Baton Rouge Lecture

Alexander Hahn, Notre Dame

Consider a group G along with a set of generators A that satisfies $A^{-1} = A$. Many such situations exist: G a Weyl group (or more generally a Coxeter group) and A the defining hyperplane reflections; or G a classical group and A a set of special elements coming from the underlying geometry (or from a single conjugacy class of such elements); or $G = SL_n(\mathbb{Z})$ with A the set of elementary matrices; or in coding theory where interesting codes are constructed from the Cayley graph arising from certain G and A (this seems to be a hot topic currently).

Question: Given G and A and $\sigma \in G$ what is the length of $\ell(\sigma)$ of σ? Or more precisely, are there parameters arising from σ from which $\ell(\sigma)$ be read off?

Example 1. Let G be the symmetric group on $\{1, \ldots, n\}$ and let A be the set of transpositions. Let $k(\sigma)$ be the the number of orbits of σ (include the trivial orbits). Then

$$\ell(\sigma) = n - k(\sigma)\ .$$

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

$$\ell(\sigma) = \frac{1}{2}(n - k(\sigma))\ .$$

Now let V be a non-degenerate $n-$dimensional quadratic space with symmetric bilinear form B over a field F with char$(F) \neq 2$. 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 $S^\perp = \{x \in V \mid \sigma(x) = x\}$. It turns out that dim S is even if and only if $\sigma \in O_n^+(V)$.

For instance, $\sigma = 1_V$ if and only if $S = 0$. If dim $S = 1$, then S is necessarily non-degenerate, and $\sigma = -1_S \perp 1_{S^\perp}$. These elements are the *hyperplane reflections* or *symmetries*. If $S = Fv$, denote σ by τ_v. They are involutions, i.e., they satisfy $\sigma^2 = 1_V$.

We will define properties of σ by referring to S. For example, σ is *non-degenerate*, *degenerate*, or *totally degenerate* if S is non-degenerate, degenerate, or totally degenerate, i.e., if the radical $\operatorname{rad} S = S \cap S^\perp$ of S is zero, non-zero, or S. Similarly, σ is *anisotropic* if S is anisotropic. Symmetries are anisotropic. It is easy to see that σ is an involution if and only if $\sigma_{|S} = -1_S$. In particular, involutions are non-degenerate. The degenerate elements σ with dim $S = 2$ are the *Eichler* transformations.

Notation: if an orthogonal transformation σ, μ, ρ, η, etc. is under consideration, then then S, U, R, and E, etc. will automatically denote its space.

Example 3. Theorem (Cartan, Scherk, Dieudonné). Let G be the group $O_n(V)$ and let A be the set of symmetries. If σ is not totally degenerate, then

$$\ell(\sigma) = \dim\, S\ .$$

If σ is totally degenerate, then $\ell(\sigma) = \dim\, S\, +\, 2$.

Note: The answer is complete and completely independent of F or V.

This example parallels Example 1. What about the analogue of Example 2?

Example 4. Let G be the commutator subgroup $\Omega_n(V)$ of $O_n(V)$ and let A be the set of short commutators of symmetries. What about $\ell(\sigma)$ in this situation?

The short answer: Nothing until recently; much more difficult; dependence on both F and V. The longer answer is the subject of this talk. Incidentally, I got interested in this question about 5 years ago thanks to John Hsia who was interested in the case F a non-dyadic local field. In this case, a complete solution is possible. I'll describe what this is; also discuss the dyadic case; then give some "global" insights.

Let $\sigma \in \Omega_n(V)$. Let $\sigma = \tau_v\tau_w\tau_v\tau_w$ be a non-trivial short commutator of symmetries. Then $S = Fv \oplus Fw$. Also, $\sigma = \tau_v\tau_{\tau_w(v)} = \tau_v\tau_{v'}$ with $Q(v) = Q(v')$, where $Q(x) = B(x,x)$. Conversely, any such product is a short commutator of symmetries. It is now a direct consequence of CSD that

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

Now let's call $\sigma \in \Omega_n(V)$ *short* if $\ell(\sigma) = \frac{1}{2}\dim S$, and *long* otherwise. Let σ be totally degenerate. Then $\sigma \in \Omega_n(V)$ and by CSD, σ is long. CSD suggests that long ought to be the exception. True?

Goal: The same as that of CSD. Namely, the complete description of the long elements of $\Omega_n(V)$ and the determination of their length.

Theorem 1. Suppose that 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, $\ell(\sigma) = \frac{1}{2}\dim\ S + 1$.

Easy consequence of CSD. Note that this result applies to $\mathbb{C}, \mathbb{R}$, and $\mathbb{F}_q$.

Knüppel (1993) noticed the following as a result of his investigations into of a different problem, namely the generation of the orthogonal groups by symmetries from a fixed conjugacy class.

i) If σ is long and not an involution, then the quotient space $S/\mathrm{rad}\, S$ is anisotropic, and

ii) If V is isotropic and σ is long, then $\ell(\sigma) = \frac{1}{2}\dim\, S\, +\, 1$.

Knüppel's observations are an important start towards the goal.

The Tools: The *Zassenhaus* splitting; the *Wall* form; and *Reduction mod the Radical.*

The *Zasssenhaus splitting.* Let $\sigma \in O_n(V)$. Consider the subspace

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

This largest space on which σ acts as a *unipotent* transformation is non-degenerate. Let R be its orthogonal complement. Note that $\sigma R = R$ and $\sigma R^\perp = R^\perp$, and hence that $\sigma = \sigma_{|R^\perp} \perp \sigma_{|R}$. 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* splitting of σ. Note that μ and ρ commute. It turns out that σ is in $\Omega_n(V)$ if and only if μ and ρ are both in $\Omega_n(V)$. Non-trivial unipotent elements exist only for isotropic V. Eichler transformations are unipotent.

The *Wall* form. For $\sigma \in O_n(V)$, 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 form is a non-degenerate, bilinear form on S (but it is almost never symmetric). Note that the space S is now equipped both with $(\ ,\ )_\sigma$ and the restriction of B. When $(\ ,\ )_\sigma$ is under consideration we will denote S by S_σ.

One can check that σ is an involution if and only if $(\ ,\ )_\sigma$ is symmetric, and that in this case, $(\ ,\ )_\sigma = -\frac{1}{2}B$. Also, σ is totally degenerate if and only if S_σ is alternating. Let $\sigma = \mu\rho$ be the Zassenhaus splitting of σ with μ totally degenerate and ρ an involution. What can you say about S_σ?

The key facts are these. Let W_1 be a non-degenerate subspace of S_σ. Then there is a unique $\sigma_1 \in O_n(V)$ - the transformation belonging to W_1 - such that $(S_1)_{\sigma_1} = W_1$. If $S_\sigma = W_1 \perp W_2$ (W_2 is the right complement of W_1), then $\sigma = \sigma_1 \cdot \sigma_2$, where σ_2 belongs to W_2. Relevant to the current context is that σ is short if and only if S_σ is a (right) orthogonal sum of planes of discriminant one that are non-alternating. (As an aside, the Wall form supplies a useful definition of the spinor norm via disc S_σ).

The *Reduction mod the Radical* construction. Let M be any subspace of V. The quotient space $M/\operatorname{rad} M$ becomes a non-degenerate quadratic space with bilinear form B' defined by

$$B'(x + \text{rad } M, y + \text{rad } M) = B(x, y) \ \text{ for all } \ x, y \in M\ .$$

Let $O[M]$ be the subgroup of $O_n(V)$ defined by

$$O[M] = \{\eta \in O_n(V) \ \mid \ E \subseteq M\}.$$

Let $\eta \in O[M]$. Since $E^\perp \supseteq M^\perp \supseteq \text{rad } M$, we see that $\eta|_{\text{rad}\, M} = 1_{\text{rad}\, M}$. So we can define

$$\sim \ : \ O[M] \longrightarrow O(M/\text{rad } M)$$

by $\widetilde{\eta}(x + \text{rad}\, M) = \eta x + \text{rad}\, M$. For $v \in M$ anisotropic, $\tau_v \in O[M]$ and $\widetilde{\tau}_v = \tau_{v+\text{rad}\, M}$. Check that

$$\ker \sim \ = \{\eta \in O[M] \mid (\eta - 1_V)M \subseteq \text{rad}\, M\}.$$

If η is in the kernel then,

$$(\eta - 1_V)^3 V \subseteq (\eta - 1_V)^2 M \subseteq (\eta - 1_V)(\text{rad}\, M) = 0.$$

In particular, η is unipotent.

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 $U = \text{rad}\, U \perp T$ with T anisotropic and the space of σ satisfies $S = \text{rad}\, U \perp (T \perp R)$ with $T \perp R$ anisotropic.

ii) The unipotent element μ is *special*. This means that μ is a product of $\frac{1}{2}(\dim\, U)$ commuting Eichler transformations and that $(\mu - 1_V)^3 = 0$. (The totally degenerate elements are precisely the unipotents with $(\mu - 1_V)^2 = 0$.)

iii) The non-degenerate element ρ is anisotropic and long.

Part (i) follows from the Zassenhaus splitting and the insight of Knüppel. That $(\mu - 1_V)^3 = 0$ is a quick consequence of reduction with $U/\text{rad}\, U$. Namely, because μ is unipotent, $\widetilde{\mu} \in O(U/\text{rad}\, U)$ is unipotent. But this quotient is anisotropic, so $\mu \in \ker \sim$. That ρ is anisotropic follows from (i); the rest of (ii) and (iii) are labor intensive.

This Theorem - it holds for any F - reduces the problem to the following two questions:

A) Determine which of the elements in Theorem 2 are actually long and compute their lengths. (Recall that if V is isotropic, then the length of any long element σ is $\frac{1}{2}\dim\, S + 1$.)

B) Classify all long anisotropic elements ρ in $\Omega_n(V)$.

Let's see what the answers are in case F is a local field. We begin with Question A:

Proposition 3. Suppose that F is a local field and consider any element $\sigma = \mu\rho \in \Omega_n(V)$ that satisfies conditions (i) - (iii) of Theorem 2. Then $T = 0$, μ is totally degenerate, dim $R = 4$, and σ is long. Finally, $\ell(\sigma) = \frac{1}{2}\dim\ S + 1$. In particular, all long elements of $\Omega_n(V)$ (excluding involutions and totally degenerate elements) can be constructed by splicing totally degenerate and long anisotropic elements together.

That $T = 0$ and dim $R = 4$, follows easily from the fact that $4 \leq \dim\ R \leq \dim\ (T \perp R) \leq 4$. That σ is long comes from a combination of reduction mod the radical with properties of the Wall form. In view of Knüppel's result, $\ell(\sigma) = \frac{1}{2}\dim\ S + 1$ only needs verification for dim $V = 4$.

In reference to Question B, there is a sharp dichotomy between the non-dyadic case and the dyadic case.

Proposition 4. If F is non-dyadic, then anisotropic long elements occur only for $n \geq 5$ and they are the following:

$$\rho = 1 \perp \rho_{|R} \quad \text{with} \quad \rho_{|R} \in O_4'(R) - \Omega_4(R)\ .$$

Such elements exist because the index of $\Omega_4(R)$ in $O_4'(R)$ is two and they are all long. To prove the proposition, it is enough to verify that all elements in $\Omega_4(V)$ are short.

Suppose that F is dyadic. Here the matter is much more subtle. In this case, $O_4'(R) = \Omega_4(R)$. So there are no long elements of the type above. It follows that all anisotropic long elements have the form

$$\rho = 1 \perp \rho_{|R} \quad \text{with} \quad \rho_{|R} \ \text{ long in } \ \Omega_4(R)\ .$$

So we need to classify the long elements in $\Omega_4(V)$ with V anisotropic. Milnor [8] provides a strategy:

Let V be any non-degenerate quadratic space over a local field F (of characteristic not 2). Let $m(X)$ be an irreducible monic polynomial in $F[X]$. Then $m(X)$ is the minimal polynomial of an element of $O_n(V)$ if and only if its degree k divides n, it is symmetric, and disc $V = (m(1)m(-1))^{\frac{n}{k}}\overset{*}{F}{}^2$. Given such a polynomial $m(X)$, then - and this is one of the main results of Milnor's paper - there is precisely one conjugacy class of elements in $O_n(V)$ with minimal polynomial $m(X)$. Notice that if ρ is long and anisotropic in $\Omega_n(V)$ then the entire conjugacy class of σ (in $O_n(V)$) consists of long and anisotropic elements of $\Omega_n(V)$. Thus when looking for long elements, we are looking for conjugacy classes of them.

Turn to the study of the long elements in $\Omega_4(V) = O_4'(V)$ (with F dyadic and V anisotropic). Let $m(X)$ be the minimal polynomial of a long element $\sigma \in \Omega_4(V)$. The factor $X + 1$ is the only linear factor that $m(X)$ can have.

1) Suppose deg $m(X) = 1$. Then $m(X) = X + 1$. So $\sigma = -1_V$. This element is in $\Omega_4(V)$, and it is long if and only if $-1 \in \overset{*}{F}{}^2$.

2) Suppose deg $m(X) = 2$. If $m(X)$ is reducible, then $m(X) = (X+1)^2$. But this means that $-\sigma$ is unipotent. But V anisotropic means that $-\sigma = 1_V$, impossible. So $m(X)$ is irreducible, hence $m(X) = X^2 - cX + 1$. It turns out that the unique corresponding conjugacy class is long if and only if $c - 2 \in \overset{*}{F}{}^2$. If σ has a minimal polynomial of this form, then σ is in $\Omega_4(V)$.

3) Suppose deg $m(X) = 3$. By Milnor, $m(X)$ is reducible. So $m(X) = (X+1)(X^2 - cX + 1)$ with $X^2 - cX + 1$ irreducible. (The quadratic factor must be irreducible by the "unipotent" argument above.) In this case, -1 and $c - 2$ must both be in $\overset{*}{F}{}^2$. This case arises.

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

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

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

I know that (a) arises. Most probably, (b) does too.

The "Long" Criterion: Let $\sigma \in \Omega_4(V)$. Then σ is long if and only if

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

The Long Criterion immediately provides the conclusion in (1). It turns out that case (2) is precisely the situation where all ϵ_x^2 are equal, namely to $c-2$. What about (3) and (4a)? These situations are similar. In each case, the factorization $m(X) = p_1(X)p_2(X)$ provides two unique planes, namely $U = p_1(\sigma)V$ and $W = p_2(\sigma)V$ on which σ acts. Check that $V = U \perp W$. In order for σ to be long, the Long Criterion that has to hold for both U and W it must be extendable to all of V.

Let's consider case (3). Note that $\sigma_{|W} = -1_W$. By the Long Criterion applied to U and W we get $c - 2$ and -1 both in $\overset{*}{F}{}^2$. So put $c - 2 = s^2$ and $-1 = i^2$. Notice that $Q(\overset{*}{U}) \cap Q(\overset{*}{W})$ is empty, otherwise V would contain a plane of discriminant $\overset{*}{F}{}^2 = -\overset{*}{F}{}^2$; not possible because V is anisotropic. Put

$$s = -2it^{-1} \text{ for some } t \in \overset{*}{F} \text{ and set } B = \frac{Q(\dot{U})}{Q(\dot{W})},$$

where $\dot{U}$ and $\dot{W}$ denote the non-zero elements of U and W. The extendability of the Long Criterion to V translates into the question of the existence - and precise description - of the elements $t \in \overset{*}{F}$ such that

$$(*) \quad 1 + \frac{t^2 - 1}{1 + \beta} \in \overset{*}{F}{}^2 \text{ for all } \beta \in B.$$

Do such t exist? YES! To see this rewrite the above as

$$\frac{1+\beta-\beta+t^{2\beta}}{1+\beta} \ = 1+\frac{t^2-1}{1+\beta^{-1}}\ .$$

Now observe that $\{|1+\beta| \mid \beta \in \overset{*}{Q}(W)\}$ is bounded below by $|4|$. For suppose that $|1+\beta| \leq |4\pi|$ for some β. Then $1+\beta = 4\alpha\pi$ for some local integer α; but this means that $-\beta = 1-4\alpha\pi \in \overset{*}{F}^2$ by the Local Square Theorem. Because $-\beta \in \overset{*}{Q}(W)$ (notice that $-1 \in Q(U)$

$), we have a contradiction. Now choose$ t $such that$—t$^2-1|$ is small enough and apply the Local Square Theorem again to get (*).

$i^2 =$Then $\overset{*}{Q}(U)$ is a subgroup of index 2 of $\overset{*}{F}$. If Global Fields?

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] A. J. Hahn, Unipotent elements and the spinor norms of Wall and Zassenhaus, *Archiv der Math.*, 32 (1979), 114-122.

[4] A. J. Hahn, The elements of the orthogonal group $\Omega_n(V)$ as products of commmutators of symmetries, J. Alg., 1995

[5] A. J. Hahn and O. T. O'Meara, The Classical Groups and K-Theory, *Grundlehren der Mathematik*, Springer-Verlag, 1989.

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

[7] T. Y. Lam, The Algebraic Theory of Quadratic Forms, Benjamin, Reading MA, 1973.

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

[9] O. T. O'Meara, Introduction to Quadratic Forms, *Grundlehren der Mathematik*, Springer-Verlag, 1971.