QUADRATIC ELEMENTS IN A CENTRAL SIMPLE ALGEBRA OF DEGREE FOUR

MARKUS ROST

Contents

Introduction

By a theorem of Albert [1, Theorem 11.9] a central simple algebra A of degree 4 contains a biquadratic subalgebra. The major point is to prove the existence of a quadratic subalgebra. See [2] for a short proof.

One can show this also using the fact from projective geometry that, given 4 generic lines in 3-space, there are exactly 2 lines which meet them all. Namely, for any (possibly non-split) A one considers a maximal commutative separable subalgebra H of A and a generic element $x \in A$. Such data determine geometrically 4 lines in projective 3-space: The subalgebra H determines geometrically 4 points and for each of these points there is the line through it and its image under x. The 2 lines which meet all those lines determine a quadratic subalgebra L of A.

It seems to be rather complicated to give explicit generators for L in terms of H and x, in particular in characteristic 2 (cf. Section 4).

However there is a way to construct quadratic elements (described in Sections 1-2) which is algebraically simpler. This construction is symmetric with respect to reversing the product in A (i. e., replacing A with A^{op}). It works smoothly for central simple algebras A of degree 4 with involution of second kind and the base ring can be any local ring. A geometric interpretation is given in Section 5.

Once a quadratic subalgebra L is at hand, it easy to extend it to a biquadratic subalgebra: Let y be a generic element in the orthogonal complement of the centralizer of L. Then L and y^2 generate a biquadratic subalgebra. See Section 3.

In the Appendix we have added (mainly for fun) some formulas for the coefficients of the characteristic polynomial in a central simple algebra of degree 4. They occurred when trying to establish Lemma 1.

Date: May 30, 2003.

1. Preliminaries

Let F be a field and let A be a central simple algebra of degree 4 over F. For the characteristic polynomial of $x \in A$ we use the notation

$$N(t-x) = t^4 - T(x)t^3 + Q(x)t^2 - S(x)t + N(x)$$

where $N\colon A \to F$ is the reduced norm of A.

For $x \in A$ we consider the linear form

$$\Phi(x)\colon \Lambda^3 A \to F$$
$$\Phi(x)(y_1 \wedge y_2 \wedge y_3) = T(xy_3xy_2xy_1 - xy_1xy_2xy_3)$$

Lemma 1. *For x, $y \in A$ one has*

$$S(xy - yx) = \Phi(x)(1 \wedge y \wedge y^2)$$

Proof. This amounts to

$$S(xy - yx) = T(x^2y^2xy - x^2yxy^2)$$

To prove this identity it suffices to consider the case $A = M_4(\mathbf{Q})$. One has

$$6S(u) = T(u)^3 - 3T(u^2)T(u) + 2T(u^3)$$

as can be easily seen from the case of diagonal matrices. Thus, if $T(u) = 0$ one has

$$3S(u) = T(u^3)$$

and the claim follows from this with $u = xy - yx$ and from $T(vw) = T(wv)$. □

Remark 1. The formula for S in Lemma 4 in the Appendix yields a "denominator free" proof of Lemma 1.

2. Construction of quadratic elements

Let H be a commutative subalgebra of A of dimension 4 and let $x \in A$.

The form $\Phi(x)$ restricts to a linear form $\Lambda^3 H \to F$. We consider the associated dual map

$$\alpha(x)\colon \Lambda^4 H \to H$$

defined by

$$\mu \wedge \alpha(x)(\omega) = \Phi(x)(\mu)\omega \tag{1}$$

for $\mu \in \Lambda^3 H$ and $\omega \in \Lambda^4 H$.

We fix a basis element $\omega \in \Lambda^4 H$ and write $\alpha = \alpha(x)(\omega)$.

Corollary 1. *Let*

$$\rho = \rho(x) = x\alpha - \alpha x$$

Then

$$T(\rho) = S(\rho) = 0$$

Proof. Clearly $T(\rho) = 0$ since ρ is a commutator. From Lemma 1 and (1) we get

$$S(\rho)\omega = 1 \wedge \alpha \wedge \alpha^2 \wedge \alpha = 0$$

□

Let us write

$$\Delta(x) = Q(\rho)^2 - 4N(\rho)$$

Corollary 2. *Let*

$$\theta = \theta(x) = \rho^2$$

One has

$$\theta^2 + Q(\rho)\theta + N(\rho) = 0$$

The characteristic polynomial of θ is

$$\big(t^2 + Q(\rho)t + N(\rho)\big)^2$$

Let $x \in A$ with $\Delta(x) \neq 0$. Then $\theta(x)$ generates a uniform quadratic subalgebra of A. (A quadratic subalgebra L of A is called uniform if it is separable and if A is as L-module of constant rank 8.)

Proof. The first claim is clear from Corollary 1. The second claim follows from

$$N(t^2 - \theta) = N(t-\rho)N(t+\rho) = \big(t^4 + Q(\rho)t^2 + N(\rho)\big)^2$$

The final claim is then clear as well. □

Suppose $(A, H) = \big(M_4(F), D_4(F)\big)$ where $D_4(F)$ denotes the 4×4 diagonal matrices. Write $H = e_1F \oplus e_2F \oplus e_3F \oplus e_4F$ with e_i the standard idempotents. Then, with $\omega = e_1 \wedge e_2 \wedge e_3 \wedge e_4$,

$$\alpha(x)(\omega) = \operatorname{diag}\begin{pmatrix} x_{23}x_{34}x_{42} - x_{24}x_{43}x_{32} \\ x_{31}x_{14}x_{43} - x_{34}x_{41}x_{13} \\ x_{41}x_{12}x_{24} - x_{42}x_{21}x_{14} \\ x_{13}x_{32}x_{21} - x_{12}x_{23}x_{31} \end{pmatrix} \tag{2}$$

For

$$x = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{3}$$

one finds $\Delta(x) = 1$.

Corollary 3 (Albert)**.** *There exists a uniform quadratic subalgebra in A.*

Proof. Choose some H, ω as above with H separable. By Corollary 2 it suffices to find $x \in A$ with $\Delta(x) \neq 0$.

As the computation for (3) shows, the polynomial $\Delta(x)$ is nonzero. Hence if F is infinite, there exists x with $\Delta(x) \neq 0$.

If F is finite, then $A = M_4(F)$ and the claim is clear anyway. □

Remark 2. Note that we have made no assumption on the characteristic on F. In fact, everything works over an arbitrary local ring.

Remark 3. Everything extends easily to the case of a central simple algebra of degree 4 with involution of second kind.

Remark 4. One has $\alpha(x+h) = \alpha(x)$ for $h \in H$. Thus $x \mapsto \alpha(x)$ is a cubic form on A/H with values in $\operatorname{Hom}(\Lambda^4 H, H)$.

3. Existence of biquadratic subextensions

Let L be a uniform quadratic subalgebra in A and let $\theta \in L$ be a generator.

Lemma 2. *For $y \in A$ let*

$$\sigma = \sigma(y) = y\theta - \theta y$$

Then

$$T(\sigma) = S(\sigma) = 0$$

Let

$$\Delta'(y) = Q(\sigma)^2 - 4N(\sigma)$$

Let $y \in A$ with $\Delta'(y) \neq 0$. Then θ and $\sigma(y)^2$ generate a biquadratic subalgebra of A.

Suppose $A = M_4(F)$,

$$\theta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

and

$$y = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Then $\Delta'(y) = 1$.

Proof. This can be shown by inspection in the split case. Suppose $A = M_4(F)$ and that L is the subalgebra of matrices of the form

$$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \end{pmatrix}$$

Then a commutator $\sigma = y\theta - \theta y$ is of the form

$$\sigma = \begin{pmatrix} 0 & U \\ V & 0 \end{pmatrix}$$

with $U, V \in M_2(F)$. The characteristic polynomial of σ is

$$t^4 - t^2 \operatorname{trace}(UV) + \det(UV)$$

and one has

$$\sigma^2 = \begin{pmatrix} UV & 0 \\ 0 & VU \end{pmatrix}$$

The element σ^2 commutes with the elements of L and generates together with L a biquadratic subalgebra as long as $\big(\operatorname{trace}(UV)\big)^2 \neq 4\det(UV)$. The last claim is easy to check. $\square$

Corollary 4 (Albert). *There exists a biquadratic subalgebra in A.*

Proof. If F is finite, then $A = M_4(F)$ and the claim is clear. Otherwise one chooses L and θ as above and picks y with $\Delta'(y) \neq 0$ (cf. Corollary 3 and its proof). $\square$

4. More quadratic elements

We have seen that for generic x the element $\theta(x)$ generates a uniform quadratic subalgebra L. The centralizer Q of L is a quaternion algebra over L.

In the following we give a description of generators for Q. This appears to be somewhat complicated.

We assume $\operatorname{char} F \neq 2$.

For $x \in A$ consider the linear form

$$\varphi(x)\colon \Lambda^3 H \to F$$
$$\varphi(x)(\mu) = \sum_{s \in \mathcal{S}_3} \operatorname{sgn}(s) T(x^2 h_{s(3)} x h_{s(2)} x h_{s(1)}) - 2T(x)\Phi(x)(\mu)$$

with $\mu = h_1 \wedge h_2 \wedge h_3$, $h_i \in H$, and let

$$\beta(x)\colon \Lambda^4 H \to H$$

be the linear map with

$$\mu \wedge \beta(x)(\omega) = \varphi(x)(\mu)\omega$$

for $\mu \in \Lambda^3 H$ and $\omega \in \Lambda^4 H$.

Let further

$$\psi(x),\ \psi'(x)\colon \Lambda^4 H \to A$$
$$\psi(x) = x\alpha(x) + \frac{1}{2}\beta(x)$$
$$\psi'(x) = \alpha(x)x + \frac{1}{2}\beta(x)$$

We fix a basis element $\omega \in \Lambda^4 H$ and write $\psi = \psi(x)(\omega)$, $\psi' = \psi'(x)(\omega)$.

Let Q be the subalgebra of A generated by ψ and ψ'. Note that $\rho = \psi - \psi' \in Q$. Let $L \subset Q$ be the subalgebra generated by $\theta = \rho^2$.

Lemma 3. *One has $\psi^2 = \psi'^2 \in F$. The algebra L is in the center of Q.*

Suppose H is separable. Then for generic x, L is a uniform quadratic subalgebra of A and Q is the centralizer of L in A.

Proof. I know only a tiresome check in the split case $(A, H) = \big(M_4(F), D_4(F)\big)$. $\square$

5. Geometric interpretation

There is an interpretation of our construction in terms of a classical theorem in projective geometry: For 4 generic lines in $\mathbf{P}^3$ there exist exactly 2 lines meeting them all.

Let V be a 4-dimensional vector space, let $A = \operatorname{End}(V)$, let $V = V_1 \oplus V_2 \oplus V_3 \oplus V_4$ be a decomposition into 1-dimensional subspaces and H be the subalgebra of elements $h \in A$ with $h(V_i) \subset V_i$, $i = 1, 2, 3, 4$. Let further $x \in A$ be a generic element.

In the projective space $\mathbf{P}(V)$ let L_i be the line through the points $[V_i]$, $[xV_i]$ and let K_1, K_2 be the lines meeting every L_i.

The lines K_1, K_2 are in fact given by the 2 2-dimensional eigenspaces of the element $\psi(x)$ above.

Let $V^* = V_1^* \oplus V_2^* \oplus V_3^* \oplus V_4^*$ be the dual decomposition of the dual space (i.e., $V_i^*(V_j) = \delta_{ij} F$).

In the projective space $\mathbf{P}(V^*)$ let L'_i be the line through the points $[V_i^*]$, $[V_i^* x]$ and let K'_1, K'_2 be the lines meeting every L'_i.

The lines K'_1, K'_2 are in fact given by the 2 2-dimensional eigenspaces of the element $\psi'(x)$ above.

Every line L in $\mathbf{P}(V^*)$ defines a line L^* in $\mathbf{P}(V)$. Let S_1, S_2 be the two lines which meet all of K_1, K_2, $(K'_1)^*$, $(K'_2)^*$.

The lines S_1, S_2 are in fact given by the 2 2-dimensional eigenspaces of the element $\theta(x)$ above.

There is also an interpretation of the element $\rho = \rho(x)$. Since ρ^2 is the identity on S_i, the element ρ is an involution on each S_i. An involution on a line is given by a pair of points. How to get a pair of points on S_i? We have two pairs of points already: the intersections of S_i with K_1, K_2 and with $(K'_1)^*$, $(K'_2)^*$, respectively. Now a pair of points on a line gives a point in the 2-fold symmetric product of the line, a $\mathbf{P}^2$. The diagonal embedding of the line to that $\mathbf{P}^2$ identifies it with a conic. Thus the two pairs of points determine a line in $\mathbf{P}^2$, which intersects the conic in a pair of points. This yields certainly the pair given by ρ (I haven't really checked this).

Appendix

Lemma 1 follows also from the additivity rule for S in the following Lemma.

Lemma 4. *For $x, y \in A$ one has*

$$\begin{aligned}
T(x+y) &= T(x) + T(y) \\
Q(x+y) &= Q(x) + T(x)T(y) - T(xy) + Q(y) \\
S(x+y) &= S(x) + Q(x)T(y) - T(x)T(xy) + T(x^2y) \\
&\quad + T(x)Q(y) - T(xy)T(y) + T(xy^2) + S(y) \\
N(x+y) &= N(x) + S(x)T(y) - Q(x)T(xy) + T(x)T(x^2y) - T(x^3y) \\
&\quad + Q(x)Q(y) - T(x)T(xy)T(y) + T(x)T(xy^2) + T(x^2y)T(y) \\
&\qquad + Q(xy) - T(x^2y^2) \\
&\quad + T(x)S(y) - T(xy)Q(y) + T(xy^2)T(y) - T(xy^3) + N(y)
\end{aligned}$$

Proof. In the power series ring $A[[t]]$ one has

$$1 + t(x+y) = (1+tx)\big[1 - t^2 \frac{x}{1+tx}\frac{y}{1+ty}\big](1+ty)$$

The middle term expands as follows:

$$1 - t^2\frac{x}{1+tx}\frac{y}{1+ty} = 1 - t^2xy + t^3x(x+y)y - t^4x(x^2+xy+y^2)y + \cdots$$

Taking norms gives in $F[[t]]/(t^5)$

$$\begin{aligned}
N\big(1+t(x+y)\big) = N(1+tx)N(1+ty)\big[1 &- t^2T(xy) + t^3T(x^2y+xy^2) \\
&+ t^4\big(Q(xy) - T(x^3y + x^2y^2 + xy^3)\big)\big]
\end{aligned}$$

Multiplying out yields the claims. $\square$

Remark 5. This argument works for central simple algebras of any degree. By further expansion one gets expressions for the coefficients of the characteristic polynomial of $x + y$ as integral polynomials in the coefficients of the characteristic polynomials of noncommutative monomials in x, y.

References

[1] A. A. Albert, *Structure of algebras*, American Mathematical Society Colloquium Publications, vol. 24, American Mathematical Society, Providence, RI, 1961, Revised printing of the 1939 edition.

[2] D. Haile, *A useful proposition for division algebras of small degree*, Proc. Amer. Math. Soc. **106** (1989), no. 2, 317–319.

Department of Mathematics, The Ohio State University, 231 W 18th Avenue, Columbus, OH 43210, USA

E-mail address: `rost@math.ohio-state.edu`

URL: `http://www.math.ohio-state.edu/~rost`