Can. J. Math., Vol. XXXI, No. 4, 1979, pp. 831–835

SIMPLE ALGEBRAS OVER RATIONAL FUNCTION FIELDS

T. NYMAN AND G. WHAPLES

The well-known Hasse-Brauer-Noether theorem states that a simple algebra with center a number field k splits over k (i.e., is a full matrix algebra) if and only if it splits over the completion of k at every rank one valuation of k. It is natural to ask whether this principle can be extended to a broader class of fields. In particular, we prove here the following extension.

THEOREM. *Let k be any field, $K = k(t)$ a rational function field in one variable over k, and A a central simple algebra over K. A necessary and sufficient condition for A to split over K is that it split locally, at the completion of K, for every valuation of K which is trivial on k.*

Using the language of [**2**], we call a K-prime (= an equivalence class of valuations of K) a K/k-prime if the valuations are trivial on k. If $\mathfrak{p}$ is a K-prime, we denote the completion of K at $\mathfrak{p}$ by $K_\mathfrak{p}$ and say that a simple algebra A with center K *splits locally at* $\mathfrak{p}$ if $A \otimes_K K_\mathfrak{p} \sim 1$. Thus we wish to prove $A \sim 1$ if and only if $A \otimes_K K_\mathfrak{p} \sim 1$ for all K/k-primes $\mathfrak{p}$.

The necessity of the local splitting is obvious. When K has characteristic 0, the sufficiency follows at once from results of [**4**] and when char $k = p$ and k has no inseparable extension, it follows from Proposition 4.1 of [**3**]. The remaining case seems new and its proof follows. (Case 1 of our proof also gives a short proof for the cases handled in [**3**] and [**4**].)

Let k be any field of characteristic $p \neq 0$ having inseparable extensions and let A be a counterexample to the theorem: namely, a central simple algebra over $K = k(t)$ which is not a full matrix algebra but $A \otimes_K K_\mathfrak{p} \sim 1$ for every K/k-prime $\mathfrak{p}$. From [**7**] it follows that there exist finite degree constant field extensions of K (extensions $L_0(t)$ with L_0/k finite algebraic) which split A.

Case 1. A is split by a separable constant field extension. By a standard argument using Sylow groups (see Theorem 4.30 of [**1**]) it follows that there exists a counter-example $B = (C/F, \sigma, b)$ which is a cyclic algebra of prime degree with $C = C_0(t)$, $F = F_0(t)$, $b \in F$ and C_0/F_0 cyclic, such that B splits at all F/F_0-primes but is not ~ 1. Then b is a local norm at every C/C_0-prime, so the principal F-divisor (b) is the norm of some degree zero C-divisor. Since C has genus 0 over C_0, every degree zero C-divisor is principal, hence there is a $\Gamma \in C$ with $|bN_{C/F}(\Gamma)|_\mathfrak{p} = 1$ for every F/F_0-prime $\mathfrak{p}$. Thus $b' = bN_{C/F}(\Gamma)$ is in the field of constants F_0 of F, and $B = (C/F, \sigma, b')$ since b and b' differ by a norm. We can now write $B = B_0 \otimes_{F_0} F_0(t)$ where $B_0 = (C_0/F_0, \sigma, b')$ is a

Received January 20, 1978 and in revised form October 10, 1978.

cyclic algebra of prime index over F_0. If B_0 is a division algebra then B cannot split locally at any degree one F/F_0-prime. Indeed, suppose $\mathfrak{p}$ is such a prime and π is a prime element at $\mathfrak{p}$. Then since $F_\mathfrak{p} = F_0\langle\pi\rangle$, the field of formal power series in π over F_0, we have $B \otimes_F F_\mathfrak{p} = (B_0 \otimes_{F_0} F) \otimes_F F_\mathfrak{p} = B_0 \otimes_{F_0} F_0\langle\pi\rangle$. But if B_0 is a division algebra, $B_0 \otimes_{F_0} F_0\langle\pi\rangle$ is just the field of formal power series in π with coefficients in B_0 and is also a division algebra. This contradicts the local splitting of B at all F/F_0-primes. So this case is impossible.

Case 2. A is not split by any separable constant field extension. If $k^{s.a.}$ is a separable algebraic closure of k, then it is easily seen that $A \otimes_K k^{s.a.}(t)$ is still a counterexample. So we can and shall assume k has no separable algebraic extension. Then A has a splitting field $L = L_0(t)$ with L_0/k pure inseparable. Since we can get from k to L_0 by a chain of pure inseparable extensions of degree p it follows that we have a counterexample $A \otimes_K L'$ which is split by an inseparable constant field extension L'' of degree p over L' where $L' = L_0'(t)$.

Now change notation: let D be the division algebra in the Brauer class over L' containing $A \otimes_K L'$ and write k, K and $K(s^{1/p})$ in place of L_0', L' and L'' respectively. Then D is a counterexample of index p with center $K = k(t)$ and a splitting field $K(s^{1/p})$ with $s \in k$. By [**1**, Lemma 7.10 and Theorem 4.17] D is a cyclic algebra $(s, \lambda]$ for some $\lambda \in K$ where we use the following notation: if K is any field of characteristic $p \neq 0$ and $s, \lambda \in K$ with $s \neq 0$, then $(s, \lambda]$ denotes the algebra generated over K by the linearly independent elements u^iv^j, $0 \leqq i, j < p$, with relations

$$(1) \quad u^p - u = \lambda, vu = (u + 1)v, v^p = s.$$

It is well-known [**8**] that the algebra $(s, \lambda]$ as constructed is a central simple algebra over K and that it is ~ 1 if and only if either the equation $x^p - x - \lambda = 0$ has a solution in K or if s is a norm from $K(u)$ to K. This describes for fixed λ the values of s making $(s, \lambda] \sim 1$. The following lemma describes for fixed s the values of λ making $(s, \lambda] \sim 1$. This lemma is due to N. Jacobson (see [**5**] and Remark 1) but we include here an elementary proof.

LEMMA. *Let K be any field of characteristic $p \neq 0$ and $s, \lambda \in K$ with $s \neq 0$. Then $(s, \lambda] \sim 1$ if and only if there are elements $a_0, a_1, \ldots, a_{p-1} \in K$ with*

$$(2) \quad \lambda = (a_0^p - a_0) + a_1^p s + a_2^p s^2 + \ldots + a_{p-1}^p s^{p-1}.$$

Proof. Suppose $(s, \lambda] \sim (s, \lambda'] \sim 1$. Then the $p \times p$ total matrix algebra $(s, \lambda]$ generated over K by u, v satisfying (1) contains elements u' and v' satisfying the relations got by substituting u', v', λ' for u, v, λ in (1). The elements v and v' are $p \times p$ matrices with minimum polynomial = characteristic polynomial = $x^p - s$, i.e., v and v' are non-derogatory matrices. Thus an inner automorphism of the matrix algebra transforms v' into v, so we can assume $v = v'$. Then the relations $vu = uv + v$ and $vu' = u'v + v$ imply that $u' - u$

https://doi.org/10.4153/CJM-1979-078-1 Published online by Cambridge University Press

commutes with v. Since v is non-derogatory this implies that $u' - u$ can be written as a polynomial in v:

(3) $u' = u + a_0 + a_1 v + a_2 v^2 + \ldots + a_{p-1} v^{p-1}$

for $a_i \in K$.

We wish to compute the minimum polynomial of u'. To do so consider the matrices

$$(4) \quad U = \begin{bmatrix} \Lambda & & & & & \\ & \Lambda - 1 & & & & \\ & & \Lambda - 2 & & & \\ & & & \cdot & & \\ & & & & \cdot & \\ & & & & & \cdot \\ & & & & & & \Lambda - p + 1 \end{bmatrix},$$

$$V = \begin{bmatrix} 0 & 0 & . & . & . & 0 & s \\ 1 & 0 & . & . & . & 0 & 0 \\ 0 & 1 & . & . & . & 0 & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 & 0 \end{bmatrix},$$

where Λ is an element of an algebraic extension of K with $\Lambda^p - \Lambda = \lambda$. One easily checks that U and V satisfy (1). Expanding by minors along the top row we find the determinant of $U + aV - xI$ is

$$(\Lambda - x)(\Lambda - x - 1) \ldots (\Lambda - x - p + 1) + (-1)^{p-1} a^p s$$
$$= (\Lambda - x)^p - (\Lambda - x) + a^p s = \lambda + a^p s - (x^p - x).$$

Using the Artin-Schreier symbol $\wp(Y) = Y^p - Y$, we have with $x = u' = u + av$:

(5) If u, v satisfy (1), then $\wp(u + av) = \lambda + a^p s$.

Let i, j be integers with $0 < i < p$ and $i \cdot j \equiv 1 \pmod{p}$. If u, v satisfy (1), then $u' = ju$ and $v' = v^i$ satisfy the relations got from (1) by substituting $\lambda' = j\lambda$ for λ and $s' = s^i$ for s. So u', v' generate $(s^i, j\lambda] \sim (s, \lambda]$ (for the rules used here see [**8**]). As in the preceding paragraph we have $\wp(ju + bv^i) = j\lambda + b^p s^i$. So multiplying by i and setting $a = ib$ we get for $x = u + av^i$:

(6) If u, v satisfy (1) and $0 < i < p$, then $\wp(u + av^i) = \wp(u) + a^p s^i$.

By repeatedly using (6) we can add the terms $a_i v^i$ to u one at a time to get

$$\wp(u') = \lambda + \wp(a_0) + a_1{}^p s + a_2{}^p s^2 + \ldots + a_{p-1}{}^p s^{p-1}$$

as the characteristic polynomial for the u' of (3). It is clear that this polynomial

https://doi.org/10.4153/CJM-1979-078-1 Published online by Cambridge University Press

of degree p has p distinct roots in the algebraic closure of K. This means the $p \times p$ matrix u' has p distinct eigenvalues implying its characteristic polynomial coincides with its minimum polynomial. So we have found the minimum polynomial of u' as desired.

Now suppose u and v satisfy (1) with $\wp(u) = \lambda = 0$. Then we have

$$\lambda' = \wp(u') = \wp(u + a_0 + a_1 v + \ldots + a_{p-1} v^{p-1})$$

and this is given by (2). Thus $(s, \lambda'] \sim 1$ implies λ' is given by (2).

For the reverse implication we note that $(s, a^p s^i] \sim 1$ and $(s, \wp(a)] \sim 1$ for all $a \in K$. Then for all $s, \lambda, a_i \in K$, $s \neq 0$,

$$(7) \quad (s, \lambda] \sim (s, \lambda + \mathscr{P}(a_0) + a_1{}^p s + \ldots + a_{p-1}{}^p s^{p-1}].$$

So if λ is given as in (2), $(s, \lambda] \sim (s, 0] \sim 1$ completing the proof of the lemma. Note that if $s \in K^p$, then the first two terms of (2) already represent all elements of K.

Returning to the proof of the theorem, suppose we have a counterexample $(s, \lambda]$ with center $K = k(t)$ where k has no separable extensions. Represent λ as a sum of partial fractions in the usual way. Namely, λ is a sum of a term $\lambda_{\mathfrak{p}(\infty)} \in k[t]$ and finitely many terms $\lambda_{\mathfrak{p}}$ whose denominator is a power of the monic irreducible polynomial corresponding to the K/k-prime $\mathfrak{p}$ and whose numerator is an element of $k[t]$ of degree less than the degree of the denominator. Thus $|\lambda_{\mathfrak{p}}|_{\mathfrak{q}} \leqq 1$ whenever $\mathfrak{p} \neq \mathfrak{q}$. Then $(s, \lambda]$ is similar to the product of the algebras $(s, \lambda_{\mathfrak{p}}]$ for the finitely many primes with $\lambda_{\mathfrak{p}} \neq 0$. Let $\mathfrak{p} \neq \mathfrak{q}$. Then $\lambda_{\mathfrak{q}}$ is integral at $\mathfrak{p}$ and the residue class field at $\mathfrak{p}$ has no separable extension because it is finite algebraic over k. Hence $\lambda_{\mathfrak{q}} = \wp(a) + b$ with $|b|_{\mathfrak{p}} < 1$; since $b \in \wp(K_{\mathfrak{p}})$ whenever $|b|_{\mathfrak{p}} < 1$, it follows that $(s, \lambda_{\mathfrak{q}}] \sim 1$ at $\mathfrak{p}$. Therefore $(s, \lambda_{\mathfrak{p}}] \sim (s, \lambda] \sim 1$ at $\mathfrak{p}$. So if $(s, \lambda]$ is a counterexample, then $(s, \lambda_{\mathfrak{p}}]$ is a counterexample for at least one $\mathfrak{p}$.

Choose one such $\mathfrak{p}$. By the lemma,

$$\lambda_{\mathfrak{p}} = \wp(a_0) + a_1{}^p s + \ldots + a_{p-1}{}^p s^{p-1}$$

for some set of $a_i \in K_{\mathfrak{p}}$. Since K is a rational function field we can use partial fractions again to find elements $b_i \in K$ with $|b_i - a_i|_{\mathfrak{p}} \leqq 1$ and $|b_i|_{\mathfrak{q}} \leqq 1$ for all $\mathfrak{q} \neq \mathfrak{p}$. By (7), $(s, \lambda_{\mathfrak{p}}] \sim (s, \lambda']$ where

$$\lambda' = \lambda_{\mathfrak{p}} - \wp(b_0) - b_1{}^p s - \ldots - b_{p-1}{}^p s^{p-1}.$$

By construction $|\lambda'| \leqq 1$ for every K/k-prime $\mathfrak{q}$, so $\lambda' \in k$. But, since k has no separable extension, $\wp(k) = k$ and thus $\lambda' \in \wp(k)$. But then $(s, \lambda'] \sim 1$ which is a contradiction and completes the proof of the theorem.

We have, of course, the following immediate corollary.

COROLLARY. *If C is a cyclic extension of $k(t)$ then an element of $k(t)$ is a norm from C if and only if it is a local norm at all primes of $k(t)$ which are trivial on k.*

Remark 1. The lemma was proved by N. Jacobson in 1937 modulo a minor change in notation. Let $\{c, d\}$ denote the algebra generated over K by w, z, with relations $w^p = c$, $z^p = d$, and $zw - wz = 1$. If u, v generate $(s, \lambda]$ as in (1), then v^{-1}, uv generate $\{s^{-1}, \lambda s\}$: i.e., $(s, \lambda] \sim \{s^{-1}, \lambda s\}$. In ([**5**], p. 670), Nathan Jacobson proved our lemma for the algebras $\{c, d\}$ as a special case of more general results.

Remark 2. From our proof we see that when k has inseparable extensions it is easy to construct algebras $(s, \lambda]$ which are locally ~ 1 at all K/k-primes except one.

Remark 3. In general a field $K = k(t)$ will have many valuations which are not trivial on k, since any valuation of k has at least one extension to a valuation of K. See [**6**].

References

1. A. A. Albert, *Structure of algebras* (A.M.S. Colloquium Publication XXIV, New York, 1939).

2. E. Artin, *Algebraic numbers and algebraic functions* (New York University and Princeton University, 1951; Gordon and Breach, 1967).

3. M. Auslander and A. Brumer, *Brauer groups of discrete valuation rings*, Indag. Math. *30* (1968), 286–296.

4. D. K. Faddeev, *Simple algebras over a field of algebraic functions of one variable*, Trudy Mat. Inst. Steklov *38* (1951), 321–344, A.M.S. Translat. Ser. II *3* (1956), 15–38.

5. Nathan Jacobson, p-*Algebras of exponent* p, Bull. A.M.S. *43* (1937), 667–670.

6. T. Nyman and G. Whaples, *Hasse's principle for simple algebras over function fields of curves. I. Algebras of index 2 and 3; curves of genus 0 and 1*, J. reine angew. Math. *299/300* (1978), 396–405.

7. C. C. Tsen, *Divisionalgebren uber Funktionenkorpern*, Gott. Nachr. (1933), 335–339.

8. E. Witt, *Der Existenzsatz fur abelsche Funktionenkorper*, J. reine angew. Math. *173* (1935), 43–51.

University of Wisconsin Center-Fox Valley,
Menasha, Wisconsin;
University of Massachusetts,
Amherst, Massachusetts