CLIFFORD ALGEBRAS OF BINARY HOMOGENEOUS FORMS

JOURNAL OF ALGEBRA, VOL. 366, 94–111, (2012).

ADAM CHAPMAN AND UZI VISHNE

Abstract. We study the generalized Clifford algebras associated to homogeneous binary forms of prime degree p, focusing on exponentiation forms of p-central spaces in division algebra.

For a two-dimensional p-central space, we make the simplifying assumption that one basis element is a sum of two eigenvectors with respect to conjugation by the other. If the product of the eigenvalues is 1 then the Clifford algebra is a symbol Azumaya algebra of degree p, generalizing the theory developed for $p = 3$. Furthermore, when $p = 5$ and the product is not 1, we show that any quotient division algebra of the Clifford algebra is a cyclic algebra or a tensor product of two cyclic algebras, and every product of two cyclic algebras can be obtained as a quotient. Explicit presentation is given to the Clifford algebra when the form is diagonal.

1. Introduction

An element y in an (associative) algebra A is called n-**central** if y^n is in the center. One way to study such elements is through n-central subspaces, which are linear spaces all of whose elements are n-central.

The n-central elements are of special importance in the theory of central simple algebras, through their connection with cyclic field extensions and cyclic algebras. Let F be a field. The **degree** of a central simple algebra over F is, by definition, the square root of the dimension. Every maximal subfield of a division algebra has dimension equal to the degree. The algebra is **cyclic** if it has a maximal subfield which is cyclic Galois over the center.

2010 *Mathematics Subject Classification.* Primary: 15A66; Secondary: 16K20, 11E76.

Key words and phrases. generalized Clifford algebra; p-central space; cyclic algebra; eigenvector decomposition.

This research was supported by the Binational US-Israel Science Foundation, grant #2010/149.

Hamilton's quaternion algebra is the classical example of a cyclic algebra of degree 2 over the real numbers. The first examples of arbitrary degree were constructed by Dickson [1], as follows: Let L/F be an n-dimensional cyclic Galois extension with σ a generator of $\mathrm{Gal}(L/F)$, and let $\beta \in F^{\times}$. Then $\oplus_{i=0}^{n-1} Ly^i$, subject to the relations $yu = \sigma(u)y$ (for $u \in L$) and $y^n = \beta$, is a cyclic algebra of degree n, denoted by $(L/F, \sigma, \beta)$; every cyclic algebra has this form. In particular, every cyclic algebra of degree n has an n-central element, which is not n'-central for any proper divisor n' of n (we call such an element *strongly n-central*. This is taken to be the definition for n-central elements in some papers, but we find the closed definition to be more suitable when dealing with spaces).

If F contains nth roots of unity, then a strongly n-central element of a division algebra generates a cyclic maximal subfield. However, there are central division algebras with strongly n-central elements which are not cyclic. The first example, for $n = 4$, was given by Albert, and an example with $n = p^2$ for an arbitrary prime p was recently constructed by Matzri, Rowen and Vishne [11]. Nevertheless, Albert proved that in prime degree, every central division algebra with a p-central element is cyclic.

When F does have nth roots of unity ρ, a cyclic maximal subfield has the form $L = F[x]$ where x is n-central, so every cyclic algebra has the 'symbol algebra' form

$$(\alpha, \beta)_{n,F} := F[x, y \mid x^n = \alpha,\ y^n = \beta,\ yx = \rho xy],$$

emphasizing even further the role of n-central elements in presentations of cyclic algebras. Moreover, in the above presentation, $Fx + Fy$ is an n-central space (Remark 2.5 below).

To every n-central space V one associates the **exponentiation form** $\Phi : V \to F$, defined by $\Phi(v) = v^n$, which is homogeneous of degree n. One then studies the space (and the algebra it generates) via the associated form.

Definition 1.1. *Let $\Phi : V \to F$ be a homogeneous form of degree n. The **generalized Clifford algebra** associated to Φ is the quotient C_Φ of the free associative algebra $F\langle x_1, \dots, x_t\rangle$, subject to the relations $(a_1x_1 + \cdots + a_tx_t)^n = f(a_1v_1 + \cdots + a_tv_t)$ for every $a_1, \dots, a_t \in F$, where $\{v_1, \dots, v_t\}$ is a basis of V.*

We will say that C_Φ is the Clifford algebra of Φ, or, oftentimes, of V itself.

Clearly, $Fx_1 + \cdots + Fx_n$ is an n-central subspace of C_Φ. A base change induces a linear isomorphism between the respective presentations of C_Φ, so the Clifford algebra is independent of the basis. This generalization of the classical construction of Clifford algebras is due to Roby, [13].

Fixing F, if A is a central simple algebra over an extension $K \supseteq F$, we call an F-subspace $V \subseteq A$ 'n-subcentral' if $v^n \in F$ for every $v \in V$. For every homogeneous form $\Phi : V \to F$, the simple quotients of C_Φ are precisely the simple algebras generated by n-subcentral spaces V, in which $v^n = \Phi(v)$ for every $v \in V$.

A homogeneous form Φ is **anisotropic** if $\Phi(v) \neq 0$ for every $v \neq 0$. We say that an n-central space is anisotropic if its exponentiation form is anisotropic, which is the case exactly when its non-zero elements are all invertible. For example, any n-central subspace of a division algebra is anisotropic.

The Clifford algebras of quadratic forms are a classical object. In this case the center of C_Φ is F (for even dimensional forms) or an étale quadratic extension (otherwise), and C_Φ is a tensor product of quaternion algebras over the center (see, e.g., [9] or [6]).

Let us briefly describe what is known for binary cubic forms, to put the results of this paper in perspective.

Clifford algebras of a binary cubic form f were first considered by Heerema in [5]. Haile studied these algebras in [2] and [3], and showed that in characteristic not 2 or 3, C_Φ is an Azumaya algebra, with center which is the coordinate ring of the affine elliptic curve $s^2 = r^3 - 27\Delta$ where Δ is the discriminant of f. He also proved that the simple homomorphic images of C_Φ are cyclic algebras of degree 3; moreover for every algebraic extension K/F there is a one to one correspondence between the K-points of the elliptic curve $s^2 = r^3 - 27\Delta$ and the simple homomorphic images, mapping the point (r_0, s_0) on the curve to the symbol algebra $(a, s_0 + \frac{1}{2}(3\rho_3(1-\rho_3)ad))_{3,F(r_0,s_0)}$.

Along these lines, it is shown in [3] that C_Φ splits if and only if the ternary form $w^3 - \Phi(v)$ has a nontrivial F-rational point.

When $d > 3$ or $n > 2$, it is known that the Clifford algebra contains a free F-algebra on two generators (Haile [4] attributes this to Revoy).

In particular, the algebra is not a finite module over its center and hence is not Azumaya.

This situation can be partially remedied by considering the **reduced Clifford algebra** A_Φ, defined as the quotient of C_Φ with respect to the intersection of the kernels of all the d-dimensional representations, where d is the degree of f. Haile and Tesser showed in [4] that A_Φ is Azumaya; also see [15]. This quotient was further studied by Kulkarni, [7],[8].

We will assume F is an infinite field. An invertible p-central element acting by conjugation decomposes the algebra into a direct sum of eigenspaces. Since the binary Clifford algebra is large even for small values of $p > 3$, our approach here is to restrict the number of eigenvectors in a basis element. More precisely, we study two-dimensional p-central spaces $V = Fx + Fy$, assuming that y can be written as a sum of two eigenvectors with respect to conjugation by x. Indeed, this much is guaranteed for $p = 3$.

After some preliminaries on homogeneous forms and eigenvector decomposition in Sections 2 and 3, we introduce **short** p-central spaces in Section 4: a p-central space is short if it is spanned by elements x, y such that x is invertible, and y is the sum of two eigenvectors corresponding to the conjugation action of x. The **type** of a short p-central space is the set of eigenvalues participating in the decomposition.

We prove (Theorem 4.12) that any division algebra, a-priori of arbitrary dimension, which is generated by a short p-space of type $\{\rho, \rho^{-1}\}$, is in fact a symbol algebra of degree p over its center. This is reinterpreted in Section 5 to show that the Clifford algebra of a short p-space of this type is an Azumaya algebra of degree p, whose center is the function ring of a hyper-elliptic curve of genus $[(p-1)/2]$.

For $p = 5$ there are, up to choosing ρ, two possible types of short p-central spaces, $\{\rho, \rho^{-1}\}$ and $\{\rho, \rho^3\}$. In Section 6 we study short 5-central spaces of type $\{\rho, \rho^3\}$. This case turns out to be very different than the previous one, resulting in quotients of the Clifford algebra which are tensor products of two cyclic algebras; and indeed, every division algebra which is either a symbol algebra of degree 5 or the tensor product of two symbol algebras is, essentially, a quotient of a suitable Clifford algebra associated to a diagonal quintic form.

2. Preliminaries

It is convenient to express n-centrality of a vector space in terms of basis elements. To this end, we adopt the notation of [12]: $x_1^{d_1} * \cdots * x_t^{d_t}$ denotes the sum of all the products with each x_i appearing d_i times. For example $x^2 * z^2 = xxzz + xzxz + xzzx + zxxz + zxzx + zzxx$; as usual we may omit exponents $d_i = 1$, so that $x^2 * y = xxy + xyx + yxx$. This notation is commutative in the sense that $x_1^{d_1} * \cdots * x_t^{d_t} = x_{\sigma(1)}^{d_{\sigma(1)}} * \cdots * x_{\sigma(t)}^{d_{\sigma(t)}}$ for any permutation $\sigma \in S_t$.

Proposition 2.1. (1) *A subspace* $V = \sum F x_i$ *of an associative algebra* A *is* n*-central iff* $x_1^{d_1} * \cdots * x_t^{d_t} \in F$ *for every partition* $d_1 + \cdots + d_t = n$.

(2) *If* V *as above is* n*-central, then the associated exponentiation form* $V \to F$ *is* $\Phi(u_1 x_1 + \cdots + u_t x_t) = \sum_{d_1+\cdots+d_t=n} (x_1^{d_1} * \cdots * x_t^{d_t}) u_1^{d_1} \cdots u_t^{d_t}$.

Proof. If every $x_1^{d_1} * \cdots * x_t^{d_t} \in F$ then clearly

$$(u_1 x_1 + \cdots + u_t x_t)^n = \sum_{d_1+\cdots+d_t=n} (x_1^{d_1} * \cdots * x_t^{d_t}) u_1^{d_1} \cdots u_t^{d_t} \in F$$

for every $u_1, \dots, u_t \in F$. On the other hand if the space is n-central, then for every linear functional $\psi : A \to F$ such that $F \subseteq \ker \psi$, we have $\sum_{d_1+\cdots+d_t=n} u_1^{d_1} \cdots u_t^{d_t} \psi(x_1^{d_1} * \cdots * x_t^{d_t}) = 0$ for every $u_1, \dots, u_t$; since we assume F is infinite, this implies $\psi(x_1^{d_1} * \cdots * x_t^{d_t}) = 0$ for every partition and every ψ. □

Corollary 2.2. *Let* V *be a subspace in an algebra* A *over* F*. Then* V *is* n*-central iff every subspace of dimension at most* n *of* V *is* n*-central.*

Stated in terms of elements, $x_1, \dots, x_t$ span an n-central space in A iff every subset of cardinality at most n spans such a space.

Corollary 2.3. *Assume* p *is prime, and let* V *be an anisotropic* p*-central space, over a field of characteristic not* p*. Then every two commuting elements of* V *are linearly dependent.*

Proof. If $x, y \in V$ commute and $Fx + Fy$ is p-central with an anisotropic exponentiation form then $x^p \neq 0$ and since every $x + \beta y$ is p-central, we have that $p x^{p-1} y = x^{p-1} * y \in F$, showing that $y \in Fx$. □

Corollary 2.4. *When the characteristic is prime to* n*, an* n*-central space* V *has zero intersection with the center, unless* $V = F$*.*

Remark 2.5. *If $x, y \in A = F[x, y]$ satisfy $yx = \rho xy$, where n is an n-primitive root of unity, then $(x+y)^n = x^n + y^n$, and $Fx + F[x]y$ is n-central.*

Proof. The equality $(x+y)^n = x^n + y^n$ follows by considering the rotation action of $\mathbb{Z}/n\mathbb{Z}$ on the monomials in $x^{n-i} * y^i$; and for every $a \in F$ and $f \in F[x]$, $(fy)(ax) = \rho(ax)(fy)$, so that $(ax + fy)^n = (ax)^n + (fy)^n = a^n x^n + \mathrm{N}_{F[x]/F}(f) y^n \in F$. $\square$

3. Eigenvector decomposition

From now on we consider p-central spaces, where p is a fixed odd prime. Let A be an algebra over a field F whose characteristic is not p.

Lemma 3.1. *Let V be a two-dimensional space with a homogeneous form $\Phi : V \to F$ of degree p, and let $x \in V$ be a vector with $\Phi(x) \neq 0$. Then there is an element z such that $V = Fx + Fz$ and the coefficient of $a^{p-1}b$ in $\Phi(ax + bz)$ is zero.*

Proof. Write $V = Fx + Fy$, and let α be the coefficient of $a^{p-1}b$ in $\Phi(ax + by)$. Take $z = y - \frac{\alpha}{p\Phi(x)} x$; then $V = Fx + Fz$ and the coefficient of $a^{p-1}b$ in $\Phi(ax + bz)$ is $\alpha - p\frac{\alpha}{p\Phi(x)}\Phi(x) = 0$. $\square$

Corollary 3.2. *Let V be a p-central two-dimensional subspace of an algebra A. If $x \in V$ satisfies $x^p \neq 0$, then there is an element z such that $V = Fx + Fz$ and $x^{p-1} * z = 0$.*

Proof. Take the exponentiation form $\Phi(v) = v^p$ in Lemma 3.1. $\square$

Lemma 3.3. *Let $x \in A$ be invertible. If $f(\lambda) = \sum_{i=0}^{n} c_i \lambda^i$ has distinct roots in F and $\sum_{i=0}^{n} c_i x^{-i} y x^i = 0$, then y is a sum of eigenvectors with respect to conjugation by x, namely $y = \sum_{j=1}^{n} z_j$ for $z_j \in A$ satisfying $x^{-1} z_j x = \alpha_j z_j$, where the α_j are the roots of f.*

Proof. Indeed, let $T_x : A \to A$ denote conjugation by x, and let $V = \sum_{i=0}^{n-1} F x^{-i} y x^i$ be the cyclic subspace generated by y. Then the restriction of T_x to a map $T_x : V \to V$ satisfies $f(\lambda)$ and hence is diagonalizable over F by the assumption. $\square$

Corollary 3.4. *Let $x \in A$ be invertible and suppose $\rho \in F$ is a pth root of unity. Every element y commuting with x^p can be written as a sum $y = y_0 + y_1 + \dots + y_{p-1}$, where $y_i x = \rho^i x y_i$.*

Proof. As before let T_x denote conjugation by x. By assumption $x^p y x^{-p} - y = 0$, so $f(T_x)(y) = 0$ for $f(\lambda) = \lambda^p - 1 = 0$. □

Lemma 3.5. *Let $x, y \in A$ be elements, such that x is invertible and $x^{p-1} * y = 0$. Then $y = z_1 + \cdots + z_{p-1}$ for some $z_1, \dots, z_{p-1}$ such that*

$$z_k x = \rho^k x z_k \tag{1}$$

($k = 1, \dots, p-1$).

Proof. Notice that $[x^p, y] = [x, x^{p-1} * y] = 0$. Since $\sum_{i=0}^{p-1} x^{-i} y x^i = x^{1-p} \cdot (x^{p-1} * y) = 0$, y satisfies the condition of Lemma 3.3 for the polynomial $\lambda^{p-1} + \cdots + 1$, whose distinct roots are $1, \rho, \dots, \rho^{p-1}$, so the claim follows. In fact, we have

$$z_k = \frac{1}{p} \sum_{i=0}^{p-1} \rho^{-ki} x^{-i} y x^i. \tag{2}$$

□

4. Short p-central spaces

Let p be an odd prime, and A an associative algebra over a field F of characteristic not p, containing p-roots of unity.

Lemma 4.1. *Let $x \in A$ be an invertible element, and assume $z_i x = \rho^i x z_i$ and $z_j x = \rho^j x z_j$, for some distinct $i, j \not\equiv 0 \pmod{p}$.*

If $(z_i + z_j)^p$ commutes with x, then $(z_i + z_j)^p = z_i^p + z_j^p$.

Proof. Replace A by the subalgebra generated by x, z_i, z_j. By assumption x^p commutes with z_i and with z_j. Therefore, the action of x on A by conjugation has order p, and we have an eigenspace decomposition $A = \oplus A_k$ where $ax = \rho^k xa$ for every $a \in A_k$. But $(z_i + z_j)^p = \sum_{k=0}^{p} z_i^{p-k} * z_j^k$, where $z_i^{p-k} * z_j^k \in A_{(j-i)k \pmod{p}}$. Since $(z_i + z_j)^p \in A_0$ by assumption, $z_i^{p-k} * z_j^k = 0$ for every $k \neq 0, p$. □

Lemma 4.2. *Let $x \in A$ be invertible, and assume $z_i x = \rho^i x z_i$ and $z_j x = \rho^j x z_j$, for some distinct $i, j \not\equiv 0 \pmod{p}$. Let $y = z_i + z_j$.*

1. *Assume $i + j \equiv 0 \pmod{p}$. Then for every $\alpha \in F$, $x^{p-2} * y^2 = \alpha$ if and only if $z_i z_j - \rho^i z_j z_i = \frac{\alpha(1-\rho^i)}{p} x^{2-p}$.*
2. *If $i + j \not\equiv 0 \pmod{p}$ and $x^{p-2} * y^2 \in F$, then in fact $x^{p-2} * y^2 = 0$.*

Proof. For any a, b, denote $g_{ab} = \sum_{0 \leq r \leq s \leq p-2} \rho^{-(ar+bs)}$. Direct computation shows that $g_{00} = \binom{p}{2}$, $g_{0b} = \frac{\rho^{2b}p}{1-\rho^b}$ for every $b \not\equiv 0 \pmod{p}$, $g_{a0} = \frac{-\rho^a p}{1-\rho^a}$ for $a \not\equiv 0$, $g_{a,p-a} = \frac{p}{1-\rho^a}$, and $g_{ab} = 0$ if $a, b, a+b \not\equiv 0$.

Writing $\alpha = x^{p-2} * y^2$ we have

$$\begin{aligned}
\alpha &= \sum_{0 \leq r \leq s \leq p-2} x^r y x^{s-r} y x^{p-s-2} \\
&= \sum_{0 \leq r \leq s \leq p-2} x^r y x^{-r} \cdot x^s y x^{-s} \cdot x^{p-2} \\
&= \sum_{0 \leq r \leq s \leq p-2} x^r (z_i + z_j) x^{-r} \cdot x^s (z_i + z_j) x^{-s} \cdot x^{p-2} \\
&= \sum_{0 \leq r \leq s \leq p-2} (\rho^{-ir} z_i + \rho^{-jr} z_j)(\rho^{-is} z_i + \rho^{-js} z_j) x^{p-2} \\
&= (g_{ii} z_i^2 + g_{ij} z_i z_j + g_{ji} z_j z_i + g_{jj} z_j^2) x^{p-2}.
\end{aligned}$$

Since $p \neq 2$, $g_{ii} = g_{jj} = 0$. If $i + j \not\equiv 0$ then $g_{ij} = g_{ji} = 0$ as well, and $\alpha = 0$. On the other hand if $j \equiv -i$ we obtain

$$\frac{\alpha(1-\rho^i)x^{2-p}}{p} = z_i z_j - \rho^i z_j z_i,$$

as asserted. □

Lemma 4.3. *Let $x, z_i, u \in A$, and assume $z_i x = \rho^i x z_i$ for some $i \not\equiv 0 \pmod{p}$.*

If $z_i u = \rho^i u z_i + \gamma x^2$ for some $\gamma \in F$, then z_i^p commutes with u.

Proof. By induction we have that

$$z_i^k u = \rho^{ki} u z_i^k + \rho^{i(k-1)} \gamma \sum_{j=0}^{k-1} \rho^{ij} x^2 z_i^{k-1}$$

for $k = 0, \ldots, p$, and in particular $z_i^p u = u z_i^p$. □

Definition 4.4. *A p-central subspace $V \subseteq A$ is* **short** *if, for some $i \not\equiv j$, it has a basis $\{x, y\}$ with x invertible and a decomposition $y = z_i + z_j$, where $z_i x = \rho^i x z_i$ and $z_j x = \rho^j x z_j$. We say that V has* **type** *$\{\rho^i, \rho^j\}$.*

Corollary 3.2 allows to assume $i, j \neq 0$. Also, if V is assumed to be anisotropic, then x is automatically invertible.

Remark 4.5. *For $p = 3$, every anisotropic p-central space is short (of type $\{\rho, \rho^{-1}\}$).*

Remark 4.6. *Every symbol algebra of degree p over F is generated by a short p-central space, of type $\{\rho\}$, taking $V = Fx + Fy$ where $yx = \rho xy$.*

Proposition 4.7. *Let V be a short anisotropic p-central space of type $\{\rho^i, \rho^{-i}\}$, generating an algebra whose center is a field. Then at least one of z_i and z_{-i} is invertible.*

Proof. Let $V = Fx + Fy$ be the space, where $y = z_i + z_{-i}$ is the assumed decomposition. By Lemma 4.1, $y^p = z_i^p + z_{-i}^p$. The element z_i^p commutes with x by assumption and with z_{-i} by Lemma 4.2.(1) and Lemma 4.3, so it is central. If z_i is non-invertible it follows that $z_i^p = 0$ and $z_{-i}^p = y^p \neq 0$ so z_{-i} is invertible. □

Replacing ρ by a suitable power, we may always assume $i = 1$ and z_1 is invertible. For $k = 1, \dots, (p-1)/2$, let us denote

$$\theta_k = \frac{1}{p} \sum_{S,S'} \rho^{\sum_{i\in S} i - \sum_{i \in S'} i}, \tag{3}$$

where the outer sum is over all pairs of disjoint subsets of cardinality k of $\{0, 1, \dots, p-1\}$. For example,

$$\theta_1 = \frac{1}{p} \sum_{i \neq i'} \rho^{i-i'} = \frac{1}{p} \left(\sum_{i,i'} \rho^{i-i'} - p \right) = -1.$$

The automorphisms of $\mathbb{Q}[\rho]/\mathbb{Q}$ leave θ_k fixed, so $\theta_k \in \mathbb{Q}$. Clearly $p\theta_k$ is an algebraic integer, and so a rational integer. But the action of $\mathbb{Z}/p\mathbb{Z}$ by rotation on the space of disjoint pairs leaves no fixed points, so each θ_k is itself an integer.

Lemma 4.8. *Let x, z be elements of an algebra, satisfying $zx = \rho xz$, $x^p = z^p = 1$ (thus $F[x, z] \cong \mathrm{M}_p(F)$). Then $x^{p-2k} * z^k * (z^{-1}x^2)^k = \rho^{-k} p \theta_k$ for every $k = 1, \dots, (p-1)/2$.*

Proof. Write $z = x\pi$, so that $\pi^p = 1$; let $F_0 = F(a, b, c)$ be a transcendental extension of F, and let $F' = F_0[\pi]$. By definition, $x^{p-2k} * z^k * (z^{-1}x^2)^k$ is the coefficient of $a^{p-2k} b^k c^k$ in $(ax + bz + cz^{-1}x^2)^p = (x(a + b\pi + \rho^{-1} c \pi^{-1}))^p$; but the conjugation action of x on F' multiplies the generator π by ρ, so this this p-power is the norm $\mathrm{N}_{F_0[\pi]/F_0}(a + b\pi + \rho^{-1} c \pi^{-1})$. Putting $b = \beta a$ and $c = \rho \beta^{-1} \gamma a$, $x^{p-2k} * z^k * (z^{-1}x^2)^k$

is ρ^{-k} times the coefficient of $\beta^0\gamma^k$ in

$$\begin{aligned}\mathrm{N}_{F_0[\pi]/F_0}(1+\beta\pi+\beta^{-1}\gamma\pi^{-1}) &= \prod_{i=0}^{p-1}(1+\beta\rho^i\pi+\rho^{-i}\beta^{-1}\gamma\pi^{-1})\\ &= \sum_{S\cap S'=\emptyset}\prod_{i\in S}(\beta\rho^i\pi)\prod_{i\in S'}(\rho^{-i}\beta^{-1}\gamma\pi^{-1})\\ &= \sum_{S\cap S'=\emptyset}\beta^{|S|-|S'|}\gamma^{|S'|}\pi^{|S|-|S'|}\prod_{i\in S}\rho^i\prod_{i\in S'}\rho^{-i},\end{aligned}$$

where the sums are over subsets of $\{0,\dots,p-1\}$. The coefficient of $\beta^0\gamma^k$ is this sum is p times our θ_k. □

Theorem 4.9. *Let A be an algebra generated by an anisotropic short p-central space $V = Fx+Fy$ of type $\{\rho,\rho^{-1}\}$, whose center is an integral domain. Then the exponentiation form is*

$$(ax+by)^p = \alpha_0 a^p + \sum_{k=1}^{[p/2]} p\theta_k\alpha_0\left(-\frac{\alpha_2}{p\alpha_0}\right)^k a^{p-2k}b^{2k} + \alpha_p b^p$$

for suitable $\alpha_0,\alpha_2,\alpha_p \in F$.

Proof. Fix the basis x, y of V as in the definition, with $i = 1$, $y = z_1 + z_{-1}$ such that $z_k x = \rho^k x z_k$ for $k = 1,-1$. Passing to the ring of central fractions does not change the exponentiation form, so by Proposition 4.7 we may assume z_1 is invertible. The exponentiation form is $\Phi(ax+by) = (ax+by)^p = \sum_{i=0}^p \alpha_i a^{p-i}b^i$ for $a, b \in F$, where by Proposition 2.1.2, $\alpha_i = x^{p-i} * y^i \in F$, $i = 0,\dots,p$. In particular $\alpha_0 = x^p$, $\alpha_1 = x^{p-1} * y = 0$ and $\alpha_2 = x^{p-2} * y^2$.

Lemma 4.2 provides the relation

$$z_1 z_{-1} = \rho z_{-1} z_1 + \frac{\alpha_2(1-\rho)}{p\alpha_0}x^2. \tag{4}$$

Let

$$w = z_{-1}x^{-1}z_1 + \frac{\alpha_2}{p\alpha_0}x,$$

so that $z_{-1} = wz_1^{-1}x - \frac{\rho\alpha_2}{p\alpha_0}z_1^{-1}x^2$. From the relations $z_1x = \rho x z_1$ and $z_{-1}x = \rho^{-1}z_{-1}x$ we see that x commutes with w, and using (4) we also have $[z_1, w] = [z_1, z_{-1}x^{-1}]z_1 + \frac{\alpha_2}{p\alpha_0}[z_1, x] = \frac{\alpha_2(1-\rho)}{p\alpha_0}xz_1 + \frac{\alpha_2}{p\alpha_0}(\rho-1)xz_1 = 0$, where $[\cdot,\cdot]$ is the additive commutator. Since $z_{-1} \in F[w, z_1^{-1}, x]$ and $y = z_1 + z_{-1}$, we see that w is central in $A = F[x, y]$. Applying

Remark 2.5 twice, we have

$$
\begin{aligned}
y^p &= (z_1 + z_{-1})^p \\
&= (z_1 + w z_1^{-1} x - \frac{\rho\alpha_2}{p\alpha_0} z_1^{-1} x^2)^p \\
&= (w z_1^{-1} x)^p + (z_1 - \frac{\rho\alpha_2}{p\alpha_0} z_1^{-1} x^2)^p \\
&= z_1^p + w^p z_1^{-p} x^p - \frac{\alpha_2^p}{p^p\alpha_0^p} z_1^{-p} x^{2p}.
\end{aligned} \tag{5}
$$

Let $v = ax + by \in V$, where $a, b \in F$. We can write

$$v = ax + by = ax + b(z_1 + z_{-1}) = bwz_1^{-1}x + z_1(b + az_1^{-1}x - b\frac{\alpha_2}{p\alpha_0}(z_1^{-1}x)^2),$$

with $bwz_1^{-1}x$ commuting with the element in parenthesis, and ρ-commuting with z_1. By Remark 2.5,

$$v^p = (bwz_1^{-1}x)^p + (bz_1 + ax - b\frac{\rho\alpha_2}{p\alpha_0} z_1^{-1}x^2)^p$$

and is in the center. Now, since

$$
\begin{aligned}
(bz_1 + ax - b\frac{\alpha_2}{p\alpha_0} z_1^{-1}x^2)^p &= \sum_{i+j+k=p} (bz_1)^i * (ax)^j * (-b\frac{\rho\alpha_2}{p\alpha_0} z_1^{-1}x^2)^k \\
&= \sum_{i+j+k=p} b^i a^j (-b\frac{\rho\alpha_2}{p\alpha_0})^k \cdot z_1^i * x^j * (z_1^{-1}x^2)^k
\end{aligned}
$$

is central, only monomials of degree zero mod p in x and in z_1 have non-zero contribution, so

$$
\begin{aligned}
v^p &= (bwz_1^{-1}x)^p + b^p z_1^p + a^p x^p + (-b\frac{\rho\alpha_2}{p\alpha_0})^p (z_1^{-1}x^2)^p \\
&\quad + \sum_{k=1}^{[p/2]} b^k a^{p-2k} (-b\frac{\rho\alpha_2}{p\alpha_0})^k \cdot z_1^k * x^{p-2k} * (z_1^{-1}x^2)^k.
\end{aligned}
$$

Because $xz_1 = \rho z_1 x$, Lemma 4.8 applies and gives the value $z_1^k * x^{p-2k} * (z_1^{-1}x^2)^k = \rho^{-k} p\theta_k x^p$. Therefore

$$v^p = \alpha_0 a^p + \alpha_p b^p + \sum_{k=1}^{[p/2]} p\theta_k (-1)^k p^{-k} \alpha_2^k \alpha_0^{1-k} a^{p-2k} b^{2k}.$$

□

Corollary 4.10. *Let $V = Fx + Fy$ be a short p-central space of type $\{\rho, \rho^{-1}\}$ with an anisotropic exponentiation form. If $x^{p-2} * y^2 = 0$, then*

$x^{p-k} * y^k = 0$ for every $k = 1, \dots, p-1$, and the form $(ax+by)^p = \alpha_0 a^p + \alpha_p b^p$ is diagonal.

Remark 4.11. *We may always assume $\alpha_2 = 0$ or $\alpha_2 = 1$. Indeed if $\alpha_2 \neq 0$, the change of variables $x \mapsto \alpha_2 x$ and $y \mapsto \alpha^{(1-p)/2} y$ takes $\alpha_2 = x^{p-2} * y^2$ to 1.*

The notion of Azumaya algebras generalizes central simple algebras over a field to algebras over arbitrary commutative ring R: an R-algebra A is Azumaya if it is a faithful projective finite R-module, and the natural map $A \otimes_R A^{\mathrm{op}} \to \mathrm{End}_R(A)$ is an isomorphism. One prominent feature of Azumaya algebras is a 1-to-1 correspondence between ideals of R and ideals of A.

Similarly to the definition of a symbol algebra in the introduction, for any $\alpha, \beta \in R$ we can define the symbol algebra $(\alpha, \beta)_R = \oplus R x^i z^j$ subject to the relations $zx = \rho xz$ and $x^n = \alpha$, $z^n = \beta$. Assume R is connected, namely has no nontrivial idempotents. Then $(\alpha, \beta)_n$ is Azumaya if and only if α, β and n are invertible in R. This is shown in [10, Sec. 2.2], using the fact that a quotient of $(\alpha, \beta)_n$ over a maximal ideal of R is simple iff α and β are invertible modulo this ideal, and ρ remains primitive.

Theorem 4.12. *Let A be an algebra generated by a short anisotropic p-central subspace V of type $\{\rho, \rho^{-1}\}$, with z_1^p invertible, and suppose the center R of A is connected. Then A is a symbol Azumaya algebra of degree p over R.*

Proof. As in Theorem 4.9, the element $w = z_{-1} x^{-1} z_1 + \frac{\alpha_2}{p\alpha_0} x$ is in the center of A. Moreover z_1^p commutes with x by the relation (1), and with z_{-1} by Lemma 4.1, so $F[z_1^p, w]$ is contained in the center of A. Since z_1 is invertible, we have that $z_{-1} \in F[w, x, z_1^{-1}]$, so A is generated over $F[z_1^p, w]$ by z_1 and x. Finally A is a symbol Azumaya algebra because p, $\alpha_0 = x^p$ and z_1^p are invertible. □

Theorem 4.13. *A simple algebra generated by a short anisotropic p-central subspace of type $\{\rho, \rho^{-1}\}$ is a symbol algebra of degree p over its center.*

Proof. By Proposition 4.7 one of z_1 or z_{-1} is invertible, so we are done by Theorem 4.12. □

5. Clifford algebras of short p-central spaces of type $\{\rho, \rho^{-1}\}$

Let V be an anisotropic p-central space generating an algebra A. Let C_Φ denote the Clifford algebra of the exponentiation form Φ of V, which, by definition, is the free algebra generated by x and y, subject to the relations $(ax+by)^p = \Phi(ax+by)$. By Proposition 2.1 these relations are equivalent to the system of relations

$$x^{p-i} * y^i = \alpha_i$$

for suitable $\alpha_0, \dots, \alpha_p \in F$. We assume V contains an invertible element x, complement the basis to x, y with $\alpha_1 = 0$ by Corollary 3.2, and write $y = z_1 + \cdots + z_{p-1}$ where z_k satisfy (1).

If we assume V is short of type $\{\rho, \rho^{-1}\}$, then Theorem 4.9 gives the values

$$\alpha_i = 0 \qquad \text{for } i \text{ odd,} \tag{6}$$

$$\alpha_i = p\theta_{i/2}\alpha_0 \left(-\frac{\alpha_2}{p\alpha_0}\right)^{i/2} \qquad \text{for } i \text{ even} \tag{7}$$

(holding trivially for $i = 1, 2$).

Equivalently, we may study the Clifford algebra of an arbitrary p-central space, presented in the form $V = Fx + Fy$ with x invertible and the eigenvector decomposition for y, modulo its ideal $\langle z_2, \dots, z_{p-2}\rangle$ (where z_k are defined by (2)). Indeed, let $V = Fx + Fy$ be a p-central space in an arbitrary algebra. Let $\alpha_i = x^{p-i} * y^i \in F$. The image of V in the quotient algebra $C_\Phi/\langle z_2, \dots, z_{p-2}\rangle$ is a short p-central space of type $\{\rho, \rho^{-1}\}$, so Theorem 4.9 forces the equalities (6) and (7). If these equalities do not originally hold, $\langle z_2, \dots, z_{p-2}\rangle$ must be the whole algebra. But if they do hold, then $C_\Phi/\langle z_2, \dots, z_{p-2}\rangle$ is the Clifford algebra of a short p-central space, so it is generic to this situation.

Therefore, we assume in this section that V is short of type $\{\rho, \rho^{-1}\}$. Then C_Φ is defined by the relations $x^p = \alpha_0$, $x^{p-2} * y^2 = \alpha_2$ and $y^p = \alpha_p$, where y has the form $y = z_1 + z_{-1}$ with $z_k x = \rho^k x z_k$. From Lemma 4.2.(1) and Remark 4.1 we obtain the presentation with generators

$$x, z_1, z_{-1},$$

and relations

$$x^p = \alpha_0, \tag{8}$$

$$z_1 x = \rho x z_1, \tag{9}$$

$$z_{-1} x = \rho^{-1} x z_{-1}, \tag{10}$$

$$z_1 z_{-1} = \rho z_{-1} z_1 + \frac{\alpha_2(1-\rho)}{p\alpha_0} x^2, \tag{11}$$

$$z_1^p + z_{-1}^p = \alpha_p, \tag{12}$$

depending of course on $\alpha_0, \alpha_2, \alpha_p \in F$.

As in Theorem 4.9, the element $w = z_{-1}x^{-1}z_1 + \frac{\alpha_2}{p\alpha_0}x$ is in the center of C_Φ. Since z_1^p is central, we may consider the algebra $C_\Phi[z_1^{-p}]$, where z_1 is invertible. Substituting $z_{-1} = wz_1^{-1}x - \frac{\rho\alpha_2}{p\alpha_0}z_1^{-1}x^2$, the presentation of $C_\Phi[z_1^{-p}]$ on the generators x, z_1, w has the relations (8), (9), $wx = xw$, $wz_1 = z_1 w$, and

$$z_1^{2p} - \alpha_p z_1^p = p^{-p}\alpha_2^p \alpha_0^{2-p} - \alpha_0 w^p, \tag{13}$$

as computed in (5) above. It follows that the center of $C_\Phi[z_1^{-p}]$, which is the centralizer of the generators x and z_1, is precisely $F[z_1^{\pm p}, w]$. From this we immediately obtain the center of C_Φ itself:

Theorem 5.1. *Let Φ be the exponentiation form of a short p-central space $V = Fx + Fy$ of type $\{\rho, \rho^{-1}\}$ in some algebra. Let $\alpha_0 = x^p$, $\alpha_2 = x^{p-2} * y^2$ and $\alpha_p = y^p$. Then the center of the associated Clifford algebra C_Φ is the function ring $Z = F[X, Y]$ of the affine curve*

$$Y(Y - \alpha_p) = \alpha_0 X^p + p^{-p}\alpha_2^p \alpha_0^{2-p}. \tag{14}$$

Proof. The center is generated by $X = -w$ and $Y = z_1^p$, subject only to Relation (13). □

Note that Z is a Dedekind domain iff the curve is smooth, namely when $\operatorname{char} F = 2$ or the discriminant $p^{-p}\alpha_2^p\alpha_0^{2-p} - 4^{-1}\alpha_p^2$ is non-zero.

Moreover, by Theorem 4.12 we have

Corollary 5.2. *$C_\Phi[z_1^{-p}]$ is the symbol Azumaya algebra (α_0, Y) over the center $Z[Y^{-1}]$ under the identification $X = -w$ and $Y = z_1^p$.*

The above treatment suffers from some asymmetry, in that we assume z_1 is invertible. However, one can apply the following formal change of variables: x, y, α_0, α_p remain unchanged, z_1 and z_{-1} are switched, and ρ is replaced by ρ^{-1}; Then w is being replaced by $\rho^{-1}w$.

Noting the sensitivity of the symbol algebra notation to the choice of root of unity, we get the following:

Corollary 5.3. *$C_\Phi[z_{-1}^{-p}]$ is the symbol Azumaya algebra $(\alpha_p - Y, \alpha_0)$ over the center $Z[(\alpha_p - Y)^{-1}]$ under the identification $X = -w$ and $Y = z_1^p$.*

By Corollary 5.2, any simple quotient of C_Φ in which z_1^p is invertible is a central simple algebra C_Φ/IC_Φ over Z/I, where $I \lhd Z$ is an ideal with $Y \notin I$. On the other hand if $z_1^p = 0$ in the quotient, then z_{-1}^p is invertible there by Lemma 4.7, and then the quotient is a quotient of $C_\Phi[z_{-1}^{-p}]$, which is Azumaya by Corollary 5.3, and therefore again a central simple algebra C_Φ/IC_Φ over Z/I, where $Y \in I$.

Corollary 5.4. *C_Φ is an Azumaya algebra.*

In particular:

Theorem 5.5. *The simple quotients of C_Φ are all symbol algebras of degree p: the 'algebra at infinity' $(\alpha_p, \alpha_0)_{p,F}$ and, for every point $(t, s) \in C(\bar{F})$ with $t \neq 0$, the symbol algebra $(\alpha_0, t)_{p,K}$ where $K = F[t, s]$.*

Proof. In every simple quotient, $Z = F[X, Y]$ maps onto an algebraic field extension K of F. Let t and s denote the images of Y and X, respectively, so that $K = F[s, t]$. For $t \neq 0$, the map $z_1^p = Y \mapsto t$ keeps z_1^p invertible, so the respective quotient $C_\Phi/\langle X - s, Y - t\rangle$ is a quotient of $C_\Phi[z_1^{-p}]$ as well, and these are computed in Corollary 5.2.

For $t = 0$, the quotient is generated by (the images of) x and $y = z_1 + z_{-1}$, where $z_{-1}^p = y^p = \alpha_p$ by Lemma 4.1; but $xz_{-1} = \rho z_{-1}x$, so this quotient is the symbol algebra (α_0, α_p). □

Remark 5.6. *Assume z_1 is not invertible in a quotient C of C_Φ. Then C is a matrix algebra iff $\alpha_2 \neq 0$.*

Proof. By assumption, $Y = 0$ in C. If $\alpha_2 \neq 0$, (14) forces $\alpha_0 = (-p\alpha_0\alpha_2^{-1}X)^p$, so $(\alpha_p, \alpha_0)_{p,F}$ splits. If $\alpha_2 = 0$ then $(ax + by)^p = (ax + bz_{-1})^p = \alpha_0 a^p + \alpha_p b^p$, which is isotropic if C is a matrix algebra. □

On passing, we note a minor inaccuracy in [2, Corollary 1.2], which can now be seen as the special case $p = 3$ of Theorem 5.5: the case $s_0 = -(3\omega(1 - \omega)ad)/2$ corresponds to $Y = 0$ in our notation, and requires special treatment as above.

6. The Clifford algebra of a diagonal binary quintic form

In this section we consider 5-central spaces which are short, but of different type than the one discussed above, with a surprisingly different outcome.

Let F be a field of characteristic not 5, containing a fifth root of unity ρ. Let V be an anisotropic two-dimensional 5-central space generating an algebra A over F. Write $V = Fx+Fy$; since the form is anisotropic, x is invertible. Let $\Phi(ax+by) = \alpha_0 a^5+\alpha_1 a^4 b+\alpha_2 a^3 b^2+\alpha_3 a^2 b^3+\alpha_4 ab^4+\beta b^5$ be the exponentiation form of V. In particular, A is a quotient of the Clifford algebra of Φ, and by Proposition 2.1.2 it satisfies the relations $\alpha_i = x^{p-i} * y^i$ for $i = 0, \dots, 5$.

By Corollary 3.2, we may assume $\alpha_1 = x^4 * y = 0$. Generalizing Definition 4.4, let us say that V has type Ω, for $\Omega \subseteq \{\rho, \rho^2, \rho^3, \rho^4\}$, if there is a decomposition $y = \sum_{k\in\Omega} z_k$ such that $z_k x = \rho^k x z_k$ for each k. Following Lemma 3.5, every anisotropic 5-space has some minimal type. If the type is a singleton, then the generated algebra is cyclic by Remark 4.6. Replacing ρ by a suitable power leaves two types of size 2: type $\{\rho, \rho^{-1}\}$ which was analyzed in Sections 4 and 5, and type $\{\rho, \rho^3\}$. From now on we assume the latter, so that

$$y = z_1 + z_3;$$

as indicated above,

$$\begin{aligned} z_1 x &= \rho x z_1, \\ z_3 x &= \rho^3 x z_3. \end{aligned} \tag{15}$$

By Lemma 4.2, it follows that $\alpha_2 = x^3 * y^2 = 0$. Let us consider the next relation, $\alpha_3 = x^2 * (z_1 + z_3)^3$, namely

$$\alpha_3 = x^2 * z_1^3 + x^2 * z_1^2 * z_3 + x^2 * z_1 * z_3^2 + x^2 * z_3^3.$$

Conjugation by x induces a direct sum decomposition of A, with respect to which the four summands in the right-hand side fall into different components. Comparing components, we deduce that $x^2 * z_1^3 = x^2 * z_1 * z_3^2 = x^2 * z_3^3 = 0$, all following tautologically from (15), and

$$\alpha_3 = x^2 * z_1^2 * z_3. \tag{16}$$

Remark 6.1. *If $z_1 = 0$ then $A = F[x, z_3]$ is the cyclic algebra (α, β^2), since $A = F[x, y]$ and $y = z_3$ ρ-commutes with x.*

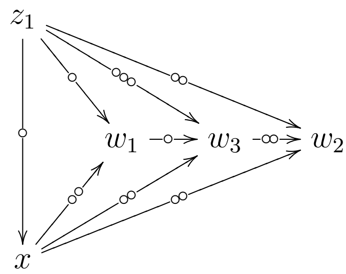

FIGURE 1. Action graph for the generators

Since we are mostly interested in quotients of A which are division algebras, we will assume z_1 is invertible. Notice that $z_1^5 = y^5 - z_3^5$ commutes with both z_3 and x, and so it is central.

Consider the linear map $T : A \to A$ defined by $T(t) = z_1^2 t - (\rho + \rho^2) z_1 t z_1 + \rho^3 t z_1^2$, so that $T(t) z_1^{-2}$ is the combination of conjugates $z_1^2 t z_1^{-2} - (\rho + \rho^2) z_1 t z_1^{-1} + \rho^3 t$. By computation, for every $t \in A$ such that $tx = \rho^3 xt$, we have that $x^2 * z_1^2 * t = (1 - \rho^3)(1 - \rho^4) x^2 T(t)$, so Equation (16) becomes $T(z_3) = (1 - \rho^3)^{-1}(1 - \rho^4)^{-1} x^{-2} \alpha_3$.

Consider $w_3 = c z_1^{-2} x^{-2}$ where $c = \frac{\alpha_3}{5\rho^2}$. Since $T(w_3) = (1 - \rho^3)(1 - \rho^4) c x^{-2} = (1 - \rho^3)^{-1}(1 - \rho^4)^{-1} \alpha_3 x^{-2}$, we obtain for $z_3' = z_3 - w_3$ that $T(z_3') = 0$.

Because of the factorization $\lambda^2 - (\rho + \rho^2)\lambda + \rho^3 = (\lambda - \rho)(\lambda - \rho^2)$, $T(z_3') = 0$ provides by Lemma 3.3 a decomposition $z_3' = w_1 + w_2$, where $z_1 w_i = \rho^i w_i z_1$ for $i = 1, 2$. By our choice of w_3, we have a decomposition

$$z_3 = w_1 + w_2 + w_3$$

with $z_1 w_i = \rho^i w_i z_1$ for $i = 3$ as well.

Remark 6.2. *The conjugation maps by x and by z_1 commute, so the eigenvectors w_i with respect to z_1 satisfy*

$$w_i x = \rho^3 x w_i \tag{17}$$

for $i = 1, 2, 3$.

Since $w_3 = c z_1^{-2} x^{-2}$ is defined in terms of x and z_1, one easily checks that $w_1 w_3 = \rho w_3 w_1$ and $w_3 w_2 = \rho^2 w_2 w_3$. Figure 1 provides an action graph for the elements of A mentioned thus far: the relation $uv = \rho^i vu$ is depicted by an arrow $u \longrightarrow v$ with i beads (we could draw a reverse arrow with $5 - i$ beads).

Remark 6.3. *A subset $S \subseteq A$ is called a p-set, if $s^p \in F^\times$ for every $s \in S$, and all commutators $s_1 s_2 s_1^{-1} s_2^{-1}$ are powers of ρ (see* [14, pp. 248–251] *for a refined definition). The generated subalgebra $F[S]$, whose center may strictly contain F, is then a tensor product of at most $|S|/2$ cyclic algebras of degree p.*

If $w_1 = 0$ then A is generated by the 5-set $\{x, z_1, w_2\}$, and therefore it is a cyclic algebra of degree 5 over a 5-dimensional extension of F. We shall assume from now on that w_1 is invertible.

We come to the final relation, $\alpha_4 = x * y^4 = x * (z_1 + z_3)^4 = x * (z_1 + w_1 + w_2 + w_3)^4$, namely

$$\alpha_4 = \sum_{i_1+i_2+i_3+j=4} x * w_1^{i_1} * w_2^{i_2} * w_3^{i_3} * z_1^j. \tag{18}$$

Conjugation by x, using (17), breaks (18) into 5 equations:

$$\sum_{i_1+i_2+i_3=4-j} x * w_1^{i_1} * w_2^{i_2} * w_3^{i_3} * z_1^j = \begin{cases} \alpha_4 & j = 1, \\ 0 & j = 0, 2, 3, 4. \end{cases}$$

The equations for $j \neq 1$ are tautological. Indeed, for $j = 0$ and $j = 4$ we get $x * z_1^4 = x * z_3^4 = 0$. For $j = 2$ one writes

$$x * w_s * w_{s'} * z_1^2 = f_{ss'} w_s w_{s'} z_1^2 x;$$

for suitable $f_{ss'} \in \mathbb{Z}[\rho]$ $(s, s' = 1, 2, 3)$; it then turns out that $f_{ss'} = 0$ unless precisely one of s, s' is 3. But $f_{13} + \rho^4 f_{31} = f_{23} + \rho^2 f_{32} = 0$, so the relations $w_3 w_s = \rho^{2(3-s)} w_s w_3$ shows that $x * w_s * w_{s'} * z_1^2 = 0$ tautologically for every $s, s' = 1, 2, 3$. For the case $j = 3$ one computes that $x * w_s * z_1^3 = 0$ for $s = 1, 2, 3$. The only remaining case is $j = 1$, which translates (18) to

$$\sum_{i_1+i_2+i_3=3} x * w_1^{i_1} * w_2^{i_2} * w_3^{i_3} * z_1 = \alpha_4.$$

Splitting this further by conjugation by z_1, we obtain the five relations

$$x * w_3^3 * z_1 + x * w_1^2 * w_2 * z_1 = \alpha_4 \tag{19}$$
$$x * w_1^3 * z_1 + x * w_2 * w_3^2 * z_1 = 0 \tag{20}$$
$$x * w_2^2 * w_3 * z_1 + x * w_1 * w_3^2 * z_1 = 0 \tag{21}$$
$$x * w_1 * w_2 * w_3 * z_1 + x * w_2^3 * z_1 = 0 \tag{22}$$
$$x * w_1 * w_2^2 * z_1 + x * w_1^2 * w_3 * z_1 = 0 \tag{23}$$

Calculating with the ρ-commutation relations, (20), (21) and (22) are tautologically satisfied. Opening up the remaining two equations, noting that each pair of generators except (possibly) for w_1, w_2 are ρ-commuting, we get

$$\begin{aligned} -5\rho^2 w_3^3 + (1-\rho)(1-\rho^2)w_1^2 w_2 \\ +\rho(1-\rho)^2 w_1 w_2 w_1 + \rho(1-\rho)(1-\rho^2)w_2 w_1^2 \end{aligned} = \alpha_4 x^{-1} z_1^{-1}, \tag{24}$$

$$\begin{aligned} (1-\rho)(1-\rho^3)w_1 w_2^2 + (1-\rho)(1-\rho^4)w_2 w_1 w_2 \\ +(1-\rho^2)(1-\rho^4)w_2^2 w_1 - 5\rho(1+\rho)w_1^2 w_3 \end{aligned} = 0. \tag{25}$$

Write $w_2 = w_2' + c' w_1^{-2} x^{-1} z_1^{-1}$, where $c' = \frac{\alpha_4}{5(1+\rho^3)} + \frac{\alpha_3^3}{25\alpha_0 z_1^5}$. Substituting $w_3 = c z_1^{-2} x^{-2}$ in (24) and dividing by $(1-\rho)(1-\rho^2)$, we obtain

$$w_1^2 w_2' + (-\rho^2 - \rho^4) w_1 w_2' w_1 + \rho w_2' w_1^2 = 0.$$

As before, the associated polynomial $\lambda^2 - (\rho^2 + \rho^4)\lambda + \rho$ factors as $(\lambda - \rho^2)(\lambda - \rho^4)$, so Lemma 3.3 provides the decomposition $w_2' = v_1 + v_2$ where $v_1, v_3 \in A$ satisfy $v_i w_1 = \rho^i w_1 v_i$ for $i = 1, 3$. Taking $v_2 = c' w_1^{-2} x^{-1} z_1^{-1}$, we get

$$w_2 = v_1 + v_2 + v_3, \tag{26}$$

where

$$v_i w_1 = \rho^i w_1 v_i$$

for $i = 1, 2, 3$. By definition of v_2 we also have that $v_2 v_1 = \rho^{-2} v_1 v_2$ and $v_2 v_3 = \rho^2 v_3 v_2$.

Remark 6.4. *Since conjugation by x, by z_1 and by w_1 commute, the eigenvectors v_i satisfy*

$$\begin{aligned} x v_i &= \rho^2 v_i x, \\ z_1 v_i &= \rho^2 v_i z_1 \end{aligned}$$

for $i = 1, 2, 3$; consequently

$$w_3 v_i = \rho^2 v_i w_3.$$

A refined diagram of the commutation relations between the generators $x, z_1, w_1, w_3, v_1, v_2, v_3$ is given as Figure 2.

It remains to solve (25). Dividing by $(1-\rho)(1-\rho^3)$ we obtain

$$w_1 w_2^2 - \rho^2(1+\rho^2) w_2 w_1 w_2 + \rho w_2^2 w_1 + (1-\rho^2)^2 w_1^2 w_3 = 0. \tag{27}$$

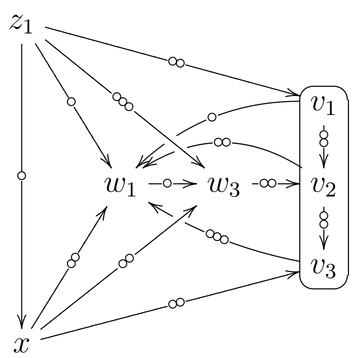

FIGURE 2. A refined action graph for the generators: an arrow to the framed zone depicts same action on v_1, v_2, v_3

We substitute (26) into (27), and collect homogeneous components with respect to conjugation by w_1:

$$\begin{aligned}
w_1v_1^2 - \rho^2(1+\rho^2)v_1w_1v_1 + \rho v_1^2 w_1 &= 0,\\
w_1v_3^2 - \rho^2(1+\rho^2)v_3w_1v_3 + \rho v_3^2 w_1 &= 0,\\
w_1v_2^2 - \rho^2(1+\rho^2)v_2w_1v_2 + \rho v_2^2 w_1 & \\
+w_1v_1v_3 - \rho^2(1+\rho^2)v_1w_1v_3 + \rho v_1v_3w_1 &= -(1-\rho^2)^2 w_1^2 w_3,\\
+w_1v_3v_1 - \rho^2(1+\rho^2)v_3w_1v_1 + \rho v_3v_1w_1 &
\end{aligned}$$

$$\begin{aligned}
w_1v_1v_2 - \rho^2(1+\rho^2)v_1w_1v_2 + \rho v_1v_2w_1 + w_1v_2v_1 - \rho^2(1+\rho^2)v_2w_1v_1 + \rho v_2v_1w_1 &= 0,\\
w_1v_3v_2 - \rho^2(1+\rho^2)v_3w_1v_2 + \rho v_3v_2w_1 + w_1v_2v_3 - \rho^2(1+\rho^2)v_2w_1v_3 + \rho v_2v_3w_1 &= 0.
\end{aligned}$$

Plugging in the fact that $v_2 = c'w_1^{-2}x^{-1}z_1^{-1}$ and the relations satisfied by w_1, v_1 and by w_1, v_3, the first two and final two equations vanish, and the third one becomes

$$(1-\rho)(1+\rho^2)w_1v_2^2 - \rho^3 w_1v_1v_3 + w_1v_3v_1 = -(1-\rho^2)w_1^2w_3.$$

Dividing by w_1 from the left and noting that $v_2^2 = \rho^3 c'^2 w_1^{-4} z_1^{-2} x^{-2}$, we obtain

$$v_3v_1 - \rho^3 v_1v_3 = -[(1-\rho)(1+\rho^2)\rho^3 c'^2 w_1^{-5} + (1-\rho^2)c]w_1 z_1^{-2} x^{-2}. \tag{28}$$

If $v_1 = 0$ then A is generated by the 5-set $\{x, z_1, w_1, v_3\}$ and is a tensor product of two cyclic algebras of degree 5, see below.

Assume v_1 is invertible. Let $u_1 = c''v_1^{-1}w_1z_1^{-2}x^{-2}$ where $c'' = \rho^2(1+\rho^3)^2 w_1^{-5} c'^2 - \rho^4 c$, and write $v_3 = u_1 + u_2$; then Equation (28) becomes

$$v_1u_2 = \rho^2 u_2 v_1,$$

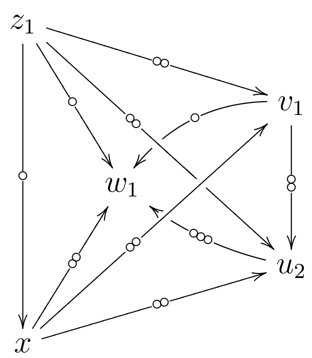

FIGURE 3. A final action graph

so we have that $v_1 u_i = \rho^i u_i v_1$ for $i = 1, 2$.

Remark 6.5. *Since conjugation by x, by z_1, by w_1 and by v_1 commute, u_2 satisfies*

$$\begin{aligned} xu_2 &= \rho^2 u_2 x \\ z_1 u_2 &= \rho^2 u_2 z_1 \\ u_2 w_1 &= \rho^3 w_1 u_2. \end{aligned}$$

In particular A is generated by the 5-set $\{x, z_1, w_1, v_1, u_2\}$, and is a tensor product of one or two cyclic algebras of degree 5 (generically two, as we see below). The commutation relations of the final generators, with the artificial ones, w_3, v_2, u_1, omitted, are given in Figure 3.

In summary, we proved:

Theorem 6.6. *Let V be an anisotropic two-dimensional 5-central space of type $\{\rho, \rho^3\}$, generating a division algebra A. Then A is a product of one or two cyclic division algebras of degree 5, whose center is some field extension of F.*

Proof. We keep the notation given above. Decompose $y = z_1 + z_3$ where z_k are eigenvectors of x as above.

(1) The case $z_1 = 0$ gives $A = F[x, z_3^2]$ where for the rest of this proof we understand that these are standard generators: the multiplicative commutator is ρ; so assume $z_1 \neq 0$.
(2) Decompose $z_3 = w_1 + w_2 + w_3$. If $w_1 = 0$ then $A = K[x, z_1]$ where $K = F[z_1^5, x^{-2} z_1^2 w_2]$; so assume $w_1 \neq 0$.

(3) Decompose $w_2 = v_1 + v_2 + v_3$. If $v_1 = 0$ and $v_3 = 0$ then $A = K[x, z_1]$, were $K = F[z_1^5, w_1^5, x^{-1}z_1^2 w_1]$.
(4) If $v_1 = 0$ and $v_3 \neq 0$ then $A = K[x, z_1] \otimes_K K[x^{-1}z_1^2 w_1, x^{-2}z_1^2 v_3]$, were $K = F[z_1^5, w_1^5, v_3^5]$.
(5) Finally if $v_1 \neq 0$, decompose $v_3 = u_1 + u_2$, and then $A = K[x, z_1] \otimes K[x^{-2}z_1^2 v_1, x^{-1}z_1^2 w_1]$ where $K = F[z_1^5, v_1^5, w_1^5, x^{-1}z_1^{-2}w_1^2 v_1 u_2]$.

□

Note that in each case the extension $K[x]/K$ splits (at least) one of the cyclic components.

Corollary 6.7. *Let V be an anisotropic 5-central space of type $\{\rho, \rho^3\}$ in an algebra A. Then every quotient division algebra of the Clifford algebra of V is either cyclic of degree 5 or a tensor product of two cyclic algebras of degree 5.*

The assumption that $y = z_1 + z_3$ forces $\alpha_1 = \alpha_2 = 0$ in the exponentiation form. In order to present A in terms of the exponentiation form of V, we need to compute quantities such as z_3^5. Remark 4.1 enables us to do so when z_3 is a sum of two ρ-commuting elements, but there is no analogous formula for more than two summands. Recall that the artificial summands w_3, v_2 and u_1 were defined in terms of constants $c = \frac{\rho^3\alpha_3}{5}$, $c' = \frac{(1+\rho+\rho^2)\alpha_4}{5} + \frac{\alpha_3^3}{25\alpha_0 z_1^5}$ and $c'' = \rho^2(1+\rho^3)^2 w_1^{-5}c'^2 - \rho^4 c$. Assuming $\alpha_3 = \alpha_4 = 0$, we find that $w_3 = 0$, $v_2 = 0$ and $u_1 = 0$. This enables us to formulate the final result.

Theorem 6.8. *Assume in Theorem 6.6 that the exponentiation form of V is diagonal, namely $\Phi(ax + by) = \alpha a^5 + \beta b^5$ for suitable $\alpha, \beta \in F$. Then one of the following holds for the algebra A generated by V:*
(1) $A = (\alpha, \beta^2)_F$.
(2) $A = (\alpha, t)_K$ *where* $K = F(t, s)$ *and* $s^5 = \alpha^3 t^2(\beta - t)$.
(3) $A = (\alpha, t)_K$ *where* $K = F(t, s)$ *and* $s^5 = \alpha^{-1}t^2(\beta - t)$.
(4) $A = (\alpha, t)_K \otimes_K (t', t'')_K$ *where* $K = F(t, t', t'')$ *and* $t^3 + \alpha t' + \alpha^2 t'' = \beta t^2$.
(5) $A = (\alpha, t)_K \otimes_K (t', t'')_K$ *where* $K = F(t, t', t'', s)$, *and* $s^5 = \alpha^3 t t' t''^2(\beta t^2 - t^3 - \alpha^2 t t' - \alpha t'')$.

Proof. In the notation of this section, the assumption that Φ is diagonal, namely, that $\alpha_3 = \alpha_4 = 0$, implies $c = c' = c'' = 0$, and so (when these elements are defined) $w_3 = 0$, $v_2 = 0$ and $u_1 = 0$.

Following the proof of Theorem 6.6, there are four cases:

(1) $z_1 = 0$. Then $y = z_3$ and A is generated by $x \longleftarrow\!\circ\!\!- y^2$. Henceforth $z_1 \neq 0$.
(2) $w_1 = 0$, so that $z_3 = w_2$. Thus $\beta = y^5 = (z_1 + z_3)^5 = z_1^5 + z_3^5$. Take $t = z_1^5$ and $s = x^3 z_1^2 z_3$. Then $K = F[t, s]$, and $t + \alpha^{-3} t^{-2} s^5 = \beta$. Henceforth $w_1 \neq 0$.
(3) $v_1 = 0$, so that $w_2 = v_3 = u_2$. Assume $v_3 = 0$. Let $t = z_1^5$. Then $A = (\alpha, t)_K$ and $K = F[t, s]$ by Theorem 6.6, where $s = x^{-1} z_1^2 w_1$ and $\beta = y^5 = z_1^5 + (w_1 + w_2)^5 = t + \alpha t^{-2} s^5$.
(4) $v_1 = 0$ and $v_3 \neq 0$. Let $t = z_1^5$, $t' = \alpha^{-1} t^2 w_1^5$ and $t'' = \alpha^{-2} t^2 v_3^5$. Then $A = (\alpha, t)_K \otimes_K (t', t'')_K$ and $K = F[t, t', t'']$ by Theorem 6.6, and $\beta = y^5 = z_1^5 + (w_1 + w_2)^5 = t + \alpha t^{-2} t' + \alpha^2 t^{-2} t''$.
(5) Assuming $v_1 \neq 0$, let $t = z_1^5$, $t' = \alpha^{-2} t v_1^5$, $t'' = \alpha^{-1} t^2 w_1^5$ and $s = x^{-1} z_1^8 w_1^2 v_1 u_2$. Then $\beta = z_1^5 + z_3^5 = z_1^5 + w_1^5 + w_2^5 = z_1^5 + v_1^5 + w_1^5 + u_2^5 = t + \alpha^2 t^{-1} t' + \alpha t^{-2} t'' + \alpha^{-3} t^{-3} t'^{-1} t''^{-2} s^5$, $A = (\alpha, t)_K \otimes_K (t', t'')_K$ and $K = F[t, t', t'', s]$.

□

Finally we observe that, in a sense, every cyclic algebra of degree 5 and every product of two cyclic algebras of degree 5 is a quotient of a Clifford algebra of a binary diagonal quintic form.

Theorem 6.9. *Let k be a field of characteristic not 5 containing 5th roots of unity.*

Let A' be a division algebra over an arbitrary extension K'/k, which is either cyclic, or a product of two cyclic algebras, containing a non-central element whose 5th power is in k.

Then A' is a scalar extension of a quotient of the Clifford algebra of some binary diagonal quintic form defined over an intermediate field $k \subseteq F \subseteq K'$, such that F is generated by a single element over k.

Proof. Let $x \in A'$ be an element such that $x^5 = \alpha \in k^\times$. If $\deg(A') = 5$ write $A' = (\alpha, t)_{K'}$ for $t \in K'$; let $\beta = \alpha^{-3} t^{-2} + t$ and let $F = k(\beta)$ and $K = F(t)$. Let $z_1 \in A'$ be an element such that $z_1^5 = t$ and $z_1 x = \rho x z_1$, and reverse the computation in Theorem 6.8.(2) by taking $z_3 = z_1^{-2} x^{-3}$, $y = z_1 + z_3$ and $V = Fx + Fy$. Then $A = K[x, z_1]$ is a quotient of the Clifford algebra of V over F, and $A' = K'A$.

If $\deg(A') = 5^2$, write $A' = (\alpha, t) \otimes (t', t'')$ for $t, t', t'' \in K'$, and take $\beta = t + \alpha t^{-2} t' + \alpha^2 t^{-2} t''$, $F = k(\beta)$ and $K = F(\beta, t, t', t'')$. In a similar manner, solving for z_1, w_1 and w_2 as in Theorem 6.8.(3), and letting $y = z_1 + w_1 + w_2$, $A = (\alpha, t)_K \otimes_K (t', t'')_K$ is a quotient of the Clifford algebra of $V = Fx + Fy$, and $A' = K'A$. □

Remark 6.10. *Let C be the Clifford algebra of an anisotropic 5-central space of type $\{\rho, \rho^3\}$ in an algebra A, and assume the exponentiation form is diagonal. Let $x, y, z_1, z_3 \in C$ be as before. Let $C' = C[z_1^{-5}]$. Let $w_1, w_2 \in C'$ be as before. Let $C'' = C'[w_1^{-5}]$. Let $v_1, v_3 \in C''$ be as before. Then $C''[v_1^{-5}]$ and $C''[v_3^{-5}]$ are Azumaya.*

The remark follows from Theorem 6.8 because the only quotients come from cases (4) and (5) and are central simple algebras of degree 5^2. However:

Corollary 6.11. *The Clifford algebra of an anisotropic 5-central space of type containing $\{\rho, \rho^3\}$ is in general not Azumaya.*

Indeed, one may choose the fields in Theorem 6.9 so that quotient division algebras exists both of degree 5 and 25.

References

[1] L. E. Dickson, *Linear associative algebras and abelian equations*, Trans. Amer. Math. Soc. **15**(1), 31–46, (1914).

[2] D. E. Haile, *On the Clifford algebra of a binary cuibc form*, Amer. J. Math. **106**(6), 1269–1280, (1984).

[3] D. E. Haile, *When is the Clifford algebra of a binary cubic form split?*, J. Algebra **146**(2), 514–520, (1992).

[4] D. E. Haile and S. Tesser, *On Azumaya algebras arising from Clifford algebras*, J. Algebra **116**(2), 372–384, (1988).

[5] N. Heerema, *An algebra determined by a binary cubic form*, Duke Math. J. **21**, 423–444, (1954).

[6] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, "The book of involutions", American Mathematical Society Colloquium Publications **44**, American Mathematical Society, 1998.

[7] R. S. Kulkarni, *On the Clifford algebra of a binary form*, Trans. Amer. Math. Soc. **355**(8), 3181–3208, (2003).

[8] R. S. Kulkarni, *The extension of the reduced Clifford algebra and its Brauer class*, Manuscripta Math. **112**(3), 297–311, (2003).

[9] T. Y. Lam, "The Algebraic Theory of Quadratic Forms", W. A. Benjamin, Inc., 1973.

[10] E. Matzri, "Azumaya Algebras", Master's thesis, Bar-Ilan University, 2004.

[11] E. Matzri, L.H. Rowen and U. Vishne, *Non-cyclic algebras with n-central elements*, Proc. Amer. Math. Soc. **140**(2), 513–518, (2012).

[12] Ph. Revoy, *Algèbres de Clifford et algèbres extérieures*, J. Algebra **46**(1), 268-277, (1977).

[13] N. Roby, *Algèbres de Clifford des formes polynomes*, C. R. Acad. Sci. Paris Se'r. I. Math. A **268**, A484–A486, (1969).

[14] L.H. Rowen, "Ring Theory", Vol. II, Academic Press, New York, 1988.

[15] S. Tesser, *Representations of a Clifford algebra that are Azumaya algebras and generate the Brauer group*, J. Algebra **119**(2), 265-281, (1988).

[16] J. H. M. Wedderburn, *A type of primitive algebra*, Trans. Amer. Math. Soc. **15**(2), 162–166, (1914).