Severi-Brauer Varieties of Semidirect Product Algebras

Daniel Krashen[1]

Received: October 9, 2003
Revised: November 18, 2003

Communicated by Alexander Merkurev

Abstract. A conjecture of Amitsur states that two Severi-Brauer varieties are birationally isomorphic if and only if the underlying algebras are the same degree and generate the same cyclic subgroup of the Brauer group. It is known that generating the same cyclic subgroup is a necessary condition, however it has not yet been shown to be sufficient.

In this paper we examine the case where the algebras have a maximal subfield K/F of degree n with Galois closure E/F whose Galois group is of the form $C_n \rtimes H$, where $E^H = K$ and $|H|$ is prime to n. For such algebras we show that the conjecture is true for certain cases of n and H. In particular we prove the conjecture in the case that G is a dihedral group of order $2p$, where p is prime.

2000 Mathematics Subject Classification: 16K50, 16S35
Keywords and Phrases: Brauer groups, Severi-Brauer varieties

1 Introduction

Let F be a field. We fix for the entire paper a positive integer n, and we suppose that either n is prime, or that F contains a primitive n'th root of unity. For a field extension L/F, and A a central simple L-algebra, we write $V(A)$ or $V(A/L)$ to denote the Severi-Brauer variety of A, consisting of $(deg\ A)$-dimensional right ideals of A, and denote the function field of this variety by $L(A)$.
We recall the following conjecture:

[1]Partially supported by NSF grant DMS-9983726

Conjecture (Amitsur, 1955 [Ami55]). Given A, B Central Simple algebras over F, $F(A) \cong F(B)$ iff $[A]$ and $[B]$ generate the same cyclic subgroup of the $Br(F)$.

Amitsur showed in [Ami55] that one of these implications hold. Namely if $F(A) \cong F(B)$, then the equivalence classes of A and B generate the same cyclic subgroup of the Brauer Group. The aim of this note is to prove the reverse implication for certain algebras A and B. We will say that the conjecture holds for the pair (A, l), or simply that (A, l) is true to mean that l is prime to $deg(A)$ and $F(A) \cong F(A^l)$. We say that the conjecture is true for A if, for all l prime to $deg(A)$, (A, l) is true.
One important case is when the algebra A has a cyclic Galois maximal splitting field. In this case we know that the conjecture is true for A ([Ami55], [Roq64]). In this paper we extend this result to certain $G - H$ crossed products. We recall the following definitions:

DEFINITION 1. Let G be a finite group, and H a subgroup of G. A field extension K/F is called $G - H$ Galois if there exists a field E containing K such that E/F is G-Galois, and $E^H = K$.

DEFINITION 2. Let A be a central simple F-algebra. A is called a $G - H$ crossed product if A has a maximal subfield K which is $G - H$ Galois. In the case $H = 1$, we call A a G-crossed product.

The main theorem in this note concerns the case of an algebra which is a so-called semidirect product algebra in the sense of [RS96]

DEFINITION 3. A is called a semidirect product algebra if it is a $G - H$ crossed product where $G = N \rtimes H$.

This can be interpreted as meaning that A becomes an N- crossed product after extending scalars by some field K/F which is H-Galois. In the case where N is a cyclic group, we will try to exploit the fact that we know Amitsur's conjecture to be true for N crossed products to prove the conjecture for G crossed products.

SEMIDIRECT PRODUCT THEOREM 1. *Let A be a semidirect product algebra of degree n as in definition 3, with $N = C_m = \langle \tau \rangle$, $H = C_n = \langle \sigma \rangle$, such that the homomorphism $N \to Aut(H)$ (induced by conjugation) is injective and $|N|$ and $|H|$ are relatively prime. Choose r so that we may write $\tau\sigma\tau^{-1} = \sigma^r$. Let*

$$S = \frac{\mathbb{Z}[\rho]}{1 + \rho + \rho^2 + \cdots + \rho^{n-1}},$$

and define an action of τ on S via $\tau(\rho) = \rho^r$, and a ring homomorphism $\overline{\epsilon} : S \to \mathbb{Z}/n\mathbb{Z}$ via $\overline{\epsilon}(\rho) = \overline{1}$. Then (A, l) is true for all l such that $\overline{l} \in \overline{\epsilon}\big((S^*)^\tau\big)$.

We give the proof of this in section 3. For now, we give the following corollary:

Corollary 1. *Suppose $deg(A) = n$, n odd. If A has a dihedral splitting field of degree $2n$. Then the conjecture is true for A.*

Proof. In this case, we have $\overline{\epsilon}((S^*)^\tau) = (\mathbb{Z}/n\mathbb{Z})^*$. If $l = 2^k$, $\overline{l}$ is the image of $(\rho + \rho^{-1})^k$. If $l = 2k+1$, then $\overline{l}$ is the image of $\rho^{-k} + \rho^{-(k-1)} + \ldots + \rho^{-1} + 1 + \rho + \ldots + \rho^{k-1} + \rho^k$. Any other unit in $(\mathbb{Z}/n\mathbb{Z})^*$ is easily seen to be the image of a product of those above. □

Remark. This theorem is already known when F contains the n'th roots of unity, since by a theorem of Rowen and Saltman [RS82], any such algebra is in fact cyclic, and so the theorem follows from [Ami55] or [Roq64].

It is worth noting that the hypothesis concerning the splitting field E can be stated in weaker terms for the case $n = p$ a prime number. In particular we have:

Proposition 1. *Suppose A is a central simple F-algebra of degree p with a maximal subfield K, and suppose that there is some extension E' of K such that E'/F is Galois with group $G = C_p \rtimes H$ where $(E')^H = K$. Then there is a subfield $E \subset E'$ containing K such that E/F is Galois with group $C_p \rtimes C_m$ where C_m acts faithfully on C_p.*

Proof. We define a homomorphism $\phi : H \to Aut(C_p)$ via the natural conjugation action of H on C_p. Since $Aut(C_p)$ is a cyclic group every subgroup is cyclic, and we may regard ϕ as a surjective map $H \to C_m$. Now we define a map

$$\begin{aligned} G = C_p \rtimes H &\to C_p \rtimes C_m \\ (a, h) &\mapsto (a, \phi(h)) \end{aligned}$$

one may check quickly that this is a homomorphism of groups and its kernel is precisely the kernel of ϕ. Set $H' = ker\phi$, and let $E = (E')^{H'}$. Since H' is normal in G (as the kernel of a homomorphism), we know that E/F is Galois and its Galois group is $G/H' = C_p \rtimes C_m$. By construction, the action of C_m is faithful on C_p. □

Note also that in the case $n = p$ a prime, S is a ring of cyclotomic integers.

2 Preliminaries

To begin, let us fix some notation. Let F be an infinite field, and let F^{alg} be an algebraic closure of F. The symbol $\otimes$ when unadorned will always denote a tensor product over F and $\times$ will denote a fiber product of schemes over $Spec(F)$. For us an F-variety will mean a quasi-projective geometrically integral seperated scheme of finite type over F (note F is not assumed to be algebraically closed). By geometrically integral we mean that the scheme remains integral when fibered up to the algebraic closure of its field of definition. If X is a variety, we denote its function field by $F(X)$. We remark that X being

geometrically integral variety implies that $F(X)$ is a regular field extension of F, that is to say, $F(X) \otimes_F F^{alg}$ is a field.
Let E/F be G-Galois for some group G. If B is an E algebra, then a homomorphism $\alpha : G \to Aut_F(B)$ defines an action of G on B (as an F algebra) which is called semilinear in case

$$\forall x \in E, b \in B, \quad \alpha(\sigma)(xb) = \sigma(x)\alpha(\sigma)(b).$$

We refer to the pair (B, α) as a G-algebra, and a morphism between two G-algebras is simply defined to be an algebra map which commutes with the G-actions. The theory of descent tells us that the category of G-algebras is equivalent to the category of F-algebras by taking a G-algebra (B, α) to its G-invariants. Conversely, an F-algebra C gives us the G-algebra $(C \otimes_F E, \iota_C)$, where $\iota_C(\sigma) = id \otimes \sigma$.
Similarly, if X is an E-variety with structure map $k : X \to Spec(E)$, a homomorphism $\alpha : G \to Aut_{Spec(F)}(X)$ defines an action of G on X (as an F-scheme) which is called semilinear in case $\sigma \circ k = k \circ \alpha(\sigma)$.
Also for B any E-algebra, given $\sigma \in G$, we define ${}^{\sigma}B$ to be the algebra with the same underlying set and ring structure as B, but with the structure map $\sigma^{-1} : E \hookrightarrow {}^{\sigma}B$.
Given A a central simple F-algebra, we recall that the functor of points of the Severi-Brauer variety $V(A)$ is given the following subfunctor of the Grassmannian functor of points (see [Jah00], [VdB88], or [See99], and [EH00] for the definition of the Grassmannian functor):

$$V(A)(R) = \left\{ I \subset A_R \,\middle|\, \begin{array}{l} I \text{ is a left ideal and } A_R/I \\ \text{is } R\text{-projective of rank } n \end{array} \right\}$$

and for a homomorphism of commutative F-Algebras $R \xrightarrow{\psi} S$ we obtain the set map

$$\begin{aligned} V(A)(\psi) : V(A)(R) &\to V_k(A)(S) \\ \text{via } I &\mapsto I \otimes_R S \end{aligned}$$

2.1 Descent and functors of points

Given X an F-variety, we obtain a functor

$$X^{E/F} : \{\text{commutative } F\text{-algebras}\} \to \{\text{sets}\}$$

by $X^{E/F}(R) = Mor_{sch_E}(Spec(R_E), X_E)$. If $f \in Mor(X, Y)$, we abuse notation, and refer to the natural transformation induced by f by f also.
For $\sigma \in G$, we have an action of σ on $X_E = X \times_{Spec(F)} Spec(E)$ induced by σ^{-1} acting on E. With this in mind, we obtain a natural transformation $\sigma : X^{E/F} \to X^{E/F}$ via for $\phi \in X^{E/F}(R)$, $\sigma \cdot \phi = \sigma \circ \phi \circ \sigma^{-1}$. We denote this action by

$$\iota_X : G \to NatAut(X^{E/F}).$$

Proposition 2. *Let $f \in Mor_E(X_E, Y_E)$. Then $f = g_E$ for $g \in Mor_F(X, Y)$ iff the following diagram commutes:*

$$\begin{array}{ccc} X^{E/F} & \xrightarrow{f} & Y^{E/F} \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} \\ X^{E/F} & \xrightarrow{f} & Y^{E/F} \end{array}$$

that is, for every commutative F-algebra R and $\phi \in X^{E/F}(R)$, we have

$$\sigma \cdot f(\phi) = f(\sigma \cdot \phi)$$

Proof. To begin, assume the above condition holds. We have (recalling that $f(\phi) = f \circ \phi$),

$$\sigma \cdot f(\phi) = \sigma \cdot (f \circ \phi) = \sigma \circ (f \circ \phi) \circ \sigma^{-1}$$
$$f(\sigma \cdot \phi) = f(\sigma \circ \phi \circ \sigma^{-1}) = f \circ \sigma \circ \phi \circ \sigma^{-1}$$

And setting these two to be equal, we have

$$\sigma \circ f \circ \phi = f \circ \sigma \circ \phi$$

which in turn gives us

$$f \circ \phi = \sigma^{-1} \circ f \circ \sigma \circ \phi$$

Since this must hold for each ϕ, this just says that the elements $f, \sigma^{-1} \circ f \circ \sigma \in Mor_E(X_E, Y_E)$ correspond to the same natural transformation when thought of as elements of $Nat(X^{E/F}, Y^{E/F})$ via the Yoneda embedding, and therefore they must actually be equal - that is to say $f = \sigma^{-1} \circ f \circ \sigma$ or $\sigma \circ f = f \circ \sigma$. But now, by Galois descent of schemes, we know $f = g_E$.
Conversely, assume that $f = g_E$. In this case it is easy to see that we have $\sigma \circ f = f \circ \sigma$. Now we simply make our previous argument backwards and find that the desired diagram does in fact commute. □

We note the following lemma, which can be checked by examining the Grassmannian in terms of its Plüker embedding:

Lemma 1. *Suppose that V is an F-vector space, and let $X = Gr_k(V)$. Then the natural semilinear action ι_X can be described functorially as the natural transformation from $X^{E/F}$ to itself such that for R a commutative F-algebra, $\sigma \in G$, $M \in X^{E/F}(R)$,*

$$X^{E/F}(\iota_X(\sigma))(M) = \sigma(M) = \{\sigma(m) | m \in M\}$$

where σ acts on the elements of $V_{R \otimes E}$ in the natural way.

COROLLARY 2. *Suppose that A is an F-central simple algebra, and let $X = V_k(A)$. Then the natural semilinear action ι_X can be described functorially as the natural transformation from $X^{E/F}$ to itself such that for R a commutative F-algebra, $\sigma \in G$, $I \subset A_{R\otimes E}$ an element of $X^{E/F}(R)$*

$$X^{E/F}(\iota_X(\sigma))(I) = \sigma(I) = \{\sigma(x)|x \in I\}$$

where σ acts on the elements of $A_{R\otimes E} = A \otimes R \otimes E$ as $id \otimes id \otimes \sigma$.

2.2 SEVERI-BRAUER VARIETIES OF CROSSED PRODUCT ALGEBRAS

We give here an explicit birational description of the Severi-Brauer Variety of a crossed product algebra. A similar discussion (without the functorial viewpoint) may be found in [Sal99] (Cor. 13.15). Let L/F be a G-galois extension of degree n. Let $A = (L, G, c)$ be a crossed product algebra, where c is taken to be a specific 2-cocycle (not just a cohomology class) normalized so that $c(id, id) = 1$.
We define the "functor of splitting 1-chains for c" via: To begin, define the functor

$$\mathcal{F} : \left\{\begin{matrix}\text{commutative } L\text{-algebras} \\ \text{with } G\text{-semilinear action}\end{matrix}\right\} \to \{\text{sets}\}$$
$$\mathcal{F}(S) = \{z \in C^1(G, S^*)|\delta z = c\}$$

Where $C^1(G, S^*)$ denotes the set of 1-cochains. From this we define the functor of splitting 1-chains of c as

$$Sp_c : \{\text{commutative } F\text{-algebras}\} \to \{sets\}$$
$$Sp_c(R) = \mathcal{F}(L \otimes R)$$

PROPOSITION 3. *Sp_c is represented by on open subvariety of U of $V(A)$, which is given as an open subfunctor by $U(R) = \{I \in V(A)(R)|I + L_R = A_R\}$. This isomorphism of functors is given by the natural isomorphism $\Lambda : U \to Sp_c$, where $\Lambda(R)(I)$ is the 1-cochain*

$$\sigma \mapsto z(I)_\sigma$$
where $z(I)_\sigma$ is the unique element of L_R such that
$$z(I)_\sigma - u_\sigma \in I.$$

Further, the inverse is given by

$$\Lambda^{-1}(z) = \sum_{\sigma\in G}(L \otimes R)(z(\sigma) - u_\sigma)$$

Proof. First we note that if $I \in U(R)$ then $I \cap L_R = 0$. This is because we have the exact sequence of R-modules

$$0 \to I \cap L_R \to L_R \to A_R/I \to 0$$

which is split since A_R/I is projective. Hence $L_R = A_R/I \oplus (I \cap L_R)$, and since L_R is projective (since L is) we have $I \cap L_R$ is also projective. By additivity of ranks, we have that $rk(A_R/I) = n$, $rk(L_R) = dim_F(L) = n$ and so $rk(I \cap L_R) = 0$. Since $I \cap L_R$ is projective, it must be trivial. Consequently, $I + L_R = A_R$ implies that $A_R = I \oplus L_R$.

To see now that $\Lambda(R)$ is well defined, we just note that $-u_\sigma \in A_R = I \oplus L_R$, and so there is a unique element $z(I)_\sigma \in I$ such that $z(I)_\sigma - u_\sigma \in I$. Next we check that $z(I)$ defines an element of $Sp_c(R)$. Since I is a left ideal,

$$\begin{gathered} z(I)_\tau - u_\tau, z(I)_{\sigma\tau} - u_{\sigma\tau} \in I \\ \Rightarrow u_\sigma\big(z(I)_\tau - u_\tau\big) - c(\sigma,\tau)\big(z(I)_{\sigma\tau} - u_{\sigma\tau}\big) \in I \end{gathered}$$

And also we have therefore:

$$\begin{gathered} \sigma\big(z(I)_\tau\big)\big(z(I)_\sigma - u_\sigma\big), \\ u_\sigma\big(z(I)_\tau - u_\tau\big) - c(\sigma,\tau)\big(z(I)_{\sigma\tau} - u_{\sigma\tau}\big) + \sigma\big(z(I)_\tau\big)\big(z(I)_\sigma - u_\sigma\big) \in I \end{gathered}$$

But this last expression can be rewritten as:

$$\begin{aligned} u_\sigma\big(z(I)_\tau - u_\tau\big) - c(\sigma,\tau)\big(z(I)_{\sigma\tau} - u_{\sigma\tau}\big) + \sigma\big(z(I)_\tau\big)\big(z(I)_\sigma - u_\sigma\big) \\ = \sigma\big(z(I)_\tau\big)u_\sigma - c(\sigma,\tau)u_{\sigma\tau} - c(\sigma,\tau)z(I)_{\sigma\tau} + \\ c(\sigma,\tau)u_{\sigma\tau} + \sigma\big(z(I)_\tau\big)z(I)_\sigma - \sigma\big(z(I)_\tau\big)u_\sigma \\ = \sigma\big(z(I)_\tau\big)z(I)_\sigma - c(\sigma,\tau)z(I)_{\sigma\tau} \in L \otimes R \end{aligned}$$

But since this quantity is also in I and $I \cap (L \otimes R) = 0$, we get $\sigma(z(I)_\tau)z(I)_\sigma = c(\sigma,\tau)z(I)_{\sigma\tau}$ which says that

$$\delta(z(I))(\sigma,\tau) = \sigma(z(I)_\tau)z(I)_\sigma(z(I)_{\sigma\tau})^{-1} = c(\sigma,\tau)$$

and therefore, $z(I) \in Sp_c(R)$.

Next, we check that Λ^{-1} is well defined. Let $z \in Sp_c(R)$ and set $I = \Lambda^{-1}(z)$. It is clear from the definition that $I + (L \otimes R) = A_R$, and $A_R/I = L \otimes R$ is free (and so projective) of rank 1. To check that I is actually a left ideal, since it follows from the definition that $(L \otimes R)I = I$, we need only check that for each $\sigma \in G$, $u_\sigma I \subset I$, and this in turn will follow if we can show $u_\sigma(z(\tau) - u_\tau) \in I$ for each $\tau \in G$. Calculating, we get

$$\begin{aligned} u_\sigma\big(z(\tau) - u_\tau\big) &= \sigma\big(z(\tau)\big)u_\sigma - c(\sigma,\tau)u_{\sigma\tau} \\ &= \sigma\big(z(\tau)\big)u_\sigma - z(\sigma)\sigma\big(z(\tau)\big)z(\sigma\tau)^{-1}u_{\sigma\tau} \\ &= \sigma\big(z(\tau)\big)\big(u_\sigma - z(\sigma)z(\sigma\tau)^{-1}u_{\sigma\tau}\big) \\ &= \sigma\big(z(\tau)\big)\Big(-\big(z(\sigma) - u_\sigma\big) + \big(z(\sigma) - z(\sigma)z(\sigma\tau)^{-1}u_{\sigma\tau}\big)\Big) \\ &= \sigma\big(z(\tau)\big)\Big(-\big(z(\sigma) - u_\sigma\big) + z(\sigma)z(\sigma\tau)^{-1}\big(z(\sigma\tau) - u_{\sigma\tau}\big)\Big) \\ &= -\sigma\big(z(\tau)\big)\big(z(\sigma) - u_\sigma\big) + z(\sigma)\sigma\big(z(\tau)\big)z(\sigma\tau)^{-1}\big(z(\sigma\tau) - u_{\sigma\tau}\big) \\ &\in (L \otimes R)\big(z(\tau) - u_\tau\big) + (L \otimes R)\big(z(\sigma\tau) - u_{\sigma\tau}\big) \subset I \end{aligned}$$

and hence I is a left ideal, and Λ^{-1} makes sense.
It remains to show that Λ and Λ^{-1} are natural transformations and are inverses to one another. It follows fairly easily that if Λ is natural and they are inverses of one another then Λ^{-1} will automatically be natural also.
To see that Λ is natural, we need to check that for $\phi : R \to S$ a ring homomorphism, and $I \in U(R)$, that

$$\Lambda(S)(U(\phi)(I)) = Sp_c(\phi)(\Lambda(R)(I))$$

the right hand side is

$$Sp_c(\phi)(\Lambda(R)(I)) = Sp_c(\phi)(z(I)) = (id_L \otimes \phi)(z(I))$$

and by definition of $z(I)$, we know for $\sigma \in G$, $z(I)_\sigma - u_\sigma \in I$ and for the left hand side we have

$$\Lambda(S)(U(\phi)(I)) = \Lambda(S)(I \otimes_R S)$$

but

$$z(I)_\sigma - u_\sigma \in I \Rightarrow z(I)_\sigma \otimes 1 - u_\sigma \in I \otimes_R S$$

and now, using the identification

$$\begin{aligned}(L \otimes R) \otimes_R S &\xrightarrow{\sim} L \otimes S \\ (l \otimes r) \otimes s &\mapsto l \otimes \phi(r)s\end{aligned}$$

$z(I)_\sigma \otimes 1$ becomes $(id_L \otimes \phi)(z(I)_\sigma)$, and so combining these facts gives

$$Sp_c(\phi)(\Lambda(R)(I))(\sigma) = (id_L \otimes \phi)(z(I)_\sigma) \in I \otimes_R S \cap (L \otimes S - u_\sigma)$$

(here, $L \otimes S - u_\sigma$ denotes translation of $L \otimes S$ by u_σ) and by definition of Λ, this means

$$\Lambda(S)(I \otimes_R S)(\sigma) = (id_L \otimes \phi)(z(I)_\sigma) = Sp_c(\phi)(\Lambda(R)(I))(\sigma)$$

as desired.
Finally, we need to check that transformations are mutually inverse. Choosing $I \in U(R)$, we want to show

$$I = \sum_{\sigma \in G} (L \otimes R)(z(I)_\sigma - u_\sigma)$$

Now, it is easy to see that the right hand side is contained in the left hand side. Furthermore, both of these are direct summands of A_R of corank n. For convenience of notation, let us call the right hand side J.

CLAIM. *I / J is projective*

We show this by considering the exact sequence

$$0 \to I/J \to A_R/J \to A_R/I \to 0$$

Since A_R/I is projective, this sequence splits and $I/J \oplus A_R/I \cong A_R/J$. But since A_R/J is projective, and I/J is a summand of it, I/J must be projective as well, proving the claim.
Now, from the exact sequence

$$0 \to J \to I \to I/J \to 0$$

we know $rank(I/J) = rank(I) - rank(J) = 0$, and so $I/J = 0$ which says $I = J$ as desired.
Conversely, if $z \in Sp_c(R)$, we need to verify that

$$I = \sum_{\sigma \in G} (L \otimes R)(z(\sigma) - u_\sigma) \Rightarrow I \cap (L \otimes R - u_\sigma) = z(\sigma) - u_\sigma$$

But since $z(\sigma) - u_\sigma \in I$, this immediately follows. □

Remark. This same proof will work for an Azumaya algebra (the case where F is a commutative ring).

This becomes simpler for the case that L/F is a cyclic extension, say $A = (L/F, \sigma, b)$. In this case, choosing c to be the standard 2-cocycle:

$$c(\sigma^i, \sigma^j) = \begin{cases} 1 & i + j < n \\ b & i + j \geq n \end{cases}$$

If $z \in Sp_c(R)$, then z is determined by its value on σ, and $z(\sigma)$ must be an element of $(L \otimes R)$ with "σ-norm" equal to b, and conversely it is easy to check that such an element will determine an element of $Sp_c(R)$. With this in mind, we will write $[N_{L/F} = b]$ for the functor Sp_c. By the above we may write (up to natural isomorphism)

$$[N_{L/F} = b](R) = \{x \in L \otimes R | x\tau(x) \cdots \tau^{m-1}(x) = b\} \tag{1}$$

and for a homomorphism $f : R \to S$, we have:

$$[N_{L/F} = b](f)(x) = (id_L \otimes f)(x)$$

and by proposition 3, this is represented by an open subvariety of $V(A)$.

2.3 Group algebra computations

For convenience of notation, since we will be dealing often with certain elements of the group algebra $R = \mathbb{Z}G$, we define for $\gamma \in G$, and j a positive integer

$$N_\gamma^j = 1 + \gamma + \gamma^2 + \ldots + \gamma^{j-1}$$

which we will call the j'th partial norm of γ.
These satisfy the following useful identity which can be easily verified:

$$(N_{\gamma}^{j})(N_{\gamma^j}^{i}) = N_{\gamma}^{ij}$$

where γ is an element of G.
Now, suppose that u is an element in a arbitrary F-algebra B, and E' is a subfield of B such that for all $x \in E'$, $ux = \gamma(x)u$ for $\gamma \in Aut_F(E')$. Then we have the identity:

$$\left(\sum_{k=0}^{i-1}\left(\prod_{j=1}^{k}\gamma^{i-j}(x)\right)u^{i-k-1}\right)(x-u) = \gamma^{i-1}(x)\gamma^{i-2}(x)\cdots\gamma(x)x - u^i$$

(where we consider the empty product in the case $k = 0$ to equal 1).
If we consider the group algebra $\mathbb{Z}\langle\gamma\rangle$ to act on E', then in the above notation, there is an element $a \in B$ such that

$$a(x-u) = N_{\gamma}^{i}x - u^i. \tag{2}$$

2.4 Galois monomial maps

As in (1), let $[N_{E/L} = b]$ be the functor representing elements of norm b. Recall, that for a commutative F-algebra R, $x \in [N_{E/L}](R)$ means that $x \in E \otimes R$ with σ-norm equal to $b^k \otimes 1 \in L \otimes R$),

Definition 4. A Galois monomial in σ is an element of the group algebra $\mathbb{Z}\langle\sigma\rangle$.

Suppose P is a Galois monomial in σ. Let $\epsilon : \mathbb{Z}\langle\sigma\rangle \longrightarrow \mathbb{Z}$ be the augmentation map defined by mapping all group elements to 1. Then if we set $l = \epsilon(P)$, for every integer k, and every commutative F-algebra R, P induces a map of sets:

$$P : [N_{E/L} = b^k](R) \to [N_{E/L} = b^{kl}](R)$$

via for $x \in [N_{E/L} = b^k](R)$, if $P = \sum_{i=0}^{p-1} n_i\sigma^i$,

$$P(x) = x^{n_0+n_1\sigma+n_2\sigma^2+\cdots+n_{p-1}\sigma^{p-1}} \stackrel{def}{=} \prod_{i=0}^{p-1}\sigma^i(x^{n_i}).$$

We refer to this as the Galois monomial map induced by P.

Lemma 2. *Let P be a Galois monomial as above with $\epsilon(P) = l$. Then the maps induced by P fit together to give a natural transformation*

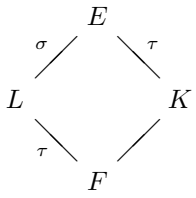
$$[N_{E/L} = b^k] \to [N_{E/L} = b^{kl}]$$

Proof. This is a routine check. □

We will refer to the induced natural transformation above also by the letter P.

3 Proof of the semidirect product theorem

We begin by fixing notation. Let A be a central simple semidirect product algebra of degree n as in the statement of theorem 1, and fix K/F maximal separable in A so that we have the following diagram of fields:



Now, as was shown in section 2.2, since A_L is a cyclic algebra, the functor $[N_{E/L} = b]$ is represented by an open subvariety of $V(A_L)$. The idea of the proving theorem 1 will be to construct rational maps of Severi-Brauer varieties by constructing natural transformations between the corresponding functors. By the lemma from the previous section, one way to construct these natural transformations is via Galois monomial maps.
Since the functor $[N_{E/L} = b^r]$ is represented by an open subvariety of $V(A_L^r)$, a Galois monomial P with $\epsilon(P) = l$ yields an L-rational map $V(A_L^k) \to V(A_L^{kl})$. Our goal will be to determine when such a map induces an F-rational map $V(A^k) \to V(A^{kl})$. To understand when this will happen, we first remark that $[N_{E/L} = b^k]$ can be written as $U_k \times_F L$ where U_k is the open subfunctor of $V(A^k)$ described in proposition 3, section 2.1. By proposition 2, section 2.1, this will happen when when the τ actions on $U_k^{L/F}$ and $U_{kl}^{L/F}$ commute with the natural transformation induced by P.

Remark. Since $U_k^{L/F}(R)$ is the same as $\big(U^k \times_F L\big)(R \otimes L) = [N_{E/L} = b^k](R \otimes L)$, we will abuse notation and write $[N_{E/L} = b^k]$ in place of $U_k^{L/F}$. This means that for an F-algebra R, the notation $x \in [N_{E/L} = b^k](R)$ means $x \in R \otimes E$ has norm $1 \otimes b^k \in R \otimes L$.

In the notation above, we now need to examine when the action of τ on $[N_{E/L} = b^k]$ and $[N_{E/L} = b^{kl}]$ commute with a given monomial P. We will proceed now to describe the actions of τ, and then to translate these into actions on the "norm set" functors, which will let us answer our question.

3.1 The Action of τ

We recall the notation of section 2. For an F-algebra C, we define the action ι_C on $C \otimes L$ by $\iota_C(\tau) = id \otimes \tau$.

Lemma 3. *Let $B = C \otimes L$, where C is a central simple F-algebra of degree n. If α is an arbitrary τ-semilinear action on B, then there is an isomorphism $(B, \alpha) \cong (B, \iota_C)$.*

Proof. Let $D = B^{\alpha}$. Then by descent, we have an isomorphism $(D \otimes L, \iota_D) \cong (B, \alpha)$
Since $m = [L : F]$ is relatively prime to $n = deg(B)$, the restriction map of Brauer groups:

$$Br_n(F) \overset{res_{L/F}}{\longrightarrow} Br_n(L)$$

is injective. Therefore, since both D and C restrict to the same element, they are F-isomorphic. We can therefore write $D \cong C$, and again by descent we get an isomorphism of $(D \otimes L, \iota_D) \cong (C \otimes L, \iota_C)$. Combining this with the isomorphism $(D \otimes L, \iota_D) \cong (B, \alpha)$, we have an isomorphism $(C \otimes L, \iota_C) \cong (B, \alpha)$. □

COROLLARY 3. *Let B be a central simple L-algebra of degree n, α, β τ-semilinear actions on B. Then $(B, \alpha) \cong (B, \beta)$.*

Proof. If B has a semilinear action α, we may write $B \cong C \otimes L$ by descent, where C is defined to the the invariants of B under the action induced by α. Therefore the result follows directly from the lemma above. □

Therefore, to understand the action of τ on A_L via $1 \otimes \tau$ up to an isomorphism of pairs, we need only define any τ-semilinear action on A_L.

3.1.1 AN ACTION OF τ ON A_L

Since the algebra A_L has a maximal subfield E which is cyclic over L, we may write $A_L = (E, \sigma, b)$ for some element $b \in L$. Our goal in this section will be to define a semilinear action of τ on A_L.
Borrowing some of the ideas of Rowen and Saltman ([RS96]), we first investigate the action of τ on $b \in L$. We first note that since A is an F-algebra, that if we consider the algebra ${}^{\tau}A_L$, then this is isomorphic to A_L by the map $id_A \otimes \tau$. On the other hand, one may also check that there is an isomorphism

$$\begin{gathered} {}^{\tau}A_L = {}^{\tau}(E, \sigma, b) \to (E, \sigma^r, \tau(b)) \\ \text{via } E \xrightarrow{\tau} E \text{ and } u \to u \end{gathered}$$

and extending to make a homomorphism. Consequently, we have an isomorphism of central simple algebras $(E, \sigma, b) \cong (E, \sigma^r, \tau(b))$. In addition, there is also an isomorphism $(E, \sigma, b) \cong (E, \sigma^r, b^r)$ ([Pie82] p.277 Cor.a), which means $(E, \sigma^r, b^r) \cong (E, \sigma^r, \tau(b))$. This implies $\tau(b) = ab^r$ where $a = N_{\sigma^r}(x) = N_{\sigma}(x)$ for some $x \in E^*$ ([Pie82] p.279 Prop.b).
Now to define an action of τ on A_L, we must first extend the action to the maximal subfield of A_L which is of the form $L(b^{1/n})$. This will be made more tractable by choosing a different b.

LEMMA 4. *There exists $b' \in L$ such that $(E, \sigma, b) \cong (E, \sigma, b')$ and such that $\tau(b') = \lambda^n (b')^r$ where $\lambda \in L$.*

Proof. In the case where F contains the n'th roots of unity, this follows directly from [RS96], Lemma 1.2.
For the case where $n = p$ is prime, We consider the exact sequence of $\mathbb{Z}/p\mathbb{Z}[\tau]$ modules:

$$0 \to \frac{N_{E/L}(E^*)}{(L^*)^p} \to \frac{L^*}{(L^*)^p} \xrightarrow{\pi} \frac{L^*}{N_{E/L}(E^*)} \to 0$$

By Maschke's theorem ([Pie82], p.51), $\mathbb{Z}/p\mathbb{Z}[\tau]$ is a semisimple algebra and hence every module is projective and every exact sequence splits. We may therefore choose a splitting map $\phi : \frac{L^*}{N_{E/L}(E^*)} \to \frac{L^*}{(L^*)^p}$. Let b' be a coset representative for $\phi(bN_{E/L}(E^*))$. Since ϕ is a splitting, $\pi(b(L^*)^p) = \pi(b'(L^*)^p)$ implies $\pi(b/b'(L^*)^p) = 1$ which means that b and b' differ by a norm and so $(E, \sigma, b) \cong (E, \sigma, b')$. Further, since ϕ is a τ-morphism,

$$\tau(b')(L^*)^p = \tau(\phi(b)(L^*)^p) = \phi(\tau(b)N_{E/L}(E^*)) = \\ \phi(ab^r N_{E/L}(L^*)) = \phi(b^r N_{E/L}(E^*)) = (b')^r(L^*)^p$$

This gives us $\tau(b') = \lambda^p (b')^r$ for some $\lambda \in L$ as desired. □

Without loss of generality, we now substitute b' for b and assume that $\tau(b) = \lambda^n b^r$.
Now consider the field $L(\beta)$, where β is defined to be a root of the polynomial $x^n - b$. We want to show that we can extend the action of τ to an order m automorphism of $L(\beta)/F$. To this effect we first define an map $\tau' : L(\beta) \to L(\beta)$, where $\tau'|_L = \tau$ and $\tau'(\beta) = \lambda\beta^r$. One may verify this defines an automorphism by considering $L(\beta) = L[x]/(x^n - b)$ and noting that τ' preserves the ideal $(x^n - b)$.

Lemma 5. *We may choose λ above so that τ' has order m in $Aut(L(\beta))$.*

Proof. Since by definition $\tau'|_L = \tau$, we have $(\tau')^m \in Aut(L(\beta)/L)$. We thereby find that $ord(\tau')|mn$, $ord(\tau) = m|ord(\tau')$. Therefore we can write $ord(\tau') = km$, $k|n$, and set $\gamma = (\tau')^k$ and $M = L(\beta)^\gamma$. Since $[M : F] = n$, $[L : F] = m$ have relatively prime degrees and are both subfields of $L(\beta)$, which has degree nm, we find that $L(\beta) = L \otimes_F M$. Hence we may define $\tau'' = \tau \otimes id_M \in Aut(L(\beta))$, which is an order m automorphism. But now

$$\tau''|_L = \tau|_L = \tau'|_L$$

and $\tau(b) = \lambda^n b^r \implies \tau''(\beta) = \rho\lambda\beta^r$ where ρ is an n'th root of unity. But we see τ'' is defined in the same way as τ' except for using $\rho\lambda$ instead of λ as a n'th root of unity. Hence, by changing our choice of λ to $\rho\lambda$ we obtain an order m automorphism. □

For simplicity of notation we denote the extension τ' of τ to $L(\beta)$ also by τ. By the above description, we have

$$\tau\beta = \lambda\beta^r$$

where $\lambda \in L$.
We now use this information to define an action of τ on A. Since $A_L = (E, \sigma, b)$ can be thought of as the free noncommutative F-algebra generated by E and u modulo the relations $ux - \sigma(x)u = 0$ and $u^n = b$, giving an F-homomorphism $A_L \to B$ is equivalent to giving an F-map $\phi : L \to B$ and choosing and element $\phi(u) \in B$ such that $\phi(u)\phi(x) - \phi(\sigma(x))\phi(u) = 0$ and $\phi(u)^n - \phi(b) = 0$. Consequently, since any F-endomorphism of A_L is an automorphism (since A_L is finite dimensional and simple), to define an action of τ on A_L, we need only define τ on E and on u and then check that our relation is preserved.
To begin, we define $\tau|_E : E \to E \subset A_L$ to be the original Galois action, and $\tau(u) = \lambda u^r$. Checking our relations we have:

$$\tau(u)\tau(x) = \lambda u^r \tau(x) = \lambda \sigma^r \tau(x) u^r = \lambda \tau\sigma(x) u^r = \tau\sigma(x)\lambda u^r = \tau(\sigma(x))\tau(u)$$

and

$$\tau(u^n) = \lambda^n u^{rn} = \lambda^n b^r = \tau(b)$$

Since $L(u) \cong L(\beta)$ where $L(\beta)$ is as above, we know that $\tau^m(u) = u$. Since τ has order m on E, together this means that τ as defined above is an order m semilinear automorphism of A_L. We will refer to this action as $\alpha : \langle \tau \rangle \to Aut_F(A_L)$.

3.1.2 An Action of τ on A_L^l

We define $A_L^l \subset \otimes^l A_L = \overbrace{A_L \otimes_L \ldots \otimes_L A_L}^{l \text{ - times}}$ to be the algebra generated by $E \otimes_L 1 \otimes_L \ldots \otimes_L 1$ (which we will identify with just E), and $v = u \otimes_L u \otimes_L \ldots \otimes_L u$.

LEMMA 6. *$[A_L^l] = [A_L]^l$, where brackets denote classes in $Br(L)$*

Proof. Since $A_L \cong (E, \sigma, b)$, we simply need to verify that A_L^l is just the symbol algebra (E, σ, b^l). But this follows because we clearly have $A_L^l = \coprod_{i=0}^{p} E v^i$, and we need only check the two defining identities:

$$\begin{aligned} v^p = (u \otimes u \otimes \ldots \otimes u)^p &= u^p \otimes u^p \otimes \ldots \otimes u^p \\ &= b \otimes b \otimes \ldots \otimes b \\ &= b^l \otimes 1 \otimes \ldots \otimes 1 \end{aligned}$$

and

$$\begin{aligned} vx &= (u \otimes u \otimes \ldots \otimes u)(x \otimes 1 \otimes \ldots \otimes 1) \\ &= (ux \otimes u \otimes \ldots \otimes u) \\ &= (\sigma(x)u \otimes u \otimes \ldots \otimes u) \\ &= (\sigma(x) \otimes 1 \otimes \ldots \otimes 1)(u \otimes u \otimes \ldots \otimes u) \\ &= \sigma(x)v \end{aligned}$$

□

Next we note that we have a τ-semilinear action on $\otimes^l A_L$ which is induced (diagonally) by the τ action on A_L, and further, since it is easy to establish that:

$$\tau v = \lambda^l v^r$$

and the action of τ is the usual one on E, we know that A_L^l is preserved by τ and hence we have an induced action on A_L^l. We call this action α^l

3.1.3 τ-Action on Norm Sets

Our goal now will be to describe an action on the norm sets which is compatible with the above τ-action on ideals. The following lemma assures us that since the actions on the algebras A_L and A_L^l given above are isomorphic to the standard actions, they also induce isomorphic actions on $V(A)^{L/F}$ and $V(A^l)^{L/F}$ respectively. Therefore, we may proceed to find actions on the norm sets compatible with the τ actions given above.
Let (B, β) be an algebra with τ-semilinear action such that B central simple over L. Then by corollary 2, we have an induced action on $V(B)(R \otimes L)$ via for $I \in V(B)(R \otimes L)$, thinking of $I \subset B \otimes_L (L \otimes R)$

$$\beta(\tau)I = \{\beta(\tau)(x) | x \in I\}$$

where $\beta(\tau)$ is acting here on $B \otimes_L (L \otimes R) = B \otimes R$ as $\beta(\tau) \otimes 1$.

Lemma 7. *If $f : (B, \beta) \to (B', \beta')$ is an isomorphism, then the induced isomorphism $V(B)(_) \to V(B')(_)$ commutes with the actions of τ*

Proof. This is a simple check:

$$f(\beta(\tau)(I)) = f(\{\beta(\tau)(x) | x \in I\}) = \{f(\beta(\tau)(x)) | x \in I\} = \\ \{\beta'(\tau)(f(x)) | x \in I\} = \beta'(\tau)(f(I))$$

□

As was shown in the previous section, we know τ acts on A_L and hence also on $A_L \otimes R$. This translates to τ acting on $E \otimes R$ via the natural action on E, and by $\tau u = \lambda u^r$ (where we abuse notation by writing u for $u \otimes 1$). Therefore, if $x - u \in I$ then $\tau x - \tau u \in \tau I$, or in other words, $\tau x/\lambda - u^r \in \tau I$. To translate this into an action on norm sets, we recall that our birational identification between $V(A_L)$ and $[N_{E/L} = x]$ is via $I \in V(A_L)^{E/L}(R)$ being identified with $I \cap (E_R - u)$. Therefore to find our τ action on norm sets, we take an ideal I with a given intersection $x - u \in E_R - u$ and find the intersection of the new ideal $\tau(I)$.

Since $GCD(r,n)=1$ (because $r^m \equiv_n 1$), we may select a positive integer t so that $rt = sn+1$. By equation 2 in 2.3, there is an $a \in A$ such that

$$\begin{aligned} a(\tau x/\lambda - u^r) &= N^t_{\sigma^r}(\tau x/\lambda) - u^{rt} \\ &= N^t_{\sigma^r}(\tau x/\lambda) - b^s u \\ &= \tau N^t_\sigma(x)/N^t_{\sigma^r}(\lambda) - b^s u \\ &= \tau N^t_\sigma(x)/\lambda^t - b^s u \end{aligned}$$

where the last step follows from the fact that $\lambda \in L = E^\sigma$.
Now, since τI is a left ideal containing $\tau x/\lambda - u^r$, it must also contain $\tau N^t_\sigma(x)/\lambda^t b^s - u$. Therefore, $\tau N^t_\sigma(x)/\lambda^t b^s - u \in \tau I \cap (E-u)$. This tells us precisely that τI corresponds to $\tau N^t_\sigma(x)/\lambda^t b^s$, and so we get an action of τ on $[N_{E/L}=b]$ via

$$x \overset{\tau}{\mapsto} \tau N^t_\sigma(x)/\lambda^t b^s$$

which makes the following diagram commute:

$$\begin{array}{ccc} V(A)^{E/L} & \xrightarrow{\tau} & V(A)^{E/L} \\ \uparrow & & \uparrow \\ [N_{E/L}=b] & \xrightarrow{\tau} & [N_{E/L}=b] \end{array}$$

Similarly, using the fact that τ acts on A^l via $v \mapsto \lambda^l v^r$, $v^p = b^l$, and v induces σ on E, we get that τ's action on $V(A^l)$ yields an action on $[N_{E/L}=b^l]$ via:

$$x \overset{\tau}{\mapsto} \tau N^t_\sigma(x)/\lambda^{lt} b^{ls}.$$

Now, suppose $P \in \mathbb{Z}\langle\sigma\rangle$, $\epsilon(P) = l$. As P can be considered as a map from $[N_{E/L}=b^k]$ to $[N_{E/L}=b^{kl}]$, it is acted upon by τ via $\tau \bullet P = \tau \circ P \circ \tau^{-1}$. On the other hand, there is a natural action of τ on the group algebra $\mathbb{Z}\langle\sigma\rangle$ given by conjugation by τ, i.e. $\sigma \overset{\tau}{\mapsto} \sigma^r$. We claim that these two actions coincide. Thinking of P as an element of the group algebra $\mathbb{Z}G$, we write $\tau P \tau^{-1}$ as the action of τ by conjugation (as a group element).

PROPOSITION 4. $\tau \bullet P = \tau P \tau^{-1}$

Proof. We aim to show $\tau \circ P = \tau P \tau^{-1} \circ \tau$. To start choose $x \in [N_{E/L}=b^k](R)$. Since $P(x) \in [N_{E/L}=b^{kl}](R)$, we have

$$\begin{aligned} \tau \circ P(x) &= \tau N^t_\sigma(P(x))/\lambda^{klt} b^{kls} \\ &= \tau P N^t_\sigma(x)/\lambda^{klt} b^{kls} \end{aligned}$$

On the other hand,

$$\begin{aligned}\tau P\tau^{-1}\circ\tau(x) &= \tau P\tau^{-1}(\tau N_\sigma^t(x)/\lambda^{kt}b^{ks})\\ &= \tau PN_\sigma^t(x)/\tau P\tau^{-1}(\lambda^{kt}b^{ks})\\ &= \tau PN_\sigma^t(x)/\lambda^{klt}b^{kls}\\ &= \tau\circ P(x)\end{aligned}$$

where the second to last step follows from the fact that $\tau P\tau^{-1}$ is a monomial in σ, and that λ and b are σ-fixed. To finish, we see that by composing on the right by the map τ, we get

$$\tau P\tau^{-1} = \tau\circ P\circ\tau^{-1} = \tau\bullet P$$

as desired. □

Corollary 4. *If $P\in\mathbb{Z}\langle\sigma\rangle^\tau$ then the induced map on norm sets*

$$P:[N_{E/L}=b^k]\to[N_{E/L}=b^{kl}]$$

commutes with the action of τ.

3.2 Proof of the Main Theorem

We recall our earlier definitions of ϵ, $\overline{\epsilon}$, and S.

Lemma 8. *Let $P_1,P_2\in\mathbb{Z}\langle\sigma\rangle$, $\epsilon(P)=l_i$. Then for any $k\in\mathbb{Z}$, P_1P_2 induces a map*

$$P_1P_2:[N_{E/L}=b^k]\to[N_{E/L}=b^{kl_1l_2}]$$

which is the composition of the maps

$$\begin{aligned}P_2:[N_{E/L}=b^k]&\to[N_{E/L}=b^{kl_2}]\\ \text{and}\quad P_1:[N_{E/L}=b^{kl_2}]&\to[N_{E/L}=b^{kl_1l_2}]\end{aligned}$$

Proof. This just comes from the fact that the group algebra acts on E^* with composition being identified with multiplication in the group algebra. □

Definition 5. For $i,k\in\mathbb{Z}$, we define a natural transformation (morphism)

$$\phi_k:[N_{E/L}=b^i]\to[N_{E/L}=b^{i+nk}]$$

by the rule: for $x\in[N=b^i](R)$, $\phi_j(x)=xb^k$.

Note that we abuse notation here, and don't specify the domain or range of ϕ_j in the notation. In any case, one may easily verify that $\phi_j\circ\phi_k=\phi_{j+k}$. In particular, these maps are all invertible and hence are birational morphisms.

Lemma 9. *ϕ_k commutes with the action of τ.*

Proof. We consider $\phi_k : [N_{E/L} = b^i] \to [N_{E/L} = b^{i+nk}]$. Using the formulas for the τ actions described earlier, we have:

$$\begin{aligned}
\tau(\phi_k(x)) &= \tau(xb^k) \\
&= \frac{\tau N_\sigma^t(b^k x)}{\lambda^{(i+nk)t} b^{(i+nk)s}} \\
&= \frac{\tau N_\sigma^t(b^k)\tau N_\sigma^t(x)}{\lambda^{it} b^{is} \lambda^{nkt} b^{nks}} \\
&= \frac{\tau(b^{tk})\tau N_\sigma^t(x)}{\lambda^{it} b^{is} \lambda^{nkt} b^{nks}} \\
&= \frac{(\lambda^n b^r)^{tk}\tau N_\sigma^t(x)}{\lambda^{it} b^{is} \lambda^{nkt} b^{nks}} \\
&= \frac{\lambda^{nkt}(b^{sn+1})^k \tau N_\sigma^t(x)}{\lambda^{it} b^{is} \lambda^{nkt} b^{nks}} \\
&= \frac{b^k \tau N_\sigma^t(x)}{\lambda^{it} b^{is}} \\
&= b^k \tau(x) \\
&= \phi_k(\tau(x))
\end{aligned}$$

□

LEMMA 10. *For P any Galois monomial in σ, $P\phi_k = \phi_{\epsilon(P)k} P$*

Proof. If $P = \sum_{i=0}^{n-1} n_i \sigma^i$ then we simply compute:

$$\begin{aligned}
P \circ \phi_k(x) = P(b^k x) &= \prod_{i=0}^{n-1} (\sigma^i(b^k x))^{n_i} = \prod_{i=0}^{n-1} (\sigma^i(b^k))^{n_i} (\sigma^i(x))^{n_i} \\
&= \prod_{i=0}^{n-1} (b^k)^{n_i} \prod_{i=0}^{n-1} (\sigma^i(x))^{n_i} = (b^k)^{\sum n_i} P(x) = b^{\epsilon(P)k} P(x) = \phi_{\epsilon(P)k} P(x)
\end{aligned}$$

□

We now prove the main theorem:

THEOREM 2. *If $l \in \mathbb{Z}$ such that $\overline{l} \in \overline{\epsilon}((S^*)^\tau)$ then there is a birational map*

$$V(A) \to V(A^l)$$

Proof. We note first that $\mathbb{Z}\langle\sigma\rangle^\tau \to S^\tau$ is surjective, since if we consider the short exact sequence:

$$0 \to N\mathbb{Z} \to \mathbb{Z}\langle\sigma\rangle \to S \to 0$$

We get a long exact sequence in group cohomology

$$N\mathbb{Z} \to \mathbb{Z}\langle\sigma\rangle^{\tau} \to S^{\tau} \to H^1(\tau, N\mathbb{Z})$$

and since as a τ-module, $N\mathbb{Z} \cong \mathbb{Z}$ with trivial action, we have

$$H^1(\tau, N\mathbb{Z}) = Hom(\langle\tau\rangle, \mathbb{Z}) = Hom(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}) = 0$$

giving us a surjective map $\mathbb{Z}\langle\sigma\rangle^{\tau} \to S^{\tau}$ as claimed.
Now, choosing $\alpha \in (S^*)^{\tau}$ with $\overline{\epsilon}(\alpha) = \overline{l}$, we can find $\widetilde{\alpha} \in \mathbb{Z}\langle\sigma\rangle^{\tau}$ mapping to α. If $\epsilon(\widetilde{\alpha}) = l'$, then by the commutativity of the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}N & \longrightarrow & \mathbb{Z}\langle\sigma\rangle & \longrightarrow & S & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \epsilon} & & \downarrow{\scriptstyle \overline{\epsilon}} & & \\ & & & & \mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & & \end{array} \tag{3}$$

we have $\overline{l'} = \overline{l}$ and so $l' = l + kn$ for some $k \in \mathbb{Z}$. This means that $\widetilde{\alpha} : [N_{E/L} = b] \to [N_{E/L} = b^{l+nk}]$, which commutes with the action of τ by 4. Composing this with the map ϕ_{-k} gives us a natural transformation $\phi_{-k} \circ \widetilde{\alpha} : [N_{E/L} = b] \to [N_{E/L} = b^l]$ which commutes with τ. We will show that this actually induces an natural isomorphism.
Next pick $\beta \in (S^*)^{\tau}$ such that $\alpha\beta = 1 \in S$, and choose $\widetilde{\beta} \in \mathbb{Z}\langle\sigma\rangle^{\tau}$ mapping to β, and let $\big(\epsilon(\widetilde{\beta})\big)l = 1 + ns$. We now have $\widetilde{\beta} : [N_{E/L} = b^l] \to [N_{E/L} = b^{1+ns}]$ and composing with ϕ_{-s} yields a natural transformation $\phi_{-s} \circ \widetilde{\beta} : [N_{E/L} = b^l] \to [N_{E/L} = b]$ which commutes with τ.
Now, we compose $\phi_{-k} \circ \widetilde{\alpha}$ with $\phi_{-s} \circ \widetilde{\beta}$, which by construction is a natural transformation $[N_{E/L} = b] \to [N_{E/L} = b]$. If we write $\widetilde{\alpha}\widetilde{\beta} = 1 + rN$, then using 10, we compute:

$$\phi_{-s} \circ \widetilde{\beta} \circ \phi_{-k} \circ \widetilde{\alpha} = \phi_{-s}\phi_{-\epsilon(\widetilde{\beta})k}\widetilde{\beta}\widetilde{\alpha} = \phi_{-(s+\epsilon(\widetilde{\beta})k)}(1 + rN)$$

But $1 + rN : [N_{E/L} = b] \to [N_{E/L} = b^{1+rn}]$ is simply the map ϕ_r, so

$$\phi_{-s} \circ \widetilde{\beta} \circ \phi_{-k} \circ \widetilde{\alpha} = \phi_{-(s+\epsilon(\widetilde{\beta})k)}\phi_r = \phi_{r-s-\epsilon(\widetilde{\beta})k}$$

which is clearly an isomorphism (one can check in fact that $r - s - \epsilon(\widetilde{\beta})k = 0$ giving that the right hand side above is the identity). This argument shows that $\phi_{-k} \circ \widetilde{\alpha} : [N_{E/L} = b] \to [N_{E/L} = b^l]$ is an also an isomorphism which therefore induces a birational map

$$V(A) \to V(A^l).$$

□

REFERENCES

[Ami55] S. A. Amitsur. Generic splitting fields of central simple algebras. *Ann. of Math. (2)*, 62:8–43, 1955.

[EH00] David Eisenbud and Joe Harris. *The geometry of schemes*. Springer-Verlag, New York, 2000.

[Jah00] Jörg Jahnel. The Brauer-Severi variety associated with a central simple algebra: A survey. Preprint 52, Linear Algebraic Groups and Related Structures Preprint Server, http://www.mathematik.uni-bielefeld.de/LAG/man/052.html, 2000.

[Pie82] Richard S. Pierce. *Associative algebras*. Springer-Verlag, New York, 1982. Studies in the History of Modern Science, 9.

[Roq64] Peter Roquette. Isomorphisms of generic splitting fields of simple algebras. *J. Reine Angew. Math.*, 214/215:207–226, 1964.

[RS82] Louis H. Rowen and David J. Saltman. Dihedral algebras are cyclic. *Proc. Amer. Math. Soc.*, 84(2):162–164, 1982.

[RS96] Louis H. Rowen and David J. Saltman. Semidirect product division algebras. *Israel J. Math.*, 96(, part B):527–552, 1996.

[Sal99] David J. Saltman. *Lectures on division algebras*. Published by American Mathematical Society, Providence, RI, 1999.

[See99] George F. Seelinger. Brauer-Severi schemes of finitely generated algebras. *Israel J. Math.*, 111:321–337, 1999.

[VdB88] Michel Van den Bergh. The Brauer-Severi scheme of the trace ring of generic matrices. In *Perspectives in ring theory (Antwerp, 1987)*, pages 333–338. Kluwer Acad. Publ., Dordrecht, 1988.

Daniel Krashen
UCLA Mathematics Dept.
Box 95155
Los Angeles, CA
90095-1555, U.S.A.
dkrashen@math.ucla.edu