $SL(2,\mathbb{Z})$ on $\mathbb{C}^2$ preserves the hermitian form $\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}$ of signature 0, and thus gives a representation $SL(2,\mathbb{Z}) \longrightarrow U(1,1)$.

9.6. An element $A \in SL(2,\mathbb{Z}) - \{\pm I\}$ has $|\operatorname{tr} A| \geq 2$ if and only if it has infinite order (proof: calculate the eigenvalues).

9.7. $SL(2,\mathbb{Z})/(\pm I) = PSL(2,\mathbb{Z}) \cong (\mathbb{Z}/2) * (\mathbb{Z}/3)$ contains any number of free subgroups by the Kurosh subgroup theorem (in fact any subgroup of finite index $6k$ is free of rank $(k+1)$). Any such subgroup lifts to $SL(2,\mathbb{Z})$ since it is free.

9.8. Remarks 9.5 and 9.7 give faithful representations $\rho : G \longrightarrow U(1,1)$ of free groups. By 9.4 and 9.6 these representations satisfy $\chi_\rho = 0$. They are irreducible, since a group which has a faithful reducible 2-dimensional representation must clearly be soluble of solubility length 2, which a free group of rank ≥ 2 is not.

The final statement of the above theorem says that characters are in general insufficient for the Witt theory of hermitian representations. Nevertheless the theorem tells us that in many interesting cases they actually do distinguish elements of the Witt group, and in any case they are a convenient numerical invariant of hermitian representations.

Via the ring homomorphisms (where $W_* = W_+ \oplus W_-$)

$$W_*(G;\mathbb{Z}) \longrightarrow W_*(G;\mathbb{Q}) \longrightarrow W_*(G;\mathbb{R}) \xrightarrow{\phi} WU(G) \xrightarrow{\chi} \mathbb{C}^G ,$$

character is also defined for integral, rational and real bilinear representations and distinguishes Witt classes up to torsion at least for G finite and G abelian (see 6.8, 7.2, 7.4). We still denote character by χ in each case. Note that

$$\chi : W_+(G;\mathbb{R}) \oplus W_-(G;\mathbb{R}) \longrightarrow \mathbb{C}^G = \mathbb{R}^G \oplus (i\mathbb{R})^G$$

preserves the direct splitting, that is, character of an ϵ -symmetric bilinear representation is real or pure imaginary according as $\epsilon = +1$ or $\epsilon = -1$.

§10. Direct limits

We have once or twice indicated the following fact, which we will now prove.

Theorem 10.1. *If $G = \varinjlim G_\alpha$ is the direct limit of groups G_α, then the natural map*

$$i: W_\epsilon(G;F) \longrightarrow \varprojlim W_\epsilon(G_\alpha;F)$$

is injective. The same holds for $WU(G;F)$ if F has an involution and for Witt rings over Dedekind domains.

It is not hard to find examples to show that this map is in general not surjective, even for abelian groups.

Proof. Let $\rho : G \to \mathrm{Aut}(V,b)$ be a bilinear representation over F and suppose $i[\rho] = 0$. Let $\pi_\alpha^* : W_\epsilon(G;F) \to W_\epsilon(G_\alpha;F)$ be the map induced by the natural map $\pi_\alpha : G_\alpha \to G$. The condition $i[\rho] = 0$ is equivalent to requiring $\pi_\alpha^*[\rho] = 0$ for each α , i.e. $[\rho\circ\pi_\alpha] = 0$ in $W_\epsilon(G_\alpha;F)$ for each α . Denote by $\mathcal{K}_\alpha$ the set of ordered bases $(a_1, \dots, a_{2n})$ of V such that $K = \langle a_1, \dots, a_n\rangle$ is an invariant kernel for $\rho\circ\pi_\alpha$ (that is $K = K^\perp$ and $\rho\circ\pi_\alpha(G_\alpha)K = K$). $\mathcal{K}_\alpha$ is by assumption non-empty and it is clearly an algebraic variety in V^{2n} . Also if $\alpha \le \beta$ then $\mathcal{K}_\alpha \supset \mathcal{K}_\beta$. Now by compactness of the Zariski topology on V^{2n} , the intersection $\mathcal{K} = \bigcap_\alpha \mathcal{K}_\alpha$ is non-empty (since each finite subintersection is non-empty). An element of $\mathcal{K}$ yields an invariant kernel for ρ , proving the theorem in this case.

The hermitian case is the same proof.

If we replace F by a Dedekind domain A then we have a commuting square, where F is now the field of fractions of A :

$$\begin{array}{ccc} W_\epsilon(G;A) & \longrightarrow & \varprojlim W_\epsilon(G_\alpha;A) \\ \downarrow & & \downarrow \\ W_\epsilon(G;F) & \longrightarrow & \varprojlim W_\epsilon(G_\alpha;F) \end{array} .$$

The vertical arrows are injective by proposition 6.3, and the bottom arrow has just been shown to be injective, so the top arrow is injective also.

Appendix: some topology

We describe briefly a direction of topological application of Witt rings.

Let M^{2n} be a compact oriented manifold, possibly with boundary. The cup product form

$$S_M : H^n(M, \partial M; \mathbb{Z}) \times H^n(M, \partial M; \mathbb{Z}) \longrightarrow \mathbb{Z}$$

defined by $S_M(x,y) = \int_M x \cup y$ is zero on $\mathrm{Ker}(H^n(M, \partial M; \mathbb{Z}) \longrightarrow H^n(M;\mathbb{Z}))$ and induces a $(-1)^n$-symmetric non-degenerate form on

$$H = \mathrm{Im}(H^n(M, \partial M; \mathbb{Z}) \longrightarrow H^n(M;\mathbb{Z}))/\mathrm{Torsion} .$$

If G is an arbitrary group acting on M, then G acts on H preserving this form, so we get an element

$$w(M,G) \in W_\epsilon(G;\mathbb{Q},\mathbb{Z}) \qquad \epsilon = (-1)^n$$

in the notation of proposition 6.4. Actually G acts from the right on H and we must convert to a left action by convening that $g \in G$ act by g^{-1} on H. This is equivalent to transposing the action via the form on H, and hence also equivalent via Poincaré-Lefschetz duality to the usual left action on homology with intersection form.

The properties of the Witt invariant are as follows.

A1. *If M is closed. Then the cup product form is non-singular, so $w(M,G)$ is in the subgroup $W_\epsilon(G;\mathbb{Z}) \subset W_\epsilon(G;\mathbb{Q},\mathbb{Z})$.*

A2. *Bordism invariance. If M is a G-equivariant oriented boundary then $w(M,G) = 0$.*

A3. *Novikov additivity. If $M = M_1 \cup M_2$ pasted G-equivariantly along boundary components then $w(M,G) = w(M_1,G) + w(M_2,G)$.*

A4. *Product formulas. If G acts on M_1 and M_2 then with the diagonal action on M_1 M_2 we have $w(M_1 \times M_2,G) = w(M_1,G) \cdot w(M_2,G)$. If G_1 acts on M_1 and G_2 on M_2, then $w(M_1 \times M_2,G_1 \times G_2) = t(w(M_1,G_1) \otimes w(M_2,G_2))$, where $t\colon W(G_1;\mathbb{Q}) \otimes W(G_2;\mathbb{Q}) \longrightarrow W_*(G_1 \times G_2;\mathbb{Q})$ is the natural map.*

The usual proofs of A2 and A3 for signature also work here. A4 is an easy application of the Künneth formula for a product. These properties show that the invariant w defines a ring homomorphism from the "equivariant bordism group" Ω_*^G to $W_*(G;\mathbb{Z})$ (and also from the equivariant "cutting and pasting group" SK_*^G to $W_*(G;\mathbb{Z})$).

Remark. The class of $w(M,G)$ in $W_*(G;\mathbb{Q},\mathbb{Z})/W_*(G;\mathbb{Z})$ is a Novikov additive invariant which vanishes for closed manifolds. It follows that it is an invariant of the boundary; call it $\ell(\partial M,G)$. In the proof of theorem 6.5, a natural injection $W_*(G;\mathbb{Q},\mathbb{Z})/W_*(G;\mathbb{Z}) \longrightarrow W_*(G;\mathbb{Z}\text{ - torsion})$ was constructed, so we can think of $\ell(\partial M,G)$ as an element of $W_*(G;\mathbb{Z}\text{ - torsion})$. For trivial G, Alexander, Hamrick and Vick [AHV] have identified $-\ell(\partial M)$ as the class of the linking form on the torsion of $H_*(\partial M;\mathbb{Z})$, so in particular $\ell(N)$ is also defined for N^{2n-1} which do not bound. Their proof also works in the present situation.

Note that the class of $\ell(N,G)$ in $\mathrm{Cok}(W_*(G;\mathbb{Q},\mathbb{Z}) \longrightarrow W_*(G;\mathbb{Z}\text{ - torsion}))$ is a bordism invariant of (N^{2n-1},G). This may be quite an interesting invariant.

The standard definition of equivariant signature for Lie group actions can be extended to arbitrary groups.

Definition. Given M^{2n} with G-action as above, define the *equivariant signature* as

$$\mathrm{sign}(M,G) := \chi w(M,G)$$

and for $g \in G$

$$\mathrm{sign}(M,g) := \chi w(M,G)(g)$$

This can be described directly as follows. Let $(H \otimes \mathbb{C},b)$ be the hermitianized, symmetrized (by multiplication by $+i$ if n is odd) cup product pairing for M. Then g induces a $\mathbb{Z}$-action on $(H \otimes \mathbb{C},b)$, and up to hyperbolic hermitian $\mathbb{Z}$-modules, $H \otimes \mathbb{C}$ splits as a sum $V^+ \oplus V^-$ of a positive and a negative definite hermitian $\mathbb{Z}$-module. Then

$$\mathrm{sign}(M,g) = \mathrm{trace}(g|V^+) - \mathrm{trace}(g|V^-) .$$

This makes it clear that if g is contained in a compact Lie group of transformations of M (equivalently g preserves some Riemannian metric on M), then $\mathrm{sign}(M,g)$ agrees with Atiyah and Singer's definition in [AS] . Note that sign(M,g) is real or pure imaginary according as n is even or odd.

For finite or abelian G , all we are doing by looking at sign(M,G) rather than w(M,G) is throwing away torsion information (theorem 9.3). However, example 9.8 can be thought of as giving examples of a linear action of a free group G on $S^1 \times S^1$ for which $\mathrm{sign}(S^1 \times S^1, G) = 0$ although $w(S^1 \times S^1, G)$ is of infinite order.

One can easily find examples of $\mathbb{Z}$-actions on closed manifolds with non-trivial equivariant signature but for which no non-trivial element has a fixed point. Thus in contrast to the situation for compact Lie groups (Atiyah-Singer-Lefschetz fixed-point theorem [AS]), the equivariant signature cannot be completely calculated in terms of the fixed-point behavior. There is however reason to hope that interesting partial results exist.

In the case of smooth orientation-preserving actions of $\mathbb{Z}$ on closed oriented manifolds, M. Kreck [Kr] has obtained complete results on the bordism group $\Omega_n^{\mathbb{Z}}$, $n > 4$, in terms of the Witt invariant. $\Omega_n^{\mathbb{Z}}$ is of course nothing more than the bordism group Δ_n of orientation-preserving diffeomorphisms of closed manifolds. The following simple theorem was proved in [N1] . We repeat it here, since it has been quoted by M. Kreck (loc. cit.).

<u>Theorem A5</u>. <u>The map</u> $w\colon \Delta_{2n} \to W_\epsilon(\mathbb{Z};\mathbb{Z})$, $\epsilon = (-1)^n$, <u>is surjective for each</u> $n > 0$.

<u>Proof</u>. For $n = 1$ this follows from the fact (Nielsen theorem plus for example Magnus, Karras, Solitar [MKS, section 3.7]) that the map

$$\mathrm{Diff}_+(F_g)/\mathrm{Diff}_o(F_g) \longrightarrow Sp(2g;\mathbb{Z})$$

is surjective. Here F_g is the orientable surface of genus g , $\mathrm{Diff}_+(F_g)$ its orientable diffeomorphism group and $\mathrm{Diff}_o(F_g)$ the component of unity. $Sp(2g;\mathbb{Z})$ is the automorphism group of $H_1(F_g;\mathbb{Z})$ with intersection form.

For $n = 2$, suppose we have a symmetric non-singular isometric structure (H,b,t) over $\mathbb{Z}$. By adding the hyperbolic structure $(\mathbb{Z}^2, \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \mathrm{id})$ if necessary we can assume the bilinear space (H,b) is indefinite and odd, so it is classified by its rank and signature alone (Serre [S]) , so it is isomorphic to the cup product form on some manifold of the form $M^4 = \mathbb{C}P^2 \# \dots \# \mathbb{C}P^2 \# -\mathbb{C}P^2 \# \dots \# -\mathbb{C}P^2 \# (S^2 \times S^2)$. By Wall [W1], any isometry of (H,b) is realizable by a diffeomorphism of M^4.

For $n > 2$ use the fact $w(N \times M, \mathrm{id} \times f) = \mathrm{sign}(N) \cdot w(M,f)$, which follows from A4 above, This completes the proof.

M. Kreck has in fact shown that the following maps are isomorphisms for $k \geq 1$:

$$\Delta_{4k} \longrightarrow \widetilde{W}_+(\mathbb{Z};\mathbb{Z}) \oplus \Omega_{4k} \oplus \widetilde{\Omega}_{4k+1} \quad ,$$

$$\Delta_{4k+1} \longrightarrow \Omega_{4k+1} \oplus \Omega_{4k+2} \quad ,$$

$$\Delta_{4k+2} \longrightarrow W_-(\mathbb{Z};\mathbb{Z}) \oplus \Omega_{4k+2} \oplus \Omega_{4k+3} \quad ,$$

$$\Delta_{4k+3} \longrightarrow \Omega_{4k+3} \oplus \widetilde{\Omega}_{4k+4} \quad .$$

Here $\widetilde{W}_+(\mathbb{Z};\mathbb{Z})$ is the reduced group $\mathrm{Ker}\,(W_+(\mathbb{Z};\mathbb{Z}) \longrightarrow W_+(\mathbb{Z}) = \mathbb{Z})$, $\widetilde{\Omega}_{4k+1}$ is the kernel of the Stiefel-Whitney number $w_2 w_{4k-1}$: $\Omega_{4k+1} \to \mathbb{Z}/2$, and $\widetilde{\Omega}_{4k+4}$ is the kernel of sign: $\Omega_{4k+4} \longrightarrow \mathbb{Z}$. The map $\Delta_n \to \Omega_n$ is just forgetting the $\mathbb{Z}$-action, and $\Delta_n \to \Omega_{n+1}$ is the map which assigns to a $\mathbb{Z}$-action on M the mapping torus $M_f = (M \times I)/(\,(x,1) \equiv (f(x),0)\,)$ of the generator of the $\mathbb{Z}$-action.

In low dimensions the calculation is still open. All that is known is that infinite $\mathbb{Z}/2$-torsion still occurs in Δ_2. Indeed, let $B_r = \begin{pmatrix} r & 1 \\ 1 & 0 \end{pmatrix}$ and $A_r = B_r^2 = \begin{pmatrix} r^2+1 & r \\ r & 1 \end{pmatrix}$. Then A_r defines a linear automorphism of the torus $T^2 = S^1 \times S^1$ and the Witt invariants all have order 2 and are independent by 8.3. On the other hand B_r induces an A_r-equivariant orientation-reversing diffeomorphism of T^2, so $[T^2, A_r] = -[T^2, A_r]$ in Δ_2 and we have infinitely many independent 2-torsion elements.

An application of the theory of Witt rings to signature of fiber bundles is described in [N2].

Another direction of application is to knot theory. If $\epsilon = \pm 1$ and A is an integral n-square matrix with $\det(A) \neq 0$ and $\det(A + \epsilon A^t) = \pm 1$, then

$$I_\epsilon(A) = (\mathbb{Q}^n, A + \epsilon A^t, -\epsilon A (A^t)^{-1})$$

is an isometric structure and hence defines an element of $W_\epsilon(\mathbb{Z};\mathbb{Q})$. Let C_ϵ be the subgroup of $W_\epsilon(\mathbb{Z};\mathbb{Q})$ generated by such elements. Then Levine [Le2] showed that C_ϵ is isomorphic to the bordism group [Le1] of spherical knots in $S^{4k+\epsilon}$, $4k+\epsilon > 5$, and that

C_ϵ, like $W_\epsilon(\mathbb{Z};\mathbb{Q})$, has the form $\mathbb{Z}^\infty \oplus (\mathbb{Z}/4)^\infty \oplus (\mathbb{Z}/2)^\infty$, see also [Ke] for a discussion of these results.

Of interest also is the subgroup F_ϵ of C_ϵ determined by those A with $\det(A) = \pm 1$, since this is isomorphic to the subgroup of the knot bordism group generated by fibered knots. Using the argument of lemma 8.3 (namely corollary 7.15) it is easy to check that F has infinitely generated free part and has infinite torsion. With a bit more work using the same methods one can show that F_{-1} has the form $\mathbb{Z}^\infty \oplus (\mathbb{Z}/4)^\infty \oplus (\mathbb{Z}/2)^\infty$; this is presumably true for F_{+1} also.

References

[ACHV] J.P. Alexander, P.E. Conner, G.C. Hamrick, J.W. Vick: Witt classes of integral representations of an abelian p-group, Bull. Amer. Math. Soc. 80(1974), 1179-1182.

[AHV] J.P. Alexander, G.C. Hamrick, J.W. Vick: Bilinear forms and cyclic group actions, Bull. Amer. Math. Soc. 80(1974), 730-734.

[AS] M.F. Atiyah, I.M. Singer: The index of elliptic operators III, Ann. of Math. 87(1968), 546-604.

[B] A. Bak: Unpublished manuscript.

[D] A.W.M. Dress: Induction and structure theorems for orthogonal representations of finite groups, Ann. of Math. 102(1975), 291-326.

[F] A. Fröhlich: On the K-theory of unimodular forms over rings of algebraic integers, Preprint 1971.

[HNK] F. Hirzebruch, W.D. Neumann, S.S. Koh: Differentiable manifolds and quadratic forms, Lecture Notes in Pure and Applied Mathematics Nr. 4 (M. Dekker, New York 1971).

[J] N. Jacobsen: Lectures in abstract algebra Vol. 3, (Van Nostrand, Princeton 1951).

[Ke] M.A. Kervaire: Knot cobordism in codimension 2, Manifolds - Amsterdam 1970, Springer Lecture Notes 197(1971), 83-105.

[Kn] M- Knebusch: Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen, Sitzungsbericht der Heidelberger Akad. der Wiss. (1969/70), 3. Abh.

[KnS] M. Knebusch, W. Scharlau: Quadratische Formen und Quadratische Reziprozitätsgesetze über algebraischen Zahlkörpern, Math. Z. 121(1971), 346-368.

[Kr] M. Kreck: Bordismusgruppen von Diffeomorphismen, in preparation (Announcement to appear in Bull. Amer. Math. Soc. 83(1976)).

[La] W. Landherr: Äquivalenz Hermitescher Formen über einem beliebigen algebraischen Zahlkörper, Abh. Math. Sem. Univ. Hamburg 11(1935), 245-248.

[Le1] J. Levine: Knot cobordism in codimension 2, Comm. Math. Helv. 44(1969), 229-244.

[Le2] J. Levine: Invariants of knot cobordism, Inventiones Math. 8(1969), 98-110.

[MKS] W. Magnus, A. Karras, D. Solitar: Combinatorial group theory, (Interscience, New York, 1966)

[MH] J. Milnor, D. Husemoller: Symmetric bilinear forms, Ergeb. der Math. Nr. 73 (Springer, Berlin, Heidelberg, New York 1973)

[N1] W.D. Neumann: Signature-related invariants of manifolds, (mimeographed notes, Bonn, 1974)

[N2] W.D. Neumann: Signature of fiber bundles, (in preparation, see also [N1, ch. 2]).

[OM] O.T. O'Meara: Introduction to quadratic forms, Die Grundlehren d. Math. Wiss. Nr.117 (Berlin,Heidelberg, N.Y. 1973)

[S] J.P. Serre: Cours d'Arithmetique, (Presses Univ. de France, Paris, 1970).

[W1] C.T.C. Wall: Diffeomorphisms of 4-manifolds, J. London Math- Soc. 39(1964), 131-140.

[W2] C.T.C. Wall: Classification of hermitian forms: VI Group rings, Ann. of Math. 103(1976), 1-80.

[Wi] E. Witt: Theorie der quadratischen Formen in beliebigen Körpern, J. Reine und Angew. Math. 176(1937), 31-44.