Division Algebras on $\mathbb{P}^2$ of Odd Index, Ramified Along a Smooth Elliptic Curve Are Cyclic

Michel Van den BERGH*

Abstract

The simplest non-trivial division algebras that can be constructed over a rational function field in two variables are those that ramify along a divisor of degree three. In this note we give a precise structure theorem for such division algebras. It follows in particular that they are cyclic if the ramification locus is singular or if the index is odd.

Résumé

Les corps gauches non-triviaux les plus simples que l'on peut construire sur un corps de fonctions rationnelles à deux variables sont ceux qui se ramifient lelong d'un diviseur de degré trois. Dans cette note, nous donnons un théorème de structure précis pour de tels corps gauches. En particulier, il en résulte qu'ils sont cycliques si le lieu de ramification est singulier ou si l'indice est impair.

1 Introduction

Let R be a discrete valuation ring with quotient field K and residue field l. We assume that both l and K are of characteristic zero. Then it is classical [5] that there is an exact sequence

$$0 \to \mathrm{Br}(R) \to \mathrm{Br}(K) \xrightarrow{\mathrm{ram}} H^1(l, \mathbb{Q}/\mathbb{Z}) \to 0$$

Here $H^1(l, \mathbb{Q}/\mathbb{Z})$ is the set of couples (l', σ) where l' is a cyclic extension of l and σ is a generator of $\mathrm{Gal}(l'/l)$. The *ramification map*, denoted by ram, is as described in [5]. Assume $[D] \in \mathrm{Br}(K)$. Then there is an unramified finite Galois extension L/K splitting D. Let S be the integral closure of R in L. S is a semi-local Dedekind domain. Let $\mathrm{Div}(S)$ be the group of divisors of S. Associating to $f \in L^*$ its divisor S yields a homomorphism

$$L^* \to \mathrm{Div}(S) \tag{1.1}$$

AMS 1980 *Mathematics Subject Classification* (1985 *Revision*): 16K20, 13A20

*The author is a director of research at the NFWO — Limburgs Universitair Centrum, Departement WNI,Campus Universitaire, 3590 Diepenbeek, Belgium

Clearly $\mathrm{Div}(S) = \mathbb{Z}G/G_{\mathfrak{p}}$ where $G = \mathrm{Gal}(L/K)$ and $G_{\mathfrak{p}}$ is the stabilizer of a prime divisor $\mathfrak{p}$ of S. Alternatively $G_{\mathfrak{p}} = \mathrm{Gal}\big((S/\mathfrak{p})/l\big)$. Taking Galois cohomology of (1.1) yields a map

$$H^2(G, L^*) \to H^2(G, \mathrm{Div}(S)) \cong H^2(G_{\mathfrak{p}}, \mathbb{Z}) \cong H^1(G_{\mathfrak{p}}, \mathbb{Q}/\mathbb{Z}) \tag{1.2}$$

where the first isomorphism is Shapiro's lemma. The composition of the maps in (1.2) is the ramification map. Now let k be an algebraically closed field of characteristic zero and let Y be a simply connected surface over k. According to [2] there is a long exact sequence

(1.3)

$$0 \to \mathrm{Br}(Y) \to \mathrm{Br}(K(Y)) \xrightarrow{\oplus \mathrm{ram}_C} \bigoplus_{\substack{C \subset Y \\ \text{irr. curve}}} H^1(K(C), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\overset{\oplus}{x \in C} r_{C,x}} \bigoplus_{x \in Y} \mu^{-1} \xrightarrow{\sum} \mu^{-1} \to 0$$

Here $\mu^{-1} = \bigcup_n \mathrm{Hom}(\mu_n, \mathbb{Q}/\mathbb{Z})$ where μ_n is the group of n'th roots of unity. Hence, non-canonically, $\mu^{-1} \cong \mathbb{Q}/\mathbb{Z}$. As above $H^1(K(C), \mathbb{Q}/\mathbb{Z}) \to \mu^{-1}$ is given by the cyclic extensions of $K(C)$. Given such a cyclic extension one may measure its ramification at a point y of the normalization $\bar{C}$ of C in terms of an element of μ^{-1}. $r_{C,x}$ is defined as the sum of the ramifications of the points $y \in \bar{C}$ lying above x. For $D \in \mathrm{Br}(K(Y))$ we write

$$R = \bigcup_C \{C \subset Y \mid \mathrm{ram}_C(D) \neq 0\}$$

and we call R the *ramification locus* of D. By construction R is a reduced divisor in Y. In the rest of this note we specialize to $Y = \mathbb{P}^2_k$. In that case $\mathrm{Br}(Y) = 0$ and so (1.3) allows us to compute $\mathrm{Br}(K(Y)) = \mathrm{Br}(k(u, v))$. The following result easily follows

Lemma 1.1 — *Let D, R, Y be as above and assume that D is non-trivial. Then*

1. $\deg R \geq 3$.
2. *If* $\deg R = 3$ *then there are the following possibilities*
   (a) *R is a union of three lines, not passing through one point.*
   (b) *R is a union of a line and a conic, not tangent to one another.*
   (c) *R is a nodal elliptic curve.*
   (d) *R is a smooth elliptic curve.*

A long standing question, due to Albert, is whether every division algebra of prime index is cyclic. Given the seemingly rather tractable nature of division algebras ramified along a cubic divisor, some people have suggested that these might be used to answer Albert's question negatively. See for example [11]. In this note we show that this is not so. That is, we show

Proposition 1.2 — *Let D be a non-trivial central division algebra over $K(\mathbb{P}^2_k)$ and let R be its ramification divisor. Assume that* $\deg R = 3$ *and that one of the following hypotheses holds.*

1. *R is singular.*
2. *R is smooth and the period of D in the Brauer group is odd.*

Then D is cyclic and has period equal to index.

Part (1) of this proposition has already been proved by T. Ford using somewhat different methods [9]. Furthermore in [15] it is shown that if R is smooth then D is similar to a tensor product of three cyclic algebras. Finally, with R still smooth, it has been shown in [11] (under considerably weaker hypotheses on k) that D is cyclic if its period is 5 or 7. Proposition 1.2 is a corollary of the following theorem

Theorem 1.3 — *Let D be a central division algebra over $K(\mathbb{P}^2_k)$ and let R be its ramification locus. Assume that* $\deg R = 3$. *Then the following holds*

1. *If R is singular then as k-algebras*

$$D \cong k(x, y; yx = \omega xy) \tag{1.4}$$

   where ω is a root of unity.

2. *If R is smooth then as k-algebras*

$$D \cong K(S)(x, \tau)^H \tag{1.5}$$

   where

   - *S is an unramified cyclic covering of R (hence in particular S is an elliptic curve).*
   - *τ is a generator for* $\mathrm{Gal}(S/R)$.
   - *$H = \{1, \sigma\}$ with $\sigma(u) = -u$ for $u \in S$ (for a choice of group law on S) and $\sigma(x) = x^{-1}$.*

That Proposition 1.2 follows from Theorem 1.3 is clear in the singular case, and in the smooth case it follows from [14]. I wish to thank Burt Fein, Zinovy Reichstein for some valuable comments and for pointing out an error in an earlier version of this note. I also wish to thank Colliot-Thélène for some private communication concerning the case where k is not algebraically closed. This is reproduced in the appendix.

2 Proof of Theorem 1.3

Let us first recall the following result

Proposition 2.1 — *Let l be a field of characteristic zero. Then there is an exact sequence*

(2.1)
$$0 \to \mathrm{Br}(l) \to \mathrm{Br}(K(\mathbb{P}^1_l)) \xrightarrow{\oplus \mathrm{ram}_x} \bigoplus_{x \in \mathbb{P}^1_l} H^1(l(x), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\oplus \mathrm{cor}_{l(x)/l}} H^1(l, \mathbb{Q}/\mathbb{Z}) \to 0$$

Here $x \in \mathbb{P}^1_l$ runs through the closed points of $\mathbb{P}^1_l$.

Proof. This is a version of the Faddeev-Auslander-Brumer sequence where one keeps track of the point at infinity. It is also very closely related to various exact sequences occurring in [7]. Let us quickly recall the proof. Let $\bar{l}$ be the algebraic closure of l and let $\mathrm{Prin}(\mathbb{P}^1_{\bar{l}})$, $\mathrm{Div}(\mathbb{P}^1_{\bar{l}})$ respectively stand for the principal divisors and the Weil divisors on $\mathbb{P}^1_{\bar{l}}$. We have exact sequences of $G = \mathrm{Gal}(\bar{l}/l)$ modules

$$0 \to \bar{l}^* \to K(\mathbb{P}^1_{\bar{l}})^* \to \mathrm{Prin}(\mathbb{P}^1_{\bar{l}}) \to 0$$
$$0 \to \mathrm{Prin}(\mathbb{P}^1_{\bar{l}}) \to \mathrm{Div}(\mathbb{P}^1_{\bar{l}}) \xrightarrow{\deg} \mathbb{Z} \to 0$$

Both these sequences are (non-canonically) split. This is clear for the second one. For the first one we send $f \in K(\mathbb{P}^1_{\bar{l}})^*$ to the first non-zero coefficient of the Taylor series expansion of f around 0 (for a G invariant uniformizing element). Hence applying $H^2(G, -)$ to these exact sequences, and afterwards combining them, yields a long exact sequence

$$0 \to \mathrm{Br}(l) \to \mathrm{Br}(K(\mathbb{P}^1_l)) \to H^2(G, \mathrm{Div}(\mathbb{P}^1_{\bar{l}})) \xrightarrow{\deg} H^2(G, \mathbb{Z}) \to 0$$

taking into account that $H^2(G, \bar{l}^*) = \mathrm{Br}(l)$ and by Tsen's theorem $H^2(G, K(\mathbb{P}^1_{\bar{l}})^*) = \mathrm{Br}(K(\mathbb{P}^1_l))$. Now $\mathrm{Div}(\mathbb{P}^1_{\bar{l}}) = \bigoplus_{x \in \mathbb{P}^1_l} \mathbb{Z}G/G_x$ where $G_x = \mathrm{Gal}(\bar{l}/l(x))$. So by Shapiro's lemma $H^2(G, \mathrm{Div}(\mathbb{P}^1_{\bar{l}})) = \bigoplus_x H^2(G_x, \mathbb{Z})$. It is now clear that the resulting map

$$\bigoplus_x H^2(G_x, \mathbb{Z}) \xrightarrow{\deg} H^2(G, \mathbb{Z})$$

is obtained by applying $H^2(G, -)$ to the "sum map" $\mathbb{Z}G/G_x \to \mathbb{Z}$ and then invoking Shapiro's lemma. It follows from [6, Prop. III.6.2] that this is precisely the corestriction. To obtain the exact form of (2.1) we use $H^2(G, \mathbb{Z}) = H^1(l, \mathbb{Q}/\mathbb{Z})$, $H^2(G_x, \mathbb{Z}) = H^1(l(x), \mathbb{Q}/\mathbb{Z})$. That the map $\mathrm{Br}(K(\mathbb{P}^1_l)) \to \bigoplus H^1(l(x), \mathbb{Q}/\mathbb{Z})$ is $\bigoplus \mathrm{ram}_x$ follows by looking at the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & l^* & \longrightarrow & K(\mathbb{P}^1_{\bar{l}})^* & \longrightarrow & \mathrm{Prin}(\mathbb{P}^1_{\bar{l}}) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{O}^*_{\mathbb{P}^1_{\bar{l}},x} & \longrightarrow & K(\mathbb{P}^1_{\bar{l}})^* & \longrightarrow & \mathrm{Div}(\mathbb{O}_{\mathbb{P}^1_{\bar{l}},x}) & \longrightarrow & 0
\end{array}$$

□

Theorem 2.2 — *Assume that l is a field of characteristic zero with trivial Brauer group, containing a primitive n^{th} root of unity. Let D be a central division algebra of period n over $K(\mathbb{P}^1_l)$.*

1. *If D is ramified in at most two points of degree one then as l-algebras*

$$D \cong L(x,\tau) \tag{2.2}$$

where L/l is cyclic of dimension n and τ is a generator of $\mathrm{Gal}(L/l)$.

2. *If D is ramified in one point u of degree two then as l-algebras*

$$D \cong L(x,\tau)^H \tag{2.3}$$

where L/l is a dihedral extension of dimension $2n$ containing $l(u)$, τ is a generator of $\mathrm{Gal}(L/l(u))$, $H = \mathrm{Gal}(l(u)/l) = \{1,\sigma\}$ (with action lifted in a arbitrary way to L) and $\sigma(x) = x^{-1}$.

Proof. The proof consists in showing that the division algebras on the right side of (2.2) and (2.3) have the same ramification as D.

1. This part can be deduced from [8, Prop. 2.1]. For completeness we give a proof. We can choose an affine coordinate y on $\mathbb{P}^1_l$ such that D is ramified on $y = 0, \infty$. Let $(L,\tau) = \mathrm{ram}_0(D)$ and put $E = L(x,\tau)$. Then $Z(E) = k(x^n)$ and if we put $y = x^n$ then E is ramified in $y = 0, \infty$ with $\mathrm{ram}_0(E) = (L,\tau)$. Hence D, E have the same ramification data and thus $D \cong E$.

2. Assume $k(u) = k(\sqrt{t})$. We can now choose an affine coordinate y on $\mathbb{P}^1_l$ such that D is ramified in the prime $(y^2 - t)$. Put $(L,\tau) = \mathrm{ram}_u(D)$. We claim that L/l is dihedral. By Kummer theory $L = l(u)(\sqrt[n]{a})$. Since u is the only place where D ramifies, the corestriction of L must be trivial by (2.1). According to [15, lemma 0.1] this corestriction is given by $l(\sqrt[n]{a\,\sigma a})$ where $\mathrm{Gal}(l(u)/l) = \{1,\sigma\}$. So $a\,\sigma a = q^n$, $q \in l$. This allows us to lift the action of σ to L by putting $\sigma(\sqrt[n]{a}) = q/\sqrt[n]{a}$. Hence L/l is dihedral.
Put $E_1 = L(x,\tau)$, $E = E_1^H$. Then $Z(E_1) = l(u)(x^n)$ and since H acts non-trivially on $l(u)(x^n)$, $Z(E) = Z(E_1)^H = k\left(\frac{\sqrt{t}(x^n-1)}{x^n+1}\right)$. Put $y = \frac{\sqrt{t}(x^n-1)}{x^n+1}$. Then using the definition of the ramification map, one easily verifies that E is only ramified in $u = (y^2 - t)$ and furthermore $\mathrm{ram}_u(E) = (L,\tau)$. Hence once again D and E have the same ramification data and thus $D \cong E$. □

Proof of Theorem 1.3. As an example we will discuss the cases where R is a nodal or a smooth elliptic curve. The other two cases in lemma 1.1 are similar. Throughout n is the period of D in the Brauer group.

***R* a nodal elliptic curve.** Let $y \in R$ be the singular point and let $B \subset \mathbb{P}^2_k$ be a line not passing through y. Our aim is to project from $\mathbb{P}^2_k$ to B with center y.