PATCHING AND ADMISSIBILITY OVER TWO-DIMENSIONAL COMPLETE LOCAL DOMAINS

by

Danny Neftin

Department of Mathematics, Technion – Israel Institute of Technology,

Haifa 3200, Israel

e-mail: neftind@tx.technion.ac.il

and

Elad Paran

Einstein Institute of Mathematics, J. Safra Campus, Givat Ram,

The Hebrew University of Jerusalem, Jerusalem 91904, Israel

e-mail: paranela@post.tau.ac.il

Abstract

We develop a patching machinery over the field $E = K((X,Y))$ of formal power series in two variables over an infinite field K. We apply this machinery to prove that if K is separably closed and G is a finite group of order not divisible by $\mathrm{char}(E)$, then there exists a G-crossed product algebra with center E if and only if the Sylow subgroups of G are abelian of rank at most 2.

MR Classification: 12E30, 16S35

Introduction

Complete local domains play an important role in commutative algebra and algebraic geometry, and their algebraic properties were already described in 1946 by Cohen's

---

The second author was partially supported by the Israel Science Foundation (grant No. 343/07), and by an ERC grant.

structure theorem. The Galois theoretic properties of their quotient fields were extensively studied over the past two decades. The pioneering work in this line of research is due to Harbater [Ha87], who introduced the method of patching to prove that if R is a complete local domain with quotient field K, then every finite group occurs as a Galois group over $K(x)$. This result was strengthened by Pop [Po96], and in a different language, by Haran-Jarden [HaJ98], who showed that if moreover R is of dimension 1, then every finite split embedding problem over $K(x)$ is solvable.

The first step towards higher dimension was made by Harbater-Stevenson [HaS05], who essentially showed that if R is a complete local domain of dimension 2, then every finite split embedding problem over $\mathrm{Quot}(R)$ has $|R|$ independent solutions. That is, the absolute Galois group of $\mathrm{Quot}(R)$ is semi-free of rank $|R|$ (see [BHH10] for details on this notion). This result was later generalized by Pop [Po10] and by the second author [Pa10], who showed that if K is the quotient field of a complete local domain of dimension exceeding 1, then $\mathrm{Gal}(K)$ is semi-free.

Despite the major progress made in the study of Galois theory over these fields, little is known about the structure of division algebras over them. A step in that direction was recently made by Harbater-Hartmann-Krashen [HHK10]. In that work, the authors consider a question relating Galois theory and Brauer theory over a field E – which groups are admissible over E ? That is, which finite groups occur as a Galois group of an **adequate** Galois extension F/E (recall that an extension F/E is called adequate if F is a maximal subfield in an E-central division algebra). Equivalently, for which groups G there is a G-crossed product division algebra with center E. Note that for E as above and a finite extension F/E, the above maximality requirement can be omitted since any F which is a subfield of an E-division algebra is also a maximal subfield of some E-division algebra (see Remark 3.9).

This question was first considered by Schacher over global fields. In [Sch68], Schacher proved that any $\mathbb{Q}$-admissible group has metacyclic Sylow subgroups and conjectured the converse. Admissibility was studied extensively over global fields (for example: [Ste82], [Son83], [SS92], [Lid96], [Fei04], [Nef10]), function fields and fields of Laurent series (for example: [FSS92], [FS95a], [FS95b]).

The main theorem of [HHK10] asserts that if E is a function field in one variable over a complete discretely valued field with an algebraically closed residue field, then a finite group G of order not divisible by $\mathrm{char}(E)$ is admissible over E if and only each of the Sylow subgroups of G is abelian of rank at most 2 (i.e. generated by two elements).

In this work, we take the next natural step, and determine the admissible groups over quotient fields of equicharacteristic (i.e. having the same characteristic as their residue field) two-dimensional complete local domains, with a separably closed residue field. In particular, we determine the admissible groups over $C((X,Y))$, whenever C is a separably closed field. This problem was posed to the first author by Harbater. We show that the result of [HHK10] holds over these fields as well.

Main Theorem: *Let R be an equicharacteristic complete local domain of dimension 2, with a separably closed residue field. Let G be a finite group of order not divisible by* $\mathrm{char}(R)$. *Then G is admissible over* $\mathrm{Quot}(R)$ *if and only if each of its Sylow subgroups is abelian of rank at most 2.*

The forward direction (i.e. the "only if" part) of the main theorem is essentially proven in [HHK10], using results of Colliot-Thélène-Ojanguren-Parimala [COP02].

The backward direction (i.e. the "if" part) of the main theorem actually holds in greater generality – the residue field need not be separably closed, it suffices that it contains a primitive root of unity of order k, for each $k \in \mathbb{N}$ not divisible by $\mathrm{char}(R)$ (Proposition 3.7). Our proof strategy for the backward direction is as follows. We first use Cohen's structure theorem to reduce the problem from $\mathrm{Quot}(R)$ to a field E of the form $K((X,Y))$. We then apply a patching argument as in [HHK10]; we explicitly realize each Sylow subgroup of G by a Galois extension of E which is a maximal subfield in some E-central division algebra. We then patch these realizations into a Galois extension F/E with group G, in a way that also patches the division algebras into an E-central division algebra D containing F as a maximal subfield.

A key ingredient in our proof is a patching machinery over fields of the form $K((X,Y))$, where K may be an arbitrary infinite field. In [Po10] and [Pa10], problems over $K((X,Y))$ are lifted to $K((X,Y))(Z)$, solved there (via different methods), and then the solutions are specialized into solutions over $K((X,Y))$ using Hilbertianity. This approach seems inapplicable to our current goal, since adequate extensions usually do not remain adequate under specialization. Instead we patch groups directly over $K((X,Y))$. To this end we define "analytic fields" over $K((X,Y))$, satisfying the axioms of algebraic patching (i.e. matrix factorization and intersection), as presented in [HaJ98] (a slightly different axiomatization from the "field patching" axiomatization of [HaH10]). The construction of these analytic rings is of a rigid-geometric nature. In recent communication with David Harbater, we learned that a formal-geometric analogue of this form of patching was carried out by him in [Ha03, Theorem 5.3.9] in order to solve split embedding problems over the field $\mathbb{C}((X,Y))$ of formal power series in two variables over the complex numbers. The core patching arguments in the proof of [Ha03, Theorem 5.3.9] can be extended to replace $\mathbb{C}$ by an arbitrary field and used to study admissible groups, in a similar fashion to our development here.

Acknowledgement: The authors wish to thank David Harbater for useful comments, and the referee, for many comments and corrections that significantly improved the presentation of this work.

1. Analytic fields

In this section we establish our patching machinery.

Fix an infinite field K, and let $E = K((X,Y)) = \mathrm{Quot}(K[[X,Y]])$ be the field of formal power series over K in the variables X, Y. Denote by v the order function of the maximal ideal $\langle X,Y\rangle$ in $K[[X,Y]]$. Then v extends uniquely to a discrete rank-1 valuation of E. Note that $K[[X,Y]]$ is strictly contained in the valuation ring of v in E.

Construction 1.1: Analytic rings over E. Let I be a finite set. For each $i \in I$ let $c_i \in K$, such that $c_i \neq c_j$ for $i \neq j$ (such a choice is possible since K is infinite). For each $i \in I$ denote $z_i = \frac{Y}{X - c_i Y} \in E$. For each $J \subseteq I$, consider the subring $K[z_j \mid j \in J][X,Y]$ of E, and let D_J be the completion of this ring with respect to v. Note that for each $J \subseteq I$, $D_J \subseteq D_I$, and that $D_\emptyset = K[[X,Y]]$, since $K[[X,Y]]$ is complete. Let $Q = \mathrm{Quot}(D_I)$, and for each $i \in I$ denote $Q_i = E \cdot D_{I \smallsetminus \{i\}}$, and $Q'_i = \bigcap_{j \neq i} Q_j$. ∎

For the rest of this section, we fix the notation of Construction 1.1. A geometric interpretation of the rings defined in Construction 1.1 appears in Remark 1.12. In order to present this interpretation, we need several lemmas.

LEMMA 1.2: *Let $i \in I$. Then v is trivial on $K(z_i)$.*

Proof: It suffices to prove that v is trivial on $K[z_i]$. Let $0 \neq f = \sum_{n=0}^{d} a_n z_i^n \in K[z_i]$, with $a_0, \dots, a_d \in K$. Without loss of generality, $a_0 \neq 0$. We have

$$\sum_{n=0}^{d} a_n z_i^n = \frac{\sum_{n=0}^{d} a_n Y^n (X - c_i Y)^{d-n}}{(X - c_i Y)^d}.$$

By opening parentheses, the numerator in this expression can be written as a sum of monomials of degree d. For $n = 0$ we get the summand $a_0 X^d$, while all other monomials in this presentation have a positive power of Y, so they do not cancel $a_0 X^d$. Thus the numerator has value d, and clearly so does the denominator, so $v(f) = 0$. ∎

COROLLARY 1.3: *The valuation v is trivial on $K[z_i \mid i \in I]$.*

Proof: Note that for each $i, j \in I$ we have $K(z_i) = K(z_j)$. Thus by the preceding lemma, v is trivial on $K(z_i) = K(z_j \mid j \in I)$, and in particular v is trivial on the subring $K[z_i \mid i \in I]$. ∎

LEMMA 1.4: *Let $J \subseteq I$ and $j \in J$. Then the ring $K[z_l \mid l \in J][X - c_j Y]$ is isomorphic to the ring of polynomials in one variable over $K[z_l \mid l \in J]$.*

Proof: To prove the claim we show that if $\sum_{n=0}^{d} a_n (X - c_j Y)^n = 0$, for $a_0, \dots, a_d \in K[z_l \mid l \in J]$, then $a_0 = \dots = a_d = 0$. If not, suppose (without loss of generality) that $a_0 \neq 0$. By Corollary 1.3, $v(a_0) = 0$ while $v(a_k (X - c_j Y)^k) = v(a_k) + k = k > 0$ for each $k > 0$. Hence $\infty = v(0) = v(\sum_{n=0}^{d} a_n (X - c_j Y)^n) = 0$, a contradiction. ∎

In view of Lemma 1.4, for each $J \subseteq I, j \in J$, each element of $K[z_l \mid l \in J][X - c_j Y]$ has a unique presentation as a polynomial in $X - c_j Y$. Thus we have a natural valuation on this ring, given by $v'(\sum_{n=0}^{d} a_n (X - c_j Y)^n) = \min(n \mid a_n \neq 0)$, and we may form the completion $K[z_l \mid l \in J][[X - c_j Y]]$ of this ring with respect to v'.

PROPOSITION 1.5: *Let $J \subseteq I$ and $j \in J$. Then $D_J = K[z_l \mid l \in J][[X - c_jY]]$, and v is given on D_J by $v(\sum_{n=0}^{\infty} a_n(X - c_jY)^n) = \min(n \mid a_n \neq 0)$.*

Proof: By Lemma 1.4, v coincides with v' (given in the paragraph preceding this proposition) on $K[z_l \mid l \in J][X - c_jY]$, hence $K[z_l \mid l \in J][[X - c_jY]]$ is the completion of $K[z_l \mid l \in J][X - c_jY]$ with respect to v, and v coincides with v' on the completion. Note that $K[z_l \mid l \in J][X - c_jY] = K[z_l \mid l \in J][X, Y]$ (since $Y = z_j(X - c_jY)$, $X = (1 + c_jz_j)(X - c_jY)$), hence by the definition of D_J we are done. ∎

LEMMA 1.6: *Let $J \subseteq I$. Then $K[z_j \mid j \in J] = \sum_{j \in J} K[z_j]$.*

Proof: For each $i \neq j \in J$ we have

$$z_i \cdot z_j = \frac{Y^2}{(X - c_iY) \cdot (X - c_jY)} = \frac{1}{c_i - c_j} \cdot z_i + \frac{1}{c_j - c_i} z_j.$$

The claim now follows by induction on $|I|$. ∎

PROPOSITION 1.7: *Let $J, J' \subseteq I$. Then for each $f \in D_{J \cup J'}$ there exist $f_1 \in D_J$ and $f_2 \in D_{J'}$ with $v(f_1), v(f_2) \geq v(f)$, such that $f = f_1 + f_2$.*

Proof: Replace J with $J \smallsetminus (J \cap J')$ to assume that $J \cap J' = \emptyset$. Moreover, without loss of generality J, J' are non-empty. Choose $j \in J, j' \in J'$ and denote $A_J = K[z_l \mid l \in J], A_{J'} = K[z_l \mid l \in J'], A = K[z_l \mid l \in J \cup J']$. By Proposition 1.5, $D_J = A_J[[X - c_jY]]$, $D_{J'} = A_J[[X - c_{j'}Y]]$, $D_{J \cup J'} = A[[X - c_jY]]$. Let $f = \sum_{n=m}^{\infty} a_n(X - c_jY)^n \in D_{J \cup J'}$, with $a_m \neq 0$. Then $v(f) = m$ by Proposition 1.5. By Lemma 1.6, $A = A_J + A_{J'}$. For each $n \geq m$, let $b_n \in A_J, b'_n \in A_{J'}$ such that $a_n = b_n + b'_n$. Denote $f_1 = \sum_{n=m}^{\infty} b_n(X - c_jY)^n$, $f_2 = f - f_1 = \sum_{n=m}^{\infty} b'_n(X - c_jY)^n$. Then $f_1 \in D_J$ and $v(f_1) \geq m$. It remains to prove that $f_2 \in D_{J'}$ and that $v(f_2) \geq m$. This follows by the following equality:

$$f_2 = \sum_{n=m}^{\infty} b'_n(X - c_jY)^n = \sum_{n=m}^{\infty} b'_n((X - c_{j'}Y) + (c_{j'} - c_j)Y)^n$$

$$= \sum_{n=m}^{\infty} (b'_n(1 + (c_{j'} - c_j)z_{j'})^n)(X - c_{j'}Y)^n.$$

∎

The next lemma is a variant of [HaH10, Lemma 3.3], allowing non-principal ideals.

Lemma 1.8: *Let $R \subseteq R_1, R_2 \subseteq R_0$ be domains such that $R_0 = R_1 + R_2$. Let w be a non-trivial discrete valuation on $\mathrm{Quot}(R_0)$ such that R is complete with respect to w and $w(x) \geq 0$ for all $x \in R_0$. Let $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_0$ be the centers of w in R, R_1, R_2, R_0, respectively. Suppose that $\mathfrak{p}R_0 = \mathfrak{p}_0$ and $R/\mathfrak{p} = R_1/\mathfrak{p}_1 \cap R_2/\mathfrak{p}_2$ (inside $R_0/\mathfrak{p}_0$). Then $R_1 \cap R_2 = R$.*

Proof: First, note that $\mathfrak{p}_0 = \mathfrak{p}_1 + \mathfrak{p}_2$. Indeed, suppose $x \in \mathfrak{p}_0 = \mathfrak{p}R_0$. Then $x = \sum_{i=1}^n a_i x_i$ for some $a_1, \ldots, a_n \in R_0$ and $x_1, \ldots, x_n \in \mathfrak{p}$. For each $1 \leq i \leq n$, write $a_i = b_i + b_i'$ with $b_i \in R_1$ and $b_i' \in R_2$. Then $\sum a_i x_i = \sum b_i x_i + \sum b_i' x_i \in \mathfrak{p}_1 + \mathfrak{p}_2$, since $\mathfrak{p} \subseteq \mathfrak{p}_1, \mathfrak{p}_2$.

Denote $S = R_1 \cap R_2$ and let $\mathfrak{q}$ be the center of w at S. Then the sequence $0 \to S \to R_1 \times R_2 \to R_0 \to 0$ is exact (where the second map is the diagonal map and the third map is substraction). This sequence induces an exact sequence $0 \to S/\mathfrak{q} \to (R_1/\mathfrak{p}_1) \times (R_2/\mathfrak{p}_2) \to R_0/\mathfrak{p}_0 \to 0$. Indeed, the only non-trivial part in showing this is to check that the kernel of the substraction map is contained in the image of the diagonal map. Suppose $(x_1 + \mathfrak{p}_1, x_2 + \mathfrak{p}_2) \in (R_1/\mathfrak{p}_1) \times (R_2/\mathfrak{p}_2)$ satisfies $x_1 - x_2 \in \mathfrak{p}_0$. Since $\mathfrak{p}_0 = \mathfrak{p}_1 + \mathfrak{p}_2$ we may choose $y_1 \in \mathfrak{p}_1, y_2 \in \mathfrak{p}_2$ such that $x_1 - y_1 = x_2 - y_2$. Then $(x_1 + \mathfrak{p}_1, x_2 + \mathfrak{p}_2) = (x_1 - y_1 + \mathfrak{p}_1, x_2 - y_2 + \mathfrak{p}_2)$ belongs to the image of the diagonal map. Thus the sequence is exact.

Since $\mathfrak{p}$ is the center of w on R and $\mathfrak{p}_1$ the center of w on R_1, we have $R \cap \mathfrak{p}_1 = \mathfrak{p}$. In particular, the diagonal map $R/\mathfrak{p} \to (R_1/\mathfrak{p}_1) \times (R_2/\mathfrak{p}_2)$ is injective. Since $R_0 = R_1 + R_2$, the substraction map $(R_1/\mathfrak{p}_1) \times (R_2/\mathfrak{p}_2) \to R_0/\mathfrak{p}_0$ is surjective. Thus, since $R/\mathfrak{p} = R_1/\mathfrak{p}_1 \cap R_2/\mathfrak{p}_2$, the sequence $0 \to R/\mathfrak{p} \to (R_1/\mathfrak{p}_1) \times (R_2/\mathfrak{p}_2) \to R_0/\mathfrak{p}_0 \to 0$ is also exact. It follows that the natural map $R/\mathfrak{p} \to S/\mathfrak{q}$ is an isomorphism. In particular, $S = R + \mathfrak{p}S$. By induction we have $S = R + \mathfrak{p}^k S$ for each $k \in \mathbb{N}$. Since $\mathfrak{p}_0 = \mathfrak{p}R_0$, $\mathfrak{p} \neq 0$. Since w is discrete, there exists an integer m such that $v(x) \geq m$ for each $x \in \mathfrak{p}$. Thus $v(x) \geq mk$ for each $x \in \mathfrak{p}^k$, hence R is w-dense in S and therefore the completion of R with respect to w contains S. By our assumptions, R is complete, hence $R = S$. ∎

Lemma 1.9: *The set $\{z_i^n \mid i \in I, n \in \mathbb{N} \cup \{0\}\}$ is K-linearly independent.*

Proof: Suppose $a_0 + \sum_{i \in I} \sum_{n=1}^{d_i} a_{i,n} z_i^n = 0$, where $d_i \in \mathbb{N}$ and $a_0, a_{i,n} \in K$ for each

i, n. We wish to show that $a_0 = a_{i,n} = 0$ for each i, n. Suppose there exist $i \in I, n \in \mathbb{N}$ such that $a_{i,n} \neq 0$. Without loss of generality, $n = d_i$. Since $X - c_i Y$ is a prime element of $K[X, Y]$, it defines a discrete valuation on $K(X, Y)$, which we denote by w. We have $w(Y) = w(Y - c_j X) = 0$ for each $j \neq i$ in I. Thus $w(a_0 + \sum_{j\neq i} \sum_{n=1}^{d_j} a_{j,n} z_j^n) \geq 0$, while $w(\sum_{n=1}^{d_i} a_{i,n} z_i^n) = -d_i$. Thus $w(0) = w(a_0 + \sum_{j\in I} \sum_{n=1}^{d_j} a_{j,n} z_j^n) = -d_i$, a contradiction. ∎

PROPOSITION 1.10: *Suppose $J, J' \subseteq I$. Then $D_J \cap D_{J'} = D_{J\cap J'}$.*

Proof: Clearly, $D_{J\cap J'} \subseteq D_J \cap D_{J'}$. For the converse inclusion, we distinguish between two cases. First suppose that $J \cap J' \neq \emptyset$, and fix $j \in J \cap J'$. Then $D_J = K[z_k \mid k \in J][[X - c_j Y]]$ and $D_{J'} = K[z_k \mid k \in J'][[X - c_j Y]]$, hence $D_J \cap D_{J'} = (K[z_k \mid k \in J] \cap K[z_k \mid k \in J'])[[X - c_j Y]]$. By Lemma 1.9 $K[z_k \mid k \in J] \cap K[z_k \mid k \in J'] = K[z_k \mid k \in J \cap J']$, hence $y \in D_{J\cap J'}$.

Now suppose that $J \cap J' = \emptyset$ and denote $R = K[[X, Y]] = D_\emptyset, R_1 = D_J, R_2 = D_{J'}, R_0 = D_{J\cup J'}$. Since $v(f) \geq 0$ for each $f \in K[z_j \mid j \in J \cup J'][X, Y]$, we also have $v(f) \geq 0$ for each f in the completion R_0. The ring R is complete with respect to v, and $R = R_1 + R_2$ by Proposition 1.7. Let $\mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_0$ be the centers of v at R, R_1, R_2, R_0, respectively. Then $\mathfrak{p}$ is generated by X, Y and $\mathfrak{p}_0$ is generated by $X - c_j Y$ for any $j \in J$, by Proposition 1.5. It follows that $\mathfrak{p} R_0 = \mathfrak{p}_0$. In order to apply Lemma 1.8, it remains to check that $R_1/\mathfrak{p}_1 \cap R_2/\mathfrak{p}_2 = R/\mathfrak{p}$ in $R_0/\mathfrak{p}_0$. Indeed, we have $R_1/\mathfrak{p}_1 = K[z_j \mid j \in J]$, $R_2/\mathfrak{p}_2 = K[z_j \mid j \in J']$, $R_0/\mathfrak{p}_0 = K$. By Lemma 1.9, we are done. ∎

PROPOSITION 1.11: *For each $i \in I$, $Q_i' \cap Q_i = E$.*

Proof: Since $Q_i' = \bigcap_{j\neq i} Q_j$, the assertion is that $\bigcap_{j\in I} Q_j = E$. Indeed, let $y \in \bigcap_{j\in I} Q_j$. For each $j \in J$ write $y = \frac{f_j}{q_j}$ with $f_j \in D_{I\smallsetminus\{j\}}$, $q_j \in K[[X, Y]]$. Taking a common denominator we may assume that q_j is independent of j, and denote $q = q_j$ (for all $j \in J$). It suffices to prove that $qy \in K[[X, Y]] \subseteq E$. But $qy = q_j y = f_j \in D_{I\smallsetminus\{j\}}$ for all $j \in I$, hence $qy \in \bigcap_{j\in I} D_{I\smallsetminus\{j\}} = D_\emptyset = K[[X, Y]]$, by Proposition 1.10. ∎

The following remark gives a rigid-geometric and a formal-geometric interpretation of the rings D_J.

Remark 1.12: Let $J \subseteq I$, $j \in J$. Denote $t = X - c_j Y$. By Proposition 1.5, $D_J = K[z_l \mid l \in J][[t]]$ is the t-adic completion of $K[z_l \mid l \in J][t]$, thus $D_J[t^{-1}]$ is the t-adic completion of $K[z_l \mid l \in J][t, t^{-1}]$. We have $K[z_l \mid l \in J][t, t^{-1}] \subseteq K((t))[z_l \mid l \in J] \subseteq D_J[t^{-1}]$, hence $D_J[t^{-1}]$ is the t-adic completion of $A := K((t))[z_l \mid l \in J]$. Denote $T = K[[t]], F = K((t)), s = \frac{X}{Y}$. Then s is a free variable over F. Let v_t be the t-adic valuation on F, and extend it to $F(s)$ by $v_t(s) = 0$. Note that $z_k = \frac{1}{s - c_k}$ and $v_t(c_l - c_k) = 0$ for all distinct $l, k \in J$. By [HaJ98, Lemma 3.1(c)] (with w_k, K, x there replaced by z_k, F, s here), each element $0 \neq f \in A$ can be uniquely written as

$$(1) \qquad f = f_0 + \sum_{k \in J} \sum_{n=1}^{\infty} f_{kn} z_k^n$$

, where $f_0, f_{kn} \in F$ are almost all zero. The uniqueness in presentation (1) implies that $v_t(f) = \min_{kn}\{v_t(f_0), v_t(f_{kn})\}$.

By [HaJ98, Lemma 3.3] the completion $D_J[t^{-1}]$ of A is the ring of holomorphic functions on the affinoid $U = \mathbb{P} \smallsetminus (\bigcup_{l \in J} B(c_l))$, where $\mathbb{P}$ is the projective s-line and $B(c_l)$ is a disc of radius 1 with center c_l for each $l \in J$ (cf. [FrP04, §2.2]). Moreover, each element $f \in D_J[t^{-1}]$ can be uniquely presented as in (1), where $f_0 \in F$ and $\{f_{ln}\}_{n=1}^{\infty}$ is a null sequence in F (with respect to v_t) for each $l \in J$. Thus, in the rigid-geometric language, D_J is the ring of holomorphic functions on U having no pole at t. Its elements are of the form (1), where the coefficients are now in T (and $\{f_{kn}\}_{n=1}^{\infty}$ is a null sequence for each $k \in J$). In particular, $T[z_l \mid l \in J]$ is dense in D_J.

Let $\hat{X}$ be the projective s-line over T, and let X be its closed fibre. Put $U = X \smallsetminus \{c_l \mid l \in J\}$. Then $R_U = T[\frac{1}{s - c_l} \mid l \in J] = T[z_l \mid l \in J]$ is the set of functions on $\hat{X}$ which are regular on U. Since R_U is t-adically dense in $D_J = K[\frac{1}{s - c_l} \mid l \in J][[t]]$, D_J is the t-adic completion of R_U. In the formal-geometric language, this means that $D_J = \hat{R}_U$ is the ring of regular functions on the t-adic thickening of U (cf. [HaH10, Notation 4.3]). ∎

Corollary 1.13: *Let $J \subseteq I, j \in J$.*

(a) *For each $0 \neq g \in D_J$, $D_J[(X - c_j Y)^{-1}] = K((X - c_j Y))[z_k \mid k \in J] + g D_J[(X - c_j Y)^{-1}]$.*

(b) *For each* $f \in D_J$ *there exist* $h \in K[[X - c_jY]][z_j], u \in D_J^\times$ *such that* $f = hu$.

(c) *The ring* Q_j *is a field.*

Proof: In the notation of Remark 1.12, each element $f \in D_J[t^{-1}]$ can be written in the form $u \cdot h$ with $u \in D_J[t^{-1}]^\times$ and $h \in F[z_j]$, by [HaJ98, Lemma 3.7]. If $f \in D_J$ then we can multiply u and h with a power of t to assume that $u \in D_J^\times$ and $h \in K[[t]][z_j]$. This proves (b). Part (a) is given by [HaJ98, Corollary 3.8]. By [HaH10, Corollary 4.8] (now viewing the rings D_J in the formal-geometric context) $\mathrm{Quot}(D_J)$ is the compositum of $K((t))(\frac{X}{Y})$ and D_J. Since $K((t))(\frac{X}{Y}) \subseteq E$, we have $\mathrm{Quot}(D_J) = ED_J$. Applying this argument for $J \smallsetminus \{j\}$ instead of J we have $Q_j = \mathrm{Quot}(D_{I \smallsetminus \{j\}}) = ED_{I \smallsetminus \{j\}}$, hence $\mathrm{Quot}(Q_j) = \mathrm{Quot}(ED_{I \smallsetminus \{j\}}) = E\mathrm{Quot}(D_{I \smallsetminus \{j\}}) = ED_{I \smallsetminus \{j\}} = Q_j$ is a field. ∎

The proof of the following proposition is based on that of [HaJ98, Corollary 4.4]. (We cannot use [HaJ98, Corollary 4.4] as it is, since condition (e') of that claim does not hold for D_I itself.)

PROPOSITION 1.14: *Let* $i \in I$, $n \in \mathbb{N}$ *and let* $b \in \mathrm{GL}_n(Q)$. *There exist* $b_1 \in \mathrm{GL}_n(Q_i)$ *and* $b_2 \in \mathrm{GL}_n(Q_i')$ *such that* $b = b_1 \cdot b_2$.

Proof: Denote by $|\cdot|$ the absolute value on Q that corresponds to v. The rings $A = D_I$, $A_1 = D_{I \smallsetminus \{i\}}, A_2 = D_{\{i\}}$ are complete with respect to $|\cdot|$ and Proposition 1.7 asserts that condition (d') of [HaJ98, Example 4.3] holds for these rings. We extend $|\cdot|$ to the maximum norm $||\cdot||$ on $M_n(Q)$, as in [HaJ98, Example 4.3]. Then $M_n(A), M_n(A_1), M_n(A_2)$ are complete with respect to $||\cdot||$ and condition (d) of [HaJ98, §4] holds. By Cartan's Lemma [HaJ98, Lemma 4.2], for each $a \in \mathrm{GL}_n(A)$ with $||a - 1|| < 1$ there exist $a_1 \in \mathrm{GL}_1(A_1)$, $a_2 \in \mathrm{GL}_1(A_2)$ such that $a = a_1 \cdot a_2$.

Denote $E_1 = \mathrm{Quot}(A_1) = Q_i, E_2 = \mathrm{Quot}(A_2) = Q_i'$. In order to factor b (which need not be in $\mathrm{GL}_n(A)$), let $t = X - c_iY$, $T = k[[t]]$. By Remark 1.12 (for $J = I$) $A_0 = T[z_k \mid k \in I]$ is a dense subring of A, and by Corollary 1.13(b) there exists $h \in A_0$ such that $hb \in \mathrm{M}_n(A)$. If $hb = b_1b_2'$ with $b_1 \in \mathrm{GL}_n(E_1)$ and $b_2' \in \mathrm{GL}_n(E_2)$, then $b = b_1b_2$ with $b_2 = \frac{1}{h}b_2' \in \mathrm{GL}_n(E_2)$. So we may assume that $b \in \mathrm{M}_n(A)$.

Let $0 \neq d = \det(b) \in A$. By Corollary 1.13(b) there are $0 \neq g \in A_0$ and $u \in A^\times$ such that $d = gu$. Let $b'' \in \mathrm{M}_n(A)$ be the adjoint matrix of b, so that $bb'' = d1$. Let

$b' = u^{-1}b''$. Then $b' \in \mathrm{M}_n(A)$ and $bb' = g1$. Put

$$V = \{a' \in \mathrm{M}_n(A[t^{-1}]) \mid ba' \in gM_n(A[t^{-1}])\}, V_0 = V \cap M_n(A_0[t^{-1}]).$$

Then V is an additive subgroup of $M_n(A[t^{-1}])$ and $gM_n(A[t^{-1}]) \leq V$. By Corollary 1.13(a) $M_n(A[t^{-1}]) = M_n(A_0[t^{-1}]) + gM_n(A[t^{-1}])$, hence $V = V_0 + gM_n(A[t^{-1}])$. Since A_0 is dense in A, $gM_n(A_0[t^{-1}])$ is dense in $gM_n(A[t^{-1}])$. It follows that $V_0 = V_0 + gM_n(A_0[t^{-1}])$ is dense in $V = V_0 + gM_n(A[t^{-1}])$. As $b' \in V$, there exists $a_0 \in V_0$ such that $||b' - a_0|| < \frac{|g|}{||b||}$. Put $a = \frac{1}{g}a_0 \in M_n(Q)$. Then $ba \in M_n(A[t^{-1}])$ and $||1 - ba|| = ||\frac{1}{g}b(b' - a_0)|| \leq \frac{1}{|g|}||b|| \cdot ||b' - a_0|| < 1$. Hence $||ba|| = 1$, so each entry in ba has a non-negative value at v. By Remark 1.12, v coincides with the t-adic valuation on A, hence all the entries of ba belong to A. Thus $ba \in M_n(A)$, and since $||1-ba|| < 1$ and $M_n(A)$ is complete, $ba \in \mathrm{GL}_n(A)$. In particular, $\det(a) \neq 0$ and hence $a \in \mathrm{GL}_n(\mathrm{Quot}(A_0)) \subseteq \mathrm{GL}_n(E_2)$. By the first paragraph, there exist $b_1 \in \mathrm{GL}_n(A_1) \subseteq \mathrm{GL}_n(E_1), b_2' \in \mathrm{GL}_n(A_2)$ such that $ba = b_1b_2'$. Then $b_2 = b_2'a^{-1} \in \mathrm{GL}_n(E_2)$ satisfies $b = b_1b_2$. ∎

COROLLARY 1.15: *Suppose G is a finite group. For each $i \in I$ let F_i be a Galois extension of E with group G_i contained in G, such that $F_i \subseteq Q_i'$. If $G = \langle G_i \mid i \in I\rangle$ then $\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i\in I}$ is a patching datum [HaJ98, Definition 1.1]. In particular, G occurs as a Galois group over E.*

Proof: By Corollary 1.13(c), Q_i is a field for each $i \in I$. Conditions (2a), (2b) and (2d) of [HaJ98, Definition 1.1] are given in the hypothesis. Conditions (2c) and (2e) are given by Proposition 1.11 and Proposition 1.14, respectively. Thus $\mathcal{E}$ is a patching datum. By [HaJ98, Lemma 1.3(a)], there exists a Galois extension F of E with group G. ∎

2. p-groups

Fix the notation of §1, including that of Construction 1.1, and let p denote a prime number. In this section we realize p-groups of rank at most 2 by adequate extensions of E, and embed these extensions into the analytic fields.

Lemma 2.1: *Let $J \subseteq I, j \in J$, $t = X - c_j Y$.*

(a) *Suppose $f = \sum_{l=0}^{d} f_l z_j^l \in K[[t]][z_j]$ is a polynomial such that $v(f_1) = 0$ and $v(f_l) > 0$ for each $l > 1$. Then f is prime in $D_J[t^{-1}]$.*

(b) *The ring $D_J[t^{-1}]$ is a unique factorization domain.*

(c) *For each $a, b, c \in K^\times$ with $a \neq -b$ and $2 \leq m \in \mathbb{N}$, the elements $1 + az_j + t^{m-1}z_j^m$, $1 + bz_j - t^{m-1}z_j^m$, $1 + cz_j$ are non-associate primes of $D_J[t^{-1}]$.*

Proof: Denote $F = K((t))$. Then $D_J[t^{-1}] = F\{z_k \mid k \in J\}$ (Remark 1.12). Viewing f as an element of $F\{z_j\}$, it is regular of pseudo degree 1 [HaV96, Definition 1.4], hence by [HaV96, Corollary 1.7] we have $f = u \cdot q$, where $u \in F\{z_j\}^\times \subseteq D_J[t^{-1}]^\times$ and $q = q_0 + z_j \in F[z_j]$ is a linear polynomial with $v(q_0) \geq 0$. Thus to prove (a), it suffices to show that q is prime in $D_J[t^{-1}]$. Without loss of generality $q_0 \neq 0$, and we denote $c = c_j - \frac{1}{q_0}$. Then $q = z_j - \frac{1}{c - c_j}$, hence by [Pa08, Lemma 6.4(a)] (with D, r, 1 there replaced by F, 1, j here) q generates the kernel of an epimorphism from $D_J[t^{-1}]$ onto a domain (actually a field here), hence q is prime. This proves (a).

Since $D_J[t^{-1}]$ is a principal ideal domain [HaJ98, Proposition 3.9], part (b) follows.

By part (a), $r = 1 + az_j + t^{m-1}z_j^m$, $r' = 1 + bz_j - t^{m-1}z_j^m$, $s = 1 + cz_j$ are primes of $D_J[t^{-1}]$. If $s|r$, then $-\frac{1}{c}$ is a root of r, a contradiction. Thus r, s (and similarly, r', s) are non-associates.

If $r|r'$ then $r|r + r'$. By the argument of the preceding paragraph, $r + r' = 2 + (a + b)z_j$ is a prime, non associate to r, a contradiction. This proves (c). ∎

Lemma 2.2: *Let K be a field that contains a primitive q-th root of unity, for some $q \in \mathbb{N}$. Let v be a discrete valuation on K which is trivial on the prime field of K, and let $a \in K$ with $v(a) = 0$. Suppose $L = K(a^{\frac{1}{q}})$ is a Kummer extension of K, and that L/K is unramified at v. Then $v(x^\sigma) = v(x)$ for each $x \in L$ and $\sigma \in \mathrm{Gal}(L/K)$.*

Proof: Extend v arbitrarily to L, let O be the valuation ring of v in K, and O' the valuation ring of v in L. Since K contains a primitive q-th root of unity, q is not divisible by $p = \mathrm{char}(K)$. Thus $d = \mathrm{disc}(T^q - a, K) = ka^{q-1}$, where $k \in \mathbb{Z}$ is not divisible by p. Hence $v(d) = 0$, and by [FrJ05, Lemma 6.1.2] we have $O' = O[a^{\frac{1}{q}}]$. Put $\alpha = a^{\frac{1}{q}}$ and let $x = \sum_{i=0}^{q-1} b_i\alpha^n \in K$, with $b_0, \ldots, b_{q-1} \in K$. We claim that $v(x) = \min_i(v(b_i))$. Indeed, since L/K is unramified at v, we may multiply x by a power of a uniformizer of v in K, to assume that $v(x) = 0$. Since $O' = O[\alpha]$, $v(b_i) \geq 0$ for each $0 \leq i \leq q-1$. On the other hand $v(x) \geq \min_i(v(b_i\alpha^i)) = \min_i(v(b_i))$, since $v(\alpha) = \frac{1}{n}v(a) = 0$. Thus $v(b_i) = 0$ for some $0 \leq i \leq q-1$, hence $v(x) = \min_i(v(b_i))$.

Now, let $\sigma \in \mathrm{Gal}(L/K)$ and let $x = \sum_{i=0}^{q-1} b_i\alpha^n \in K$, with $b_0, \ldots, b_{q-1} \in K$, be an arbitrary element. We have $\alpha^\sigma = \zeta\alpha$, where ζ is some q-th root of unity. Then $v(x^\sigma) = v(\sum_{i=0}^{q-1} b_i\zeta^i\alpha^i) = \min_i(v(b_i\zeta^i)) = \min_i(v(b_i)) = v(x)$. ∎

Recall that given a field K, any K-central simple algebra A is of the form $\mathrm{M}_n(D)$ for some K-division algebra D. The index of A is defined to be $\mathrm{ind}(A) = \sqrt{\dim_K D}$. So, A is a division algebra if and only if $\mathrm{ind}(A) = \sqrt{\dim_K A}$. Let us denote Brauer equivalence by $\sim$ and the exponent of A (its order in the Brauer group) by $\exp(A)$. A subfield F of A is a maximal subfield of A if and only if $\dim_K A = [F : K]^2$. Furthermore, a field F is a maximal subfield of A if and only if $\dim_K A = [F : K]^2$ and F splits A (see [Rei75, Theorem 28.4 and Corollary 28.11]).

The proof of the next proposition is partially based on that of [HHK10, Proposition 4.4].

Proposition 2.3: *Fix $i \in I$, and let H be an abelian p-group of rank at most 2, where $p \neq \mathrm{char}(K)$. Suppose K contains an $|H|$-th primitive root of unity. Let E' be a finite extension of E. Then there exists an H-Galois extension F_i/E such that:*

(a) $F_i \subseteq Q_i'$.

(b) *F_i is contained as a maximal subfield in an E-division algebra D_i', and $D_i' \otimes_E E'Q_i$ remains a division algebra (where $E'Q_i$ is the compositum of E' and Q_i in an algebraic closure of Q).*

Proof: Let us start by constructing F_i. Write $H = C_q \times C_q'$, where q, q' are powers of p. For each $k \in \mathbb{N}$, the elements $X - c_iY + Y^k$, $X + c_iY - Y^k$ are irreducible and hence prime in the unique factorization domain $K[[X,Y]]$. Only finitely many primes of $K[[X,Y]]$ are ramified at E'/E, hence for a sufficiently large $2 \leq k \in \mathbb{N}$, $f = X - c_iY + Y^k$ and $g = X + c_iY - Y^k$ are unramified at E'/E. That is, the corresponding valuations v_f, v_g are unramified. Let $a = \frac{f}{X - c_iY}$, $b = \frac{g}{X - c_iY}$. Clearly $v_f(X - c_iY) = v_f(g) = 0$, hence $v_f(a) = 1, v_f(b) = 0$. Similarly, $v_g(a) = 0, v_g(b) = 1$. Consider the polynomial $h(U) = U^q - a$ over $D_{\{i\}} = K[z_i][[X - c_iY]]$. Note that $a = 1 + z_i^k(X - c_iY)^{k-1}$, hence $h(1) \in (X - c_iY)D_{\{i\}}$ and $h'(1) = q \in K^\times \subseteq D_{\{i\}}^\times$. By the ring version of Hensel's Lemma (for the ideal $(X-c_iY)D_{\{i\}}$) $h(U)$ has a root $s \in D_{\{i\}}$. Note that $v_f(s) = \frac{1}{q} \notin \mathbb{Z}$, hence $s \notin E$. Since K contains a primitive $|H|$-th root of unity, it contains a primitive q-th root of unity. By Kummer theory $E(s)/E$ is a Galois extension with group C_q. Similarly, there exists $s' \in D_{\{i\}}$ satisfying $(s')^{q'} = b$, and $E(s')/E$ is Galois with group $C_{q'}$. Let $F_i = E(s, s') \subseteq Q_i'$.

Since $v_f(a) = 1$, $h(U)$ is irreducible over E, by Eisenstein's criterion. Denoting the reduction modulo g by $\bar{\cdot}$, $\bar{h}(U) = U^q - \bar{a}$ is separable, since $\bar{a} \neq 0$. Thus by [FrJ05, Lemma 2.3.4], $E(s)/E$ is unramified at v_g. Clearly, $E(s')/E$ is totally ramified at v_g. Thus $E(s), E(s')$ are linearly disjoint over E, hence $\mathrm{Gal}(F_i/E) = H$.

Let D_i' be the quaternion algebra $(a, b)_{qq'}$ (see [Pie82, Section 15.4]). Note that D_i' can be also viewed as the cyclic algebra $(E(a^{\frac{1}{qq'}})/E, \sigma, b)$, for some generator σ of $\mathrm{Gal}(E(a^{\frac{1}{qq'}})/E)$. We claim that F_i splits D_i'. By [Rei75, Theorem 30.8], $D_i' \otimes_E E(s) \sim (E(s^{\frac{1}{q'}})/E(s), \sigma^q, b)$ and thus $D_i' \otimes_E F_i \sim (F_i(s^{\frac{1}{q'}})/F_i, \sigma^q, b)$. The cyclic algebra $(F_i(s^{\frac{1}{q'}})/F_i, \sigma^q, b)$ is split if and only if b is a norm from $F_i(s^{\frac{1}{q'}})$ (see for example [Rei75, Theorem 30.4]), i.e. if and only if $b \in N_{F_i(s^{\frac{1}{q'}})/F_i}(F_i(s^{\frac{1}{q'}}))$. This holds since $b = N_{F_i(s^{\frac{1}{q'}})/F_i}(s')$. Thus F_i splits D_i'. As $[F_i : E] = qq'$, F_i is a maximal subfield of the E-central simple algebra D_i'. We shall show that $D_i' \otimes_E E'Q_i$ is a division algebra and from this it will follow that D_i' is a division algebra.

In order to show that $D_i' \otimes_E E'Q_i$ is a division algebra we construct auxiliary valuations. Choose $j \in I \smallsetminus \{i\}$, denote $t = X - c_jY$ and $r = 1 + (c_j + c_i)z_j - t^{k-1}z_j^k, r' = 1 + (c_j - c_i)z_j + t^{k-1}z_j^k$. By Lemma 2.1(c) r, r' are non-associate prime elements in $D_{I\smallsetminus\{i\}}[t^{-1}]$, so they define discrete valuations $v_r, v_{r'}$ on $Q_i = \mathrm{Quot}(D_{I\smallsetminus\{i\}}) = \mathrm{Quot}(D_{I\smallsetminus\{i\}}[t^{-1}])$ such that $v_r(r') = v_{r'}(r) = 0$. By Lemma 2.1(c) we also have $v_{r'}(1 + (c_j - c_i)z_j) = v_r(1 + (c_j - c_i)z_j) = 0$.

Note that

$$b = \frac{X - c_jY + (c_j + c_i)Y - Y^k}{X - c_jY + (c_j - c_i)Y} = \frac{t + (c_j + c_i)tz_j - t^j z_j^k}{t + (c_j - c_i)tz_j} = \frac{r}{1 + (c_j - c_i)z_j}.$$

Similarly, $a = \frac{r'}{1+(c_j-c_i)z_j}$. Thus $v_r(b) = 1, v_{r'}(b) = 0, v_r(a) = 0, v_{r'}(a) = 1$. Then the polynomial $U^{qq'} - a$ is irreducible over $D_{I \smallsetminus \{i\}}$, by Eisenstein's Criterion (using $v_{r'}$). Thus $Q_i(a^{\frac{1}{qq'}})/Q_i$ is unramified at v_r (again by [FrJ05, Lemma 2.3.4]), hence so is $E'Q_i(a^{\frac{1}{qq'}})/E'Q_i$.

Only finitely many primes of the unique factorization domain $D_{I \smallsetminus \{i\}}[t^{-1}]$ (Lemma 2.1(b)) are ramified at the finite extension $E'Q_i/Q_i$, hence without loss of generality, we may assume that $E'Q_i/Q_i$ is unramified at $v_{r'}$ (by possibly choosing an even larger k before hand). On the other hand, $Q_i(a^{\frac{1}{qq'}})/Q_i$ is totally ramified at $v_{r'}$, hence $[E'Q_i(a^{\frac{1}{qq'}}) : E'Q_i] = [Q_i(a^{\frac{1}{qq'}}) : Q_i] = qq'$.

We can now show that $D_i' \otimes_E E'Q_i$ is a division algebra. A sufficient condition for this to hold is that $\exp(D_i' \otimes_E E'Q_i) = qq'$. This happens if and only if for every $1 \leq m \leq qq'-1$ the algebra $(E'Q_i(a^{\frac{1}{qq'}})/E'Q_i, \sigma, b^m) \sim (D_i' \otimes_E E'Q_i)^m$ does not split. Let N denote the norm $N_{E'Q_i(a^{\frac{1}{qq'}})/E'Q_i}$. For any $1 \leq m \leq qq'-1$, the algebra $(D_i' \otimes_E E'Q_i)^m$ splits if and only if $b^m \in N(E'Q_i(a^{\frac{1}{qq'}})^\times)$ ([Rei75, Theorem 30.4]).

As $E'Q_i(a^{\frac{1}{qq'}})/E'Q_i$ is unramified at v_r, we have $v_r(x) = v_r(x^\sigma)$ for each $x \in E'Q_i(a^{\frac{1}{qq'}})$, by Lemma 2.2. Hence $v_r(N(x)) = \sum_{l=0}^{qq'-1} v_r(x^{\sigma^l}) = qq' v_r(x)$ for all $x \in E'Q_i(a^{\frac{1}{qq'}})$. Since $v_r(b) = 1$, $b^m \notin N(E'Q_i(a^{\frac{1}{qq'}})^\times)$ for all $1 \leq m \leq qq'-1$. Thus, $\exp(D_i' \otimes_E E'Q_i) = qq'$ and $D_i' \otimes_E E'Q_i$ is a division algebra. ∎

3. Patching and admissibility

We have established the patching machinery needed to prove our Main Theorem (Theorem 3.8 below). We first recall some general properties of induced algebras and Frobenius algebras.

Remark 3.1: Induced Algebras. Let G be a finite group and $H \leq G$. Let P/Q be a finite field extension with $H = \mathrm{Gal}(P/Q)$. Let $N = \mathrm{Ind}_H^G P = \Big\{ \sum_{\theta \in G} a_\theta \theta \mid a_\theta \in P,\ a_\theta^\tau = a_{\theta\tau} \text{ for all } \theta \in G,\ \tau \in H \Big\}$ be a ring with respect to point-wise addition and multiplication. Then P can be embedded as a subring of N by choosing representatives $\theta_1 = 1, ..., \theta_k$ of $H \setminus G$ and sending an element $x \in P$ to $\sum_{i=1,\tau \in H}^k x^\tau \theta_i \tau$. Furthermore, by choosing different representatives N can be presented as a direct sum of copies of P.

If P splits a central simple Q-algebra A then $\operatorname{Ind}_H^G P \otimes_Q A \cong \operatorname{Ind}_H^G P \otimes_P (P \otimes_Q A) \sim \operatorname{Ind}_H^G P \otimes_P P \cong \operatorname{Ind}_H^G P$ and hence A splits over $\operatorname{Ind}_H^G P$ (for a definition of a split separable (Azumaya) algebra over a ring see [DI71, §5]). ∎

The following definition, remark and proposition will be useful in the sequel and all appear in [Jac96, Section 2.1].

Definition 3.2: Frobenius algebras. Let F be a field. An F-algebra A is a Frobenius algebra if A contains a hyperplane that does not contain any non-zero one sided ideal of A.

Remark 3.3: An algebra $A_1 \oplus \ldots \oplus A_s$ is Frobenius if and only if A_i is Frobenius for each $1 \leq i \leq s$. Any algebra $F[a]$ (with a single generator) is Frobenius. Let L/K be an H-extension. By Remark 3.1, $\operatorname{Ind}_H^G L$ can be decomposed into a sum of copies of L and it follows that $\operatorname{Ind}_H^G L$ is a Frobenius algebra. ∎

Proposition 3.4 [Jac96, Theorem 2.2.3]: *Let A be an F-central simple algebra and K a commutative Frobenius subalgebra of A such that $\dim_F A = [K:F]^2$. Then any embedding of K into A can be extended to an inner automorphism of A.*

Lemma 3.5: *Let R be an equicharacteristic complete local domain of dimension r. Suppose that the residue field of R contains a primitive root of unity of order k, for each $k \in \mathbb{N}$ with $\operatorname{char}(R) \nmid k$. Then R is a finite module over a subring of the form $K[[X_1, \ldots, X_r]]$, where K is a field containing a primitive root of unity of order k, for each $k \in \mathbb{N}$ with $\operatorname{char}(K) \nmid k$.*

Proof: By Cohen's structure theorem [Mat86, §29], R is finitely generated over a subring of the form $B = K_0[[X_1, \ldots, X_n]]$, for some field K_0. Since $\dim B = \dim R = r$, we have $n = r$.

Let K be the field obtained by adjoining all primitive roots of unity of order not divisible by $\operatorname{char}(R)$ to K_0. By our assumptions, K is contained in the residue field of R, hence K/K_0 is a finite (separable) extension. By Hensel's lemma, R contains K. Since $[K:K_0]$ is finite, $K(K_0[[X_1, \ldots, X_r]]) = K[[X_1, \ldots, X_r]]$. Thus R is finite over $K[[X_1, \ldots, X_r]]$ (since it is finite over $K_0[[X_1, \ldots, X_r]]$). ∎

The final ingredient we need in order to prove our main theorem is patching of central simple algebras. The content of the following proposition is essentially given in [HHK10], but for specific fields Q_i, while here we present it for general fields satisfying a matrix factorization property. We note that [HHK10, Theorem 4.1] uses the terminology of categories and equivalence of categories. Here we prefer a more explicit presentation, working with vector spaces and bases, as in [HaJ98]. The proof of the proposition combines the proof of [HaJ98, Lemma 1.2] (where a more restricted assertion is made for specific types of algebras), and the proof of [HaH10, Theorem 7.1(vi)] (where the assertion is made for specific types of fields).

PROPOSITION 3.6: *Let I be a finite set. For each $i \in I$ let Q_i be a field contained in a Q_i-algebra A_i. Let Q be a field containing Q_i for each $i \in I$, and contained in a Q-algebra A_Q which contains A_i for each $i \in I$. Moreover, suppose that $A_iQ = A_Q$ and $\dim_{Q_i} A_i = \dim_Q A_Q$ for each $i \in I$. Finally, suppose that:*

(2) *For each $B \in \mathrm{GL}_n(Q)$ there exist $B_i \in \mathrm{GL}_n(Q_i)$ and $B'_i \in \mathrm{GL}_n(\bigcap_{j\neq i} Q_j)$ such that $B = B_iB'_i$.*

Then, denoting $E = \bigcap_{i\in I} Q_i$, $A = \bigcap_{i\in I} A_i$ is an E-algebra satisfying $AQ_i = A_i$ for each $i \in I$. Moreover, if each A_i is central simple, then so is A.

Proof: For each $i \in I$, let $\mathcal{C}_i$ be a basis for A_i over Q_i. Since $A_iQ = A_Q$, $\mathrm{Span}_Q(\mathcal{C}_i) = A_Q$, and since $\dim_{Q_i} A_i = \dim_Q A_Q$, $\mathcal{C}_i$ is a basis for A_Q over Q, for each $i \in I$. We now construct a basis $\mathcal{C}$ for A_Q over Q, which is also a basis for A_i over Q_i, for **all** $i \in I$.

For each subset J of I, we find by induction on $|J|$, a basis $\mathcal{V}_J$ for A_Q over Q which is also a basis for A_j over Q_j, for each $j \in J$. Then for $I = J$ we will get the basis $\mathcal{C}$.

If $J = \emptyset$ there is nothing to prove. Suppose that $|J| \geq 1$, choose $k \in J$ and let $J' = J \smallsetminus \{k\}$. By assumption there is a basis $\mathcal{V}_J$ for A_Q over Q which is a basis for A_i over Q_i for each $i \in J'$. Since $\mathcal{C}_i$ is a common basis for A_Q and A_i, there is a matrix $B \in \mathrm{GL}_n(Q)$ such that $\mathcal{C}_kB = \mathcal{V}_{J'}$. By (2), there exist $B_k \in \mathrm{GL}_n(Q_k)$ and $M \in \mathrm{GL}_n(\bigcap_{k\neq j\in I} Q_j) \subseteq \bigcap_{j\in J'} \mathrm{GL}_n(Q_j)$ such that $B = B_kM$. Put $\mathcal{V}_J = \mathcal{V}_{J'}M^{-1}$. Then $\mathcal{V}_J$ is a basis for A_Q over Q which is also a basis for A_j over Q_j for each $j \in J'$.

Moreover, $\mathcal{V}_J$ is also a basis for A_k over Q_k, since $\mathcal{V}_J = \mathcal{V}_k B M^{-1} = \mathcal{V}_k B_k$. This completes the induction.

The existence of the common basis C implies that $AQ_i = A_i$ for each $i \in I$. As A_i is a Q_i-central simple algebra for any $i \in I$ (a single i suffices), A is an E-central simple algebra (this follows for example by [Sal99, Theorem 2.2.c]).

PROPOSITION 3.7: *Let R be an equicharacteristic complete local domain of dimension 2, with residue field containing a primitive root of unity of order k for each $k \in \mathbb{N}$ with* $\mathrm{char}(R) \nmid k$. *Let G be a finite group of order not divisible by* $\mathrm{char}(R)$, *whose Sylow subgroups are abelian of rank at most 2. Then G is admissible over* $\mathrm{Quot}(R)$.

Proof: By Lemma 3.5, R is a finite module over a subring of the form $B = K[[X,Y]]$, where K contains a primitive root of unity of order k for each $k \in \mathbb{N}$ not divisible by $p = \mathrm{char}(R)$. Denote $E = \mathrm{Quot}(B) = K((X,Y))$, $E' = \mathrm{Quot}(R)$. Then E' is a finite extension of E.

PART A: *A patching datum.* Let $(p_i)_{i\in I}$ be the prime factors of $n = |G|$, for some index set I. For each $i \in I$, let G_i be a p_i-Sylow subgroup of G. Apply Construction 1.1 to obtain rings Q_i, $i \in I$, contained in the common field Q. For each $i \in I$, we may apply Proposition 2.3 to obtain a Galois extension F_i/E with group G_i, such that $F_i \subseteq Q_i'$ and F_i is contained as a maximal subfield in a division E-algebra D_i'. Moreover, $D_i' \otimes_E E'Q_i$ remains a division algebra. Thus $D_i := D_i' \otimes_E Q_i$ is also a division algebra. By Corollary 1.13(c), Q_i is a field for each $i \in I$. Put $P_i = F_i Q_i$. Since F_i splits D_i', P_i splits D_i, and since $[P_i : Q_i] = [F_i : E] = \mathrm{ind}(D_i') = \mathrm{ind}(D_i)$, P_i is a maximal subfield of D_i. Let $\mathcal{E} = (E, F_i, Q_i, Q; G_i, G)_{i\in I}$. By Corollary 1.15, $\mathcal{E}$ is a patching datum.

PART B: *Induced Algebras [HaJ98, §1].* Consider the induced algebra $N = \mathrm{Ind}_1^G Q$ of dimension n over Q, and the Q_i-subalgebra $N_i = \mathrm{Ind}_{G_i}^G P_i$ for each $i \in I$ (Remark 3.1). Then G acts on N by $\left(\sum_{\theta\in G} a_\theta \theta\right)^\sigma = \sum_{\theta\in G} a_\theta \sigma^{-1}\theta = \sum_{\theta\in G} a_{\sigma\theta}\theta$ for each $\sigma \in G$. The field Q is embedded diagonally in N, which induces an embedding of Q_i in N_i, for each $i \in I$. We view these embeddings as containments. By [HaJ98, Lemma 1.2] there is a basis for N over Q, which is also a basis for N_i over Q_i, for each $i \in I$. In particular, we have $N_i Q = N$ for each $i \in I$. By [Ha98, Lemma 1.3] $F = \bigcap_{i\in I} N_i$ is a Galois field extension of E with group G, and there exists an E-embedding of F into Q. Denote the image of F under this embedding by F'.

Part C: *Division algebras.* It remains to prove that the extension F'/E is adequate. Let $A_Q = \mathrm{M}_n(Q)$, and for each $i \in I$ let $n_i = [G : G_i]$. As A_Q is split of dimension n^2 and N is of dimension n over Q, we also have an embedding of N into A_Q. We view N as a subalgebra of A_Q via this embedding.

Fix $i \in I$. Since $P_i = F_iQ_i$ splits D_i, it follows by Remark 3.1 that N_i also splits D_i. Moreover, by [DI71, Theorem 5.5] there is a central simple Q_i-algebra A_i which is Brauer equivalent to D_i, in which N_i embeds as a maximal commutative separable Q_i-subalgebra so that $\dim_{Q_i}(A_i) = \dim_{Q_i}(N_i)^2 = n^2$. We view N_i as contained in A_i via this embedding.

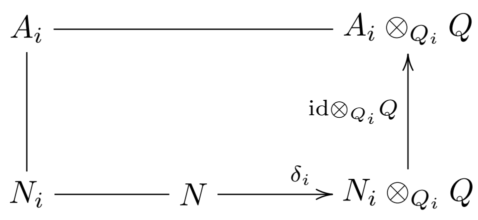
Since P_i splits D_i, we have

$$D_i \otimes_{Q_i} Q \cong (D_i \otimes_{Q_i} P_i) \otimes_{P_i} Q \cong \mathrm{M}_{\frac{n}{n_i}}(P_i) \otimes_{P_i} Q \cong \mathrm{M}_{\frac{n}{n_i}}(Q).$$

Since $\mathrm{ind}(D_i) = \frac{n}{n_i}$ and $\dim_Q A_Q = n^2$ we get that $A_i \cong M_{n_i}(D_i)$. Thus we have $A_i \otimes_{Q_i} Q \cong M_{n_i}(D_i) \otimes_{Q_i} Q \cong M_n(Q) = A_Q$, and we denote the induced Q-algebras isomorphism $A_i \otimes_{Q_i} Q \to A_Q$ by ψ_i. We cannot identify these two algebras via this isomorphism, since it might not be compatible with the containments $N_i \subseteq A_i$ and $N \subseteq A_Q$. This compatibility problem can be settled similarly to [HHK10, Lemma 4.2]:

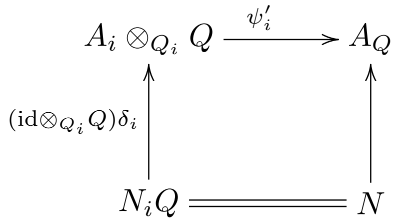
By Part B we have $N = N_iQ$ and $\dim_{Q_i} N_i = \dim_Q N = n$. Thus we have an isomorphism δ_i: $N = N_iQ \to N_i \otimes_{Q_i} Q$ for which the following diagram commutes:

(3)

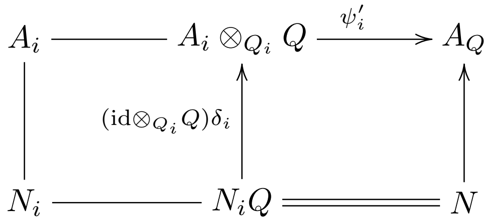


By Remark 3.3, $N = \mathrm{Ind}_1^G Q$ is a Frobenius (commutative) subalgebra of A_Q. By Proposition 3.4, the embedding $\psi_i(\mathrm{id} \otimes_{Q_i} Q)\delta_i$: $N \to A_Q$ extends to an inner automorphism α_i of A_Q. Denote $\psi_i' = \alpha_i^{-1}\psi_i$. Then $\alpha_i^{-1}\psi_i(\mathrm{id} \otimes_{Q_i} Q)\delta_i$ is the identity map on $N = N_iQ$, so we have the following commutative diagram:

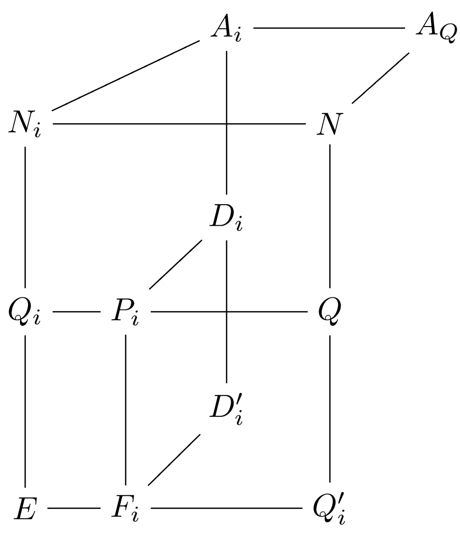
(4)



Combining diagrams (3) and (4), we get the following commutative diagram



This diagram gives an embedding $A_i \to A_Q$ which is compatible with the containments $N_i \subseteq A_i$ and $N \subseteq A_Q$, so we may now identify A_i as a subring of A_Q, via this embedding. Moreover, since ψ'_i is an isomorphism, we have $A_i \otimes_{Q_i} Q = A_i Q = A_Q$ by this identification. The following diagram explains the containment relations:



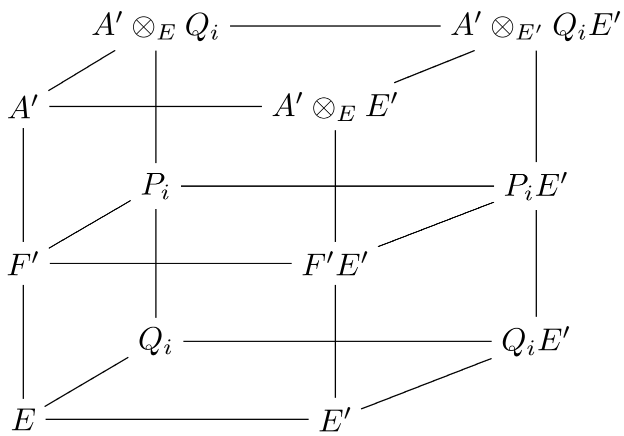
Let $A = \bigcap_{i \in I} A_i$. By Proposition 3.6, A is a central simple E-algebra for which $AQ_i = A_i$ for each $i \in I$. In particular, $A = M_k(D)$ for some division algebra D of index $\frac{n}{k}$.

Now, $D \otimes_E Q_i$ is Brauer equivalent to $A \otimes_E Q_i \cong A_i$ which is Brauer equivalent to D_i. Thus, $\frac{n}{n_i} = \text{ind}(D_i) | \text{ind}(D)$ for each $i \in I$ and $n = \text{lcm}_i(\frac{n}{n_i}) | \text{ind}(D)$. It follows that $k = 1$ and A is a division algebra. Naturally, F is a subfield of A and $\text{ind}(A) = [F : E]$. It follows that F is a maximal subfield of the division algebra A.

By choosing a basis for A/F and considering the corresponding structure constants one can form an E-division algebra A' which is E-isomorphic to A such that F' is a maximal subfield of A'.

We shall show that $A' \otimes_E E'$ is an E'-division algebra, but first let us show that this implies that $F'E'/E'$ is an adequate G-extension (and hence G is E'-admissible). Indeed, if $A' \otimes_E E'$ is a division algebra, then $F' \otimes_E E'$ is a field. It follows that $F' \otimes_E E' \cong F'E'$, since $F' \otimes_E E'$ is G-Galois over E' [Sal99, Theorem 6.3]. Thus, $[F'E' : E'] = [F' : E]$ and $F' \cap E' = E$. Since $F'E'$ splits $A' \otimes_E E'$ and as $\text{ind}(A' \otimes_E E') = [F'E' : E']$, $F'E'$ is a maximal subfield of $A' \otimes_E E'$ and hence an adequate G-extension.

In order to show that $A' \otimes_E E'$ is an E'-division algebra, we first note that for each $i \in I$, $P_i = F_i Q_i = F' Q_i$, by [HaV96, Lemma 3.6(b)]. Thus, we have the following diagram:



As mentioned above, $A' \otimes_E Q_i$ is Brauer equivalent to $D_i = D_i' \otimes_E Q_i$. Thus $A' \otimes_E Q_i E'$ is Brauer equivalent to $D_i' \otimes_{Q_i} Q_i E'$ which by choice of D_i' is a division algebra. Then,

$$\frac{n}{n_i} = \text{ind}(D_i') = \text{ind}(D_i' \otimes_{Q_i} Q_i E') | \text{ind}(A' \otimes_E Q_i E') | \text{ind}(A' \otimes_E E')$$

for all $i \in I$. It follows that $n = \mathrm{lcm}_{i\in I}(\frac{n}{n_i})|\mathrm{ind}(A' \otimes_E E')$. Hence $n = \mathrm{ind}(A' \otimes E')$, which shows that $A' \otimes_E E'$ is a division algebra. ∎

As a corollary, we get our main theorem.

THEOREM 3.8: *Let R be an equicharacteristic complete local domain of dimension 2, with a separably closed residue field. Let $E = \mathrm{Quot}(R)$ and let G be a finite group of order not divisible by $\mathrm{char}(E)$. Then G is E-admissible if and only if all the Sylow subgroups of G are abelian of rank at most 2.*

Proof: By Proposition 3.7, if the Sylow subgroups of G are abelian of rank at most 2 then G is E-admissible. For the converse, assume G is E-admissible. For a prime v of E, let ram_v denote the ramification map ram_v: $\mathrm{Br}(E) \to \mathrm{H}^1(G_{E_v}, Q/Z)$ (see [Sal99]). Following [HHK10], we say that an $\alpha \in \mathrm{Br}(E)$ is determined by ramification with respect to a set of primes Ω if there is a prime $v \in \Omega$ for which $\exp(\alpha) = \exp(\mathrm{ram}_v(\alpha))$. Let D be an E-division algebra with maximal subfield L that has Galois group $G = \mathrm{Gal}(L/E)$. Let $p = \mathrm{char}(E)$ (possibly $p = 0$). By [HHK10, Theorem 3.3], if D satisfies:
(1) the order of D is prime to p and $\mathrm{ind}(D) = \exp(D)$,
(2) D is determined by ramification with respect to some set of discrete valuations whose residue characteristic is prime to $|G|$,
then G has Sylow subgroups that are abelian of rank at most 2. Condition (1) is satisfied for any α of order prime to p by [COP02, Theorem 2.1], while Condition (2) is satisfied by [COP02, Corollary 1.9 (c)] with respect to the set of codimension 1 primes of R. ∎

Remark 3.9: Let E be as above. By [COP02, Theorem 2.1], any Brauer class $\alpha \in \mathrm{Br}(E)$ of order prime to $\mathrm{char}(E)$ has $\mathrm{ind}(\alpha) = \exp(\alpha)$. Thus by [Sch68, Proposition 2.2], a subfield of an E-division algebra is also a maximal subfield of some E-division algebra. ∎

References

[BHH10] L. Bary-Soroker, D. Haran and D. Harbater, *Permanence criteria for semi-free profinite groups*, Mathematische Annalen, to appear.

[COP02] J.-L. Colliot-Thélène, M. Ojanguren and R. Parimala, *Quadratic forms over function fields of two-dimensional Henselian rings and Brauer groups of related schemes,* Proceedings of the International Colloquium on Algebra, Arithmetic and Geometry, Tata Inst. Fund. Res. Stud. Math., vol. 16, pp. 185–217, Narosa Publ. Co., 2002.

[DI71] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings,* Springer-Verlag, Berlin, 1971.

[Fei04] W. Feit, PSL2(11) *is admissible for all number fields,* Algebra, arithmetic and geometry with applications (West Lafayette, IN, 2000), Springer, Berlin, 2004, pp. 295-299.

[FrJ05] M. Fried and M. Jarden, *Field Arithmetic, 2nd edition, revised and enlarged by M. Jarden,* Ergebnisse der Mathematik III **11**, Springer 2005.

[FrP04] J. Fresnel and M. v.d. Put, *Rigid Analytic Geometry and its Applications,* Progress in Mathematics **218**, Birkhäuser Boston, 2004.

[FS95a] B. Fein and M. Schacher, $\mathbb{Q}(t)$ *and* $\mathbb{Q}((t))$*-admissibility of groups of odd order,* Proc. Amer. Math. Soc. **123** (1995).

[FS95b] B. Fein and M. Schacher, *Crossed products over algebraic function fields,* Journal of Algebra **171** (1995), 531–540.

[FSS92] B. Fein, D. Saltman and M. Schacher, *Brauer-Hilbertian fields,* Trans. Amer. Math. Soc. **334** (1992), 915–928.

[Ha87] D. Harbater, *Galois coverings of the arithmetic line,* in Number Theory — New York 1984–85, ed. by D. V. and G. V. Chudnovsky, Lecture Notes in Mathematics **1240**, Springer, Berlin, 1987, pp. 165–195.

[HaH10] D. Harbater and J. Hartmann, *Patching over fields,* Israel Journal of Mathematics, to appear.

[HaJ98] D. Haran and M. Jarden, *Regular split embedding problems over complete valued fields,* Forum Mathematicum **10** (1998), 329–351.

[Ha03] D. Harbater, *Patching and Galois theory,* In "Galois groups and Fundamental groups" (L. Schneps, ed.), MSRI Publication series, vol. 41, Cambridge Univ. Press, 2003, pp. 313–424.

[HaS05] D. Harbater and K. Stevenson, *Local Galois theory in dimension two,* Advances in Mathematics **198** (2005), 623–653.

[HaV96] D. Haran and H. Völklein, *Galois groups over complete valued fields,* Israel Journal of Mathematics **93** (1996), 9–27.

[HHK10] D. Harbater, J. Hartmann and D. Krashen, *Patching subfields of division algebras,* Transactions of the AMS, to appear.

[Jac96] N. Jacobson, *Finite-dimensional division algs. over fields,* Springer-Verlag, Berlin, 1996.

[Lid96] S. Liedahl, *K-admissibility of wreath products of cyclic p-groups,* J. Number Theory **60** (1996), no. 2, 211–232

[Mat86] H. Matsumura, *Commutative ring theory,* Cambridge University Press, 1986.

[Nef10] D. Neftin, *Admissibility and realizability over number fields,* submitted

[Pa08] E. Paran, *Algebraic patching over complete domains,* Israel Journal of Mathematics **166** (2008), 185–219.

[Pa10] E. Paran, *Galois theory over complete local domains domains,* Mathematische Annalen, to appear.

[Pie82] R. S. Pierce, *Associative algebras,* Springer-Verlag, Heidelberg (1982).

[Po96] F. Pop, *Embedding problems over large fields,* Annals of Mathematics **144** (1996) 1–34.

[Po10] F. Pop, *Henselian implies large,* Annals of Mathematics, to appear.

[Rei75] I. Reiner, *Maximal orders,* Academic Press, New York, 1975.

[Sal99] D.J. Saltman, *Lectures on division algebras,* CBMS Regional Conference series no. 94. American Mathematical society, Providence RI, 1999.

[Sch68] M. Schacher, *Subfields of division rings,* Journal of Algebra **9** (1968), 451-477.

[Son83] J. Sonn, *$\mathbb{Q}$-admissibility of solvable groups,* Journal of Algebra **84** (1983), no. 2, 411-419.

[SS92] M. Schacher and J. Sonn, *K-admissibility of A_6 and A_7,* Journal of Algebra **145** (1992), no. 2, 333-338.

[Ste82] L. Stern, Ph.D Thesis. Technion 1982.