Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 40 (1994)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: UNIMODULAR LATTICES WITH A COMPLETE ROOT SYSTEM
Autor: Kervaire, Michel
Kapitel: 3. The Witt class associated with a root system
DOI: https://doi.org/10.5169/seals-61105

The existence of a mere metabolizer for $(T(R), b)$, perhaps not admissible, is already a strong restriction on R. We study this condition in the next Section 3.

We give some necessary conditions for the existence of an admissible metabolizer using coding theory in Section 4.

In Section 6, after explaining the notations used in the tables, we list the even unimodular lattices with complete root systems in dimension 32.

3. The Witt class associated with a root system

Recall the Witt group $W(\mathbf{Q}/\mathbf{Z})$ of finite scalar product modules: If T and T' are two finite abelian groups with non-degenerate bilinear forms $b : T \times T \to \mathbf{Q}/\mathbf{Z}$, $b' : T' \times T' \to \mathbf{Q}/\mathbf{Z}$, then T and T' are said to be Witt equivalent if there exist finite scalar product modules H, H' each with a metabolizer $M = M^{\perp} \subset H$, $M' = M'^{\perp} \subset H'$ such that $T \boxplus H$ and $T' \boxplus H'$ are isometric. The Witt equivalence classes of finite scalar product modules form an abelian group $W(\mathbf{Q}/\mathbf{Z})$ under the operation induced by orthogonal direct sum $\boxplus$.

We recall below the explicit determination of $W(\mathbf{Q}/\mathbf{Z})$.

Let $R \subset \mathbf{Q}^n$ be a root system. As before, we denote by $T(R)$ the associated finite scalar product module. As a group, $T(R) = (\mathbf{Z}R)^{\#}/\mathbf{Z}R$, where

$$(\mathbf{Z}R)^{\#} = \{v \in \mathbf{Q}R = \mathbf{Q}^n : (v, R) \subset \mathbf{Z}\} .$$

The bilinear form $b : T(R) \times T(R) \to \mathbf{Q}/\mathbf{Z}$ is induced from the scalar product in $\mathbf{Q}^n$, restricted to $(\mathbf{Z}R)^{\#}$.

The Witt class of $(T(R), b)$ is an element of $W(\mathbf{Q}/\mathbf{Z})$ which we call the Witt class associated with the root system R and denote by $w(R) \in W(\mathbf{Q}/\mathbf{Z})$.

As we saw in Section 2, if R is the root system of a unimodular lattice $L \subset \mathbf{Q}^n$, and R is complete in L, i.e. $\mathbf{Q}R = \mathbf{Q}L = \mathbf{Q}^n$, then $(T(R), b)$ possesses a metabolizer and therefore $w(R)$ must be 0 in $W(\mathbf{Q}/\mathbf{Z})$.

If $R = R_1 \boxplus R_2$ is an orthogonal decomposition of the root system R, i.e. if R is the disjoint union $R_1 \sqcup R_2$ of two mutually orthogonal root systems R_1, R_2, then

$$w(R) = w(R_1) + w(R_2) .$$

Indeed,

$$(\mathbf{Z}R)^{\#} = (\mathbf{Z}R_1)^{\#} \boxplus (\mathbf{Z}R_2)^{\#} ,$$

and $T(R)$ is the direct product of the two subgroups $T(R_1)$ and $T(R_2)$ which are mutually orthogonal under the form b.

Now, any root system is an orthogonal sum of uniquely determined indecomposable root systems. It is therefore sufficient to calculate the Witt class associated with the indecomposable orthogonal summands.

As is well known, the list of indecomposable root systems (in which every root has scalar square 2) consists of the two infinite families $\mathbf{A}_l$, $l \geqslant 1$ and $\mathbf{D}_l$, $l \geqslant 4$ and of three exceptional systems $\mathbf{E}_6$, $\mathbf{E}_7$, $\mathbf{E}_8$. In each case the index indicates the rank, i.e. $dim_{\mathbf{Q}} \mathbf{Q}R$. (See [B].)

If the decomposition of the root system R contains a_i copies of the indecomposable system R_i, $i = 1, \ldots, r$, we write

$$R = a_1 R_1 \boxplus a_2 R_2 \boxplus \ldots \boxplus a_r R_r \, .$$

By the above, we have

$$w(R) = \textstyle\sum_{i=1}^{r} a_i w(R_i) \in W(\mathbf{Q}/\mathbf{Z}) \, ,$$

and $w(R) = 0$ *is a necessary condition for* R *to be the complete root system of a unimodular lattice.*

In order to evaluate $w(R)$ for a given root system R, we have to determine the Witt classes $w(\mathbf{A}_l)$, $w(\mathbf{D}_l)$ and $w(\mathbf{E}_l)$ in $W(\mathbf{Q}/\mathbf{Z})$ associated with the indecomposable root systems. This is the purpose of this section.

We first briefly recall the calculation of $W(\mathbf{Q}/\mathbf{Z})$. (See [Sch], p. 166-170 for more details.)

THEOREM. $W(\mathbf{Q}/\mathbf{Z}) = \oplus_{p \in P} W(\mathbf{F}_p)$, *where* $P = \{2, 3, 5, \ldots\}$ *is the set of prime numbers, and where* $W(\mathbf{F}_p)$ *is the Witt group of the finite field* $\mathbf{F}_p$.

$$W(\mathbf{F}_2) = \mathbf{Z}/2\mathbf{Z} \, ,$$

where the generator, denoted $\langle 1 \rangle$, *is represented by the finite group* $T = \mathbf{Z}/2\mathbf{Z}$ *endowed with the bilinear form* $b : T \times T \to \mathbf{Q}/\mathbf{Z}$ *determined by* $b(1, 1) = \frac{1}{2} \bmod \mathbf{Z}$.

For p *an odd prime, we have*

$$W(\mathbf{F}_p) = \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} \quad \textit{if} \quad p \equiv 1 \mod 4 \, .$$

The group $W(\mathbf{F}_p)$ *is generated in this case by the classes, denoted* $\langle 1 \rangle$ *and* $\langle \varepsilon \rangle$, *of* (T, b), (T', b'), *where as finite groups* $T = T' = \mathbf{F}_p$ *and* b, b' *are respectively determined by*

$$b(1, 1) = \tfrac{1}{p} \bmod \mathbf{Z} \, , \qquad b'(1, 1) = \tfrac{\varepsilon}{p} \bmod \mathbf{Z} \, ,$$

where $\varepsilon \in \mathbf{Z}$ *is a non-square* $\bmod p\mathbf{Z}$. *(The class of* b' *is of course independent of the choice of* ε.*)*

$$W(\mathbf{F}_p) = \mathbf{Z}/4\mathbf{Z} \quad \textit{if} \quad p \equiv -1 \mod 4 .$$

The group $W(\mathbf{F}_p)$ *is generated in this case by the class, denoted* $\langle 1 \rangle$, *of* (T, b), *where* $T = \mathbf{F}_p$ *and* b *is the bilinear form determined by*

$$b(1, 1) = \tfrac{1}{p} \mod \mathbf{Z} .$$

Proof. For every finite scalar product module (T, b), we have an obvious orthogonal sum decomposition

$$(T, b) = \boxplus_{p \in P(T)} (T_p, b_p) ,$$

where $P(T)$ is the set of primes dividing the order of T and T_p is the p-primary subgroup of T (consisting of the elements whose order is a power of p), and where b_p is the restriction of b to the subgroup T_p.

It follows that

$$W(\mathbf{Q}/\mathbf{Z}) = \oplus_{p \in P} W_p ,$$

where W_p is the Witt group of finite scalar product modules (T, b), where T is a p-group and $b: T \times T \to \mathbf{Z}\left[\frac{1}{p}\right]/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$ is a non-degenerate bilinear form.

The isomorphism $W_p = W(\mathbf{F}_p)$, where $W(\mathbf{F}_p)$ is the Witt group of the finite field $\mathbf{F}_p$ is a consequence of the following lemma: If (T, b) is a finite scalar product module and $U \subset T$ is a subgroup of T, let $U^\perp$ denote the orthogonal subgroup of U, i.e. $U^\perp = \{x \in T : b(x, U) = 0\}$.

LEMMA. *With these notations, suppose that* $U \subset T$ *is a self-orthogonal subgroup of* T, *i.e.* $U \subset U^\perp$. *Let* $T' = U^\perp/U$. *Then the form* b *induces on* T' *a non-degenerate bilinear form* $b' : T' \times T' \to \mathbf{Q}/\mathbf{Z}$ *and* (T, b), (T', b') *represent the same Witt class.*

Proof. Consider the scalar product module

$$(T, b) \boxplus (T', -b') = (T \oplus T', b \oplus (-b')) .$$

The subgroup $M = f(U^\perp)$, where $f: U^\perp \to T \oplus T'$ is given by $f(x) = (x, x')$, with x' the class of $x \in U^\perp$ modulo U, is a metabolizer.

It follows that $(T, b) \boxplus (T', -b') \sim \mathbf{O}$, where $\sim$ denotes Witt equivalence and $\mathbf{O}$ on the right hand side is the trivial scalar product module.

Hence,

$$(T, b) \boxplus (T', -b') \boxplus (T', b') \sim (T', b') .$$

Since $(T', -b') \boxplus (T', b') \sim \mathbf{O}$, the lemma follows. □

It is easy to see by induction on the order of T that this lemma implies $W_p = W(\mathbf{F}_p)$.

Finally, the asserted values of $W(\mathbf{F}_p)$ for the various primes p result from the classification of inner product spaces over finite fields. See for instance [MH, p. 87, Lemma 1.5]. □

In concrete examples, such as the scalar product module $(T(R), b)$ associated with a root system R, the above lemma enables us to find the Witt class $w(R) \in W(\mathbf{Q}/\mathbf{Z})$ by explicit calculation.

CASE $R = \mathbf{A}_l$.

Here,

$$\mathbf{ZA}_l = \{\sum_{i=0}^{l} x_i e_i : x_i \in \mathbf{Z},\ \sum_{i=0}^{l} x_i = 0\} \subset \mathbf{Q}^{l+1} \quad ,$$

where $e_0, e_1, \ldots, e_l$ is the standard basis of $\mathbf{Q}^{l+1}$, such that $(e_i, e_j) = \delta_{ij}$.

The root system proper $\mathbf{A}_l$ is the set $\{e_i - e_j : i \neq j\}$ of vectors in $\mathbf{ZA}_l$ with square length 2.

It is well known and easy to verify that the coset decomposition of $(\mathbf{ZA}_l)^{\#}$ modulo $\mathbf{ZA}_l$ reads

$$(\mathbf{ZA}_l)^{\#} = \bigsqcup_{r=0}^{l} (\mathbf{ZA}_l + x_r) \ ,$$

where

$$x_r = \tfrac{r}{l+1} \sum_{i=0}^{l-r} e_i - \tfrac{l-r+1}{l+1} \sum_{j=l-r+1}^{l} e_j \ .$$

Whenever the root system $\mathbf{A}_l$ has to be specified in the notation, we denote x_r by $x_r(\mathbf{A}_l)$.

The group $T(\mathbf{A}_l) = (\mathbf{ZA}_l)^{\#}/\mathbf{ZA}_l$ is cyclic of order $l+1$, generated by the class of x_1 modulo $\mathbf{ZA}_l$.

An easy calculation shows that

$$(x_r, x_r) = \tfrac{r(l-r+1)}{l+1} \ ,$$

and in fact, this number is the minimum of the scalar square of any vector in the class of x_r modulo $\mathbf{ZA}_l$. Thus $\mathbf{n}(x_r) = \frac{r(l-r+1)}{l+1}$ for $r = 0, 1, \ldots, l$, where $\mathbf{n}(x_r)$ is the norm of x_r, as defined in Section 2.

Let p be a prime and let e be the exponent of the largest power of p dividing $l+1$. Set $q = p^e$ and $s = (l+1)/q$, prime to p.

The p-primary subgroup T_p of $T(\mathbf{A}_l)$ is cyclic of order q generated by the class of x_s modulo $\mathbf{ZA}_l$. The scalar square of this element is

$$(x_s, x_s) = \tfrac{s(l-s+1)}{l+1} = -\tfrac{s}{q}\ mod\,\mathbf{Z}\ .$$

Thus we have to calculate the Witt class represented by a cyclic p-group with non-degenerate bilinear form.

Let T be the cyclic group $\mathbf{Z}/q\mathbf{Z}$, where $q = p^e$ is a power of the prime p. Let a be an integer prime to p and let

$$b : T \times T \to \mathbf{Z}\left[\tfrac{1}{p}\right]/\mathbf{Z}$$

be the bilinear form on T determined by

$$b(1, 1) = \tfrac{a}{q} \; mod\, \mathbf{Z} .$$

Then the Witt class of (T, b) in $W(\mathbf{F}_p)$ is given by

$$w(T, b) = \begin{cases} \langle a \rangle & \text{if } e \text{ is odd,} \\ 0 & \text{if } e \text{ is even,} \end{cases}$$

where $\langle a \rangle$ is the Witt class in $W(\mathbf{F}_p)$ of the form b on $\mathbf{F}_p$ given by $b(1, 1) = \frac{a}{p} \; mod\, \mathbf{Z}$.

Indeed, if e is even, $e = 2f$, then the subgroup generated by p^f in $\mathbf{Z}/q\mathbf{Z}$ is a metabolizer. If $e = 2f - 1$, let $U = p^f\mathbf{Z}/q\mathbf{Z}$ be the subgroup generated by p^f. Then, $U^{\perp} = p^{e-f}\mathbf{Z}/q\mathbf{Z} = p^{f-1}\mathbf{Z}/q\mathbf{Z}$. The quotient $T' = U^{\perp}/U$ with the induced form is isomorphic, as a scalar product module, to $\mathbf{F}_p$ with the form given by $(1, 1) = \frac{a}{p}$. By the lemma above, (T, b) and (T', b') belong to the same Witt class. The result follows.

Applying this to our example arising from the root system $\mathbf{A}_l$ with $T(\mathbf{A}_l) = \mathbf{Z}/(l + 1)\mathbf{Z}$, $q = p^e$ the exact power of p dividing $l + 1$ and $s = (l + 1)/q$, we get:

The p-component of the Witt class associated with $\mathbf{A}_l$ is

$$w_p(\mathbf{A}_l) = \begin{cases} \langle -s \rangle & \text{if } e = v_p(l + 1) \text{ is odd,} \\ 0 & \text{if } e = v_p(l + 1) \text{ is even,} \end{cases}$$

where $e = v_p(l + 1)$ is the exponent of the exact power of p dividing $l + 1$.

Note that for $p \equiv 1 \; mod\; 4$,

$$\langle -s \rangle = \langle s \rangle = \langle 1 \rangle, \text{ resp. } \langle \varepsilon \rangle$$

in $W(\mathbf{F}_p) = \mathbf{Z}/2\mathbf{Z}\langle 1 \rangle \oplus \mathbf{Z}/2\mathbf{Z}\langle \varepsilon \rangle$ depending on whether s is or is not a square $mod\, p$ respectively.

For $p \equiv -1 \; mod\; 4$, then

$$\langle -s \rangle = \langle 1 \rangle \text{ in } W(\mathbf{F}_p) = \mathbf{Z}/4\mathbf{Z}\langle 1 \rangle ,$$

if $-s$ is a square $mod\, p$, and

$$\langle -s \rangle = \langle -1 \rangle = -\langle 1 \rangle \text{ in } W(\mathbf{F}_p) = \mathbf{Z}/4\mathbf{Z}\langle 1 \rangle ,$$

if $-s$ is a non-square $mod\, p$.

CASE $R = \mathbf{D}_l$.

By definition

$$\mathbf{ZD}_l = \{ \textstyle\sum_{i=1}^{l} x_i e_i : x_i \in \mathbf{Z},\ \sum_{i=1}^{l} x_i \equiv 0 \ mod\, 2\mathbf{Z} \} .$$

It is easy to check that

$$(\mathbf{ZD}_l)^{\#} = \{ \textstyle\sum_{i=1}^{l} \xi_i e_i : \xi_i \in \frac{1}{2}\mathbf{Z},\ \xi_1 \equiv \xi_2 \equiv \ldots \equiv \xi_l \, mod\, \mathbf{Z} \} ,$$

and thus

$$T(\mathbf{D}_l) = (\mathbf{ZD}_l)^{\#}/\mathbf{ZD}_l = \begin{cases} \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z} & \text{if } l \text{ is even,} \\ \mathbf{Z}/4\mathbf{Z} & \text{if } l \text{ is odd.} \end{cases}$$

In this case, the associated finite scalar product module $T(\mathbf{D}_l)$ always represents 0 in the Witt group $W(\mathbf{Q}/\mathbf{Z})$.

The coset decomposition of $(\mathbf{ZD}_l)^{\#}$ modulo $\mathbf{ZD}_l$ is

$$(\mathbf{ZD}_l)^{\#} = \mathbf{ZD}_l \sqcup (\mathbf{ZD}_l + y_1) \sqcup (\mathbf{ZD}_l + y_2) \sqcup (\mathbf{ZD}_l + y_3) ,$$

with

$$\begin{aligned} y_1 &= \tfrac{1}{2} \textstyle\sum_{i=1}^{l} e_i , \\ y_2 &= e_l , \\ y_3 &= \tfrac{1}{2} (\textstyle\sum_{i=1}^{l-1} e_i - e_l) , \end{aligned}$$

and y_1, y_2, y_3 as above are of minimal square length in their class $mod\, \mathbf{ZD}_l$. Therefore, $\mathbf{n}(y_1) = \mathbf{n}(y_3) = \frac{l}{4}$ and $\mathbf{n}(y_2) = 1$.

When we need to include the root system in the notations, we write $x_k(\mathbf{D}_l)$ for y_k.

CASE $R = \mathbf{E}_6$.

Recall that

$$\mathbf{ZE}_6 = \{ \textstyle\sum_{i=1}^{8} x_i e_i : 2x_i \in \mathbf{Z},\ x_i - x_j \in \mathbf{Z},\ \sum_{i=1}^{6} x_i = x_7 + x_8 = 0 \} .$$

$$(\mathbf{ZE}_6)^{\#} = \mathbf{ZE}_6 \sqcup (\mathbf{ZE}_6 + z_1) \sqcup (\mathbf{ZE}_6 - z_1) ,$$

where

$$z_1 = \tfrac{1}{3} (e_1 + e_2 + e_3 + e_4 - 2(e_5 + e_6))$$

and $(z_1, z_1) = \frac{4}{3}$. Here again, z_1 has minimal square length in its class modulo $\mathbf{ZE}_6$ and hence $\mathbf{n}(z_1) = (z_1, z_1) = \frac{4}{3}$.

We write $x_1(\mathbf{E}_6)$ for z_1 when convenient.

The associated Witt class is

$$w(\mathbf{E}_6) = \langle 1 \rangle \quad \text{in} \quad W(\mathbf{F}_3) .$$

CASE $R = \mathbf{E}_7$.

The definition is

$$\mathbf{ZE}_7 = \{ \textstyle\sum_{i=1}^{8} x_i e_i : 2x_i \in \mathbf{Z},\ x_i - x_j \in \mathbf{Z},\ \sum_{i=1}^{8} x_i = 0 \} .$$

Here,

$$(\mathbf{ZE}_7)^{\#} = \mathbf{ZE}_7 \sqcup (\mathbf{ZE}_7 + z_1) ,$$

where

$$z_1 = \tfrac{1}{4} (e_1 + e_2 + e_3 + e_4 + e_5 + e_6 - 3(e_7 + e_8))$$

satisfies $(z_1, z_1) = \frac{3}{2}$ and is of minimal scalar square in its class $mod\, \mathbf{ZE}_7$.

Again, z_1 is noted $x_1(\mathbf{E}_7)$ if convenient.

The Witt class $w(\mathbf{E}_7)$ is the generator $\langle 1 \rangle$ of $W(\mathbf{F}_2) = \mathbf{Z}/2\mathbf{Z}$.

CASE $R = \mathbf{E}_8$.

Here, $T(\mathbf{E}_8) = 0$. The associated Witt class is 0.

4. WEIGHT ENUMERATORS OF FINITE SCALAR PRODUCT MODULES

Let T be a finite abelian group with a non-degenerate bilinear form $b: T \times T \to \mathbf{Q}/\mathbf{Z}$.

Suppose that we have a decomposition of T as an orthogonal direct sum of subgroups $T_1, \ldots, T_s$:

$$T = T_1 \boxplus T_2 \boxplus \ldots \boxplus T_s .$$

Then we can define the weight $x^{w(u)} \in \mathbf{Z}[x_1, \ldots, x_s]$ of an element $u \in T$ by tabulating its non-zero components in the decomposition $u = u_1 + u_2 + \ldots + u_s$, $u_i \in T_i$, as

$$x^{w(u)} = x_1^{w(u_1)} \cdot x_2^{w(u_2)} \cdot \ldots \cdot x_s^{w(u_s)} ,$$

where

$$w(u_i) = \begin{cases} 0 & \text{if } u_i = 0, \\ 1 & \text{if } u_i \neq 0 . \end{cases}$$