The Zassenhaus Decomposition for the Orthogonal Group: Properties and Applications

Alexander Hahn[1]

Received: May 29, 2001

Communicated by Ulf Rehmann

Abstract. Zassenhaus [17] constructed a decomposition for any element in the orthogonal group of a non-degenerate quadratic space over a field of characteristic not 2 and used it to provide an alternative description of the spinor norm. This decomposition played a central role in the study of question of the length of an element in the commutator subgroup of the orthogonal group with respect to the generating set of all elementary commutators of hyperplane reflections. See Hahn [6]. The current article develops the fundamental properties of the Zassenhaus decomposition, e.g., those of uniqueness and conjugacy, and applies them to sharpen and expand the analysis of [6].

2000 Mathematics Subject Classification: 20G15, 20G25, 20F05.

1. Introduction. We begin with a discussion of the length question just mentioned. For the moment, consider any group G along with a set of generators A (not containing the identity element of G) that satisfies $A^{-1} = A$. Of all the factorizations of an element $\sigma \in G$ as a product of elements from A choose one that involves the smallest number of factors. This smallest number is defined to be the length $\ell(\sigma)$ of σ. One very basic question - necessarily in the context of specific examples - is this: are there parameters attached to σ from which $\ell(\sigma)$ can be read off?

A number of theorems have responded to this question. For G a Weyl group - or more generally a Coxeter group - and A an appropriate set of hyperplane reflections, see Humphreys [7]. Refer to Dyer [3] for a recent result in this

[1]The author wishes to thank the algebraists of Louisiana State University for their splendid organization of *Quadratic Forms 2001* and their warm hospitality throughout the conference.

context. For G a classical group and A a set of canonical elements coming from the underlying geometry, see Hahn-O'Meara [5] for a comprehensive treatment of the theorems of Dieudonné, Wall, and others. For G a classical group and A a set of generators coming from a single conjugacy class of elements, see Ellers-Malzan [2] and Knüppel [10]. In a related direction, interesting codes have been constructed starting with $G = SL_2(\mathbb{Z})$ and carefully selected A. See Margulis [12, 13] and Rosenthal-Vontobel [16] for details. The connection with the length problem is provided by the associated Cayley graph and its diameter.

Example 1. Let G be the symmetric group on $\{1, \dots, n\}$ and let A be the set of transpositions. Let $k(\sigma)$ be the the number of cycles of σ including the trivial cycles. Then $\ell(\sigma) = n - k(\sigma)$.

The fact that $\ell(\sigma) \leq n - k(\sigma)$ follows from the decomposition of σ into its disjoint cycles. The other inequality is a consequence of the fact that $k(\sigma\tau) = k(\sigma) \pm 1$ for any transposition τ. A similar (but more complicated) argument provides

Example 2. Let G be the alternating group on $\{1, \dots, n\}$ and let A be the set of three cycles, or equivalently, the set of elementary commutators of transpositions. This time, let $k(\sigma)$ be the number of cycles of odd cardinality again including the trivial cycles. Then $n - k(\sigma)$ is even and $\ell(\sigma) = \frac{1}{2}(n - k(\sigma))$.

We now turn to the orthogonal group and begin by recalling some of the basics. For the details, see [5], especially Sections 5.2A, 5.2B, Chapter 6 (all specialized to the orthogonal case $\Lambda = 0$) and Section 8.2A.

Let V be a non-zero, non-degenerate, $n-$dimensional quadratic space with symmetric bilinear form B over a field F with char$(F) \neq 2$. Denote $B(x,x)$ by $Q(x)$ and $\frac{1}{2}Q(x)$ by $q(x)$. Check that $B(x,y) = q(x+y) - q(x) - q(y)$. Two vectors x and y are *orthogonal* if $B(x,y) = 0$. A non-zero vector x in V that is orthogonal to itself is *isotropic* and it is *anisotropic* otherwise. A non-degenerate plane that contains isotropic vectors is a *hyperbolic plane* and an orthogonal sum of hyperbolic planes is a *hyperbolic space*. If U and W are orthogonal subspaces that intersect trivially, then $U \oplus W$ is denoted $U \perp W$. The orthogonal complement of a subspace U of V is denoted by $U^{\perp}$, and the radical of U is defined by Rad $U = U \cap U^{\perp}$. If W is a complement of Rad U in U, then W is non-degenerate and $U =$ Rad $U \perp W$ is a *radical splitting* of U. Any two such complements of Rad U are isometric.

Let $O_n(V)$ be the orthogonal group of V. For $\sigma \in O_n(V)$, let S be the subspace $S = (\sigma - 1_V)V$ of V. This S is the *space* of σ. Intuitively, this is where the "action" of σ is. In particular, there is no action on the orthogonal complement $S^{\perp}$ of S; the fact is that $S^{\perp} = \{x \in V \mid \sigma(x) = x\}$. Clearly, $\sigma = 1_V$ if and only if $S = 0$. It turns out that dim S is even if and only if $\sigma \in O_n^+(V)$, the subgroup of $O_n(V)$ consisting of the elements of determinant 1. If $\eta \in O_n(V)$ commutes with σ, then $\eta S = S$. We will "transfer" properties of S to σ. For example, σ is *non-degenerate*, *degenerate*, or *totally degenerate*, if S is non-degenerate, degenerate, or totally degenerate, that is, if the radical $\operatorname{Rad} S$ of S is, respectively, zero, non-zero, or S. In the same way, σ is *anisotropic* if S is anisotropic.

An element $\sigma \in O_n(V)$ is an involution if $\sigma^2 = 1$. It is easy to see that σ is an involution if and only if $\sigma_{|S} = -1_S$. In particular, involutions have the form $\sigma = -1_S \perp 1_{S^\perp}$ and are non-degenerate. Let v be an anisotropic vector and define τ_v in $O_n(V)$ by

$$\tau_v(x) = x - B(x, v)q(v)^{-1}v \quad \text{for all} \quad x \in V \ .$$

Check that the space of τ_v is Fv and that $\tau_{v|_{Fv}} = -1_{Fv}$. So τ_v is an involution. These involutions are the *hyperplane reflections* or *symmetries*.

THEOREM 1. (Cartan-Scherk-Dieudonné) Let G be the group $O_n(V)$ and let A be the set of hyperplane reflections. If σ is not totally degenerate, then $\ell(\sigma) = \dim S$. If σ is totally degenerate, then $\ell(\sigma) = \dim S + 2$.

Theorem 1 in combination with Examples 1 and 2 calls attention to the length problem in the situation where G is the commutator subgroup $\Omega_n(V)$ of $O_n(V)$ and A the set of elementary commutators of symmetries. It seems surprising that this question did not receive scrutiny until recently. John Hsia first called attention to it in the case of a non-dyadic local field and it was solved in this context in Hahn [6]. The answer is not simply a modification of the conclusion of Theorem 1, as a comparison of Examples 1 and 2 might suggest. We will see that, unlike Theorem 1, it depends critically on the arithmetic of the field F.

2. THE ZASSENHAUS DECOMPOSITION. An element σ in $O_n(V)$ is *unipotent* if its minimal polynomial has the form $(X - 1)^m$ for some positive integer m. A non-trivial unipotent element is degenerate and can, therefore, exist only if V is isotropic. The elements with minimal polynomial $(X - 1)^2$ are precisely the non-trivial totally degenerate elements. A degenerate element σ with dim $S = 2$ is an *Eichler* transformation. Let S be a degenerate plane and put $S = Fu \perp Fv$ with $u \in \operatorname{Rad} S$ and $v \in S$. Define $\Sigma_{u,v} \in O_n(V)$ by

$$\Sigma_{u,v}(x) = x + B(x, v)u - B(x, u)v - q(v)B(x, u)u \quad \text{for all} \quad x \in V \,.$$

Then $\Sigma_{u,v}$ is an Eichler transformation and all Eichler transformations have this form. A totally degenerate Eichler transformation has minimal polynomial $(X-1)^2$ and one that is not totally degenerate has minimal polynomial $(X-1)^3$. In particular, all Eichler transformations are unipotent.

Let σ be any element in $O_n(V)$. Consider the subspace

$$X = \{x \in V \mid (\sigma - 1_V)^j x = 0 \ \text{ some } \ j\}$$

of V. This unique largest space on which σ acts as a unipotent transformation turns out to be non-degenerate. Let $R = X^{\perp}$. Then R is non-degenerate and $X = R^{\perp}$. Notice that $\sigma R^{\perp} = R^{\perp}$. So $\sigma R = R$ and hence $\sigma = \sigma_{|_{R^\perp}} \perp \sigma_{|_R}$. Put $\mu = \sigma_{|_{R^\perp}} \perp 1_R$ and $\rho = 1_{R^\perp} \perp \sigma_{|_R}$. Then

$$\sigma = \mu \cdot \rho$$

with μ unipotent and ρ non-degenerate with space R. This is the *Zassenhaus decomposition or splitting* of σ. Note that μ and ρ commute.

To develop the essential properties of the Zassenhaus splitting, we need the *Wall* form. Let $\sigma \in O_n(V)$. Define

$$(\ ,\ )_\sigma : S \times S \longrightarrow F$$

by the equation $(\sigma x - x, \sigma y - y)_\sigma = B(\sigma x - x, y)$ for all $\sigma x - x$ and $\sigma y - y$ in S. This is the *Wall form* on S. It is non-degenerate and bilinear, but it is almost never symmetric. In fact, $(\ ,\ )_\sigma$ is symmetric if and only if σ is an involution, and in this case, $(s, s')_\sigma = -\frac{1}{2}B(s, s')$ for all s, s' in S. Also, $(\ ,\ )_\sigma$ is alternating if and only if σ is totally degenerate.

The space S is now equipped with both the Wall form $(\ ,\ )_\sigma$ and the restriction of B. When the focus is on $(\ ,\ )_\sigma$, then S is denoted by S_σ. Similarly, the space S_1 of σ_1 in $O_n(V)$ is written S_{σ_1} when $(\ ,\ )_{\sigma_1}$ is under consideration, and analogously for σ_2. The spaces of orthogonal transformations μ, ρ, μ', ρ' and so on, will be denoted by U, R, U', R' and so on, with appropriate subscripts when the focus is on the Wall form.

The key facts are these. Let S_1 be a non-degenerate subspace of S_σ. Then there is a unique $\sigma_1 \in O_n(V)$ - the transformation belonging to S_1 - such that $S_{\sigma_1} = S_1$. Let S_2 be the right complement of S_1 in S_σ. Then S_2 is non-degenerate. If σ_2 is the transformation belonging to S_2, then $\sigma = \sigma_1\sigma_2$. Conversely, if $\sigma = \sigma_1\sigma_2$ with $S_1 \cap S_2 = 0$, then $S_\sigma = S_{\sigma_1} \perp S_{\sigma_2}$. This means that the Wall forms of both S_{σ_1} and S_{σ_2} are obtained by restricting the Wall form $(\ ,\ )_\sigma$ and that $(s_1, s_2)_\sigma = 0$ for all $s_1 \in S_1$ and $s_2 \in S_2$ (but it is not required that $(s_2, s_1)_\sigma = 0$). For example, if $\sigma = \mu\rho$ is the Zassenhaus splitting of σ, then because μ and ρ commute,

$$S_\sigma = U_\mu \perp R_\rho = R_\rho \perp U_\mu \,.$$

Another important fact asserts that elements σ and σ_1 in $O_n(V)$ are conjugate in $O_n(V)$ if and only if the spaces S_σ and S_{σ_1} are isometric.

To conclude this discussion of the Wall form, we note that the map

$$\Theta : O_n^+(V) \ \longrightarrow \ \overset{*}{F}/\overset{*}{F}{}^2$$

defined by $\Theta(\sigma) = (\text{disc } S_\sigma)\overset{*}{F}{}^2$, where disc S_σ is the discriminant of the space S_σ, provides one of the (equivalent) definitions of the spinor norm. Its kernel is denoted by $O'_n(V)$. All unipotent elements are in $O'_n(V)$. It is clear that $O'_n(V) \supseteq \Omega_n(V)$ and it is a standard fact that if V is isotropic, then $O'_n(V) = \Omega_n(V)$. A formula useful for computations is

$$\Theta(\sigma) = \Theta(\rho) = \det\, (\rho - 1_V)_{|_R}\ \text{disc } R\,,$$

where ρ is the non-degenerate component of the Zassenhaus decomposition of σ and disc $R \in \overset{*}{F}/\overset{*}{F}{}^2$ is the discriminant of the space R relative to the form B.

Proposition 1. Let $\sigma = \mu\rho$ be the Zassenhaus splitting of an element $\sigma \in O_n(V)$. Then $S = U \perp R$, and

i) σ is in $\Omega_n(V)$ if and only if both μ and ρ are in $\Omega_n(V)$.

ii) An element in $O_n(V)$ commutes with σ if and only if it commutes with both μ and ρ.

Proof: Recall that $O_n(V)$ has non-trivial unipotent elements only if V is isotropic. So any non-trivial unipotent element of $O_n(V)$ is in $O'_n(V) = \Omega_n(V)$. This implies (i). As to (ii), observe that if $\eta \in O_n(V)$ commutes with σ, then η stabilizes $X = R^\perp$. So $\eta = \eta_{|_{R^\perp}} \perp \eta_{|_R}$ and it follows that η commutes with both μ and ρ. QED.

We next consider the question of the uniqueness of the Zassenhaus splitting. It is not difficult to construct situations of the following sort: a non-degenerate element σ and a non-trivial unipotent element μ_0 with $U_0 \subseteq S$ such that μ_0 commutes with σ and the space of $\rho_0 = \mu_0^{-1}\sigma$ is S. In such a situation, $\sigma = 1_V\sigma = \mu_0\rho_0$ are two different ways of writing σ as a commuting product of a unipotent element and a non-degenerate element. We will see that such situations are in essence the only obstruction to the uniqueness of the Zassenhaus splitting.

Let $\sigma = \mu\rho$ be the Zassenhaus splitting of $\sigma \in O_n(V)$. Suppose that $\sigma = \mu'\rho'$ is any factorization of σ with μ' unipotent, ρ' non-degenerate, and such that μ' and ρ' commute.

Denote by W the orthogonal complement $W = R'^{\perp}$ of the space R' of ρ'. By an application of Proposition 1 (ii), the elements μ, μ', ρ, and ρ' all commute with each other. In particular, σ commutes with ρ'. So $\sigma R' = R'$ and hence $\sigma W = W$. Therefore, $\sigma = \sigma_{|_W} \perp \sigma_{|_{R'}}$. The fact that $\rho'_{|_W} = 1_W$, tells us that $\sigma_{|_W} = \mu'_{|_W}$. So σ is unipotent on W and hence $W \subseteq R^\perp$. Therefore, $R' = W^\perp \supseteq R$. Let T be the orthogonal complement of R in R'. Because R'

and R are both non-degenerate, $R' = T \perp R$ with T non-degenerate. Because $R^\perp$ is the largest space on which σ is unipotent, T is the largest space on which $\sigma_{|_{R'}}$ is unipotent. So

$$\sigma_{|_{R'}} = (\mu_{|_T} \perp 1_R)(1_T \perp \rho_{|_R})$$

is the Zassenhaus splitting of $\sigma_{|_{R'}}$. Notice that $1_T \perp \rho_{|_R} = \rho_{|_{R'}}$ and hence that $\mu_{|_T} \perp 1_R = \mu_{|_{R'}}$. Since μ' and ρ' commute with with both ρ' and ρ, it follows that μ' and ρ' stabilize the spaces R', R, and therefore T. So

$$\mu_{|_T} = \sigma_{|_T} = (\mu'_{|_T})(\rho'_{|_T}) \ .$$

Therefore, $\rho'_{|_T}$ is a product of two commuting unipotent transformations. So $\rho'_{|_T}$ is unipotent. If T where to be non-zero, then ρ' would fix a non-zero vector in T. But this is impossible, because ρ' is non-degenerate with space R'. So $T = 0$. Hence $R' = R$ and $W = R^\perp$. This means that $\mu'_{|_{R^\perp}} = \sigma_{|_{R^\perp}} = \mu_{|_{R^\perp}}$ and hence that $\mu' = \mu_{|_{R^\perp}} \perp \mu'_{|_R}$. Because $\mu'_{|_R} \cdot \rho'_{|_R} = \sigma_{|_R} = \rho_{|_R}$, it follows that $\rho' = 1_{R^\perp} \perp (\mu'_{|_R})^{-1}(\rho_{|_R})$. Therefore the obstruction to the uniqueness of the Zassenhaus splitting is as described earlier.

Notice that $U' \cap R' = U' \cap R = 0$ if and only if $\mu'_{|_R} = 1_R$. In this case, $\mu' = \mu$ and $\rho' = \rho$. If R is anisotropic, then $O_r(R)$ has no non-trivial unipotent elements, and this condition is met. The following uniqueness criterion is a special case of our discussion.

PROPOSITION 2. (Uniqueness) Let $\sigma = \mu\rho$ be the Zassenhaus splitting of $\sigma \in O_n(V)$. Suppose that $\sigma = \mu'\rho'$ where μ' is unipotent, ρ' non-degenerate, and $S = U' \perp R'$. Then

$$\mu' = \mu \ \text{ and } \ \rho' = \rho \ .$$

PROPOSITION 3. (Conjugacy) Let σ and σ_1 be elements in $O_n(V)$ and let $\sigma = \mu\rho$ and $\sigma_1 = \mu_1\rho_1$ be their Zassenhaus splittings. Then σ_1 is conjugate to σ if and only if μ_1 is conjugate to μ and ρ_1 is conjugate to ρ.

PROOF: If σ_1 is conjugate to σ then by an application of Proposition 2, μ_1 is conjugate to μ and ρ_1 is conjugate to ρ. As to the converse, observe first that $S_\sigma = U_\mu \perp R_\rho = R_\rho \perp U_\mu$ and similarly for S_{σ_1}. If μ_1 is conjugate to μ and ρ_1 is conjugate to ρ, then U_{μ_1} is isometric to U_μ and R_{ρ_1} is isometric to R_ρ. Therefore S_{σ_1} is isometric to S_σ, and hence σ_1 is conjugate to σ. QED.

3. APPLICATION TO THE LENGTH PROBLEM. Our study of the length problem for the group $\Omega_n(V)$ and its set of generators

$$A = \{\tau_v\tau_w\tau_v\tau_w | \tau_v \text{ and } \tau_w \text{ non-commuting hyperplane reflections in } O_n(V)\}$$

will expand on the results of Hahn [6].

Let $\sigma \in \Omega_n(V)$ be arbitrary. Note that the typical element $\tau_v\tau_w\tau_v\tau_w$ in A is equal to $\tau_v\tau_{\tau_w(v)} = \tau_v\tau_{v'}$ where $Fv \neq Fv'$ and $Q(v) = Q(v')$. Conversely, any such product is an element in A. It is a direct consequence of this fact and Theorem 1, that

$$\ell(\sigma) \geq \frac{1}{2} \dim S.$$

We will therefore define $\sigma \in \Omega_n(V)$ to be *short* if $\ell(\sigma) = \frac{1}{2} \dim S$ and *long* if $\ell(\sigma) > \frac{1}{2} \dim S$.

Our goal is the same as that of Theorem 1, namely the complete description of the long elements of $\Omega_n(V)$ and the determination of their lengths.

Let σ in $\Omega_n(V)$ be an involution. By an application of the Wall form, σ is short if and only if $S = W_1 \perp \cdots \perp W_k$ with $\dim W_i = 2$ and $\operatorname{disc} W_i = 1$. Totally degenerate elements are in $\Omega_n(V)$. It follows from Theorem 1 that they are long. We now focus on the elements in $\Omega_n(V)$ that are neither involutions nor totally degenerate.

Theorem 2. Let $\sigma \in \Omega_n(V)$ be long with σ neither totally degenerate nor an involution. Let $\sigma = \mu\rho$ be the Zassenhaus splitting of σ. Then

i) The space of μ satisfies $U = \operatorname{Rad} U \perp T$ with T anisotropic. The element μ is a product of $\frac{1}{2}(\dim U)$ commuting Eichler transformations, exactly $\dim T$ of which are not totally degenerate. In particular, $(\mu - 1_V)^3 = 0$.

ii) The element ρ is long and its space R is anisotropic.

iii) (Splicing Condition) The space $T \perp R$ is anisotropic.

Finally, if V is isotropic, then $\ell(\sigma) = \frac{1}{2} \dim S + 1$.

Proof: In view of Hahn [6] and in particular Proposition 15, only the existence of the factorization in (i) requires proof. By the same proposition, we know that $(\mu - 1_V)U \subseteq \operatorname{Rad} U$. If $T = 0$, then μ is totally degenerate. By Hahn-O'Meara [5], μ is a product of $\frac{1}{2}(\dim U)$ totally degenerate commuting Eichler transformations. So we may assume that $T \neq 0$. Let $w_1 \in T$ be non-zero. If $\mu w_1 = w_1$, then w_1 is in the fixed space $U^\perp$ of μ. But this implies that $w_1 \in U \cap U^\perp = \operatorname{Rad} U$, a contradiction. So $\mu w_1 - w_1$ is a non-zero vector in $\operatorname{Rad} U$. Put $\mu w_1 = u_1 + w_1$ with $u_1 \in \operatorname{Rad} U$. Note that $\mu(Fu_1 \perp Fw_1) = Fu_1 \perp Fw_1$ and (because μ is unipotent) that the restriction of μ to this plane has determinant 1. Let $\alpha_1 = B(w_1, w_1)^{-1}$ and consider the Eichler transformation $\Sigma_{u_1,\alpha_1 w_1}$. Check that $\Sigma_{u_1,\alpha_1 w_1}(u_1) = u_1$ and $\Sigma_{u_1,\alpha_1 w_1}(w_1) =$

$w_1 + u_1$. Observe that $\mu\Sigma^{-1}_{u_1,\alpha_1 w_1}\big|_{(Fu_1 \perp Fw_1)} = 1_{(Fu_1 \perp Fw_1)}$. By 8.2.16 of [5], μ commutes with $\Sigma^{-1}_{u_1,\alpha_1 w_1}$. Put $\mu_1 = \Sigma^{-1}_{u_1,\alpha_1 w_1}\mu$. By general facts, $U_1 \subseteq (Fu_1 \perp Fw_1) + U \subseteq U$. Because μ_1 fixes w_1 while μ does not, the fixed space $U_1^\perp$ of μ_1 strictly contains the fixed space $U^\perp$ of μ. It follows that $\dim U_1 = \dim U - 2$. Because $\mu = \Sigma_{u_1,\alpha_1 w_1} \cdot \mu_1$, $U \subseteq (Fu_1 \perp Fw_1) + U_1$. By dimensions, $U = (Fu_1 \perp Fw_1) \oplus U_1$. Since $\Sigma_{u_1,\alpha_1 w_1}$ commutes with μ, it commmutes with μ_1. Therefore, $U = (Fu_1 \perp Fw_1) \perp U_1$. Note that $\mathrm{Rad}\ U = Fu_1 \perp \mathrm{Rad}\ U_1$. Put $U_1 = \mathrm{Rad}\ U_1 \perp T_1$. Because

$$U = (Fu_1 \perp \mathrm{Rad}\ U_1) \perp (Fw_1 \perp T_1)$$

is a radical splitting of U we know that $Fw_1 \perp T_1$ is isometric to T and hence that T_1 is anisotropic. The element μ_1 is unipotent because it is a product of two commuting unipotent elements. An induction completes the proof. QED.

REMARK: By dimension considerations, the spaces of the Eichler transformations in Theorem 2 (i) are planes with trivial intersection. Because these Eichler transformations commute, these planes are orthogonal. Observe also that $\frac{1}{2}\dim U \geq \dim T$, and hence that $\dim \mathrm{Rad}\ U \geq \dim T$.

The next two results will show that the limitations that Theorem 2 imposes on the components μ and ρ of the Zassenhaus splitting of a long element σ are considerable.

Let $p(X) = a_k X^k + \cdots + a_1 X + a_0$ be a polynomial in $F[X]$. We call $p(X)$ *symmetric* if the two sequences of coefficients $a_k, \ldots, a_0$ and $a_0, \ldots, a_k$ are identical.

THEOREM 3. Let $\sigma \in \Omega_n(V)$ be long. Then the prime decomposition of the minimal polynomial of σ has the form

$$(X-1)^m\, p_1(X) \ \cdots \ p_j(X)$$

where $0 \leq m \leq 3$ and the $p_i(X)$ are distinct, monic, symmetric, and irreducible.

PROOF: If σ is an involution or totally degenerate, this is clear. So assume that Theorem 2 applies to σ. Consider $\rho_{|_R}$. Because R is anisotropic, any non-zero subspace W of R is non-degenerate. It follows that $R = W_1 \perp \cdots \perp W_j$ where each W_i is invariant under ρ, but $\rho_{|_{W_i}}$ has no non-trivial invariant subspaces. By applying the results of Huppert, e.g., Satz 2.4 of [8] and Satz 4.1 of [9], (also see the references to Cikunov in Milnor [14]), we see that the minimal polynomial of $\rho_{|_{W_i}}$ is symmetric and irreducible. QED.

PROPOSITION 4. Let i be the Witt index of V. Let $\sigma \in \Omega_n(V)$ be a unipotent element with minimal polynomial $(X-1)^m$.

i) If V is hyperbolic, then $m \leq 2i - 1$.

ii) If V is not hyperbolic, then $m \leq 2i + 1$.

In either case, there exist unipotent elements such that equality holds.

Proof: The inequalities follow by induction on i. The case $i = 0$ is the anisotropic case, where we already know that 1_V is the only unipotent element. So assume that $i \geq 1$. Now refer to case (2) of the proof of Theorem 2.4 of [4] and in particular to the unipotent element $\tau = \sigma_Y \in \Omega_{n-2}(X)$. Let k be the degree of the minimal polynomial of τ. Notice that $V = Z \perp X$ with Z a hyperbolic plane. So the Witt index of X is $i - 1$. Applying the induction hypothesis to τ, provides the inequality $k \leq 2(i-1) - 1 = 2i - 3$ if X is hyperbolic and $k \leq 2(i-1) + 1 = 2i - 1$ if not. It follows from the way σ and τ are related that $m \leq k + 2$. This completes the proof of the inequalities.
The construction of the required elements also follows inductively. If V is a hyperbolic plane, then 1_V is the only unipotent element and it satisfies the equality trivially. Note next that a hyperbolic space of Witt index i contains a non-degenerate space of Witt index $i - 1$ that is not hyperbolic. This implies that it suffices to carry out the construction of the required unipotent element in case (ii). So suppose that V is not hyperbolic with Witt index i. To get the induction off the ground, take $i = 1$. Let $\sigma = \Sigma_{u,v}$ be a non-degenerate Eichler transformation. Then $m = 3 = 2i + 1$ as required. It is also easy to check that $(\sigma - 1_V)^2 V = Fu$. Because V is spanned by isotropic vectors, there is an isotropic vector w in V such that $(\sigma - 1_V)^2 w = u$. Because $i = 1$, it follows that $B(\sigma(\sigma - 1_V)^2 w, w) = B(u, w) \neq 0$.
Suppose that $i \geq 2$ and let $V = H \perp W$ with H a hyperbolic plane. Note that W is not hyperbolic and that it has Witt index $i - 1$. For the induction hypothesis, assume that τ is a unipotent element in $\Omega_{n-2}(W)$ and that the minimal polynomial of τ is $(X-1)^k$ with $k = 2(i-1) + 1 = 2i - 1$. Assume further that $(\tau - 1_W)^{k-1} W$ is a line spanned by $(\tau - 1_W)^{k-1} w$ with w isotropic and $B(\tau(\tau - 1)^{k-1} w, w) \neq 0$. Put $H = Fu \oplus Fv$ with u and v isotropic and $B(u, v) = 1$. To complete the proof, we will show that $\sigma = \Sigma_{u,w} \cdot (1_H \perp \tau)$ is a unipotent element in $\Omega_n(V)$ that satisfies all the properties of τ with $k + 2$ in place of k. ¿From the defining equation of $\Sigma_{u,w}$ we see that $\sigma u - u = 0, \sigma v - v = w$, and that

$$\sigma x - x = \tau x - x + B(\tau x, w)u \quad \text{for all } x \in W\,.$$

This formula and an induction shows that

$$(\sigma - 1_V)^j x = (\tau - 1_W)^j x + B(\tau(\tau - 1_W)^{j-1} x, w)u \quad \text{for all} \quad x \in W \text{ and } j \geq 1\,.$$

We claim that σ has minimal polynomial $(X-1)^{k+2}$, that $(\sigma - 1_V)^{k+1} V$ is spanned by $(\sigma - 1_V)^{k+1} v$, and that $B(\sigma(\sigma - 1_V)^{k+1} v, v) \neq 0$. To see this, observe first that $(\sigma - 1_V)^{k+1} x = 0$ for all $x \in W$. Because $(\sigma - 1_V)u = 0$, it follows that $(\sigma - 1_V)^{k+1}V$ is spanned by $(\sigma - 1_V)^{k+1}v$. Recall that $(\sigma - 1_V)v = w$. Therefore,

$$\begin{aligned}(\sigma - 1_V)^{k+1}v &= (\sigma - 1_V)^k w \\ &= (\tau - 1_W)^k w + B(\tau(\tau - 1_W)^{k-1}w, w)u \\ &= B(\tau(\tau - 1_W)^{k-1}w, w)u \neq 0\ .\end{aligned}$$

Because $\sigma u = u$, we see that $(\sigma - 1_V)^{k+2}v = 0$ and hence that σ has minimal polynomial $(X - 1)^{k+2}$. Finally, $B(\sigma(\sigma - 1_V)^{k+1}v, v) = B(B(\tau(\tau - 1_W)^{k-1}w, w)u, v) = B(\tau(\tau - 1_W)^{k-1}w, w)B(u, v) \neq 0$. The proof is complete. QED.

The elements of Theorem 2 can be constructed as follows: Start with a long anisotropic ρ in $\Omega_n(V)$. Choose a subspace $U = \text{Rad } U \perp T$ in $R^\perp$ such that $T \perp R$ is anisotropic and $\dim \text{Rad } U \geq \dim T$. Split U into an orthogonal sum of degenerate planes. For each plane choose an Eichler transformation that has the plane as its space. Let μ be the product of these Eichler transformations and set $\sigma = \mu\rho$. This - by its uniqueness property - is the Zassenhaus decomposition of σ. Therefore, the description of the long elements of $\Omega_n(V)$ has been reduced to the following two problems:

A. Classify all long anisotropic elements ρ in $\Omega_n(V)$ and compute their lengths in the case of an anisotropic V.

B. Determine which of the elements in Theorem 2 are actually long.

Notice that the conjugates of a long element in $\Omega_n(V)$ are long elements of $\Omega_n(V)$. If the long element is anisotropic, then the conjugates are also anisotropic. Thus, the problem of classifying long elements calls for the classification of their conjugacy classes.

4. Local Fields. The study of the arithmetic theory of quadratic forms flows classically via the progression

$$\mathbb{C},\ \mathbb{R},\ \text{finite fields},\ \text{local fields},\ \text{and global fields}$$

from the easy situations to the hard ones. The theory over local fields makes use of that over finite fields (via the residue class field) and the theory over global fields - in characteristic zero these are the finite extensions of $\mathbb{Q}$ - is based via local/global principles on the theory over local fields and $\mathbb{C}$ and $\mathbb{R}$.

The benefit of hindsight, namely that the length problem that is being considered depends on the arithmetic of the field, suggests that its analysis should proceed along the same path. Theorem 4 below is a routine application of

Theorem 1. See Hahn [6] for the details. Observe that it applies at once to $\mathbb{C}$, $\mathbb{R}$, and finite fields.

Theorem 4. Suppose that $\operatorname{card} \overset{*}{F}/\overset{*}{F}{}^2 \leq 2$. Then the totally degenerate elements σ are the only long elements in $\Omega_n(V)$, and for these $\ell(\sigma) = \frac{1}{2}\dim\ S + 1$.

Let's turn next to the case of a local field. $\mathbb{R}^+$ be the set of positive real numbers. A *local field* is a field F that has a valuation

$$|\ \ | : F \longrightarrow \mathbb{R}^+ \cup \{0\}$$

which satisfies the strong triangle inequality and with respect to which $|\overset{*}{F}|$ is discrete and F is complete. Let

$$\mathfrak{o}\ = \{\alpha \in F \mid |\alpha| \leq 1\}$$

be the *valuation ring* of F and $\mathfrak{p} = \{\alpha \in F \mid |\alpha| < 1\}$ its unique maximal ideal. As part of the definition of local field, the *residue class field* $\mathfrak{o}/\mathfrak{p}$ is assumed to be finite. We continue the assumption that char $F \neq 2$. Denote by $\mathfrak{u} = \{\varepsilon \in \mathfrak{o} \mid |\varepsilon| = 1\}$ the group of invertible elements of $\mathfrak{o}$. Because the maximal ideal $\mathfrak{p}$ is principal, $\mathfrak{p} = \mathfrak{o}\pi$ for some $\pi \in \mathfrak{o}$. Any such π is a *prime* element in $\mathfrak{o}$. Note that $|\pi|$ is the largest value such that $|\pi| < 1$.

We refer to O'Meara [15] for the notation and the basic properties of local fields, their quadratic forms and orthogonal groups. Two important facts about quadratic forms over local fields are these: any non-degenerate quadratic space of dimension five or more is isotropic, and there is, up to isometry, a unique anisotropic four dimensional quadratic space.

It will be necessary to distinguish non-dyadic local fields from dyadic local fields. The local field F is *non-dyadic* if 2 is invertible in $\mathfrak{o}$ and *dyadic* if not. So F is non-dyadic if $|2| = 1$ and dyadic if $|2| < 1$. If V is the unique 4-dimensional anisotropic quadratic space, then $\Omega_4(V)$ has index two in $O'_4(V)$ if F is non-dyadic, and $\Omega_4(V) = O'_4(V)$ if F is dyadic.

Consider a long element $\sigma \in \Omega_n(V)$ that is neither totally degenerate nor an involution and return to the properties of the Zassenhaus decomposition $\sigma = \mu\rho$ provided by Theorem 2. The fact that ρ is long implies that $\dim\ R \geq 4$. Therefore,

$$4 \leq \dim\ R \leq \dim\ (T \perp R) \leq 4\,.$$

So $T = 0$, and μ is totally degenerate. In reference to Theorem 3, it follows that the bound on m is $0 \leq m \leq 2$. Also, $\dim\ R = 4$ and R is the unique 4-dimensional anisotropic space over F. What else can be said about ρ?

PROPOSITION 5. Let ρ in $\Omega_n(V)$ be anisotropic with dim $R = 4$. Then $\rho_{|_R} \in O'_4(R)$, and

i) If F is non-dyadic, then ρ is long if and only if $n \geq 5$ and $\rho_{|_R} \in O'_4(R) - \Omega_4(R)$.

ii) If F is dyadic, then ρ is long if and only if $\rho_{|_R} \in O'_4(R) = \Omega_4(R)$ is long.

This initial answer to Question A is proved in [6]. Suppose that F is non-dyadic. Then Proposition 5 together with Theorem 2 tell us that $\ell(\sigma) = \frac{1}{2}\dim S + 1$ for any long element σ. Proposition 5 also provides a complete answer to Question B. See Theorem 3 of [6]. It asserts that the long elements in $\Omega_n(V)$ that are not involutions and not totally degenerate are those of Theorem 2, namely they are precisely the elements with Zassenhaus decomposition $\sigma = \mu\rho$, where $\mu = 1_V$ or μ is totally degenerate and ρ satisfies (i) above. If F is dyadic, then Question B is as yet not resolved. However, it is known that $\ell(\sigma) = \frac{1}{2}\dim S + 1$ for all long elements σ.

Let V be the anisotropic 4-dimensional space over F. In view of Proposition 5 we will analyze the elements σ in $O'_4(V)$ that satisfy

(A) σ in $O'_4(V) - \Omega_4(V)$ if F is non-dyadic, and

(B) σ a long element in $O'_4(V) = \Omega_4(V)$ if F is dyadic.

Is there a criterion that pinpoints when an element in $O'_4(V)$ satisfies (A) or (B)? A theorem of Milnor [14] tells us where to look.

THEOREM 5. Let V be an n-dimensional, non-degenerate quadratic space over a local field F. Let $m(X)$ be a monic, irreducible polynomial in $F[X]$ and let deg $m(X) = k$. Assume that $m(X)$ is neither $X - 1$ nor $X + 1$.

i) $m(X)$ is the minimal polynomial of an element of $O_n(V)$ if and only if k is even and divides n, $m(X)$ is symmetric, and disc $V = (m(1)m(-1))^{\frac{n}{k}}\overset{*}{F}{}^2$.

ii) Given such a polynomial $m(X)$ there is precisely one conjugacy class of elements in $O_n(V)$ with minimal polynomial $m(X)$.

Milnor's result no longer holds when $m(X)$ is reducible. Any Eichler transformation that is not totally degenerate has minimal polynomial $(X - 1)^3$ and provides an example showing that (i) no longer holds. The nontrivial totally degenerate elements - all of which have minimal polynomial $(X - 1)^2$ - show that (ii) fails. Let μ and μ_1 be totally degenerate elements. Then μ is conjugate to μ_1 if and only if their respective spaces U and U_1 have the same dimension. This follows from the conjugacy criterion given by the Wall form and the fact U_μ and U_{μ_1} are both alternating.

Let $\sigma \in O_4'(V)$ and let $m(X)$ be its minimal polynomial. Milnor's theorem suggests that it should be possible to look at $m(X)$ and decide whether σ satisfies condition (A) or (B) or not. In reference to Theorem 3, we are interested in precise information about the product $p_1(X)\cdots p_k(X)$. In the discussion that follows, only the arithmetic aspects of the proofs will be provided.

Proposition 6. Let V be anisotropic with dim $V = 4$ and let $\sigma \in O_4'(V)$. Then σ satisfies (A) or (B) if and only if σ satisfies the *long criterion*:

$$Q(\sigma x - x) = -\beta_x^2 Q(x) \text{ for all } x \in V \text{ and some } \beta_x \in \overset{*}{F}.$$

Suppose that $m(X)$ has a factor of the form $X - a$. So $\sigma x = ax$ for some non-zero x in V. Because x is anisotropic, $a = \pm 1$. Since $\sigma x = x$ violates the long criterion, we must have $\sigma x = -x$. So $a = -1$. Therefore, $X + 1$ is the only possible monic linear factor of $m(X)$. If $(X+1)^2$ is a factor of $m(X)$, then $-\sigma$ is a non-trivial unipotent element on some subspace of V. But this is impossible, because V is anisotropic.

1. Suppose deg $m(X) = 1$. This implies that $m(X) = X + 1$ and hence that $\sigma = -1_V$. Because disc $V = 1$, $-1_V \in O_4'(V)$. Check that $\sigma = -1_V$ satisfies the long criterion precisely when $-1 \in \overset{*}{F}{}^2$.
2. Suppose deg $m(X) = 2$. Observe that $m(X)$ must be irreducible. By Theorem 5, $m(X) = X^2 - cX + 1$ for some $c \in F$. Notice that $c \neq \pm 2$. Every line of V contains a plane that is invariant under σ. Let W be any such plane. By Theorem 5, disc $W = -(c-2)(c+2)\overset{*}{F}{}^2$. Because V is anisotropic, W is not a hyperbolic plane, and therefore, $(c-2)(c+2) \notin \overset{*}{F}{}^2$. Again by Theorem 5, there is precisely one conjugacy class of such elements σ for a given c. A spinor norm computation shows that $\Theta(\sigma) = (c-2)^2\overset{*}{F}{}^2 = \overset{*}{F}{}^2$. So any σ with minimal polynomial of this form is in $O_4'(V)$. It turns out that σ satisfies the long criterion if and only if $c - 2 \in \overset{*}{F}{}^2$.
3. Suppose deg $m(X) = 3$. By Theorem 5, $m(X)$ is reducible. It follows that $m(X) = (X+1)(X^2 - cX + 1)$ with $X^2 - cX + 1$ irreducible. Again, $c \neq \pm 2$. Let $p_1(X) = X + 1$ and $p_2(X) = X^2 - cX + 1$. Put $U = p_2(\sigma)V$ and $W = p_1(\sigma)V$. Observe that U and W are planes that are invariant under σ, that $V = U \perp W$, that $\sigma_{|U} = -1_U$, and that $\sigma_{|W}$ has minimal polynomial $X^2 - cX + 1$. As in the previous case, disc $W = -(c-2)(c+2)\overset{*}{F}{}^2$ and $(c-2)(c+2) \notin \overset{*}{F}{}^2$. By Theorem 63:20 of [15], there are two isometry classes of anisotropic planes of a given

discriminant. An application of Theorem 5 implies that there are two conjugacy classes of σ for a given c. By a spinor norm computation, $\Theta(\sigma) = -(c-2)\overset{*}{F}{}^2$. So $\sigma \in O_4'(V)$ if and only $-(c-2) \in \overset{*}{F}{}^2$ and $-(c+2) \notin \overset{*}{F}{}^2$. The analysis of the long criterion for $\sigma \in O_4'(V)$ will follow shortly. We will see that if it holds, then $-1 \in \overset{*}{F}{}^2$ and $c-2 \in 4\mathfrak{u}^2$. This implies in turn that $c \in 2\mathfrak{u}$. If F is non-dyadic, the converse is true. Namely, $-1 \in \overset{*}{F}{}^2$ and $c-2 \in \mathfrak{u}^2$ together imply the long criterion.

4. Suppose $\deg m(X) = 4$. In this case, either

   $m(X) = (X^2 - cX + 1)(X^2 - dX + 1)$ with distinct irreducible factors,

   or

   $m(X) = X^4 - cX^3 - dX^2 - cX + 1$ is irreducible.

   The first case is very similar to case (3). The second seems complicated and is as yet not completely understood.

We now return to case (3) and to the analysis of the long criterion. Let $\dot{U}$ and $\dot{W}$ denote the non-zero elements of U and W and let

$$C = Q(\dot{W})/Q(\dot{U})\,.$$

The set C is closed under multiplication by squares and hence under taking inverses.

Assume that the long criterion holds. Applying it to U and W we get that

$$\text{(i)} \qquad -1 \;\text{ and }\; c-2 \;\text{ are both in }\; \overset{*}{F}{}^2.$$

Put $-1 = i^2$ and $c - 2 = s^2$ and let $t = -2is^{-1}$. Applying the long criterion to the vectors $x = u + w$ with $u \in U$ and $w \in W$, tells us that

$$\text{(ii)} \qquad \frac{1+\gamma t^2}{1+\gamma} \in \overset{*}{F}{}^2 \quad \text{for all} \quad \gamma \in C\,.$$

Conversely, the long criterion is equivalent to the combination of (i) and (ii).

We assume that (i) and (ii) hold and consider the consequences for the constant c. We show first that $t \in \mathfrak{u}$. It follows from the discussion in paragraph 63.C of O'Meara [15] that C contains a prime element π. Therefore C contains π^i for any odd i either positive or negative. Put $t = \delta\pi^k$ with $\delta \in \mathfrak{u}$. Taking $\gamma = \pi$ we get,

$$\frac{1+\gamma t^2}{1+\gamma} = \frac{1+\delta^2\pi^{2k+1}}{1+\pi}\,.$$

If $k < 0$, then $2k+1 < 0$, and $\frac{|1+\delta^2\pi^{2k+1}|}{|1+\pi|} = |\pi|^{2k+1}$ by the Principle of Domination. Because $2k+1$ is odd, the element above cannot be a square. This contradicts (ii). If $k > 0$, a similar contradiction is obtained by taking $\gamma = \pi^{-1}$. Therefore, $k = 0$ and $t \in \mathfrak{u}$ as required. Let $\varepsilon = -it^{-1} \in \mathfrak{u}$. Because $s = 2\varepsilon$, we get

$$c - 2 = 4\varepsilon^2.$$

Therefore, $c - 2 \in 4\mathfrak{u}^2$ as asserted earlier. Note that $c = 2(2\varepsilon^2 + 1)$. If F is dyadic, then by domination, $c \in 2\mathfrak{u}$. This is also true in the non-dyadic case. If $c \notin \mathfrak{u}$, then $c \in \mathfrak{p}$. But this would imply by Hensel's Lemma that $X^2 - cX + 1$ is reducible.

We now explore the converse. Assume both $-1 \in \overset{*}{F}{}^2$ and $c - 2 \in 4\mathfrak{u}^2$. Does $\sigma \in O_4'(V)$ with such a c satisfy the long criterion, or equivalently, conditions (i) and (ii)? Condition (i) holds trivially, so the focus is on (ii). Put $c-2 = 4\varepsilon^2$ with $\varepsilon \in \mathfrak{u}$. Set $s = 2\varepsilon$ and $t = -2is^{-1} = -i\varepsilon^{-1}$. Notice that $t \in \mathfrak{u}$. Because C is closed under taking inverses, (ii) is equivalent to $1 + \frac{t^2-1}{1+\gamma} \in \overset{*}{F}{}^2$ for all γ in C. Check that $t^2 - 1 = -\frac{4+s^2}{s^2} = -\frac{c+2}{c-2} = -\frac{c+2}{4\varepsilon^2}$. So the question is this: Is it the case that

$$\text{(iii)} \qquad 1 \;-\; \frac{c+2}{4\varepsilon^2(1+\gamma)} \;\in\; \overset{*}{F}{}^2$$

for all $\gamma \in C$?

The first step toward the answer is the observation that $\{|1+\gamma| \mid \gamma \in C\}$ is bounded below by $|4|$. For suppose that $|1+\gamma| \leq |4\pi|$ for some $\gamma \in C$. Then $1 + \gamma = 4\alpha\pi$ for some $\alpha \in \mathfrak{o}$. But this means that $-\gamma = 1 - 4\alpha\pi \in \overset{*}{F}{}^2$ by the Local Square Theorem. Because C is closed under multiplication by squares, $-\gamma \in C$. But this implies that the intersection $Q(\dot{U}) \cap Q(\dot{W})$ is not empty. This would mean that V contains a plane of discriminant $\overset{*}{F}{}^2 = -\overset{*}{F}{}^2$, i.e., a hyperbolic plane. This is not possible because V is anisotropic. Now assume that $|c+2| < |4|^3$. Given the bound just established, $|\frac{c+2}{4\varepsilon^2(1+\gamma)}| < |4|$ for all $\gamma \in C$. Therefore by another application of the Local Square Theorem,

$$1 \;-\; \frac{c+2}{4\varepsilon^2(1+\gamma)} \;\in\; \overset{*}{F}{}^2$$

for all γ in C.

We conclude the discussion of the converse by assuming that F is non-dyadic. In this case (iii) is satisfied for any c (such that $c-2 \in 4\mathfrak{u}^2$). Because $|4| = 1$, we already know that (iii) holds when $c+2 \in \mathfrak{p}$. Since $c+2 \in \mathfrak{o}$, only the case $c+2 \in \mathfrak{u}$ remains. Instead of (iii), we will verify the equivalent condition (ii). Recall from the beginning of the analysis of case (3) that disc $W = -(c-2)(c+2)\overset{*}{F}{}^2$ and $-(c+2) \notin \overset{*}{F}{}^2$. So disc $W = -(c+2)\overset{*}{F}{}^2$ and, by an application of Example 63:15 of [15], $C = \pi\mathfrak{u}\overset{*}{F}{}^2$. Let $\gamma = \pi\delta\alpha^2 \in C$ with $\delta \in \mathfrak{u}$ and $\alpha \in \overset{*}{F}$ be arbitrary. If $|\alpha| \leq 1$, then $|\gamma| < 1$. So $1+\gamma$ and $1+t^2\gamma$ are both in $\overset{*}{F}{}^2$ by the Local Square Theorem. Therefore (ii) holds. Suppose $|\alpha| > 1$. Now $|\gamma| > 1$ and the Local Square Theorem tells us that $1+\gamma^{-1}$ and $1+t^{-2}\gamma^{-1}$ are both squares. So $\frac{1+t^{-2}\gamma^{-1}}{1+\gamma^{-1}}$ is a square. Therefore $\frac{1+\gamma t^2}{1+\gamma}$ is a square as well and (ii) holds in this case also. The proof of the converse in the non-dyadic case is complete. The dyadic situation is much more delicate and is not completely settled.

5. Global Fields. Let F be a global field, let V be a non-degenerate quadratic space over F, and consider the group $\Omega_n(V)$. Not much is known about the length question in this situation, but it is clear that local-global considerations are relevant. Let $\mathfrak{p}$ be a prime - Archimedean or not - and consider the completion $V_{\mathfrak{p}}$. The first indication is the theorem that tells us that $\sigma \in \Omega_n(V)$ if and only if $\sigma_{\mathfrak{p}} \in \Omega_n(V_{\mathfrak{p}})$ for all $\mathfrak{p}$. Another is the fact (analogous to what was observed in the local case) that the analysis of the anisotropic long elements in $\Omega_n(V)$ reduces to the 4-dimensional anisotropic long elements. This is true not only in the situation where F is a function field or a totally complex number field (in these situations there are no anisotropic spaces of dimension 5 or more) but in general. More precisely, if σ is an anisotropic long element, then

$$\sigma = \omega_1 \cdots \omega_k \sigma_1,$$

where all ω_i are elementary commutators of hyperplane reflections, the space $S = W_1 \oplus \cdots \oplus W_k \oplus S_1$, and σ_1 is long with dim $S_1 = 4$.

Bibliography

1. E. Artin, *Geometric Algebra,* Wiley Interscience, New York, 1966.
2. E. W. Ellers and J. Malzan, Products of reflections in the kernel of the spinorial norm, *Geom. Ded.* 36 (1990), 279-285.
3. M. Dyer, On minimal length of expressions of Coxeter group elements as products of reflections, *Proceedings of the AMS*, to appear.
4. A. J. Hahn, Unipotent elements and the spinor norms of Wall and Zassenhaus, *Archiv Math.* (Basel) 32 (1979), 114-122.
5. A. J. Hahn and O. T. O'Meara, *The Classical Groups and K-Theory,* Grundlehren der Mathematik, Springer-Verlag, 1989.

6. A. J. Hahn, The elements of the orthogonal group $\Omega_n(V)$ as products of commutators of symmetries, *J. Algebra* 184 (1996), 927-944.

7. J. E. Humphreys, *Reflection Groups and Coxeter Groups,* Cambridge University Press, 1990.

8. B. Huppert, Isometrien von Vektorräumen I, *Archiv Math.* (Basel) 35 (1980), 164-176.

9. B. Huppert, Isometrien von Vektorräumen II, *Math. Z.* 175 (1980), 5-20.

10. F. Knüppel, Products of simple isometries of given conjugacy types, *Forum Math.* 5 (1993), 441-458.

11. T. Y. Lam, *The Algebraic Theory of Quadratic Forms,* Benjamin, Reading MA, 1973.

12. G. A. Margulis, Explicit constructions of graphs without short cycles and low density codes, *Combinatorica* 2 (1) 1982, 71-78.

13. G. A. Margulis, Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators, *Communication Network Theory* 1988, 39-46.

14. J. Milnor, On Isometries of Inner Product Spaces, *Inventiones Math.* 8 (1969), 83-97.

15. O. T. O'Meara, *Introduction to Quadratic Forms,* Classics in Mathematics, Springer-Verlag, 2000, a reprint of the 1973 Springer Grundlehren edition.

16. J. Rosenthal and P. O. Vontobel, Construction of LDPC codes using Ramanujan graphs and ideas from Margulis, *Proceedings 38th Allerton Conference on Communication, Control and Computing, October 4-6, 2000*, to appear.

17. H. Zassenhaus, On the spinor norm, *Archiv Math.* (Basel) 13 (1962), 434-451.

Alexander Hahn
Department of Mathematics
University of Notre Dame
Notre Dame, IN 46556
USA
hahn.1@nd.edu