PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 137, Number 4, April 2009, Pages 1265–1273
S 0002-9939(08)09746-3
Article electronically published on November 13, 2008

RELATIVE BRAUER GROUPS IN CHARACTERISTIC p

ROBERTO ARAVIRE AND BILL JACOB

(Communicated by Martin Lorenz)

Abstract. This paper gives a description of the relative Brauer group $\mathrm{Br}(E/F)$ when F has characteristic p, $[E : F] = p$, and the Galois group $\mathrm{Gal}(E_1/F)$ is solvable, where E_1 is the Galois closure of E over F.

In the theory of central simple algebras, splitting fields are of special importance. In particular they provide information about maximal subfields and hence insight into the structure of an algebra. Turning this around, it is often useful to determine the relative Brauer group of a field extension, namely to characterize the Brauer classes that vanish in the extension. For example, if E/F is a cyclic extension and if D is an algebra for which $[D] \in \mathrm{Br}(E/F) := \ker(\mathrm{Br}\, F \to \mathrm{Br}\, E)$, then of course D is a cyclic algebra and we can express $D = (E/F, \sigma, t)$ for a generator σ of $\mathrm{Gal}(E/F)$ and $t \in F$. It is well-known (see, for example, [6], pp. 259-262) that the map $F^* \to \mathrm{Br}\, F$ given by $t \mapsto (E/F, \sigma, t)$ is multiplicative with $t \mapsto 0$ if and only if $t \in N_{E/F}(E^*)$. In other words, in the cyclic case the relative Brauer group $\mathrm{Br}_p(E/F)$ is computed by the classical exact sequence

$$0 \to \frac{F^*}{N_{E/F}(E^*)} \to \mathrm{Br}_p F \to \mathrm{Br}_p E.$$

A natural approach to try to generalize this is to use the restriction-corestriction sequence. For example, if $[E : F] = p$ is separable of prime degree, then there exists an extension F_1 of F so that $E_1 = E \cdot F_1$ is cyclic Galois over F_1 and with $[F_1 : F] = s$, where $(s, p) = 1$. Since the composite $\mathrm{cor}_{F_1/F} \circ \mathrm{res}_{F_1/F} : \mathrm{Br}_p F \to \mathrm{Br}_p F_1 \to \mathrm{Br}_p F$ is multiplication by s, it is injective, so we have an embedding $\mathrm{Br}_p F \hookrightarrow \mathrm{Br}_p F_1$. This induces an inclusion $\mathrm{Br}_p(E/F) \hookrightarrow \mathrm{Br}_p(E_1/F_1)$ and reduces the problem of determining $\mathrm{Br}_p(E/F)$ to explicitly computing its image in $\mathrm{Br}_p(E_1/F_1)$. In general, however, this is not an easy thing to do; that is, it can be very difficult to find an explicit description of the image. In this paper we show how to carry this out in characteristic p where $[E : F] = p$ and where E/F is no longer cyclic, but has solvable Galois group. In this case we find $a \in F$ and decompositions $F_1^*/F_1^{*p} = \nu_{F_1}(1) = \bigoplus_{i=1}^{s-1} \nu_F^{a^i}(1)$ and $E_1^*/E_1^{*p} = \nu_{E_1}(1) = \bigoplus_{i=1}^{s-1} \nu_E^{a^i}(1)$ for which the norm acts on summands as $N_{E_1/F_1} = \bigoplus_{i=1}^{s-1} N_{E/F}^{a^i} : \bigoplus_{i=1}^{s-1} \nu_E^{a^i}(1) \to \bigoplus_{i=1}^{s-1} \nu_F^{a^i}(1)$. It is then shown that the image of $\mathrm{Br}_p(E/F)$ in

Received by the editors April 24, 2008.
2000 *Mathematics Subject Classification.* Primary 16K20, 16K50.
The first author was supported by Fondecyt 1050 337 and Proyecto Anillos, PBCT, ACT05.
The second author was supported by Proyecto Anillos, PBCT, ACT05.

$\mathrm{Br}_p(E_1/F_1)$ is the quotient $\nu_F^a(1)/N_{E/F}^a(\nu_E^a(1))$, so one obtains an analogue of the above exact sequence,

$$0 \to \frac{\nu_F^a(1)}{N_{E/F}^a(\nu_E^a(1))} \to \mathrm{Br}_p F \to \mathrm{Br}_p E.$$

As a corollary of this work we obtain a new proof of Albert's result [1] that p-algebras of index p with solvable group are cyclic. The decomposition of relative norm groups indicates why one should expect such a result. Away from characteristic p it is known that dihedral algebras are cyclic ([5], [7]), but those calculations do not appear to give a general description of the relative Brauer group.

1. The basic setup

Let F be a field of characteristic $p > 0$ and assume that E is a separable extension of F of degree p. Suppose that E_1 is the Galois closure of E over F and that $\mathrm{Gal}(E_1/F)$ is solvable. Our main result is an explicit computation of $\mathrm{Br}(E/F) := \ker(\mathrm{Br}\, F \to \mathrm{Br}\, E)$. In this first lemma we show that the extension E has a simple form. This result is presumably well-known, but is included for lack of a reference.

Lemma 1.1. *Suppose that $[E : F] = p$ and $\mathrm{Gal}(E_1/F)$ is solvable, where E_1 is the Galois closure of E over F. Then $E = F(\beta)$, where $\beta^p - a\beta - b = 0$ for some $a, b \in F^p$. Moreover, $E_1 = F(\alpha, \beta)$, where $\alpha^{p-1} = a$ and $[F(\alpha) : F] = s$ for some $s \mid p-1$.*

Remark 1.2. The calculations also show that $E_1 = F(\alpha, \beta')$, where $\beta' = \beta/\alpha$ and $\wp(\beta') = \beta'^p - \beta' = b/\alpha^p \in F_1 := F(\alpha)$.

Proof. According to ([3], Th. 7, p. 77), as p is prime one knows that $\mathrm{Gal}(E_1/F)$ is a Frobenius subgroup of $AGL(\mathbf{F}_p)$; that is, there exists a cyclic extension F_1 of F of degree s with $s \mid p-1$ such that $E_1 = E \cdot F_1$ is the Galois closure of E over F and such that E_1/F_1 is cyclic of degree p. Since F contains primitive $(p-1)$th roots of unity we express $F_1 = F(\alpha_1)$, where $\alpha_1^s = a_1 \in F$. Without loss of generality, replacing α_1 by $\alpha_1^{p^3}$ we can assume that $\alpha_1^s = a_1 \in F^{p^3}$ and $\alpha_1 \in (F(\alpha_1))^{p^3}$.

We let τ be a generator of $\mathrm{Gal}(F_1/F)$, so $\tau(\alpha_1) = \zeta\alpha_1$ where $\zeta \in \mathbf{F}_p$ is a primitive sth root of unity. As $F_1 = F \oplus \alpha_1 F \oplus \cdots \oplus \alpha_1^{s-1} F$ and since E_1/F_1 is Galois and cyclic of degree p we know by Artin-Schreier theory that $E_1 = F_1(\beta_1)$, where $\wp(\beta_1) = c_0 + c_1\alpha_1 + \cdots + c_{s-1}\alpha_1^{s-1}$ for $c_i \in F$. Replacing β_1 by β_1^p and α_1 by α_1^p if necessary we can assume each $c_i \in F^p$, $\alpha_1 \in F(\alpha_1)^{p^2}$ and $a_1 \in F^{p^2}$. Now, as $\tau^j(\alpha_1) = \zeta^j\alpha_1$ we have $\tau^j(\alpha_1^i) = \zeta^{ij}\alpha_1^i$ and therefore $\wp(\tau^j(\beta_1)) = c_0 + \zeta^j c_1\alpha_1 + \cdots + \zeta^{j(s-1)}c_{s-1}\alpha_1^{s-1}$. Since the $s \times s$ matrix with (i,j) entry ζ^{ij} is invertible over $\mathbf{F}_p$ it is possible to find $\mathbf{F}_p$-linear combinations of $\tau^j(\beta_1)$, $\beta_{1,j}$, so that $\wp(\beta_{1,j}) = c_j\alpha_1^j$, where $c_j \in F^p$ for $j = 0, 1, \ldots, s-1$. (This uses the fact that $\wp$ is $\mathbf{F}_p$-linear.)

Now, as $\beta_1 \notin F$, and as β_1 is an $\mathbf{F}_p$-linear combination of the $\beta_{1,j}$, we see that for some j, $\beta_{1j} \notin F$. We express $\alpha_1 = \alpha'^p$ for $\alpha' \in (F(\alpha_1))^p$ so that

$$\wp(\beta_{1,j}) = c_j\alpha_1^j = c_j(\alpha'^p)^j = c_j(\alpha'^p)^s/(\alpha'^p)^{s-j}$$

and therefore

$$(\alpha'^{s-j}\beta_{1,j})^p - \alpha'^{(p-1)(s-j)}(\alpha'^{s-j}\beta_{1,j}) = c_j\alpha'^{ps}.$$

We set $a = \alpha'^{(p-1)(s-j)}$ and $b = c_j\alpha'^{ps}$ so that $\beta = \alpha'^{s-j}\beta_{1,j}$ satisfies $\beta^p - a\beta = b$. We claim that $a, b \in F^p$. As $(\alpha'^s)^p = \alpha_1^s = a_1 \in F$ and $[F(\alpha'^s) : F] < p$, since F

has characteristic p we must have $\alpha'^s \in F$. As $s \mid p-1$ and as $\alpha'^{ps} = a_1 \in F^{p^2}$ we find that $\alpha'^s \in F^p$. Finally, since $c_j \in F^p$, so are a and b.

If we set $\alpha = \alpha'^{s-j}$ we find $\alpha^{p-1} = a$ as required. We note as $\beta^p - a\beta = b$ that $\wp(\beta/\alpha) = b/\alpha^p$. Therefore, as $[F(\beta,\alpha) : F(\alpha)] = p$ (Artin-Schreier extensions either have degree p or 1), we must have $[F(\beta) : F] = p$ as well. As all extensions of degree p over F inside E_1 must be isomorphic to $F(\beta)$, we find $E \cong F(\beta)$, and this proves the lemma. □

For the remainder of this paper we use the notation set up in Lemma 1.1. In particular, $a, b \in F^p$, and we denote by $F_1 := F(\alpha)$ a cyclic extension of F, where $\alpha^{p-1} = a$ and s is chosen minimal with $s \mid p-1$ and $\alpha^s \in F$. We set $E = F(\beta)$ where $\beta^p - a\beta - b = 0$ and we assume E is a separable extension of F of degree p. The extension $E_1 = F(\alpha,\beta)$ is the cyclic extension of degree p over F_1 given by $E_1 = F_1(\beta/\alpha)$, where $\wp(\beta/\alpha) = b/\alpha^p \in F_1$. We will denote by σ the generator of the Galois group $\mathrm{Gal}(E_1/F_1)$ for which $\sigma(\beta/\alpha) := \beta/\alpha + 1$. This also implies that $\sigma(\beta) = \beta + \alpha$.

2. Differential forms

We use the standard notation for differential forms in characteristic p (see [2] for details) and will repeatedly make use of the Bloch-Kato-Gabber [4] theorem which gives the exact sequence

$$0 \to F^*/F^{*p} \xrightarrow{\mathrm{dlog}} \Omega^1_F \xrightarrow{\wp} \Omega^1_F/dF \to H^2_p(F) \to 0$$

and which defines the group $H^2_p(F) := \Omega^1_F/(\wp(\Omega^1_F) + dF)$. Here $\wp : \Omega^1_F \to \Omega^1_F/dF$ is defined by $\wp(a\frac{df}{f}) = (a^p - a)\frac{df}{f}$. It was proved by Witt [8] that $\mathrm{Br}_p(F) \cong H^2_p(F)$ where the class of a cyclic algebra $(t,b]$ corresponds to the class of the form $b\frac{dt}{t}$, and therefore we can use differential forms to study $\mathrm{Br}_p(E/F)$. We also use the exact sequence to repeatedly express certain $w \in \Omega^1_F$ for which $\wp(w) \in dF$ as $w = \mathrm{dlog}(f)$ for some $f \in F$.

We use notation from [2] when computing $\wp$. If $t_1, t_2, \ldots$ is a fixed p-basis for F and if $u = \sum_{i=1}^n c_i \frac{dt_i}{t_i} \in \Omega^1_F$, then one can define relative to this p-basis $u^{[p]} := \sum_{i=1}^n c_i^p \frac{dt_i}{t_i}$. One then knows that $\wp(u) \equiv u^{[p]} - u \pmod{dF}$, and for the purposes of computation, whenever $a \in F$, $(au)^{[p]} = a^p u^{[p]}$. Finally, the image of F^*/F^{*p} under dlog is denoted $\nu_F(1)$, and so by the exact sequence we have $\nu_F(1) \cong \ker(\wp)$.

We now consider the problem of describing $\ker(Br_p(F) \to Br_p(E))$. Let $w \in \Omega^1_F$ be a differential form such that

$$w = \wp(u) + d(v) \ \text{ in } \ \Omega^1_E$$

for $u \in \Omega^1_E$, $v \in E$. Since $\Omega^1_E = \Omega^1_F + \beta\Omega^1_F + \cdots + \beta^{p-1}\Omega^1_F$ we have that

$$w \equiv \wp(u_0 + \beta u_1 + \cdots + \beta^{p-1}u_{p-1}) \pmod{dE} \tag{2.1}$$

with $u_i \in \Omega^1_F$. Expanding (1) we obtain

$$\begin{aligned} w &\equiv \wp(u_0) + \left(\beta^p u_1^{[p]} - \beta u_1\right) + \cdots + \left(\beta^{(p-1)p} u_{p-1}^{[p]} - \beta^{p-1} u_{p-1}\right) \\ &\equiv \wp(u_0) + \left((a\beta + b)\, u_1^{[p]} - \beta u_1\right) + \cdots \\ &\qquad + \left((a\beta + b)^{p-1}\, u_{p-1}^{[p]} - \beta^{p-1} u_{p-1}\right) \pmod{dE}. \end{aligned}$$

Since $dE = dF + \beta dF + \cdots + \beta^{p-1}dF$ we have inside Ω^1_F:

$$\begin{aligned} w &\equiv \wp(u_0) + bu_1^{[p]} + b^2u_2^{[p]} + \cdots + b^{p-1}u_{p-1}^{[p]} \pmod{dF},\\ 0 &\equiv au_1^{[p]} - u_1 + \tbinom{2}{1}abu_2^{[p]} + \tbinom{3}{1}ab^2u_2^{[p]} + \cdots + \tbinom{p-1}{1}ab^{p-2}u_{p-1}^{[p]} \pmod{dF},\\ &\vdots\\ 0 &\equiv a^{p-2}u_{p-2}^{[p]} - u_{p-2} + \tbinom{p-1}{p-2}a^{p-2}bu_{p-1}^{[p]} \pmod{dF},\\ 0 &\equiv a^{p-1}u_{p-1}^{[p]} - u_{p-1} \pmod{dF}. \end{aligned} \tag{2.2}$$

For $u = u_0+\beta u_1+\cdots+\beta^{p-1}u_{p-1}$, let k be the maximal index such that $u_k \neq 0$. The last two nontrivial equations in (2) above will be

$$0 \equiv a^{k-1}u_{k-1}^{[p]} - u_{k-1} + ka^{k-1}bu_k^{[p]} \pmod{dF}, \tag{2.3}$$

$$0 \equiv a^k u_k^{[p]} - u_k \pmod{dF}. \tag{2.4}$$

The proof of our main theorem will be based on reducing to the case where $k = 1$.

To carry out our proof we need to be able to compute norms additively inside $\Omega^1_{E_1}$. That is the point of the next lemma. The automorphism σ of E_1 induces an automorphism of $\Omega^1_{E_1}$ which can be used to compute the norm.

Lemma 2.1. *The operator $(\sigma-1)^{p-1}$ on $\Omega^1_{E_1}$ is equivalent to the trace map tr_*; that is, $(\sigma-1)^{p-1}(u) = tr_*(u)$ for each $u \in \Omega^1_{E_1}$. Moreover,*

$$(\sigma-1)^{p-1}\left(\frac{d\gamma}{\gamma}\right) = tr_*\left(\frac{d\gamma}{\gamma}\right) = \frac{dN_{E_1/F_1}(\gamma)}{N_{E_1/F_1}(\gamma)}$$

for each $\gamma \in E_1^*$.

Proof. Since the Galois group $\mathrm{Gal}(E_1/F_1)$ is cyclic, we have

$$(\sigma-1)^{p-1} = \sum_{s=0}^{p-1}(-1)^{p-1-s}\tbinom{p-1}{s}\sigma^s.$$

As $(-1)^{p-1-s}\binom{p-1}{s} = (-1)^{p-1-s}\frac{(p-1)(p-2)\cdots(p-s)}{s!} \equiv (-1)^{p-1-s}\frac{(-1)(-2)\cdots(-s)}{s!} \equiv 1 \pmod{p}$ for each s, we have

$$(\sigma-1)^{p-1} = \sum_{s=0}^{p-1}\sigma^s = tr_*.$$

According to ([2], Lem. 2.5) the trace restricts to a map $tr_* : \nu_{E_1}(1) \to \nu_{F_1}(1)$, where it coincides with the norm. Thus we have

$$(\sigma-1)^{p-1}\left(\frac{d\gamma}{\gamma}\right) = tr_*\left(\frac{d\gamma}{\gamma}\right) = \frac{dN_{E_1/F_1}(\gamma)}{N_{E_1/F_1}(\gamma)}$$

as desired. □

Our initial computations will take place over F_1, and then we will pull back to F. For this we need some notation. We have

$$\Omega^1_{E_1} = \beta^{p-1}\Omega^1_{F_1} \oplus \cdots \oplus \beta\Omega^1_{F_1} \oplus \Omega^1_{F_1}.$$

This decomposition provides a filtration of $\Omega^1_{E_1}$, given next.

Definition 2.2. For t with $0 \le t < p$ we denote by V_t the subgroup of $\Omega^1_{E_1}$ defined by $V_t = \beta^t \Omega^1_{F_1} \oplus \beta^{t-1}\Omega^1_{F_1} \oplus \cdots \oplus \Omega^1_{F_1}$.

Remark 2.3. As $\sigma(\beta) = \beta + \alpha$ where $\alpha \in F_1$ it is clear that the operator $(\sigma - 1)$ has the property $(\sigma - 1)(V_t) \subseteq V_{t-1}$ for $1 \le t \le p-1$. In particular, we find $(\sigma-1)^j(V_t) \subseteq V_{t-j}$, where $V_{t-j} = 0$ in case $j > t$.

The next result shows how the operators $(\sigma-1)^i$ can be used to study elements of $\Omega^1_{E_1}$.

Lemma 2.4. *Suppose* $\eta \in \Omega^1_{E_1}$ *and* $(\sigma-1)^{k-1}(\eta) \equiv \beta\alpha^{k-1}u_k \pmod{\Omega^1_{F_1}}$, *where* $1 \le k \le p-1$ *and* $u_k \in \Omega^1_{F_1}$. *Then* $\eta \equiv k^{-1}\beta^k u_k \pmod{V_{k-1}}$.

Proof. We express $\eta = \sum_{i=0}^{t} \beta^i \eta_i$, where $\eta_i \in \Omega^1_{F_1}$ and t is chosen to be the maximal index i with $\eta_i \neq 0$. By a direct calculation, as $(\sigma-1)(\beta) = (\beta+\alpha)-\beta = \alpha$ we find $(\sigma-1)^\ell \beta^j \equiv \binom{j}{\ell}\beta^{j-\ell}\alpha^\ell \pmod{V_{j-\ell-1}}$, and from this we see that $(\sigma-1)^{k-1}(\eta) \equiv \binom{t}{k-1}\beta^{t-k+1}\alpha^{k-1}\eta_t \pmod{V_{k-1}}$. The hypothesis shows we have $t-k+1 = 1$, so in fact $t = k$. From this it follows that $\eta_k = k^{-1}u_k$. □

We have an analogous decomposition of $\Omega^1_{F_1}$ as

$$\Omega^1_{F_1} = \alpha^{s-1}\Omega^1_F \oplus \cdots \oplus \alpha\Omega^1_F \oplus \Omega^1_F.$$

Thus we can uniquely express $\eta \in \Omega^1_{F_1}$ as $\eta = \sum_{i=0}^{s-1} \alpha^i \eta_i$ with $\eta_i \in \Omega^1_F$. Further, since $\alpha \in F_1^p$ and $F_1 = \alpha^{s-1}F \oplus \cdots \oplus \alpha F \oplus F$ we have

$$dF_1 = \alpha^{s-1}dF \oplus \cdots \oplus \alpha dF \oplus dF$$

with each $\alpha^i dF \subseteq \alpha^i \Omega^1_F$. As these direct-sum decompositions are compatible, it makes sense to consider the quotient $\alpha^i\Omega^1_F/\alpha^i dF$. Further, for any i and $\eta_i \in \Omega^1_F$ we have $\wp(\alpha^i\eta_i) = (\alpha^{pi}\eta_i^{[p]} - \alpha^i\eta_i) = \alpha^i(a^i\eta_i^{[p]} - \eta_i)$, and therefore $\wp(\alpha^i\Omega^1_F) \subseteq \alpha^i\Omega^1_F$. So the following definition makes sense. It is the key to our computation of the relative Brauer group $\mathrm{Br}(E/F)$.

Definition 2.5. Suppose $F_1 = F(\alpha)$ where $\alpha^{p-1} = a \in F^p$, $[F_1 : F] = s$, and $s \mid p-1$. Then for i with $0 \le i \le s-1$ we denote by

$$\nu_F^{a^i}(1) := \ker(\alpha^i\Omega^1_F \xrightarrow{\wp} \alpha^i\Omega^1_F/d\alpha^i F).$$

Of course, in this notation, $\nu_F^{a^0}(1) = \nu_F(1)$. Analogously we have groups $\nu_E^{a^i}(1)$ for each i with $0 \le i \le s-1$.

The direct sum decompositions above give that

$$\Omega^1_{F_1}/dF_1 = (\alpha^{s-1}\Omega^1_F/\alpha^{s-1}dF) \oplus \cdots \oplus (\alpha\Omega^1_F/\alpha dF) \oplus (\Omega^1_F/dF),$$

so it is reasonable to expect a similar decomposition for $\nu_{F_1}(1)$. This is given next.

Lemma 2.6. *Assume* $F_1 = F(\alpha)$ *as in Definition* 2.5 *and* $\eta = \sum_{i=0}^{s-1}\alpha^i\eta_i \in \Omega^1_{F_1}$ *where* $\eta_i \in \Omega^1_F$. *Then* $\wp(\eta) \in dF_1$ *if and only if for each* i, $\wp(\alpha^i\eta_i) \in \alpha^i dF \subseteq \alpha^i\Omega^1_F$. *In particular,* $\nu_{F_1}(1) = \bigoplus_{i=0}^{s-1}\nu_F^{a^i}(1)$.

Proof. If $\eta = \sum_{i=0}^{s-1}\alpha^i\eta_i \in \Omega^1_{F_1}$ with $\eta_i \in \Omega^1_F$ we calculate

$$\wp(\eta) = \sum_{i=0}^{s-1}\wp(\alpha^i\eta_i) = \sum_{i=0}^{s-1}(\alpha^{pi}\eta_i^{[p]} - \alpha^i\eta_i) = \sum_{i=0}^{s-1}\alpha^i(a^i\eta_i^{[p]} - \eta_i).$$

As $dF_1 = \bigoplus_{i=0}^{s-1} \alpha^i dF$, we obtain $\wp(\eta) \in dF_1$ if and only if for each i, $\wp(\alpha^i \eta_i) = \alpha^i(a^i \eta_i^{[p]} - \eta_i) \in \alpha^i dF$, giving the first statement. The final statement now follows because $\nu_{F_1}(1) = \ker(\wp : \Omega^1_{F_1} \to \Omega^1_{F_1}/dF_1) \cong \bigoplus_{i=0}^{s-1} \ker(\alpha^i \Omega^1_F \xrightarrow{\wp} \alpha^i \Omega^1_F / d\alpha^i F) = \bigoplus_{i=0}^{s-1} \nu_F^{a^i}(1)$. □

We next note that the norm behaves well when restricted to the decompositions of $\nu_{E_1}(1)$ and $\nu_{F_1}(1)$.

Lemma 2.7. *The norm $N_{E_1/F_1} : \nu_{E_1}(1) \to \nu_{F_1}(1)$ restricts on summands to maps $N^{a^i}_{E/F} : \nu_E^{a^i}(1) \to \nu_F^{a^i}(1)$.*

Proof. The group $\nu_E^{a^i}(1)$ is the subgroup $\ker(\wp) \cap \alpha^i \Omega^1_E \subseteq \Omega^1_{E_1}$, and by Lemma 2.1 the norm is given by the operator $(\sigma - 1)^{p-1}$ on this subgroup. Since $(\sigma - 1)^{p-1}$ vanishes on V_{p-2}, if $\eta = \beta^{p-1}\eta_1 + \eta_2 \in \nu_E^{a^i}(1)$ where $\eta_1 \in \alpha^i \Omega^1_F$ and $\eta_2 \in V_{p-2}$, to prove the result it suffices to verify that $(\sigma - 1)^{p-1}(\beta^{p-1}\eta_1) \in \alpha^i \Omega^1_F$. As the operator $(\sigma - 1)$ is F_1-linear on $\Omega^1_{E_1}$ and as $(\sigma - 1)^{p-1}(\beta^{p-1}) = -a \in F$, the result follows. □

Remark 2.8. It is possible to define the groups $\nu_F^{a^i}(1)$ without reference to the field extension $F_1 = F(\alpha)$. In view of the isomorphism $\alpha^i \Omega^1_F \cong \Omega^1_F$ these groups are given by $\nu_F^{a^i}(1) \cong \ker(\Omega^1_F \xrightarrow{\wp_{a^i}} \Omega^1_F/dF)$, where $\wp_{a^i}(c\frac{df}{f}) = (a^i c^p - c)\frac{df}{f}$. In our case the well-definition of $\wp_{a^i}$ follows by extending to $F(\alpha)$ where $\alpha^{p-1} = a$, although there is presumably a direct proof. The norm map $N^{a^i}_{E/F} : \nu_E^{a^i}(1) \to \nu_F^{a^i}(1)$ can also be defined without reference to the field extensions. It is induced by the trace $\Omega^1_E \to \Omega^1_F$. However, in our applications we need to view $\nu_F^a(1) \subset \nu_{F_1}(1)$ and explicitly represent elements of $\nu_F^a(1)$ as $\frac{df}{f}$ for $f \in F_1$, so we have given the definition in terms of the extension $F_1 = F(\alpha)$.

3. The main theorem

The idea behind studying an element $w \in \ker(Br_p(F) \to Br_p(E))$ is to systematically reduce the power k of β in an expression $w \equiv \wp(u_0 + \beta u_1 + \cdots + \beta^k u_k) \pmod{dE}$ to where we have a useful description of w over F. This next lemma is the key to this reduction.

Lemma 3.1. *Suppose $2 \le k \le p-1$ and $u_k, u_{k-1} \in \Omega^1_F$ satisfy equations* (3) *and* (4) *in Section* 2 *above. Then there exists $\gamma \in E$ such that*

$$\frac{d\gamma}{\gamma} = \beta^k u_k + \beta^{k-1} v_{k-1} + \cdots + \beta v_1 + v_0,$$

where $v_i \in \Omega^1_F$ for $0 \le i \le k-1$.

Proof. As $\alpha \in F_1^p$ and as $\alpha^{kp} = a^k \alpha^k$, multiplying equation (4) by α^k gives that $\alpha^{kp} u_k^{[p]} - \alpha^k u_k = \wp(\alpha^k u_k) \in \alpha^k dF \subseteq dF_1$. Consequently, we find

$$\alpha^k u_k = \frac{df}{f} \quad \text{for some} \quad f \in F_1.$$

It now follows, multiplying equation (3) by α^{k-1}, that

$$\begin{aligned}\alpha^{(k-1)p}u_{k-1}^{[p]} - \alpha^{k-1}u_{k-1} + k\alpha^{(k-1)p}bu_k^{[p]} &= \wp(\alpha^{k-1}u_{k-1}) + k(b/\alpha^p)\alpha^{kp}u_k^{[p]} \\ &= \wp(\alpha^{k-1}u_{k-1}) + k(b/\alpha^p)\left(\frac{df}{f}\right)^{[p]}\end{aligned}$$

lies in $\alpha^{k-1}dF_1 = dF_1$. As $\wp(k(\beta/\alpha)) = k(b/\alpha^p)$ we get $\wp(\alpha^{k-1}u_{k-1} + k(\beta/\alpha)\frac{df}{f}) \in dE_1$, from which we find

$$\alpha^{k-1}u_{k-1} + k(\beta/\alpha)\frac{df}{f} = \frac{d\delta}{\delta} \quad \text{for some} \quad \delta \in E_1.$$

Using Remark 2.3 we apply $(\sigma-1)^{p-1}$ to the latter equation to find that $\frac{dN_{E_1/F_1}(\delta)}{N_{E_1/F_1}(\delta)} = 0$. Consequently, $N_{E_1/F_1}(\delta) \in F^{*p}$, and by Hilbert's Theorem 90 we can express $\delta = t\gamma_1^{\sigma-1}$ for $t \in F_1$ and $\gamma_1 \in E_1$. From this we obtain

$$\alpha^{k-1}u_{k-1} + k(\beta/\alpha)\frac{df}{f} = \frac{dt}{t} + (\sigma-1)\frac{d\gamma_1}{\gamma_1}.$$

Assume we have shown that

$$\alpha^{k-1}u_{k-1} + k(\beta/\alpha)\frac{df}{f} = \frac{dt}{t} + (\sigma-1)^{\ell}\frac{d\gamma_\ell}{\gamma_\ell}$$

for $\gamma_\ell \in E_1$. If $p - (\ell+1) > 1$, then (as $\frac{df}{f} \in \Omega^1_{F_1}$) we apply $(\sigma-1)^{p-\ell-1}$ to find $(\sigma-1)^{p-1}(\frac{d\gamma_\ell}{\gamma_\ell}) = 0$. So we can write $\gamma_\ell = t_\ell\gamma_{\ell+1}^{\sigma-1} \in E_1$. Substitution gives

$$\alpha^{k-1}u_{k-1} + k(\beta/\alpha)\frac{df}{f} = \frac{dt}{t} + (\sigma-1)^{\ell+1}\frac{d\gamma_{\ell+1}}{\gamma_{\ell+1}}.$$

So by induction we have produced $\gamma_1, \gamma_2, \ldots, \gamma_j$ as long as $p - j > 1$. But we have $k < p$ so $p - (k-1) > 1$, and we have produced $\gamma_{k-1} \in E_1$ with

$$\alpha^{k-1}u_{k-1} + k(\beta/\alpha)\frac{df}{f} = \frac{dt}{t} + (\sigma-1)^{k-1}\frac{d\gamma_{k-1}}{\gamma_{k-1}}.$$

We note that $(\sigma-1)\frac{d\gamma_1}{\gamma_1} = (\sigma-1)^2\frac{d\gamma_2}{\gamma_2} = \cdots = (\sigma-1)^{k-1}\frac{d\gamma_{k-1}}{\gamma_{k-1}} \in V_1$ and also that $(\sigma-1)^{k-1}\frac{d\gamma_{k-1}}{\gamma_{k-1}} \equiv k(\beta/\alpha)\frac{df}{f} = k(\beta/\alpha)\alpha^k u_k \pmod{\Omega^1_{F_1}}$. Applying Lemma 2.4 with $\eta = \frac{d\gamma_{k-1}}{\gamma_{k-1}}$ shows $\frac{d\gamma_{k-1}}{\gamma_{k-1}} \equiv s\beta^k u_k \pmod{V_{k-1}}$, where $s \neq 0 \in \mathbf{F}_p$. By Lemma 2.6 applied to E_1/E we may uniquely express $\eta = \sum_{i=0}^{p-2}\alpha^i\eta_i$ where $\eta_0 \equiv s\beta^k u_k \pmod{V_{k-1}}$ with $\wp(\eta_0) \in dE$, and when $i > 0$ we have $\alpha^i\eta_i \in V_{k-1}$. We now select $\gamma \in E$ with $\frac{d\gamma}{\gamma} = s^{-1}\eta_0$, and the lemma is proved. □

We may now give the proof of the main result.

Theorem 3.2. *Suppose that* $\mathrm{char}(F) = p$, $[E:F] = p$ *and* $\mathrm{Gal}(E_1/F)$ *is solvable, where* E_1 *is the Galois closure of* E *over* F. *Let* $a, b \in F^p$ *with* $\alpha^{p-1} = a$ *be as in Lemma* 1.1. *Then* $\mathrm{Br}_p(E/F) \cong \nu_F^a(1)/N_{E/F}^a(\nu_E^a(1))$.

Proof. We define $\phi : \nu_F^a(1) \to \Omega^1_{F_1}/dF_1$ to be the homomorphism given by $\phi(\frac{df}{f}) = (b/\alpha^p)\frac{df}{f} \pmod{dF_1}$. Then by the classical theory of cyclic algebras, as $E_1 = F_1(\wp^{-1}(b/\alpha^p))$ we know that the class $[(b/\alpha^p)\frac{df}{f}] = 0 \in \mathrm{Br}_{\mathrm{p}}\, F_1$ if and only if

$\frac{df}{f} \in N_{E_1/F_1}(\nu_{E_1}(1))$. However, by Lemma 2.7 we know that $\nu_F^a(1) \cap N_{E_1/F_1}(\nu_{E_1}(1)) = N_{E/F}^a(\nu_E^a(1))$, so ϕ induces an embedding

$$\overline{\phi} : \frac{\nu_F^a(1)}{N_{E/F}^a(\nu_E^a(1))} \hookrightarrow \mathrm{Br}_p(E_1/F_1).$$

We claim that $\mathrm{im}(\overline{\phi}) = \mathrm{im}(i_{F_1/F})$, where $i_{F_1/F} : \mathrm{Br}_p(E/F) \hookrightarrow \mathrm{Br}_p(E_1/F_1)$ is the map given by scalar extension. From this claim the theorem follows.

We suppose that $w \in \Omega_F^1$ corresponds to a class in $\mathrm{Br}_p(E/F)$, and we assume that k is minimal such that

$$w = \wp(u_0 + \beta u_1 + \cdots + \beta^k u_k) + dv$$

for $u_i \in \Omega_F^1$ and $v \in E$. First we assume $k > 1$, and then we can apply Lemma 3.1 to obtain $\gamma \in E$ such that $\frac{d\gamma}{\gamma} = \beta^k u_k + \beta^{k-1} v_{k-1} + \cdots + \beta v_1 + v_0$, where $v_i \in \Omega_F^1$. Since $\wp(\frac{d\gamma}{\gamma}) = dv'$ for some $v' \in E$, subtracting we see that

$$w = \wp((u_0 - v_0) + \beta(u_1 - v_1) + \cdots + \beta^{k-1}(u_{k-1} - v_{k-1})) + d(v + v'),$$

contradicting the minimality of k.

We are now in the case where $k = 1$. We have that

$$\begin{aligned} w &= u_0^{[p]} - u_0 + b u_1^{[p]} + dv_0, \\ 0 &= a u_1^{[p]} - u_1 + dv_1, \end{aligned}$$

where $u_0, u_1 \in \Omega_F^1$ and $v_0, v_1 \in F$. As in the proof of Lemma 3.1 we find that $\wp(\alpha u_1) \in dF_1$, and consequently we can express $\alpha u_1 = \frac{df}{f}$ where $f \in F_1$. As $u_1 \in \Omega_F^1$ this means that $\frac{df}{f} \in \nu_F^a(1)$. Altogether we have

$$w \equiv b u_1^{[p]} = b\left(\frac{1}{\alpha}\frac{df}{f}\right)^{[p]} \equiv \frac{b}{\alpha^p}\frac{df}{f} \pmod{\wp(\Omega_{F_1}^1) + dF_1}.$$

This shows that $\mathrm{im}(i_{F_1/F}) \subseteq \mathrm{im}(\overline{\phi})$. Conversely, if $\frac{df}{f} \in \nu_F^a(1)$, then $\overline{\phi}(\frac{df}{f}) = (b/\alpha^p)\frac{df}{f} = (b/a)\frac{1}{\alpha}\frac{df}{f} \in \mathrm{im}(i_{F_1/F} : H_p^2(F) \to H_p^2(F_1))$ as $\frac{1}{\alpha}\frac{df}{f} \in \Omega_F^1$. So $\mathrm{im}(\overline{\phi}) \subseteq \mathrm{im}(i_{F_1/F})$, and the theorem follows. □

As a consequence of this calculation we obtain the result of Albert [1] that algebras in $\mathrm{Br}(E/F)$ must be cyclic. Albert proved his result by finding a purely inseparable splitting field of such an algebra. The proof below gives more information by explicitly describing its Brauer class as a symbol.

Corollary 3.3 (Albert)**.** *Suppose that* $\mathrm{char}(F) = p$*,* $[E : F] = p$*, and* $\mathrm{Gal}(E_1/F)$ *is solvable where* E_1 *is the Galois closure of* E *over* F*. If a division algebra* D *is split over* E*, then* D *is a cyclic algebra.*

Proof. In the proof of Theorem 3.2 we established that if $w \in \Omega_F^1$ corresponds to a class in $\mathrm{Br}_p(E/F)$, then $w = u_0^{[p]} - u_0 + b u_1^{[p]} + dv_0$, where $u_0, u_1 \in \Omega_F^1$, $v_0 \in F$, and $\alpha u_1 = \frac{df}{f}$ for $f \in F_1$. We express $f = x_0 + \alpha x_1 + \cdots + \alpha^{p-2} x_{p-2}$, where each $x_i \in F$. As $\alpha f u_1 = df$ we see that

$$\alpha(x_0 + \alpha x_1 + \cdots + \alpha^{p-2} x_{p-2}) u_1 = dx_0 + \alpha dx_1 + \cdots + \alpha^{p-2} dx_{p-2}$$

and consequently

$$u_1 = \frac{dx_1}{x_0} = \frac{dx_2}{x_1} = \cdots = \frac{dx_{p-2}}{x_{p-3}} = \frac{dx_0}{ax_{p-2}}.$$

From this we obtain

$$u_1^{[p]} = \left(\frac{dx_1}{x_0}\right)^{[p]} = \left(\frac{x_1}{x_0}\frac{dx_1}{x_1}\right)^{[p]} \equiv \left(\frac{x_1}{x_0}\right)^p \frac{dx_1}{x_1} \pmod{dF}.$$

But now we obtain from the first equation

$$w \equiv b\left(\frac{x_1}{x_0}\right)^p \frac{dx_1}{x_1} \pmod{\wp(\Omega_F^1) + dF}.$$

So by Witt's isomorphism it follows that D must be the cyclic algebra

$$D \cong \left(x_1, b\left(\frac{x_1}{x_0}\right)^p\right].$$

This gives the corollary. □

References

1. A. A. Albert, *A note on normal division algebras of prime degree*, Bull. Amer. Math. Soc., **44** (1938), 649–652. MR1563842
2. J. Arason, R. Aravire, R. Baeza, *On some invariants of fields of characteristic $p > 0$*, J. Algebra, **311** (2007), 714–735. MR2314731 (2008g:13034)
3. E. Artin, *Galois Theory*, second edition, University of Notre Dame Press, South Bend, IN, 1959. MR0265324 (42:234)
4. S. Bloch, K. Kato, *p-adic étale cohomology*, Publ. Math. IHES, **63** (1986), 107–152. MR849653 (87k:14018)
5. P. Mammone, J.-P. Tignol, *Dihedral algebras are cyclic*, Proc. Amer. Math. Soc., **101** (1987), 217–218. MR902530 (89b:12005)
6. I. Reiner, *Maximal Orders*, Academic Press, London, 1975. MR0393100 (52:13910)
7. L. H. Rowen, D. J. Saltman, *Dihedral algebras are cyclic*, Proc. Amer. Math. Soc., **84** (1982), 162–164. MR637160 (83c:16013)
8. E. Witt, *p-Algebren und Pfaffsche Formen*, Abh. Math. Sem. Univ. Hamburg, **22** (1958), 308–315. MR0097377 (20:3846)

Universidad Arturo Prat, Casilla 121, Iquique, Chile
E-mail address: raravire@unap.cl

University of California, Santa Barbara, Santa Barbara, California 93106
E-mail address: jacob@math.ucsb.edu