ALGEBRAIC ELEMENTS IN DIVISION ALGEBRAS OVER FUNCTION FIELDS OF CURVES

BY

MICHEL VAN DEN BERGH[a,†] AND JAN VAN GEEL[b,††]

[a] *Universiteit Antwerpen, U.I.A., Departement Wiskunde, Universiteitsplein 1, 2610 Wilrijk, Belgium; and* [b] *Rijksuniversiteit Gent, Seminarie Algebra en Functionaalanalyse, Galglaan 2, 9000 Gent, Belgium*

ABSTRACT

Let D be a division algebra with center K a function field of a curve $\mathscr{C}$ over k; $k(\mathscr{C}) = K$. We study the maximal k-algebraic subfields of D. In Theorem 3.1 it is shown that if D is unramified and $\mathscr{C}$ is an elliptic curve then D contains a k-algebraic splitting field. This enables us to give a new class of counter examples to the Hasse principle for division algebras.

Introduction — Preliminary results

Let $\mathscr{C}$ be a complete regular curve over some field k, let $K = k(\mathscr{C})$ be its function field, k is considered to be algebraically closed in K. Take D a central simple K-algebra, say of degree N^2 over K (i.e. of index N).

If $\mathcal{O}_{\mathscr{C}}$ is the structure sheaf on $\mathscr{C}$, consider sheafs $\mathcal{O}_\Lambda$ of maximal $\mathcal{O}_{\mathscr{C}}$-orders in D; i.e. $\Gamma(\mathscr{U}, \mathcal{O}_\Lambda)$ is a maximal $\Gamma(\mathscr{U}, \mathcal{O}_{\mathscr{C}})$-order in D for all affine open $\mathscr{U}$ in $\mathscr{C}$.

It follows that D is obtained as $\mathcal{O}_{\Lambda,\gamma}$ with γ a generic point of $\mathscr{C}$, the center of D is $K = \mathcal{O}_{\mathscr{C},\gamma}$.

We fix embeddings of $\mathcal{O}_{\mathscr{C}}$ and $\mathcal{O}_\Lambda$ in the constant sheafs $\boldsymbol{K}$ and $\boldsymbol{D}$ over $\mathscr{C}$.

In [4] we obtained the following duality theorem:

THEOREM 0.1. *Let $\omega_{\mathscr{C}}$ be the sheaf of differentials on $\mathscr{C}$, define $\omega_\Lambda = \mathrm{Hom}_{\mathcal{O}_{\mathscr{C}}}(\mathcal{O}_\Lambda, \omega_{\mathscr{C}})$.*

† The first author is supported by an N.F.W.O. grant.

†† The second author is grateful to the Universities of Antwerp U.I.A. and R.U.C.A. for making it possible for him to do this research.

Received November 9, 1983

Let $\mathcal{F}$ be a coherent $\mathcal{O}_\Lambda$-module, define the dual sheaf $\mathcal{F}^\vee = \mathrm{Hom}_{\mathcal{O}_\Lambda}(\mathcal{F}, \mathcal{O}_\Lambda)$. *Then there exists a natural isomorphism*:

$$H^1(\mathcal{C}, \mathcal{F}) \cong H^0(\mathcal{C}, \mathcal{F}^\vee \otimes \omega_\Lambda)^*. \qquad \square$$

For invertible subsheafs of $\boldsymbol{D}$, this result gives rise to a Riemann–Roch theorem, which gives information on the dimensions of the k-spaces $H^0(\mathcal{C}, -)$, cf. [4]. Invertible subsheafs of $\boldsymbol{D}$ are related to the (one-sided) ideal theory of the max-$\Gamma(\mathcal{U}, \mathcal{O}_\Lambda)$-orders.

Let $\mathcal{L}$ be such an (invertible) sheaf of (left) $\mathcal{O}_\Lambda$-ideals, i.e. $\Gamma(\mathcal{U}, \mathcal{L})$ is a left $\Gamma(\mathcal{U}, \mathcal{O}_\Lambda)$-ideal for all affine open $\mathcal{U}$. The norm map of D defines a norm map on the one-sided ideals, so it is possible to define $N(\mathcal{L})$ which is an invertible sheaf on the curves $\mathcal{C}$. We define $\deg \mathcal{L} := \deg N(\mathcal{L})$, the right-hand side being the usual notion from algebraic geometry, cf. [1].

The Riemann–Roch theorem then states, cf. [4]:

THEOREM 0.2. *Let* $g_D = \dim_k H^1(\mathcal{C}, \mathcal{O}_\Lambda) - \dim_k H^0(\mathcal{C}, \mathcal{O}_\Lambda) + 1$ *be called the genus of D. Then*:

(1) $\dim_k H^0(\mathcal{C}, \mathcal{L})$ *is finite*,

(2) $\dim_k H^0(\mathcal{C}, \mathcal{L}) = \dim_k H^0(\mathcal{C}, \mathcal{L}^{-1}\omega_\Lambda) + 1 - g_D + \deg \mathcal{L}$. $\square$

We make these results more precise in the case $\mathcal{L}$ is a two-sided $\mathcal{O}_\Lambda$-ideal.

For a point p of $\mathcal{C}$, $\mathcal{O}_{\mathcal{C},p}$ is a discrete valuation ring in K; its maximal ideal is denoted by p too. $\mathcal{O}_{\Lambda,p}$ is a maximal $\mathcal{O}_{\mathcal{C},p}$-order with maximal ideal P.

Some notations and terminology: the degree $[\mathcal{O}_{\Lambda,p}/P : \mathcal{O}_{\mathcal{C},p}/P] = \phi_p$ is the *residue class-degree* of p in D.

One has that $p\mathcal{O}_{\Lambda,p} = p^{e_p}$ for some $e_p \in \mathbf{N}$, e_p is the ***ramification index*** of p in D. Furthermore for all $p \in \mathcal{C}$, $c_p\phi_p = N^2$, cf. [3].

The degree of P is $f_p = [\mathcal{O}_{\Lambda,p}/P : k]$.

A *divisor* δ of D with respect to $\mathcal{O}_\Lambda$ is a formal sum $\Sigma_{p\in\mathcal{C}} \mathrm{ord}_p(\delta)P$, with $\mathrm{ord}_p(\delta) \in \mathbf{Z}$ which is zero for almost all p.

The *degree* of δ is the number $\deg \delta = \Sigma_{p\in\mathcal{C}} f_p \,\mathrm{ord}_p(\delta)$, with f_p the degree of P.

For every divisor δ we construct an invertible subsheaf of $\boldsymbol{D}$, denoted $\mathcal{L}(\delta)$, as follows:

$$\mathcal{L}(\delta)(\mathcal{U}) = \{r \in \Gamma(\mathcal{U}, \boldsymbol{D}) \mid r \in \mathcal{P}_{\Lambda,p}^{-\mathrm{ord}_p\delta}, \forall p \in \mathcal{C}\}.$$

Here $\mathcal{P}$ is the sheaf with stalk $\mathcal{P}_{\Lambda,p} = P$ in every p of $\mathcal{C}$.

The inverse of $\mathcal{L}(\delta)$ is given by the dual sheaf $\mathcal{L}(\delta)^\vee$; one can show that $\mathcal{L}(\delta)^\vee \cong \mathcal{L}(-\delta)$, cf. [4]. It follows from the definition that $\deg \mathcal{L}(\delta) = \deg \delta$.

The sheaf ω_Λ can be obtained in this way, it is associated to κ, a canonical divisor of D; κ is obtained by extending a canonical divisor of the center K with the different $\Delta = \Sigma_{p \in \mathscr{C}} (e_p - 1)P$ of D.

If ξ is the zero divisor, i.e. $\text{ord}_p(\xi) = 0$ for all p, and let

$$\mathscr{L}(\delta) = \dim_k H^0(\mathscr{C}, \mathscr{L}(\delta)),$$

then Theorem 0.2 yields the following:

THEOREM 0.3. *g_D is the genus of D, g_K the genus of K.*

(1′) *$\ell(\delta)$ is finite.*

(2′) $\ell(\delta) = \deg \delta + 1 - g_D + \ell(\kappa - \delta)$.
And if D is a division algebra then $\ell(\kappa - \delta) = 0$ if $\deg \delta > 2g_D - 2$.

(3) *$H^0(\mathscr{C}, \mathscr{L}(\xi)) = \bigcap_{p \in \mathscr{C}} \mathcal{O}_{\Lambda,p}$ consists of k-algebraic elements in D. In the case D is a division algebra, $H^0(\mathscr{C}, \mathscr{L}(\xi))$ is a k-algebraic division algebra.*

(4) *$\ell(\xi) = g_\Lambda - g_D + 1$, $\ell(K) = g_\Lambda$ where $g_\Lambda = \dim_K H^1(\mathscr{C}, \mathcal{O}_\Lambda)$ called the genus of $\mathcal{O}_\Lambda$.*

(5′) $\deg \kappa = 2g_D - 2 = 2g_\Lambda - 2\ell(\xi)$.

(6) $g_D = N^2 g_K - N^2 + 1 + \frac{1}{2}\Sigma_p f_p(e_p - 1)$.

PROOF. Cf. [4], [5]. (In [5] an idelic proof of this form of the Riemann–Roch theorem is given). □

If $\mathcal{O}_\Lambda$ is viewed as representing a noncommutative curve, as defined e.g. in [6], there is some ambiguity on what should be the field of definition. For example, in the case D is a division algebra, there are reasons to take the "curve" to be defined over $L(\xi) = H^0(\mathscr{C}, \mathscr{L}(\xi))$. It is in general very difficult to obtain structural information on these division algebras $L(\xi)$. This problem is one of the basic motivations for the work reported in this paper.

First of all we provide some quantitative information on the numbers g_D and g_Λ, by means of examples. It follows from (6) that g_D is independent of the choice of the sheaf $\mathcal{O}_\Lambda$; it is an invariant of D. This is in general not true for g_Λ as we will show. So it follows using (4) and (3) that also the $\ell(\xi)$, and therefore the $L(\xi)$, depends on the sheaf $\mathcal{O}_\Lambda$ chosen.

We restrict ourselves throughout the paper to the case where D is a division algebra.

In [5] it is shown that if d is a maximal k-algebraic subring of D it can be obtained as an $L(\xi_\Lambda)$ for a suitable choice of $\mathcal{O}_\Lambda$ in D. The converse is not true.

In view of this we consider the following questions:

I. For which D are the $\ell(\xi_\Lambda)$ (equivalently g_Λ) invariants, i.e. independent of the sheaf $\mathcal{O}_\Lambda$?

For which D are the maximal k-algebraic sub-division algebras isomorphic (or the far more weaker problem: when do the maximal k-algebraic sub-division algebras have the same degree over k)?

The first part of the question is answered positively in the case K has genus 0 and the genus of D is minimal. In view of the examples we do not expect that this result can be improved much more.

The second part, although not true in general, leads to some nice results:

(a) It is answered positively for all division algebras over function fields with finite field of constants. (This is a result of A. Schofield.)

(b) The weak form can be attacked in the case of function fields of genus 1, for division algebras which are everywhere unramified. The latter result is related to question II.

II. For which D is k algebraically closed?

It follows from the results obtained that these questions are related to what is known as "Hasse's principle". A field E is said to satisfy Hasse's principle iff:

(HP.I) *The only central simple algebras A over E split at every discrete valuation v of E, i.e. $A \otimes_E \hat{E}_v \cong M_s(\hat{E}_v)$, are the full matrix rings over E.*

The hypotheses that A is split at v, yields that v is unramified ($e_v = 1$) in A. The converse is not true; this is easily seen by considering "constant extensions", e.g. the c.s.a. $\mathbf{H}(X)$ over $\mathbf{R}(X)$, where $\mathbf{H}$ are the Hamilton quaternions over $\mathbf{R}$, is everywhere unramified ($e_p = 1$ for all p) but is not everywhere split since the residue algebra of the point at infinity is isomorphic to $\mathbf{H}$.

This leads us to reformulate the Hasse principle for function fields as follows:

(HP.II) *A function field E over k is said to satisfy* HP.II *iff central simple algebras A over E which are unramified at every k-discrete valuation v of E are constant extensions, i.e. $A \cong a \otimes_k E$ for some c.s.a. a over k.*

In general there is no implication between HP.I and HP.II in either direction. But it is not difficult to see that the following properties hold:

1. *Let E be the function field of a curve $\mathscr{C}$ with a rational point over k; then if E satisfies* HP.II *it also satisfies* HP.I.

PROOF. Let D over E be a division algebra which is everywhere split; by HP.II $D \cong d \otimes_k E$. So d is imbeddable in every residue algebra of D. But if p is the rational point of $\mathscr{C}$, the residue algebra of D at p is $M_N(k)$, $N = \operatorname{index} D = \operatorname{index} d$. This is impossible unless $d \cong M_N(k)$ which implies $D \cong M_N(E)$. □

2. *If k is a C_1-field then both principles are equivalent.*

Note also that HP.II states that division algebras over function fields which are unramified everywhere need to contain "enough" k-algebraic elements.

Our results for genus 0 fields show that HP.II holds in this case. For genus 1 fields they yield the existence of algebraic splitting fields. An example is given to show that it is the best possible result. Since the example is constructed over a C_1-field ($k = \mathbf{C}(t)$) it also gives a counterexample to HP.I.

Although the H.P. is a very strong property, not many counterexamples seemed to be known. In [7] Witt gives counterexamples for fields of genus 0 and in [2] Nyman and Whaples give classes of counterexamples over fields of genus 0 and 1. However, all these examples are "constant field extensions" over function fields of curves with no rational points.

The examples following from our results on genus 1 fields are not of this form.

The authors are grateful to A. Schofield for his interesting comments on the results obtained in this paper. He also gave permission to include his unpublished result, Theorem 1.1, with proof in this paper.

1. Maximal k-algebraic sub-division algebras of D

We start this section with three examples all showing the rather wild behaviour of k-algebraic sub-division algebras of D, a division algebra over a function field K.

EXAMPLE 1. This will show that not all $\mathcal{L}(\xi_\Lambda)$ are maximal k-algebraic subrings of D. It then follows that $\ell(\xi_\Lambda)$ (and therefore g_Λ) are not invariants for the division algebra D.

We take $k = \mathbf{R}$ the field of real numbers and K a finite extension of $\mathbf{R}(X)$.

Consider the division algebra $H = \mathbf{H} \otimes_{\mathbf{R}} K$, where $\mathbf{H}$ are the Hamilton quaternions over $\mathbf{R}$.

Define the sheaf $\mathcal{O}_\Lambda$ by $\mathcal{O}_{\Lambda,p} = \mathbf{H} \otimes_{\mathbf{R}} \mathcal{O}_{\mathscr{C},p}$. Clearly $\mathcal{L}(\xi_\Lambda) = \mathbf{H}$, so $\ell(\xi_\Lambda) = 4$.

Now suppose K is chosen so that the type number of max. $\Gamma(\mathcal{U}, \mathcal{O}_{\mathscr{C}})$-orders in H is not 1, for some affine open $\mathcal{U}$, i.e. there are non-isomorphic $\Gamma(\mathcal{U}, \mathcal{O}_{\mathscr{C}})$-orders in H. Let $\mathcal{O}_{\Lambda'}$ be a sheaf of max. $\mathcal{O}_{\mathscr{C}}$-orders whose sections over $\mathcal{U}$, $\Gamma(\mathcal{U}, \mathcal{O}_{\Lambda'})$ form a max. $\Gamma(\mathcal{U}, \mathcal{O}_{\mathscr{C}})$-order not isomorphic to $\Gamma(\mathcal{U}, \mathcal{O}_\Lambda)$. If $\mathcal{L}(\xi) \cong \mathcal{L}(\xi')$ then $\mathbf{H}$ embeds in $\Gamma(\mathcal{U}, \mathcal{O}_{\Lambda'})$. But $\mathbf{H}$ contains a basis for H over K so $\Gamma(\mathcal{U}, \mathcal{O}_{\Lambda'}) \cong \mathbf{H} \otimes \Gamma(\mathcal{U}, \mathcal{O}_{\mathscr{C}}) \cong \Gamma(\mathcal{U}, \mathcal{O}_\Lambda)$, a contradiction.

Therefore $\mathcal{L}(\xi')$ is either isomorphic to $\mathbf{C}$ or $\mathbf{R}$. It follows from the theory of c.s.a. that in either case $\mathcal{L}(\xi')$ is embedded in some copy of $\mathbf{H}$ in D.

The same ideas may be used to give analogous examples over other ground fields.

EXAMPLE 2. We now give a division algebra in which maximal k-algebraic subrings are not isomorphic.

Let $K = \mathbf{Q}(X)$ and a_1, a_2 be elements of $\mathbf{Q}\backslash\mathbf{Q}^2$ such that

$$\mathbf{Q}(\sqrt{a_1}) \not\cong \mathbf{Q}(\sqrt{a_2}).$$

Consider the quaternion algebras over $\mathbf{Q}(X)$:

$$H_1 = \left(\frac{X^2 - a_1a_2, \quad a_1}{\mathbf{Q}(X)}\right) \quad \text{and} \quad H_2 = \left(\frac{X^2 - a_1a_2, \quad a_2}{\mathbf{Q}(X)}\right);$$

these H_1, H_2 are division algebras.

The equation $(X^2 - a_1a_2)Z_1^2 + a_iZ_2^2 = 1$ has a solution in $\mathbf{Q}(X)$ if $(X^2 - a_1a_2)Z_1^2 + a_iZ_2^2 = Z_3^2$ has a solution in $\mathbf{Q}[X]$. The latter equation modulo $X^2 - ab$ yields $a_i\bar{Z}_2^2 = \bar{Z}_3^2$; this implies either $\sqrt{a_i} \in \mathbf{Q}(\sqrt{a_1a_2})$, contradicting the assumptions, or $\bar{Z}_2^2 = \bar{Z}_3^2 = 0 \bmod (X^2 - a_1a_2)$. So $(X^2 - a_1a_2) \mid Z_2, Z_3$ and therefore also $(X^2 - a_1a_2) \mid Z_1$; starting off with a solution Z_1, Z_2, Z_3 of relative prime polynomials yields a contradiction too.

We claim that $H_1 \cong H_2$. To see this consider the symbols $(X^2 - a_1a_2, a_i)$ in the $\mathrm{Br}(\mathbf{Q}(X))$. We have:

$$(X^2 - a_1a_2, a_1)\cdot(X^2 - a_1a_2, a_2) = (X^2 - a_1a_2, a_1a_2) = 1.$$

Since a quaternion algebra is of exponent 2 in $\mathrm{Br}(\mathbf{Q}(X))$ it follows that $(X^2 - a_1a_2, a_1) = (X^2 - a_1a_2, a_2)$, i.e. $H_1 \cong H_2$. So H_1 contains both $\mathbf{Q}(\sqrt{a_1})$ and $\mathbf{Q}(\sqrt{a_2})$; it is easily seen that H_1 is not a constant extension, therefore both $\mathbf{Q}(\sqrt{a_1})$ and $\mathbf{Q}(\sqrt{a_2})$ are maximal $\mathbf{Q}$-algebraic subrings in H_1.

REMARK. The above quaternion algebra H_1 can also be obtained from the free product of the fields $\mathbf{Q}(\sqrt{a})$ and $\mathbf{Q}(\sqrt{b})$.

Put $x = \sqrt{a}$, $y = \sqrt{b}$, consider $H = Q(\mathbf{Q}(x) * \mathbf{Q}(y))$, the quotient algebra of the free product.

The center of H is

$$K = \mathbf{Q}(xy + yx) \quad \text{and} \quad H = \left(\frac{(xy - yx)^2 \quad a}{\mathbf{Q}(xy + yx)}\right).$$

Take $T = xy - yx$; then $T^2 = (xy + yx)^2 - 4ab$ and if $X = xy + yx$ we obtain:

$$H = \left(\frac{X^2 - 4ab \quad a}{\mathbf{Q}(X)}\right).$$

In this way many other analogous examples can be obtained.

EXAMPLE 3. We push the above a bit further by giving a division algebra in which maximal k-algebraic subrings have different dimension over k. Take $k = \mathbf{Q}(\xi)$, ξ a primitive 4th root of unity, $K = k(X)$.

Let $a, b \in k$ such that $k(\sqrt{a})$ and $k(\sqrt[4]{b})$ are linearly disjoint, furthermore we suppose $[k(\sqrt{a}):k] = 2$ and $[k(\sqrt[4]{b}):k] = 4$. Consider the cyclic algebra (cf. [3] for the notation):

$$D = \begin{pmatrix} 1 - aX^2 & b \\ & k(X) \end{pmatrix}_4 .$$

It is clear that $k(\sqrt[4]{b}) \subset D$. We claim $k(\sqrt{ab}) \subset D$. This follows from the fact that

$$1 - aX^2 = N_{L(\sqrt[4]{b})/L}\left(\frac{\sqrt[4]{abX^2} - \sqrt[4]{b}}{\sqrt[4]{b}}\right) \qquad \text{with} \quad L = k(X, \sqrt[4]{abX^2})$$

because this shows L splits D and therefore, having degree 4 over $k(X)$, it is embeddable in D. $k(\sqrt{ab}) \subset L$ yields $k(\sqrt{ab}) \subset D$.

To prove that both are maximal k-algebraic subfields, we embed them in the residue algebra of D at the prime $p = (1 - aX^2)$. From

$$\hat{D}_p = D \otimes \widehat{k(X)}_p = \begin{pmatrix} T & b \\ k(\sqrt{a})((T)) & \end{pmatrix}$$

it follows that the residue algebra is $k(\sqrt{a}, \sqrt[4]{b})$.

k-algebraic subfields ℓ of D now satisfy two conditions:

(a) ℓ is embeddable in $k(\sqrt{a}, \sqrt[4]{b})$.

(b) The index of $\hat{D}_p \otimes_k \ell$ is equal to $4/[\ell : k]$.

Straightforward calculation shows that both $k(\sqrt{ab})$ and $k(\sqrt[4]{b})$ are maximal with respect to these conditions.

The examples show that in order to obtain structural information on the k-algebraic sub-division algebras one probably needs rather strong conditions on k or on the division algebra.

In the case k is a finite field there is a general result due to A. Schofield.

THEOREM 1.1. *Let K be a function field in one variable over a finite field $k = \mathbf{F}_q$. If D is any division algebra with center K then the maximal $\mathbf{F}_q$-algebraic subfields of D are all conjugated.*

PROOF. Let ℓ_1, ℓ_2 be two finite extensions of $\mathbf{F}_q$ in D. Let $q_1, \dots, q_n$ be the primes dividing $[\ell_1:\mathbf{F}_q][\ell_2:\mathbf{F}_q]$. Then

$$\ell_i \cong \ell_{i1}\otimes_{\mathbf{F}_q}\cdots\otimes_{\mathbf{F}_q}\ell_{in}$$

where ℓ_{ij} is the maximal subfield of ℓ_i such that $[\ell_{ij}:\mathbf{F}_q]$ is a power of q_j.

The unique field join of ℓ_1 and ℓ_2 is the field

$$\ell' \cong \ell'_1\otimes_{\mathbf{F}_q}\cdots\otimes_{\mathbf{F}_q}\ell'_m$$

where ℓ'_j is the largest of the two fields ℓ_{1j}, ℓ_{2j}. Since ℓ_1 and ℓ_2 are in D, also the ℓ'_j embed in D for each j.

Put $[\ell'_j:\mathbf{F}_q] = q_j^{n_j}$. We claim that ℓ' embeds in D. The ring

$$\ell'\otimes_{\mathbf{F}_q}D \cong (\ell'\otimes_{\mathbf{F}_q}K)\otimes_K D,$$

but $\ell'\otimes_{\mathbf{F}_q}K$ is a field, since $\mathbf{F}_q$ is supposed to be algebraically closed in K. So $\ell'\otimes_{\mathbf{F}_q}D$ is simple artinian, therefore it has a unique simple module. The module $\ell'\otimes_{\ell'_j}D$ has dimension $\Pi_{k\neq j}q_{qk}^{n_k}$ over D, so the dimension over D of the simple module divides h.c.f. $\{\Pi_{k\neq j}q_k^{n_k}\} = 1$. It follows that ℓ' embeds in D^0, the centraliser of the simple module; ℓ' is commutative so it embeds in D.

It is clear that it follows from this that maximal $\mathbf{F}_q$-algebraic subfields of D need to be isomorphic. A "Skolem–Noether" argument proves that they are conjugated in D. □

REMARK. The proof is a simplified version of Schofield's proof. Schofield proves actually more, namely that the result holds for k a locally finite field and with K a field of any transcendence degree over k.

It is possible to obtain more quantitative information on the degree of maximal $\mathbf{F}_q$-algebraic subfields of a division algebra. However we then use that the Hasse principle holds for global fields; this is a far more deeper result than the ones used in the proof of Theorem 1.1.

Let D, K be as in the theorem, ℓ a maximal $\mathbf{F}_q$-algebraic subfield of D. From the Hasse principle it follows that:

$$\text{index}(D\otimes_{\mathbf{F}_q}\ell) = \underset{p}{\text{l.c.m}}\ \text{index}(\ell\otimes_{\mathbf{F}_q}\hat{D}_p)$$

(p running over all primes of K).

The local indices can be calculated via the residue algebra degrees in terms of $[\ell:\mathbf{F}_q]$. Since moreover $\text{index}(D\otimes_{\mathbf{F}_q}\ell) = N/[\ell:\mathbf{F}_q]$, we obtain a formula in $[\ell:\mathbf{F}_q]$ and known numbers (local information). This formula is a condition on $[\ell:\mathbf{F}_q]$ for ℓ to be maximal $\mathbf{F}_q$-algebraic.

2. The genus of the center is zero

We start this section with some explicit calculations of genera in quaternion algebras over rational function fields.

Let k be any field of characteristic not equal to 2. A quaternion algebra H over $k(X)$ is determined by elements f, g in $k(X)$. We denote

$$H = \left(\begin{matrix} f, & g \\ & k(X) \end{matrix}\right).$$

We have a basis $1, i, j, ij$ for H over $k(X)$ such that $i^2 = f$, $j^2 = g$, $ij = -ji$. It can be shown that such a quaternion algebra has a normalised form

$$H = \left(\begin{matrix} p(X) & q(X) \\ & k(X) \end{matrix}\right),$$

with $p(X)$, $q(X)$ relatively prime polynomials in $k[X]$ without square factors. Define $p'(X)$, $(q'(X))$ to be the product of all prime factors of $p(X)$ (respectively $q(X)$) for which $q(X)$ (respectively $p(X)$) is a quadratic residue, and normalised such that $\bar{p}(X) = p(X)/p'(X)$ (resp. $\bar{q}(X) = q(X)/q'(X)$) is monic. Then the discriminant of ($k[X]$-maximal orders in) H is given by the polynomial

$$\Delta^{2^*} = (\bar{p}(X)\bar{q}(X))^2$$

up to a constant factor in k.

This enables us to determine the primes which ramify in H, namely, exactly those primes of $k[X]$ which divide Δ. Normalisation with respect to $k[X^{-1}]$ then yields the ramification in the point at infinity, i.e. at the prime X^{-1}.

We distinguish three cases:

1. *H contains a field of algebraic elements of degree 4 over k*

Then $H = h \otimes_k k(X) = h(X)$ for some quaternion algebra h over k; this follows from the fact that a k-basis for k remains linearly independent over $k(X)$.

The genus of H is minimal: i.e. $g_H = -4 + 1 = -3$ and $g_\Lambda = 0$ for all $\mathcal{O}_\Lambda$. (Apply formula (6) from the R.R. theorem.)

2. *H contains a field of algebraic elements of degree 2 over k*

So the normalised form is:

$$H = \left(\begin{matrix} a & f(X) \\ & k(X) \end{matrix}\right),$$

with $a \in k \backslash k^2$ and $f(X)$ a square free polynomial in $k[X]$. The square root of the discriminant Δ divides $f(X)$. Furthermore the degree of Δ is even if and only if the degree of $f(X)$ is even. This follows from the fact that a prime factor p of $f(X)$ does not divide Δ iff a is a square in $k[X]/(p)$, since $a \in k\backslash k^2$; the latter is only possible if $\deg p$ is even. Let $m = \deg \Delta$, then we obtain:

$$\begin{cases} g_H = -4+1+m & \text{if } X^{-1} \text{ is unramified in } H, \\ g_H = -4+1+m+1 & \text{if } X^{-1} \text{ is ramified in } H. \end{cases}$$

Use formula (6) of R.R. again and the fact that $\deg \Delta^2 = 2m = \Sigma_{p \neq X^{-1}} f_p(e_p - 1)$.

Changing the normalisation of H by multiplying with an even power of X^{-1} yields:

$$H = \begin{pmatrix} a & f(X)X^{-r} \\ & k(X^{-1}) \end{pmatrix} = \begin{pmatrix} a & g(X^{-1}) \\ & k(X^{-1}) \end{pmatrix}$$

with

$$\begin{cases} r = \deg f & \text{if } \deg f \text{ is even}, \\ r = \deg f + 1 & \text{if } \deg f \text{ is odd}. \end{cases}$$

It follows that X^{-1} divides $g(X^{-1})$, and is therefore ramified in H, iff $\deg f$ is odd or equivalently iff m is odd. It follows that g_H is an odd number.

It is easy to see that one can obtain examples of quaternion algebras with genus any odd integer greater than or equal to -1.

3. *The case k algebraically closed in H*

Take $p(X)$ an irreducible polynomial of degree m, $q(X)$ an irreducible polynomial of degree m', m and m' both even or both odd numbers. Furthermore let $p(X)$ be a quadratic residue modulo $q(X)$ but not vice versa.

Consider the quaternion algebra:

$$H = \begin{pmatrix} p(X) & q(X) \\ & k(X) \end{pmatrix}, \qquad H \text{ has genus: } g_H = -4+1+m.$$

Since m can be any number >1 we obtain quaternion algebras with genus any integer greater than or equal to -1.

In general k is not algebraically closed in H. The calculations in Example 2 show that for odd m, i.e. even g_H, examples where k is algebraically closed are obtained. The converse of the latter is not true: e.g. if k is a finite field, it follows from classfield theory that there exists a quaternion algebra in which exactly two given prime polynomials ramify. Let H' be a quaternion algebra in which 2 polynomials of even degree ramify then $g_{H'}$ is odd. Local calculations show that k is algebraically closed in H'.

From Proposition 2.2 below (the HP.II for genus zero fields) it follows that if $g_H < 0$ then k is not algebraically closed in H in the case H is a division algebra.

LEMMA 2.1. *Let D be a division algebra with center K, a function field of a complete regular curve over k.*

Then $g_D < 0$ if and only if $g_K = 0$ and $g_D = 1 - n$, where $n = \ell(\xi)$, ξ the zero divisor with respect to a sheaf $\mathcal{O}_\Lambda$. In this case g_Λ and $\ell(\xi)$ are invariants for the division algebra D.

PROOF. If $g_D \leqq 0$, $\deg(\xi) = 0 > 2g_D - 2$ where ξ is the unit divisor with respect to some choice of $\mathcal{O}_\Lambda$. Part (2) in Theorem 0.2 yields $n = \ell(\xi) = 1 - g_D$. Since g_D is an invariant for D, so is $\ell(\xi)$ and consequently g_Λ. □

REMARK. The fact that negative genera occur is not strange. It follows from the fact that the dimensions are calculated over k instead of over "algebraic closures" of k in D. It is therefore natural that $g_D = 1 - n$ is the analogue of genus zero in the commutative case. Note also that in these cases $g_\Lambda = 0$.

We now prove that HP.II holds for fields of genus zero.

PROPOSITION 2.2. *Let $K = k(\mathscr{C})$ be a field of genus zero over k. Let D be a division algebra with center K which is everywhere unramified, i.e. $e_p = 1$ for all $p \in \mathscr{C}$. Then D is a "constant extension", this means $D \cong d \otimes_k K$ with d a division algebra over k.*

PROOF. The hypotheses yield $g_D = 1 - N^2$, using (6) in the R.R. theorem. Lemma 1.1 then implies that D contains a subring d of k-algebraic elements of degree N^2. Since elements of a k-basis in d remain linearly independent in D it follows that d contains a K-basis for D. □

REMARKS. (1) In the last section we show that HP.II does not hold for fields of genus 1. However a weaker form of the above proposition still holds, i.e. the fact that with the same hypotheses, k is not algebraically closed in D remains true.

(2) Standard examples of division algebras of negative genus are fields of fractions of skew polynomial rings, D's of the form $d(X, \varphi)$, φ an automorphism of d. Cf. [5] for detailed calculations. These are, however, not the only ones: Let $H_1 = \mathbf{C}(X, -)$, then

$$H_1 = \left(\frac{T \quad -1}{\mathbf{R}(T)} \right) \qquad \text{with } T^2 = X;$$

let $H_2 = \left(\frac{-T, -1}{\mathbf{R}(T)}\right)$. Suppose $H_2 \cong d(X, \varphi)$, then necessarily $H_2 \cong \mathbf{C}(X, -) \cong H_1$. But

$$H_1 \otimes_{\mathbf{R}(T)} H_2 \sim \left(\frac{-T^2 \quad -1}{\mathbf{R}(T)}\right) \cong \left(\frac{-1 \quad -1}{\mathbf{R}(T)}\right)$$

($\sim$ means equivalent in the Brauer group); the latter is not a full matrix ring over $\mathbf{R}(T)$, so $H_1 \not\cong H_2$.

3. The genus of the center is 1

In this section we consider division algebras with center function fields of elliptic curves.

We obtain the following analogue for Proposition 2.2 in this case:

THEOREM 3.1. *Let D, K, k be as before. Suppose $g_K = 1$ and $\mathscr{C}$ has a rational point over k, say x. If D is everywhere unramified, $e_p = 1$ for all $p \in C$, and if $\hat{D}_x$ is a full matrix ring. Then the maximal k-algebraic extensions in D have all the same degree which is equal to $N = \operatorname{index} D$.*

PROOF. Suppose k is algebraically closed in D. Let $\mathcal{O}_{\mathscr{C}}$ be the structure sheaf of D, $\mathcal{O}_\Lambda$ a sheaf of max.$\mathcal{O}_{\mathscr{C}}$-orders in D. Let $\mathcal{M}$ be a maximal right ideal of $\mathcal{O}_\Lambda$ such that $\mathcal{O}_{\Lambda,y} = \mathcal{M}_{\Lambda,y}$ for $y \neq x$.

$$\dim_k H^0(\mathscr{C}, \mathcal{M}^{-1}) = \dim H^0(\mathscr{C}, \mathcal{M}\omega_\Lambda) + n_\Lambda - g_\Lambda + \deg \mathcal{M}^{-1}$$

where $n_\Lambda = \ell(\xi)$.

Since k is algebraically closed in D, $n_\Lambda = 1$, $\deg \mathcal{M}\omega_\Lambda < 0$ so $\dim H^0(\mathscr{C}, \mathcal{M}\omega_\Lambda) = 0$.

Since $g_K = 1$, $\omega_{\mathscr{C}} = \mathcal{O}_{\mathscr{C}}$ implying $\omega_\Lambda = \mathcal{O}_\Lambda$ so $g_\Lambda = n_\Lambda = 1$. Substituting in the formula yields $\dim_k H^0(\mathscr{C}, \mathcal{M}^{-1}) = N > 1$. Let now $t \in H^0(\mathscr{C}, \mathcal{M}^{-1})$, $t \notin k$. The coefficients of the reduced characteristic polynomial of t are in $nr(\mathcal{M}^{-1})$. Since $\deg(nr(\mathcal{M}^{-1})) = 1$ and $\mathscr{C}$ is elliptic these coefficients must be in k.

So k cannot be algebraically closed in D.

To prove that the degree of max. alg extensions of k is $\geqq N$, we remark:

LEMMA 3.2. *Let ℓ be a maximal commutative algebraic subfield of D. If $\ell \otimes_k D \cong M_r(E)$ then ℓ is algebraically closed in E.*

PROOF. Let ℓ' be a commutative algebraic extension of ℓ in E, with $[\ell' : \ell] = r'$. Then $D \otimes_k \ell' = (D \otimes_k \ell) \otimes_\ell \ell' = M_{rr'}(E')$. This implies $\ell' \subset D$, contradicting the assumption that ℓ is max. k-algebraic in D. □

So if ℓ is a max. commutative algebraic extension of k in D, let $\ell \otimes_k D = M_r(E)$ for some division algebra E. Then according to the lemma ℓ is algebraically closed in E. But E inherits all hypotheses of D so E must be equal to a commutative field. Therefore $[\ell : k] = N$.

It follows that for max. algebraic sub-division rings d in D the degree $\geqq N$. However since d is imbeddable in all residue algebras of D, also in $M_N(k)$ the residue algebra of x, so $[d:k] \leqq N$. This implies that all max. k-algebraic subrings are commutative fields of degree N. □

This theorem yields a class of counterexamples for HP.II. The following example shows that this class is not empty. Since in the example the ground field k is a C_1 field it also gives a counterexample to the classical Hasse principle (HP.I).

$$k = \mathbf{C}(t), \qquad \mathscr{C} = ;\ Y^2 = X^3 - X.$$

Take

$$H = \begin{pmatrix} t & x \\ & k(x, y) \end{pmatrix}.$$

The principle divisor $(x) = 2O - 2P$, where O is the point at infinity and P is the origin.

Since k is C_1 it follows that x is locally a norm so H is locally trivial everywhere. But H itself is a division algebra.

To see this consider $tf^2 + xg^2 = 1$. First note that f or g cannot have poles in t since tf^2 has then an odd pole in t and g^2 has an even pole in t; these cannot cancel out.

Now substitute $t = 0$, then $xg'^2 = 1$ cannot have a solution in $\mathbf{C}(x, y)$ since x is not a square in $\mathbf{C}(x, y)$. So the above equation has no solution in $\mathbf{C}(t)(x, y)$.

References

1. R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.

2. T. Nyman and G. Whaples, *Hasse's principle for simple algebras over function fields of curves. I*, J. Reine Angew. Math. **299/300** (1978), 396–405.

3. I. Reiner, *Maximal Orders*, Academic Press, London, 1975.

4. M. Van den Bergh and J. Van Geel, *A duality theorem for orders in central simple algebras over function fields*, J. Pure Appl. Alg. **31** (1984), 227–239.

5. J. Van Geel, *Places and Valuations in Noncommutative Ring Theorey*, Lecture Notes 71, Marcel Dekker, New York, 1981.

6. F. Van Oystaeyen and A. Verschoren, *Noncommutative Algebraic Geometry*, Lecture Notes in Math. 887, Springer-Verlag, Heidelberg, 1981.

7. E. Witt, *Uber ein Gegenbeispiel zum Normensatz*, Math. Z. **39** (1934), 462–467.