Division algebras and patching

AWS course notes

David Harbater and Julia Hartmann

March 5, 2012

These are notes for the minicourse on division algebras and patching at the 2012 Arizona Winter School. The final version of these notes will be posted *after* the winter school. The first part concerns patching over fields. The second part deals with division algebras and applications of patching to that situation. For an overview of the course, along with some additional references, see the Course and Project Outline that is posted on the AWS website.

Part I

1 Patching Algebraic Structures

Patching is a principle that enables the study of algebraic objects over a field F by studying corresponding objects over extension fields of F. It is motivated by geometry, where F is the function field of some space, and the extension fields are the fields of functions on subsets. (From an algebraic perspective, patching can be regarded as a form of descent, though it is different from étale and flat descent.) Our focus will be on the case in which F is the function field of a curve over a complete discretely valued field. For example, if the curve is the projective line over $k((t))$, then $F = k((t))(x)$.

Before turning to this situation, we will consider patching for more general fields F. To keep the situation simple, we concentrate on the case of two extension fields F_1, F_2 of F, together with a common overfield F_0, such that F is the intersection of F_1 and F_2 inside F_0. Given structures over F_1 and F_2 together with an isomorphism between the structures that they induce over F_0, we would like to assert that there exists a unique structure over F that induces them compatibly. We begin with the case of vector spaces.

First recall that if V is a finite dimensional vector space over a field F, and if E is an extension field of F, then $V_E := V \otimes_F E$ is a finite dimensional vector space over E, and there is a natural inclusion $V \hookrightarrow V_E$. Viewing V as a subset of V_E, any F-basis of V is also an E-basis of V_E. (Here and elsewhere, we view V as a two-sided vector space over F.)

With respect to extension fields F_i as above, an F-vector space *patching problem* $\mathcal{V}$ consists of finite dimensional F_i-vector spaces V_i for $i = 1, 2$ together with an F_0-vector

space isomorphism $\mu : V_1 \otimes_{F_1} F_0 \to V_2 \otimes_{F_2} F_0$. A *solution* to the patching problem $\mathcal{V}$ consists of a finite dimensional F-vector space V together with F_i-vector space isomorphisms $\iota_i : V \otimes_F F_i \to V_i$ for $i = 1, 2$ such that the following diagram commutes.

$$\begin{array}{ccccc} (V \otimes_F F_1) \otimes_{F_1} F_0 & \xrightarrow{\sim} & V \otimes_F F_0 & \xrightarrow{\sim} & (V \otimes_F F_2) \otimes_{F_2} F_0 \\ \downarrow{\scriptstyle \iota_1 \otimes 1} & & & & \downarrow{\scriptstyle \iota_2 \otimes 2} \\ V_1 \otimes_{F_1} F_0 & & \xrightarrow{\qquad\qquad \mu \qquad\qquad} & & V_2 \otimes_{F_2} F_0 \end{array}$$

Here the top horizontal arrows are the natural identifications of $V \otimes_F F_0$ with $(V \otimes_F F_i) \otimes_{F_i} F_0$ for $i = 1, 2$. Thus with respect to these identifications, the condition is that $\mu \circ (\iota_1 \otimes 1) = \iota_2 \otimes 1$.

Note that for any vector space patching problem as above, $\dim_{F_1}(V_1) = \dim_{F_2}(V_2)$. Hence for any F-vector space V of that same dimension, $V \otimes_F F_i$ will be F_i-isomorphic to V_i for $i = 1, 2$. But the point of the above definition is that the maps must also be compatible; and so the existence of a solution is not automatic.

Given a patching problem $\mathcal{V}$ as above, let $V_0 = V_2 \otimes_{F_2} F_0$. As above, V_2 naturally includes into V_0. By composing μ with the analogous inclusion for V_1, we may also regard V_1 as contained in V_0. Given a solution V to $\mathcal{V}$, we may also regard V as contained in V_i via ι_i, by identifying V with $V \otimes_F F \subseteq V \otimes_F F_i$. Here the two compositions $V \hookrightarrow V_1 \hookrightarrow V_0$ and $V \hookrightarrow V_2 \hookrightarrow V_0$ agree because $\mu \circ (\iota_1 \otimes 1) = \iota_2 \otimes 1$.

Proposition 1.1. *Let F_1, F_2 be subfields of a field F_0, with $F = F_1 \cap F_2$. Consider an F-vector space patching problem $\mathcal{V}$ given by n-dimensional F_i-vector spaces V_i and an isomorphism μ. For $i = 1, 2$ choose an F_i-basis B_i for V_i, and let $A_0 \in \mathrm{GL}_n(F_0)$ be the transition matrix between B_1 and B_2. Then $\mathcal{V}$ has a solution if and only if $A_0 = A_1^{-1} A_2$ for some matrices $A_i \in \mathrm{GL}_n(F_i)$, $i = 1, 2$.*

By regarding V_i as contained in V_0 as above, the basis vectors can all be viewed as elements of V_0. By the *transition matrix* we mean the matrix A_0 such that $B_1 A_0 = B_2$, where $B_i \in V_i^n$ is viewed as a row vector whose entries are the chosen basis elements of V_i.

Proof. First suppose that $\mathcal{V}$ has a solution given by an F-vector space V and isomorphisms $\iota_i : V \otimes_F F_i \to V_i$ for $i = 1, 2$. Choose an F-basis B for V; and for $i = 1, 2$ let $A_i \in \mathrm{GL}_n(F_i)$ be the transition matrix between B and B_i. Thus $BA_i = B_i$ for $i = 1, 2$. Hence $BA_1A_0 = B_1A_0 = B_2 = BA_2$. Since B is a basis, it follows that $A_1A_0 = A_2$; i.e. $A_0 = A_1^{-1}A_2$.

Conversely, suppose that $A_0 = A_1^{-1}A_2$ for some $A_i \in \mathrm{GL}_n(F_i)$. Let $B = B_1A_1^{-1} \in V_0^n$. Then $B_2A_2^{-1} = B_1A_0A_2^{-1} = B_1A_1^{-1} = B$ in $(V_1 \cap V_2)^n$. Let $V \subseteq V_1 \cap V_2$ be the F-vector space spanned by the vectors in B. Since A_i is invertible, the set of vectors in B is linearly independent over F_i and hence over F; and so it is an F-basis of V. The inclusion $V \hookrightarrow V_i$ taking B to itself then induces an F_i-isomorphism $\iota_i : V \otimes_F F_i \to V_i$, for $i = 1, 2$. Thus $\mu \circ (\iota_1 \otimes 1)(B) = \mu(B_1)A_1^{-1} = \mu(B_1)A_0A_2^{-1} = B_2A_2^{-1} = (\iota_2 \otimes 1)(B)$, where the third equality uses that A_0 is the transition matrix between B_1 and B_2, with respect to the above inclusions of V_1, V_2 into V_0. Hence $\mu \circ (\iota_1 \otimes 1) = \iota_2 \otimes 1$; so V and the maps ι_i define a solution to $\mathcal{V}$. $\square$

In fact, in the above situation, the solution V to a patching problem $\mathcal{V}$ is unique as a subset of V_0, and can be explicitly described:

Proposition 1.2. *In the situation of Proposition 1.1, suppose that the patching problem $\mathcal{V}$ has a solution V, which we regard as contained in each V_i via the inclusions defined by ι_i. Then $V = V_1 \cap V_2 \subseteq V_0$.*

Proof. See Problem 1.5. □

The power of patching comes from its applicability to various other structures besides vector spaces. The reason that patching applies in such situations is that for many types of algebraic structures over a field F, such as F-algebras, an object consists of an F-vector space together with a finite collection of F-vector space homomorphisms that satisfy certain commutative diagrams. The key to using this observation is to be able to assert that giving an F-vector space homomorphism $f : V \to W$ is equivalent to giving a collection of compatible F_i-vector space homomorphisms $f_i : V_i \to W_i$ for $i = 1, 2$, where $V_i = V \otimes_F F_i$ and $W_i = W \otimes_F F_i$. Here compatibility asserts that the restrictions of f_1 and f_2 to V agree, as maps to W_0.

In the situation of Proposition 1.1, if V is a solution to the patching problem $\mathcal{V}$, the above equivalence between giving f and giving a compatible pair (f_1, f_2) does in fact hold. This can be seen by identifying $\mathrm{Hom}_F(V, W) \otimes_F F_i$ with $\mathrm{Hom}_{F_i}(V_i, W_i)$, and using Proposition 1.2 to conclude that $\mathrm{Hom}_F(V, W)$ is the intersection of $\mathrm{Hom}_{F_1}(V_1, W_1)$ and $\mathrm{Hom}_{F_2}(V_2, W_2)$ inside $\mathrm{Hom}_{F_0}(V_0, W_0)$. (Alternatively, one can define f as the common restriction of f_1 and f_2 to $V = V_1 \cap V_2$, using that $W = W_1 \cap W_2$.)

A more precise phrasing is possible using categorical language. Given categories $\mathcal{C}_i$ for $i = 0, 1, 2$, and functors $\alpha_i : \mathcal{C}_i \to \mathcal{C}_0$ for $i = 0, 1$, we may consider their *2-fiber product* category $\mathcal{C} := \mathcal{C}_1 \times_{\mathcal{C}_0} \mathcal{C}_2$ defined as follows. Its objects are triples (V_1, V_2, μ) where V_i is an object in $\mathcal{C}_i$ for $i = 1, 2$ and where $\mu : \alpha_1(V_1) \to \alpha_2(V_2)$ is an isomorphism; and its morphisms $(V_1, V_2, \mu) \to (V_1', V_2', \mu')$ are pairs of maps $V_i \to V_i'$ such that the induced square is commutative.

In our situation, for any field E let $\mathrm{Vect}(E)$ be the category of finite dimensional E-vector spaces. Given a field F_0 and subfields F_1, F_2, consider the functor $\alpha_j : \mathrm{Vect}(F_j) \to \mathrm{Vect}(F_0)$ that takes an F_j-vector space V_j to $V_j \otimes_{F_j} F_0$. The objects in the 2-fiber product category $\mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$ thus consist of triples (V_1, V_2, μ) where V_j is a finite dimensional F_j-vector space and $\mu : V_1 \otimes_{F_1} F_0 \to V_2 \otimes_{F_2} F_0$ is an isomorphism. Hence giving an object in $\mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$ is equivalent to giving an F-vector space patching problem with respect to the fields F_i, where $F = F_1 \cap F_2$.

Given fields $F \subseteq F_1, F_2 \subseteq F_0$ with $F = F_1 \cap F_2 \subseteq F_0$, there is a functor $\beta : \mathrm{Vect}(F) \to \mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$ that is defined by base change (i.e. extension of constants), and which assigns to each vector space an induced patching problem of which it is the solution. (See Problem 1.7.)

Theorem 1.3. *The functor $\beta : \mathrm{Vect}(F) \to \mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$ is an equivalence of categories if and only if for every positive integer n and every matrix $A_0 \in \mathrm{GL}_n(F_0)$ there exist matrices $A_i \in \mathrm{GL}_n(F_i)$ such that $A_0 = A_1^{-1} A_2$.*

Proof. See Problem 1.8. □

Using the above results, we can apply patching to associative F-algebras. For any field E, let $\mathrm{Alg}(E)$ denote the category of finite dimensional associative E-algebras (not necessarily with multiplicative identity). If E' is an extension of E, then there is a base change functor $\mathrm{Alg}(E) \to \mathrm{Alg}(E')$ that takes an E-algebra A to the E'-algebra $A \otimes_E E'$.

Proposition 1.4. *In the situation of Theorem 1.3, suppose that β is an equivalence of categories. Then so is the base change functor*

$$\mathrm{Alg}(F) \to \mathrm{Alg}(F_1) \times_{\mathrm{Alg}(F_0)} \mathrm{Alg}(F_2).$$

Proof. A finite dimensional associative F-algebra consists of a finite dimensional F-vector space A together with a vector space homomorphism $p : A \otimes_F A \to A$ that satisfies an identity corresponding to the associative law of multiplication. More precisely, the following diagram commutes:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{p \otimes 1} & A \otimes A \\ \downarrow{\scriptstyle 1 \otimes p} & & \downarrow{\scriptstyle p} \\ A \otimes A & \xrightarrow{p} & A \end{array}$$

A given object in $\mathrm{Alg}(F_1) \times_{\mathrm{Alg}(F_0)} \mathrm{Alg}(F_2)$ induces an object in $\mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$ by the forgetful functor. Since β is an equivalence of tensor categories (see Problem 1.9(b)), having compatible maps p_i over the vector spaces $A_i := A \otimes_F F_i$ satisfying the above property implies that there is such a map p over A that induces them. Thus the object in $\mathrm{Vect}(F)$ that yields the given object in $\mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$ has the structure of an associative F-algebra, compatibly with the given structures on the A_i. The result then follows. □

Analogs of Proposition 1.4 can also be proven for other algebraic structures. See Problem 1.11.

Problems for Section 1

Problem 1.5. Prove Proposition 1.2. (One approach is to consider the exact sequence

$$0 \to F \to F_1 \times F_2 \to F_0 \to 0$$

of F-vector spaces, where the first map takes a to (a, a) and the second map takes (a_1, a_2) to $a_1 - a_2$, and then to tensor this sequence over F with V.)

Problem 1.6. In the situation of Proposition 1.1, show that $V := V_1 \cap V_2$ is a solution to an F-vector space patching problem $\mathcal{V}$ if and only if $\dim_F(V) = \dim_{F_i}(V_i)$.

Problem 1.7. Given fields $F \subseteq F_1, F_2 \subseteq F_0$ with $F = F_1 \cap F_2 \subseteq F_0$, define an obvious functor $\beta : \mathrm{Vect}(F) \to \mathrm{Vect}(F_1) \times_{\mathrm{Vect}(F_0)} \mathrm{Vect}(F_2)$ that assigns to each vector space an induced patching problem of which it is the solution.

Problem 1.8. Prove Theorem 1.3. The converse asserts that under the factorization condition, β defines a surjection on isomorphism classes of objects, and that for every pair of finite dimensional F-vector spaces V, V', the set of F-vector space homomorphisms $V \to V'$ is sent bijectively to the set of morphisms $\beta(V) \to \beta(V')$. (Note that these conditions automatically imply injectivity on isomorphism classes of objects.)

Problem 1.9. Suppose that the above functor β is an equivalence of categories.

(a) Show that up to isomorphism, the inverse of β is given by intersection. More precisely, show that if $\beta(V) = (V_1, V_2, \mu)$, then V is naturally isomorphic to the intersection of V_1 and V_2 inside $V_0 := V_2 \otimes_{F_2} F_0$, where we regard V_1 as a contained in V_0 via μ.

(b) Show that β is an equivalence of tensor categories, i.e. that it preserves tensor product.

Problem 1.10. We have been assuming that F is the intersection $F_1 \cap F_2 \subseteq F_0$. If we weaken this assumption by supposing merely that F is contained in F_1 and F_2 as subfields of F_0, which of the above assertions remain true? Where has the intersection hypothesis been used?

Problem 1.11. Prove the analog of Proposition 1.4 for each of the following structures:

(i) Finite dimensional associative F-algebras with identity.

(ii) Finite dimensional commutative F-algebras (with identity).

(iii) Finite dimensional separable commutative F-algebras. (These are the finite direct products of finite separable field extensions of F.)

(iv) G-Galois F-algebras, where G is a given finite group. (Such an object is a finite dimensional separable commutative F-algebra A such that $\dim_F(A) = |G|$, together with a faithful action of G on A as an F-algebra such that F is the subset of A consisting of elements fixed by G. One example is a G-Galois field extension of F; another is a direct product of copies of F indexed by the elements of G, which each act by permuting the copies via left multiplying the indices.)

Problem 1.12. Does the analog of Proposition 1.4 hold for the category of finite field extensions of F?

Problem 1.13. Let F be a field, let V be an F-variety, and let GL_n denote the subvariety of $\mathbb{A}_F^{n^2}$ corresponding to invertible $n \times n$ matrices. Suppose that $\sigma : \mathrm{GL}_n \times V \to V$ is an F-morphism that defines a group action of GL_n on V. Assume moreover that σ is transitive in the strong sense that for every field extension E of F the action of $\mathrm{GL}_n(E)$ is transitive on the set of E-points of V.

(a) Suppose that $F \subseteq F_1, F_2 \subseteq F_0$ are as in Problem 1.7 and the functor β is an equivalence of categories. Show that if V has an F_1-point and an F_2-point, then it has an F-point.

(b) Let G be a linear algebraic group over F; i.e. a subvariety of GL_n that is also a group under the same operation. Suppose that σ is instead an action of G on V with the analogous transitivity condition. Does the same conclusion on F-points still automatically hold? Or is some additional condition needed in order for the argument to work?

2 Patching on Curves

In this section we apply the previous results to the situation of function fields of curves over complete discretely valued fields, especially the case of the projective line over a Laurent series field. Given a field k, the power series ring $T := k[[t]]$ is a complete discrete valuation ring with uniformizer t and residue field k. Its fraction field $K := k((t))$ is the same as $T[t^{-1}]$, and it is a complete discretely valued field.

We may consider the projective x-line $\mathbb{P}^1_K$. This K-curve can be covered by two affine open subsets, each of them a copy of the affine K-line: one with parameter x, and the other with parameter $\bar{x}$, where $x\bar{x} = 1$. These affine lines are $\mathrm{Spec}(K[x])$ and $\mathrm{Spec}(K[\bar{x}])$, with the overlap being $\mathrm{Spec}(K[x, x^{-1}])$. The point where $\bar{x} = 0$ can be regarded as the point at infinity, with respect to the parameter x.

We may also consider the projective x-line $\widehat{X} := \mathbb{P}^1_T$. (This scheme is of relative dimension one over T.) It can also be covered by two Zariski open sets, the affine lines over T with respect to the parameters x and $\bar{x}$, viz. $\mathrm{Spec}(T[x])$ and $\mathrm{Spec}(T[\bar{x}])$. See also Problem 2.10.

Recall that a commutative ring has *Krull dimension* d if there is a chain of (possibly zero) prime ideals $I_0 \subset I_1 \subset \cdots \subset I_d$ but there is no such chain of greater length. (Here and below, the notation $\subset$ indicates strict inclusion, whereas $\subseteq$ is used to indicate the possibility that the inclusion is actually an equality.) Similarly, the *dimension* of a scheme is the maximal d such that there are distinct (not necessarily closed!) points $P_0, P_1, \cdots, P_d$ in the scheme such that P_{i+1} is contained in the closure of P_i. See Problem 2.11 for a consideration of these quantities in the case of the rings T and $T[x]$ and their spectra, as well as of the projective line $\mathbb{P}^1_T$.

For the remainder of this section, we preserve the above notation: k is a field, $T = k[[t]]$, $K = k((t))$, and $\widehat{X} = \mathbb{P}^1_T$, which has function field $F = k((t))(x)$ and closed fiber $X = \mathbb{P}^1_k$ (see Problems 2.12 and 2.13). Given a non-empty subset $U \subseteq X$, we will write R_U for the subring of F consisting of the rational functions on $\widehat{X}$ that are regular at the points of U. Its t-adic completion will be denoted by $\widehat{R}_U$. We also write $R_\varnothing$ for the subring of F consisting of the rational functions on $\widehat{X}$ that are regular at the generic point of X, and we write $\widehat{R}_\varnothing$ for its t-adic completion.

The rings $\widehat{R}_U$ can be described explicitly in terms of U; see Problem 2.14. See also Problems 2.15, 2.16, and 2.17 for more about the behavior of these rings. See Problem 2.18 for another interpretation of these rings.

Lemma 2.1. *Suppose $U_1, U_2 \subseteq X$ and let $U_0 = U_1 \cap U_2$. Then for every $a \in \widehat{R}_{U_0}$ there exist $b \in \widehat{R}_{U_1}$ and $c \in \widehat{R}_{U_2}$ such that $a \equiv b + c \pmod{t}$ in $\widehat{R}_{U_0}$.*

Proof. By Problem 2.14(a), a is a power series in t with coefficients in a subring $A \subseteq k(x)$, and its constant term $a_0 \in A$ is a rational function on $\mathbb{P}^1_k$ having poles disjoint from U_0. By partial fraction decomposition, we may write $a_0 = b + c$, where $b, c \in k(x) \subset F$ such that the poles of b on X are disjoint from U_1 and the poles of c on X are disjoint from U_2. Hence $b \in R_{U_1} \subseteq \widehat{R}_{U_1}$ and $c \in R_{U_2} \subseteq \widehat{R}_{U_2}$. The conclusion follows since $a \equiv a_0 \pmod{t}$ in $\widehat{R}_{\varnothing}$. □

See Problem 2.19 for explicit examples of this additive decomposition.

Proposition 2.2. *Let $U_1, U_2 \subseteq X$ and set $U_0 = U_1 \cap U_2$. Let $n \geq 1$ and let $A_0 \in \mathrm{GL}_n(\widehat{R}_0)$ such that $A_0 \equiv I \pmod{t}$ in $\mathrm{Mat}_n(\widehat{R}_0)$. Then there exist $A_1 \in \mathrm{GL}_n(\widehat{R}_1)$ and $A_2 \in \mathrm{GL}_n(\widehat{R}_2)$ such that $A_0 = A_1^{-1}A_2$ in $\mathrm{GL}_n(\widehat{R}_0)$.*

Proof. Write $\widehat{R}_i$ for $\widehat{R}_{U_i}$. We will inductively construct matrices $B_j \in \mathrm{GL}_n(\widehat{R}_1)$ and $C_j \in \mathrm{GL}_n(\widehat{R}_2)$, for $j \geq 0$, such that

$$\begin{aligned} &B_0 = C_0 = I, \\ &B_j \equiv B_{j-1} \pmod{t^j} \text{ in } \mathrm{Mat}_n(\widehat{R}_1), \\ &C_j \equiv C_{j-1} \pmod{t^j} \text{ in } \mathrm{Mat}_n(\widehat{R}_2), \\ &A_0 \equiv B_j^{-1}C_j \pmod{t^{j+1}} \text{ in } \mathrm{Mat}_n(\widehat{R}_0). \end{aligned}$$

Doing this will prove the assertion, by taking $A_1 \in \mathrm{Mat}_n(\widehat{R}_1)$, $A_2 \in \mathrm{Mat}_n(\widehat{R}_2)$ to be the t-adic limits of the sequences $\{B_j\}$, $\{C_j\}$ respectively. Note that A_i actually lies in $\mathrm{GL}_n(\widehat{R}_i)$ because its determinant, being congruent to 1 modulo t, is a unit by Problem 2.14(a).

To construct these sequences, suppose that $j > 0$ and that B_ℓ, C_ℓ have already been constructed, satisfying the above conditions, for $\ell < j$. Thus

$$A_0 - B_{j-1}^{-1}C_{j-1} = t^j \tilde{A}_j$$

for some $\tilde{A}_j$ with entries in $\widehat{R}_0$. Applying Lemma 2.1 to the entries of $\tilde{A}_j$, there exist matrices $B'_j \in \mathrm{Mat}_n(\widehat{R}_1)$ and $C'_j \in \mathrm{Mat}_n(\widehat{R}_2)$ such that

$$\tilde{A}_j \equiv B'_j + C'_j \pmod{t} \text{ in } \mathrm{Mat}_n(\widehat{R}_0).$$

The matrices

$$B_j := B_{j-1} - t^j B'_j \in \mathrm{Mat}_n(\widehat{R}_1) \text{ and } C_j := C_{j-1} + t^j C'_j \in \mathrm{Mat}_n(\widehat{R}_2)$$

have determinant congruent to 1 modulo (t) and so are invertible. It is straightforward to check that they have the desired properties, using the corresponding properties for B_{j-1} and C_{j-1} together with the congruence $A_0 \equiv I \pmod{t}$. □

The proof of the above result can be carried out explicitly when given a specific matrix. See Problem 2.20 for an example.

We now introduce fields for which the ideas of the previous section apply. Suppose $U \subseteq X$. If U does not contain all the closed points of X, we write F_U for the fraction field of $\widehat{R}_U$. Otherwise, if U does contain all the closed points of X, we let $F_U = F$. (In this latter case, F_U is not the fraction field of $\widehat{R}_U$.)

Theorem 2.3 (Weierstrass Preparation)**.** *If $U \subseteq X$ then every element $f \in F_U$ may be written as a product $f = au$ with $a \in F$ and $u \in \widehat{R}_U^\times$.*

Proof. The result is trivial if U contains all the closed points of X, so we may assume otherwise. By Problems 2.14(c) and 2.15, the result is immediate if U contains no closed points, since we may take $a = t^r$ where r is the t-adic valuation of f in the complete discretely valued field $F_\varnothing$. So now assume that U contains some but not all of the closed points of X.

It suffices to prove the result in the case that $f \in \widehat{R}_U = A[[t]]$, since every element of F_U is a quotient of two such elements. We may also assume that f is non-zero; and after factoring out a power of t we may assume that f has a non-zero constant term $f_0 \in A$. Let U_1 be the complement of U in X; and write $U_2 = U$ and $\widehat{R}_i = \widehat{R}_{U_i}$. Since $\tilde{f} := f/f_0 \in \widehat{R}_\varnothing$ has constant term 1, it is a unit. Proposition 2.2 (with $n = 1$) then implies that $\tilde{f} = f_1 f_2$ with $f_i \in \widehat{R}_i^\times$ for $i = 1, 2$. Now $f_0 \in A$ and $f \in \widehat{R}_U = \widehat{R}_2$; so $f_0 f_1 = f f_2^{-1} \in \widehat{R}_1[f_0] \cap \widehat{R}_2 \subseteq F$ by Problem 2.17(c). Hence we may take $a = f_0 f_1$ and $u = f_2$. □

Remark 2.4. In the case that U consists just of the point $x = 0$ on X, Theorem 2.3 is closely related to the standard algebraic form of the Weierstrass Preparation Theorem. Compare Proposition 6 in Section VII.3.8 of [Bou72].

Theorem 2.5. *Let $U_1, U_2 \subseteq X$, and write $U_0 = U_1 \cap U_2$ and $U = U_1 \cup U_2$. Then $F_{U_1} \cap F_{U_2} = F_U$ inside F_{U_0}.*

Proof. By Problem 2.15, we may assume that U_1, U_2 each contain the generic point η of X. Hence so does U.

The assertion is trivial if U_1 or U_2 is equal to X; so we may assume that the U_i are proper subsets of X, each missing at least one closed point. Write $\widehat{R}_i = \widehat{R}_{U_i}$ and $F_i = F_{U_i}$, for $i = 0, 1, 2$. Problem 2.16 implies that $\widehat{R}_U \subseteq \widehat{R}_i$ and hence $F_U \subseteq F_i$, for $i = 1, 2$. Let $f \in F_1 \cap F_2$. It remains to show that $f \in F_U$. By Theorem 2.3, $f = f_1 u_1 = f_2 u_2$ for some $f_1, f_2 \in F \subseteq F_U$ and some $u_i \in \widehat{R}_i^\times$.

If U is strictly contained in X, then F_U is the fraction field of $\widehat{R}_U$. So $f_i = a_i/b_i$ for some $a_i, b_i \in \widehat{R}_U$, and thus $f = a_1 u_1/b_1 = a_2 u_2/b_2$. Hence $a_1 b_2 u_1 = a_2 b_1 u_2 \in \widehat{R}_1 \cap \widehat{R}_2 = \widehat{R}_U$ by Problem 2.17(a). Since also $b_1 b_2 \in \widehat{R}_U$, it follows that $f = a_1 b_2 u_1/b_1 b_2$ lies in F_U.

Now suppose instead that $U = X$. By Problem 2.14(a), $\widehat{R}_i = A_i[[t]]$ for some $A_i \subseteq k(x)$. Since U_2 is strictly contained in $X = U_1 \cup U_2$, it follows that U_1 is not contained in U_2. Hence $\widehat{R}_2$ is not contained in $\widehat{R}_1$ by Problem 2.16, and A_2 is not contained in A_1. Take $f_0 \in A_2$ that does not lie in A_1. By Problem 2.17(c), $R' := \widehat{R}_1[f_0] \cap \widehat{R}_2$ is a subring of F whose fraction field is F. Thus $f_i = a_i/b_i$ for some $a_i, b_i \in R'$; so $f = a_1 u_1/b_1 = a_2 u_2/b_2$. Hence $a_1 b_2 u_1 = a_2 b_1 u_2 \in \widehat{R}_1[f_0] \cap \widehat{R}_2 = R'$. Since $b_1 b_2 \in R'$, it follows that $f = a_1 b_2 u_1/b_1 b_2$ lies in $F = F_U$, the fraction field of R'. □

Using this, we can generalize Proposition 2.2.

Theorem 2.6. *Let $U_1, U_2 \subseteq X$, set $U_0 = U_1 \cap U_2$, and write F_i for F_{U_i} ($i = 0, 1, 2$). Then for every $n \geq 1$ and $A_0 \in \mathrm{GL}_n(F_0)$ there exist $A_1 \in \mathrm{GL}_n(F_1)$ and $A_2 \in \mathrm{GL}_n(F_2)$ such that $A_0 = A_1^{-1} A_2$ in $\mathrm{GL}_n(F_0)$.*

Proof. First consider the case that U_0 is empty. After multiplying A_0 by a power of t, we may assume that A_0 lies in $\mathrm{Mat}_n(\widehat{R}_\varnothing)$, with non-zero determinant. Thus $A_0^{-1} \in t^{-r}\,\mathrm{Mat}_n(\widehat{R}_\varnothing) \subset \mathrm{Mat}_n(F_0)$ for some $r \geq 0$, by Problem 2.14(c). Since $R_\varnothing \subset F$ is t-adically dense in $\widehat{R}_\varnothing$, there exists $C_0 \in \mathrm{Mat}_n(R_\varnothing)$ that is congruent to $t^r A_0^{-1}$ modulo t^{r+1} in $\mathrm{Mat}(\widehat{R}_\varnothing)$. Write $C = t^{-r}C_0 \in t^{-r}\,\mathrm{Mat}_n(R_\varnothing) \subset \mathrm{Mat}_n(F) \subseteq \mathrm{Mat}_n(F_1)$. Then $C - A_0^{-1} \in t\,\mathrm{Mat}_n(\widehat{R}_\varnothing)$ and so $CA_0 - I \in t\,\mathrm{Mat}_n(\widehat{R}_\varnothing)$. This implies that $CA_0 \in \mathrm{GL}_n(\widehat{R}_\varnothing)$ and hence that the determinant of C is non-zero. Thus $C \in \mathrm{GL}_n(F_1)$. Now $CA_0 \equiv I \pmod{t}$ in $\mathrm{Mat}_n(\widehat{R}_\varnothing)$, hence $CA_0 \in \mathrm{GL}_n(\widehat{R}_\varnothing)$ by Problem 2.14(c). It follows from Proposition 2.2 that there exist $A_1' \in \mathrm{GL}_n(F_1)$ and $A_2 \in \mathrm{GL}_n(F_2)$ satisfying $CA_0 = A_1'^{-1}A_2$ in $\mathrm{GL}_n(F_0)$. Let $A_1 = A_1'C \in \mathrm{GL}_n(F_1)$. Then $A_0 = A_1^{-1}A_2$.

Now consider the general case. Let U_2' be the complement of U_0 in U_2, and write $F_2' = F_{U_2'}$. Thus $F_2' \cap F_0 = F_2$ by Theorem 2.5, since $U_2' \cup U_0 = U_2$. Also $U_1 \cap U_2'$ is empty. Any $A_0 \in \mathrm{GL}_n(F_0)$ lies in $\mathrm{GL}_n(F_\varnothing)$, and so by the above special case we may write $A_0 = A_1^{-1}A_2$ with $A_1 \in \mathrm{GL}_n(F_1) \subseteq \mathrm{GL}_n(F_0)$ and $A_2 \in \mathrm{GL}_n(F_2')$. But $A_2 = A_1A_0 \in \mathrm{GL}_n(F_0)$. Hence $A_2 \in \mathrm{GL}_n(F_2') \cap \mathrm{GL}_n(F_0) = \mathrm{GL}_n(F_2)$. □

We can now apply the results of Section 1 to this situation. For any subset $U \subseteq X$ we will write $\mathrm{V}(U)$ for $\mathrm{Vect}(F_U)$, the category of finite dimensional vector spaces over F_U. (Recall that if U contains all the closed points of X then F_U is just F.) If $U \subseteq U' \subseteq X$ then there is a functor $\mathrm{V}(U') \to \mathrm{V}(U)$ given by base change; i.e. which sends an $F_{U'}$-vector space V to $V \otimes_{F_{U'}} F_U$.

Theorem 2.7. *Let $U_1, U_2 \subseteq X$, and write $U = U_1 \cup U_2$ and $U_0 = U_1 \cap U_2$. Then the functor*

$$\mathrm{V}(U) \to \mathrm{V}(U_1) \times_{\mathrm{V}(U_0)} \mathrm{V}(U_2)$$

induced by base change is an equivalence of categories.

Proof. By Theorem 2.5, $F_{U_1} \cap F_{U_2} = F_U \subseteq F_{U_0}$. And by Theorem 2.6, every element $A_0 \in \mathrm{GL}_n(F_0)$ can be factored as $A_0 = A_1^{-1}A_2$ with $A_1 \in \mathrm{GL}_n(F_1)$ and $A_2 \in \mathrm{GL}_n(F_2)$. So Theorem 1.3 yields the assertion. □

The above result can be generalized to the case of more subsets of X:

Theorem 2.8. *Let $U_1, \ldots, U_r \subseteq X$, and assume that the pairwise intersections $U_i \cap U_j$ (for $i \neq j$) are each equal to a common subset $U_0 \subseteq X$. Let $U = \bigcup_{i=1}^r U_i$. Then the base change functor*

$$\mathrm{V}(U) \to \mathrm{V}(U_1) \times_{\mathrm{V}(U_0)} \cdots \times_{\mathrm{V}(U_0)} \mathrm{V}(U_r)$$

is an equivalence of categories.

Proof. See Problem 2.21. □

Example 2.9. (a) Let $r \geq 2$ and let $P_1, \ldots, P_{r-1}$ be distinct closed points of X. Then Theorem 2.8 applies with $U_i = \{P_i\}$ for $1 \leq i < r$ and with U_r equal to the complement of $\{P_1, \ldots, P_{r-1}\}$ in X. Here $U = X$ and $U_0 = \varnothing$.

(b) Let $r \geq 2$ and let $P_1, \ldots, P_r$ be distinct closed points of X. Let U_0 be the complement of $\{P_1, \ldots, P_r\}$ in X. Then Theorem 2.8 applies with $U = X$ and with $U_i = U_0 \cup \{P_i\}$ for $1 \leq i \leq r$.

Applying Proposition 1.4 and Problem 1.11 in the context of Theorem 2.7 yields analogs of Theorem 2.7 for various types of algebras. Similarly, using induction, one obtains such analogs of Theorem 2.8, e.g. in the context of the situations in Example 2.9.

In particular, the analog of Problem 1.11(iv) can be used to show that every finite group G is the Galois group of some field extension of $F = k((t))(x)$. This is done by considering G-Galois algebras over the fields F_{U_i}, where the subsets U_i are as in Example 2.9. If these are chosen appropriately, and if the isomorphisms over F_{U_0} are also chosen appropriately, then it can be shown that the resulting G-Galois F-algebra is in fact a field. See Section 7.2 of [HH10] for details. A similar strategy will be used later in the context of admissibility.

Above we have worked only over the complete discrete valuation ring $T = k[[t]]$ and its fraction field $K = k((t))$. In fact, the above results can be carried over to arbitrary complete discrete valuation rings and their fraction fields, though the descriptions of the rings $\widehat{R}_U$ and fields F_U become less explicit, and some of the arguments also become somewhat more involved. (See Section 4 of [HH10] for more details.) For example, one can work over the ring $\mathbb{Z}_p$ of p-adic integers, and its fraction field $\mathbb{Q}_p$ of p-adic numbers. As a result, it is possible to carry over applications to such situations. In particular, it can be shown that every finite group is the Galois group of a field extension of $\mathbb{Q}_p(x)$. The inverse Galois assertion in Section 7.2 of [HH10] is in fact stated for general complete discretely valued fields. See Problem 2.23 for the case of the line over the ring $\mathbb{Z}_p$.

As another generalization, one can consider T-curves other than the projective T-line. In particular, consider a smooth projective T-curve, i.e. a scheme $\widehat{X}$ together with a smooth projective morphism $\widehat{X} \to \mathrm{Spec}(T)$ whose fibers have dimension one. In this situation, the main results above can be carried over, though the arguments become more complicated (e.g. due to phenomena related to the Riemann-Roch theorem). This is carried out in Section 4 of [HH10]. Using a more complicated set of overfields, and a more involved version of Theorem 2.8, it is even possible to handle the case of singular curves whose closed fibers are reducible. This is carried out in Section 6 of [HH10]. But we do not need this for our purposes here.

On the other hand, for a number of purposes, one can study curves other than the projective line just by using the results above. One way to do this is to map the given curve $\widehat{Y}$ to the projective line $\widehat{X}$. The function field E of $\widehat{Y}$ is a finite field extension of F, and for each i we may consider the F_{U_i}-algebra $E_i := F_{U_i} \otimes_F E$, where the subsets $U_i \subseteq X$ are as before. A vector space over E can be viewed as a vector space over F with additional structure; and one can then proceed along the lines of Proposition 1.4 and Problem 1.11.

Another approach to handling other curves is to construct objects over the field $F = k((t))(x)$ and then to base change from F to E, the function field of the given curve (where again we view E as a finite extension of F by mapping the curve to the line). For example, once G-Galois field extensions A of F are constructed, one obtains G-Galois E-algebras $A_E := A \otimes_F E$. If A is chosen suitably (viz. linearly disjoint from E over F; e.g. if they have

disjoint branch loci), then A_E is a G-Galois field extension of E.

Problems for Section 2

Problem 2.10. Describe the prime ideals and the maximal ideals in T and in $T[x]$. Describe the (prime) spectra of these rings geometrically, in particular discussing the closed subsets of each.

Problem 2.11. (a) Find the Krull dimension of T and of $T[x]$. For each of these two rings, do all maximal chains of prime ideals in that ring have the same length?

(b) Find the dimensions of the schemes $\mathrm{Spec}(T)$, $\mathrm{Spec}(T[x])$, and $\mathbb{P}^1_T$. In each case, are all maximal chains of the same length?

Problem 2.12. Show that every closed point in $\mathbb{P}^1_T$ lies in the zero locus of the ideal (t); i.e., in the closed set defined by this ideal. Show also that this locus is the fiber X of the morphism $\mathbb{P}^1_T \to \mathrm{Spec}(T)$ over the closed point of $\mathrm{Spec}(T)$. (Here X is called the *closed fiber* of $\widehat{X}$.) Show that X is isomorphic to $\mathbb{P}^1_k$ and that the complement of X in $\widehat{X}$ is isomorphic to $\mathbb{P}^1_K$.

Problem 2.13. Show that the field of rational functions on $\mathbb{P}^1_T$ is $k((t))(x)$.

Problem 2.14. Let $U \subseteq X$.

(a) Show that $\widehat{R}_U$ is a domain, and that $\widehat{R}_U = A[[t]]$ for some k-algebra A which is a domain having fraction field $k(x)$. Describe the ring A explicitly in terms of U.

(b) Prove that every element of $\widehat{R}_U$ that is congruent to 1 modulo t is a unit in this ring. More generally, show that $f \in \widehat{R}_U = A[[t]]$ is a unit if and only if its constant term is a unit in A.

(c) Find A explicitly in each of these cases: U is a Zariski affine open subset of X; $U = \{P\}$ for some closed point P of X; $U = \varnothing$; $U = X$. In the last two cases show that $\widehat{R}_U$ is a discrete valuation ring with uniformizer t and find its residue field. In each of the cases find the Krull dimension of $\widehat{R}_U$.

(d) In the case that U is the affine x-line over k, compare the rings $\widehat{R}_U$, R_U, and $T[x]$. In particular, what natural containments are there, as T-algebras? For each such containment, can a non-unit in the smaller ring become a unit in the larger ring?

Problem 2.15. Let η be the generic point of X; this is the unique point of X that is not a closed point. Suppose that $U \subseteq X$, and let $U' = U \cup \{\eta\}$. Show that $R_U = R_{U'}$ and $\widehat{R}_U = \widehat{R}_{U'}$. (Note that the definition of $R_\varnothing$ ensures that this equality holds even if U is empty.)

Problem 2.16. Suppose that U_1, U_2 are sets of closed points of X.

(a) Show that the following are equivalent:

(i) $U_1 \subset U_2$;

(ii) $R_{U_2} \subset R_{U_1}$;

(iii) $\widehat{R}_{U_2} \subset \widehat{R}_{U_1}$.

(b) Show that the three analogous conditions, with containment replaced by equality, are also equivalent.

(c) What if instead U_1, U_2 are subsets of X that each contain the generic point η of X?

Problem 2.17. Suppose that $U_1, U_2 \subseteq X$ and let $U = U_1 \cup U_2$. Write $\widehat{R}_i$ for $\widehat{R}_{U_i}$.

(a) Show that $\widehat{R}_1 \cap \widehat{R}_2 = \widehat{R}_U$.

(b) Find $\widehat{R}_1[x] \cap \widehat{R}_2$ explicitly if U_1 is the complement in X of the point $x = 0$, and U_2 is the complement of the point at infinity. In particular, observe that this intersection is contained in F and that its fraction field is equal to F.

(c) More generally, suppose that $U = X$ and that $f \in A_2$ where $\widehat{R}_i = A_i[[t]]$. Show that $\widehat{R}_1[f] \cap \widehat{R}_2 \subseteq F$. Show moreover that the fraction field of this intersection is equal to F provided that $f \notin k$.

Problem 2.18. Let R be a ring that is complete with respect to a non-archimedean absolute value $|\cdot|$. That is, $|\cdot| : R \to \mathbb{R}$ satisfies $|a| \geq 0$ for all $a \in R$, with $|a| = 0$ precisely for $a = 0$; $|ab| = |a|\,|b|$; and $|a+b| \leq \max(|a|, |b|)$. Let $R\{x\}$ be the subset of $R[[x]]$ consisting of power series whose coefficients approach 0 in the metric defined by the absolute value. Similarly define $R\{x_1, \ldots, x_n\}$.

(a) Show that $R\{x\}$ is a subring of $R[[x]]$.

(b) Show that $f(x) \in R[[x]]$ lies in $R\{x\}$ if and only if the infinite sum $f(a)$ converges in R for all $a \in R$ of absolute value at most 1.

(c) Let $T = k[[t]]$ and $K = k((t))$ as before, and let U be the affine line over k, with parameter x. Show that $T\{x\} = \widehat{R}_U$ and that $K\{x\} = \widehat{R}_U[t^{-1}]$. Can you interpret the rings $T\{x^{-1}\}$, $K\{x^{-1}\}$, $T\{x, x^{-1}\}$, and $K\{x, x^{-1}\}$ in an analogous way? (Here $T\{x, x^{-1}\}$ is shorthand for $T\{x, y\}/(xy - 1)$ and similarly for $K\{x, x^{-1}\}$.)

Problem 2.19. (a) Find an explicit additive decomposition as in Lemma 2.1 if U_1 is the complement of the point $x = 0$ in X; U_2 is the complement of the point $x = 1$; and the constant term of a, as a power series in t, is $(x^2 + 1)/(x^2 - x)$.

(b) Do the same if U_1 is as before but U_2 is the complement of the point at infinity and the constant term of a is $(x^2 + x - 1)/x$.

Problem 2.20. Assume that k has characteristic zero. Let U_1 be the complement of the point $x = 0$ in X, and let U_2 be the complement of the point at infinity. Take $n = 1$ and let A_0 be the 1×1 matrix whose entry is $\displaystyle\sum_{n=0}^{\infty} \frac{(x^4+1)^n}{n!\, x^{2n}} t^n$. Explicitly find the first several terms in the entries of A_1 and A_2 as in Proposition 2.2, as power series in t. Can you express A_1 and A_2 fully?

Problem 2.21. Using Theorem 2.7 and induction, prove Theorem 2.8. Before doing so, write down a precise definition of the category and the functor that appear in the statement of the theorem.

Problem 2.22. Let $k = \mathbb{C}$, let $U_1 \subset X = \mathbb{P}^1_{\mathbb{C}}$ consist of the point $x = 0$, let U_2 be the complement of U_1 in X, and let $U_0 = \varnothing$. Let F be the function field of $\widehat{X} = \mathbb{P}^1_{\mathbb{C}[[t]]}$, and write $F_i = F_{U_i}$ for $i = 0, 1, 2$.

(a) Consider the Galois field extension E_1 of F_1 given by $y^2 = x - t$, and the Galois field extension E_2 of F_2 given by $z^2 = x^{-1} - t$. Give an isomorphism $\mu : E_1 \otimes_{F_1} F_0 \to E_2 \otimes_{F_2} F_0$ of field extensions of F_0, and then find a field extension E of F such that $E \otimes_F F_i$ is isomorphic to E_i for $i = 1, 2$, compatibly with μ. Is E Galois over F?

(b) What changes if instead we replace E_1, E_2 by the extensions given by $y^2 = x^2 - t^2$ and $z^2 = x^{-2} - t^2$? What stays the same?

(c) Now replace E_1, E_2 by the extensions given by $y^4 = x^4 - t^4$ and $z^4 = x^{-4} - t^4$. What can go wrong depending on the choice of μ? (Cf. Problems 1.11 and 1.12.)

Problem 2.23. (a) State and carry out the analog of Problems 2.10 and 2.11, with T replaced by $\mathbb{Z}_p$.

(b) Do the same for Examples 2.12 and 2.13.

(c) Try to find an analog of Problem 2.14.

Problem 2.24. Do the results of this section hold if T is replaced by $k[[s, t]]$?

Problem 2.25. Let S be a smooth projective surface over a field k, and write F for the function field of S. Let X denote an isomorphic copy of $\mathbb{P}^1_k$ in S. For $U \subseteq X$ non-empty, let R_U denote the subring of F consisting of the rational functions on $\widehat{X}$ that are regular at the points of U. Let $\mathcal{I}$ be the ideal sheaf defining X in S, and let $\widehat{R}_U$ denote the $\mathcal{I}$-adic completion of the ring R_U. Also write $R_\varnothing$ for the subring of F consisting of the rational functions that are regular at the generic point of X, and write $\widehat{R}_\varnothing$ for its $\mathcal{I}$-adic completion. To what extent to the results of this section remain true in each of the cases below?

(i) $S = \mathbb{P}^1_k \times \mathbb{P}^1_k$, and $X = \mathbb{P}^1_k \times O$ where O is the point 0 on $\mathbb{P}^1_k$.

(ii) $S = \mathbb{P}^2_k$, and X is the line at infinity.

(iii) S is the result of blowing up the point $x = y = 0$ in $\mathbb{P}^2_k$, and X is the exceptional divisor.

Can you make any conjectures about how the behavior depends on the choice of the pair (S, X)?

Problem 2.26. (a) Let p be a prime number and consider $\mathbb{P}^1_{\mathbb{F}_p}$, with function field $\mathbb{F}_p(x)$. Can one define fields F_1, F_2, F_0 in this context, such that analogs of the results of this section hold?

(b) What if instead F is replaced by $\mathbb{Q}$?

Part II

A prominent question considered in Galois theory is the so called *inverse problem*: Given a field F, determine all finite groups that occur as Galois groups over F. Of course, the answer depends on F. For example, it is known that all finite groups occur when F is a rational function field $C(t)$ with C algebraically closed or complete, or more generally an algebraic function field over such a field C. It is an open question when $F = \mathbb{Q}$, the field of rational numbers.

There are various types of methods used to prove results like the ones mentioned above or to realize certain groups as Galois groups. One of them, which works in the case of $C(t)$ for a complete field C, is *patching*, which is the subject of Part I of these notes. In this second part, we are going to apply the patching method to study a variant of the inverse Galois problem.

3 Basics on central simple algbras, division algebras, and the Brauer group

Throughout this section, F denotes a field.

Definition 3.1. A *central simple F-algebra* is a finite dimensional F-algebra with center F and without nontrivial two-sided ideals. It is called a *division algebra* if every nonzero element is a unit.

Here are some basic but important examples:

(1) Let F be a field of characteristic unequal to two, and let $a, b \in F \setminus F^2$. Then there is a *quaternion algebra* defined as

$$H(a, b) = F \cdot 1 \oplus F \cdot i \oplus F \cdot j \oplus F \cdot ij$$

with multiplication given by

$$i^2 = a, j^2 = b, ij = -ji.$$

When $F = \mathbb{R}$, $a = b = -1$, this construction gives the usual *Hamilton quaternions* $\mathbb{H}$.

(2) Let G be a finite group and let $\rho : G \to \mathrm{GL}_n(F)$ be an irreducible representation. Then Schur's Lemma asserts that $\mathrm{End}_G(\rho)$ is a division algebra (and so it is central simple).

(3) The algebra $\mathrm{Mat}_n(F)$ is a central simple F-algebra (see Problem 3.15). It is not a division algebra if $n > 1$.

(4) Suppose that n is a positive integer and F is a field that contains a primitive nth root of unity ζ. For any $a, b \in F^\times$, we define the *symbol algebra* $A_\zeta(a, b, F)$ to be the F-algebra with generators i, j and relations $i^n = a$, $j^n = b$, and $ij = \zeta ji$. It is well known that this is a central simple F-algebra of dimension n^2. (This generalizes the first example.)

We will not be able to provide proofs for all of the material covered in this section. These proofs are however not very difficult, and we encourage the reader to look them up. The reference [BO] seems particularly accessible (though long).

In order to check whether a given algebra is a central simple algebra, it is often useful to consider a base change:

Lemma 3.2. *Let A be an associative algebra over F and let L/F be a finite field extension. Then A is central simple over F if and only if $A \otimes_F L$ is central simple over L.*

The famous structure theorem of Wedderburn classifies central simple algebras.

Theorem 3.3 (Wedderburn)**.** *(1) Let n, m be positive integers and let D, D' be division algebras over F. If $\mathrm{Mat}_n(D) \xrightarrow{\sim} \mathrm{Mat}_m(D')$ then D and D' are isomorphic, and $n = m$.*

(2) Every F-central simple algebra is isomorphic to $\mathrm{Mat}_n(D)$ for some n and some F-division algebra D. This division algebra is uniquely determined (up to isomorphism).

Another important theorem concerns automorphisms of central simple algebras. Recall that an *inner automorphism* of an F-algebra A is an automorphism given by conjugation with an invertible element from A.

Theorem 3.4 (Skolem-Noether)**.** *Let A be a central simple F-algebra, and let B be a simple F-algebra (i.e., B is a central simple algebra over a field L which may be a proper overfield of F). Let $\varphi_1, \varphi_2 : B \to A$ be two F-algebra homomorphisms. Then there exists an inner automorphism ρ of A such that $\varphi_2 = \rho \circ \varphi_1$. In particular, every automorphism of A is inner.*

We have already seen that an easy example of a central simple algebra is given by a matrix algebra. In fact, after a base change, every central simple algebra becomes isomorphic to such an algebra.

Definition 3.5. Let A be a central simple F-algebra. A field L is called a *splitting field* of A if it contains F and $A \otimes_F L \xrightarrow{\sim} \mathrm{Mat}_n(L)$ for some n. In this situation, we also say that A splits over L, or that L splits A.

It is clear that splitting fields always exist. For example, one can show that every F-central simple algebra splits over an algebraic closure of F (see Problem 3.17).

It is not hard to conclude that there is always a splitting field which is a finite extension of F. But much more is true:

Theorem 3.6. *Every central simple F-algebra has a Galois splitting field of finite degree over F.*

It follows from the above that the dimension of a central simple F-algebra A is always a square. Hence the square root of the dimension is a natural number, which allows us to make the following definition.

Definition 3.7. Let A be a central simple F-algebra, and let D the division algebra associated to A by Wedderburn's theorem. The square root of the dimension of A is called the *degree* of A, $\deg(A)$. The *index* of A is the degree of D, denoted $\operatorname{ind}(A)$.

As an example, the symbol algebra defined in the previous section has dimension n^2 and hence it has degree n. Note that by definition, $\operatorname{ind}(A) | \deg(A)$, and $\deg(A) = \operatorname{ind}(A)$ if and only if A is division algebra over F. It can also be shown that the index divides the degree of any splitting field. In fact, the index is equal to the degree of a splitting field of minimal degree.

Again, it is useful to know what happens under base change:

Proposition 3.8. *Let A be a central simple algebra over F and let L/F be a field extension. Then* $\operatorname{ind}(A \otimes_F L) \mid \operatorname{ind}(A)$.

We are now going to study the set of all central simple algebras over F up to isomorphism. To this end, we note that one may define a tensor product.

Proposition 3.9. *If A and B are central simple algebras over F, then so is $A \otimes_F B$.*

Definition 3.10. Let A and B be central simple algebra over F. We say A *is Brauer equivalent* to B if $A \otimes_F \operatorname{Mat}_n(F) \xrightarrow{\sim} B \otimes_F \operatorname{Mat}_m(F)$ for suitable $n, m \in \mathbb{N}$. The *Brauer group of F*, $\operatorname{Br}(F)$, is the set of equivalence classes of central simple algebras over F. It is an abelian group with the multiplication

$$[A][B] := [A \otimes_F B],$$

where $[A]$ denotes the class of A etc.

It is not hard to see that this multiplication is indeed well defined (see Problem 3.18).

The following lemma records some basic properties of Brauer equivalence.

Lemma 3.11. *Let A and B be central simple F-algebras, and let L/F be a field extension. Then the following holds:*

(1) Brauer equivalent central simple F-algebras have the same index and isomorphic division algebras (as associated by Wedderburn's theorem).

(2) Two central simple F-algebras are Brauer equivalent if and only if their underlying division algebras are isomorphic.

(3) Brauer equivalent central simple algebras are isomorphic if and only if they have the same degree.

(4) If A is Brauer equivalent to B, then $A \otimes_F L$ is Brauer equivalent to $B \otimes_F L$.

Thus elements of $\mathrm{Br}(F)$ correspond bijectively to isomorphism classes of F-division algebras.

Theorem 3.12. *For any field F, the Brauer group $\mathrm{Br}(F)$ is a torsion group.*

That is, every element in $\mathrm{Br}(F)$ is of finite order.

Definition 3.13. Let α be an element of $\mathrm{Br}(F)$. The *period* of α is defined as the order of α in the Brauer group, denoted $\mathrm{per}(A)$.

The prime factorization of the period of a Brauer class gives information about the class itself, by the following decomposition property:

Proposition 3.14. *Let e_1 and e_2 be coprime integers, and let A be a central simple F-algebra of period e_1e_2. There exist two central simple F-algebras A_1 and A_2, uniquely determined up to isomorphism, such that:*

(1) $\mathrm{per}(A_i) = e_i$, $i = 1, 2$,

(2) $A_1 \otimes_F A_2 \xrightarrow{\sim} A$.

Moreover, A is a division algebra if and only if A_1 and A_2 are.

This statement can be deduced from the Primary Decomposition Theorem (which is a similar result concerning factorizations of the degree) and its proof, see [BO], Theorem 20.7 and following.

Problems for Section 3

Problem 3.15. Show that the center of $\mathrm{Mat}_n(F)$ is (isomorphic to) F. Determine the structure of left and right ideals in $\mathrm{Mat}_n(F)$. Conclude that $\mathrm{Mat}_n(F)$ is an F-central simple algebra.

Problem 3.16. Give an example of two non-isomorphic central simple algebras (resp. division algebras) over $\mathbb{Q}$ of the same degree.

Problem 3.17. Let F be a field and A a central simple algebra over F.

(1) Show that A is split over any algebraic closure of F.

(2) Conclude that the dimension of A (as a vector space over F) must be a square.

(3) Show that an extension L/F is a splitting field for A if and only if it splits the division algebra D associated to A by Wedderburn's theorem.

Problem 3.18. (1) Show that the multiplication in the Brauer group is well defined, associative, and commutative.

(2) Let A be a central simple F-algebra. Show that there is a central simple F-algebra B such that $A \otimes_F B \xrightarrow{\sim} \mathrm{Mat}_n(F)$.

(3) Determine $\mathrm{Br}(F)$ in the cases when F is algebraically closed or finite.

(4) Can you determine $\mathrm{Br}(\mathbb{R})$?

4 Crossed Product Algebras and the admissibility problem

Definition 4.1. A finite group G is called *admissible* over a field F if there is a G-Galois extension E/F contained in an F-division algebra D such that

$$[E : F] = \deg_F(D).$$

Note that if E is any subfield of an F-division algebra D, then $[E : F] \leq \deg_F(D)$. Hence if G is admissible, the field E in the above definition is a maximal subfield of D. Conversely, any maximal subfield E of an F-division algebra D satisfies $[E : F] = \deg_F(D)$ (however, this does not remain true for central simple algebras which are not division).

There is another way of expressing the same property in different terms.

Definition 4.2. Let E/F be a finite Galois extension with Galois group G. A *G-crossed product algebra* A is defined by the following data:

- A vector space $A := \bigoplus_{\sigma \in G} E u_\sigma$ for some generators u_σ (where we set $u_1 = 1$ for simplicity)
- a (normalized) 2-cocycle c of G in $E^\times$, i.e., a map $c : G \times G \to E^\times$ satisfying $c(1, \sigma) = c(\tau, 1) = 1$ and $\sigma(c(\tau, \rho)) \cdot c(\sigma, \tau\rho) = c(\sigma\tau, \rho) \cdot c(\sigma, \tau)$ for all $\sigma, \tau, \rho \in G$.
- a multiplication defined by $u_\sigma \cdot b = \sigma(b) u_\sigma$ for $b \in E$, and by $u_\sigma u_\tau = c(\sigma, \tau) u_{\sigma\tau}$.

In Problem 4.13 below, you are going to show the following

Lemma 4.3. *Let E/F be a finite Galois extension with group G, and let A be a G-crossed product algebra. Then A is an F-central simple algebra.*

If the cocycle condition looks confusing to you, the proof of the lemma will also show you that it is exactly ensuring the associativity of A (which will hopefully make it look more natural). Whereas the definition may seem pretty technical, crossed product algebras are by no means rare:

Proposition 4.4. *Any central simple algebra is Brauer equivalent to a crossed product algebra (for some group G).*

You will prove this statement in Problem 4.15.

We can now give another characterization of admissibility:

Proposition 4.5. *A finite group G is admissible over a field F if and only if there is a G-crossed product division algebra over F.*

It is not true that crossed product algebras are always division algebras (see Problem 4.14), so the word *division* in the above proposition cannot be omitted.

If one looks at crossed products from the viewpoint of maximal subfields, there is also a relationship to splitting fields:

Proposition 4.6. *Let A be central simple F-algebra, and let L be a field extension satisfying $[L : F] = \deg(A)$. Then L is a splitting field of A if and only if it isomorphic to a maximal commutative subfield of A.*

Let us exhibit an important class of examples of crossed product algebras.

Lemma 4.7. *Let G be a cyclic group of order n, and let L/F be a G-Galois extension. Let σ be a generator of G, and let $a \in F^\times$.*

For all $0 \leq i, j \leq n-1$, set

$$\zeta_{\sigma,a}(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i+j < n \\ a & \text{if } i+j \geq n. \end{cases}$$

Then the map $\zeta_{\sigma,a} : G \times G \to L^\times$ is a 2-cocycle.

The proof is a simple case by case analysis which we leave to the reader.

Definition 4.8. Define the F-algebra $(a, L/F, \sigma)$ to be the crossed product algebra given by $\zeta_{\sigma,a}$. This is called a *cyclic algebra*. It is the F-algebra generated by one element e satisfying

(1) $(a, L/F, \sigma) = \bigoplus_{i=0}^{n-1} Le^i$,

(2) $e \cdot b = \sigma(b)e$ for all $b \in L$ and

(3) $e^n = a$.

The reader is advised to check the claims implicitly made in the above definition. Conversely, it can be checked that any central simple F-algebra of degree n satisfying the three conditions given above is indeed a crossed product with respect to a cyclic group.

The nice thing about this specific type of crossed product is that there is an easy criterion that can be used to ensure that a cyclic algebra is a division algebra.

Proposition 4.9. *Suppose that F is a discretely valued field which contains an nth root of unity, and let L/K be a cyclic Galois extension of degree n. Suppose that v is a valuation on L that commutes with the action of $\mathrm{Gal}(L/F)$, i.e., that it is the unique extension of the given valuation to L. Assume moreover that $a \in F^\times$ is an element such that the order of $v(a)$ in $v(L)/nv(L)$ is n. Then for any generator σ of $\mathrm{Gal}(L/F)$, the cyclic algebra $(a, L/F, \sigma)$ is a division algebra over F.*

Proof. Let $A := (a, L/F, \sigma)$. With notation as in Definition 4.8, show that the formula

$$v\left(\sum_{i=0}^{n-1} a_i e^i\right) = \min\{v(a_i) + \frac{i}{n}v(a) |\ i = 0, \ldots, n-1, a_i \neq 0\}$$

defines a map $v : A \setminus \{0\} \to \frac{1}{n}v(L)$ which satisfies $v(a+b) \geq min(v(a), v(b))$, for all $a, b \in A \setminus \{0\}$ with $b \neq -a$ and $v(a+b) = min(v(a), v(b))$, whenever $v(b) \neq v(a)$. Deduce that A cannot contain any zero divisors. □

The division algebra version of the inverse Galois problem now reads as follows: Given a field F, which finite groups are admissible over F?

We start with a brief summary of known results. For example, if $F = \mathbb{Q}$, a theorem of Brauer, Hasse, and Noether may be reformulated to read

Theorem 4.10. *Every cyclic group is admissible over the field $\mathbb{Q}$ of rational numbers.*

One reason why the admissibility problem is fun is that one can *not* expect all groups to be admissible. This is due to Schacher, who found the following necessary condition in 1968 ([Sch68]):

Theorem 4.11. *If a finite group G is admissible over $\mathbb{Q}$, then all its Sylow subgroups must be metacyclic.*

Here, a (finite) group is called *metacyclic* if it is an extension of a cyclic group by a cyclic group (i.e., if it contains a normal cyclic subgroup such that the quotient is also cyclic). Groups that satisfy the necessary condition of the theorem are also called *Sylow metacyclic* for short. In the same paper, Schacher conjectures that this condition is indeed sufficient, i.e., that the admissible groups over $\mathbb{Q}$ are exactly those that are Sylow metacyclic. This conjecture is still open. In fact, there are Sylow metacyclic groups that are not even known to be Galois groups over $\mathbb{Q}$. But of course the conjecture created a whole industry of showing that certain examples or classes of Sylow metacyclic groups are admissible over $\mathbb{Q}$. One of the most far reaching results in this direction is due to Sonn ([Son83]), who showed that every solvable Sylow metacyclic group is admissible over $\mathbb{Q}$. (For solvable groups, the inverse Galois problem also has a positive solution due to Shafarevich, so at least there's nothing to worry about in that respect.)

There is a statement similar to Schacher's Theorem 4.11 and a corresponding conjecture for function fields over finite fields (which are generally expected to behave in analogy to number fields). In our course, we are going to apply patching methods to show the following:

Theorem 4.12. *Let K be a complete discretely valued field with algebraically closed residue field k, and let F be an algebraic function field over K. Let G be a finite group of order not divisible by the characteristic of k. Then G is admissible over F if and only if every Sylow subgroup of G is abelian of rank at most two.*

Note that instead of *abelian of rank at most two* we could have said *abelian metacyclic*, to emphasize the analogy with Schacher's theorem. We already mentioned that over a field F as in the theorem, all groups occur as Galois groups.

The forward direction of the proof is indeed very similar to Schacher's original proof. Just like Schacher it uses that over the field F, the period of a central simple algebra equals its index, at least for classes of period not divisible by the characteristic of k. The proof of this ([HHK09] or [Lie07]) uses the fact that k is algebraically closed. This direction will be treated only briefly in the course, for the sake of completeness.

The backward direction, i.e., the realization of a given group G as the Galois group of a maximal subfield of some division algebra, extends the patching methods used to prove the inverse Galois problem to solve this new noncommutative inverse Galois type problem.

Problems for Section 4

Problem 4.13. (1) Show that the algebra A given in the definition of a crossed product is associative.

(2) Show that the center of A is F.

(3) Use Lemma 3.2 to show that A is an F-central simple algebra.

Problem 4.14. Find an example of a Galois extension E/F and a $\mathrm{Gal}(E/F)$-crossed product algebra which is not a division algebra.

Problem 4.15. Let F be a field and let A be an F-central simple algebra. Then there exists a finite Galois extension E/F and a $\mathrm{Gal}(E/F)$-crossed product algebra B such that A and B are Brauer equivalent.

Problem 4.16. Find an example of a Sylow-metacyclic group which is not solvable.

Problem 4.17. Study the classes of groups whose Sylow subgroups are all metacyclic or all abelian of rank two, respectively. In particular, give examples of such groups.

Problem 4.18. (1) Find an example of a cyclic extension F of $\mathbb{Q}$ of degree four such that F is a maximal subfield of a $\mathbb{Q}$-division algebra.

(2) Do the same with respect to the group $V_4 = C_2 \times C_2$, instead of C_4.

(3) Show that this new example necessarily contains a C_4-Galois subfield, and exhibit one such subfield explicitely.

You can first try to do this over $\mathbb{Q}(i)$ instead of $\mathbb{Q}$.

Problem 4.19. Find explicit examples of admissible groups over F whose order is divisible by the characteristic of k.

5 Patching crossed product algebras

In order to construct crossed product division algebras with respect to a prescribed group G (which satisfies the necessary condition on the Sylow subgroups given in Theorem 4.12), we are going to use the patching method introduced in the first part of the notes. For simplicity, we restrict our attention to the following situation: Let k denote an algebraically closed field, let $T = k[[t]]$ be the ring of power series over k with field of fractions K, and let $F = K(x)$. Just as the patching methods generalize to more general one variable function fields (see the comments at the end of Section 2), so do the results of this section.

The basic strategy is now the following: Assuming we have crossed product division algebras for the Sylow subgroups of G over some patches we want to glue them together using a version of Theorem 2.8. But there is one technical difficulty we have to overcome: The objects we construct *a priori* have different dimensions (as vector spaces). To resolve this, we introduce *induced algebras*.

Given a finite group G and a subgroup H, any H-Galois field extension L/F gives rise to a G-Galois F-algebra $E = \mathrm{Ind}_H^G L$, called the F-algebra obtained from L by *inducing* up to G. In fact, the construction goes as follows:

(1) Pick left coset representatives $c_1, \ldots, c_n$ of H in G.

(2) As an algebra, define $E = L^{\oplus |G|}$. We identify the standard vector space basis with $c_1, \ldots, c_n$.

(3) If we fix i, each $g \in G$ can be written in the form $c_j h c_i^{-1}$ for some $h \in H$ and some $j \in \{1, \ldots, n\}$. This can be used to define a G-action on E by $g(c_i \cdot a) = c_j \cdot h(a)$ (where $a \in L$).

This is a commutative algebra which is independent of all the choices and has good properties (see Problem 5.3).

Now suppose we are given an H-crossed product division algebra D over F with H-Galois subfield L. The above construction yields a G-Galois algebra E. The following lemma gives the right analog for D.

Lemma 5.1. *In the above situation, let $n = [G : H]$. Then $E = \mathrm{Ind}_H^G(L)$ embeds as a maximal commutative subalgebra of $\mathrm{Mat}_n(D)$.*

Proof. Since $[L : F] = \deg(D)$, the central simple L-algebra $D \otimes_F L$ is isomorphic to $\mathrm{Mat}_m(L)$, where $m = [L : F]$. By the definition of E, this implies that $D \otimes_F E$ is a direct sum of copies of $\mathrm{Mat}_m(L)$. One may conclude that E is a maximal commutative separable subalgebra of some central simple F-algebra B which is Brauer equivalent to D (this uses [DI71], Theorem II.5.5. and Proposition V.1.2). For dimension reasons, B is a matrix algebra over D and isomorphic to $\mathrm{Mat}_n(D)$. □

At this point we are ready to get the patching machinery to work. Recall the notation introduced at the beginning of Section 2.

Theorem 5.2. *Let F be as above and let G be a finite group. Let $H_1, \dots, H_r$ be subgroups of G, and let $Q_1, \dots, Q_r$ be closed points on $\mathbb{P}^1_k$. Let $F_i := F_{\{Q_i\}}$. Suppose for each $i = 1, \dots, r$, we are given an H_i-crossed product division algebra D_i over F_i with H_i-Galois maximal subfield L_i. Suppose moreover that $L_i \otimes_{F_i} F_\varnothing$ is a direct sum of copies of $F_\varnothing$, for each i. Then there exists a central simple F-algebra A with maximal G-Galois subalgebra E such that $E \otimes_F F_i \xrightarrow{\sim} E_i := \mathrm{Ind}_{H_i}^G(L_i)$ for all $i = 1, \dots, r$. If moreover the greatest common divisor of the indices $n_i := [G : H_i]$ is equal to 1, then A is a division algebra and E is a Galois field extension of F.*

Proof. The first step is to use patching to obtain a G-Galois F-algebra E for which $E \otimes_F F_i \xrightarrow{\sim} E_i$ for all $i = 1, \dots, r$. Then one needs to patch the algebras A_i, compatibly with the inclusions of E_i into A_i. Both of these steps are done in Problem 5.4.

Finally, assume the condition on the indices $n_i = [G : H_i]$. First, note that

$$|G|/n_i = |H_i| = [L_i : F_i] = \deg(D_i) = \mathrm{ind}(A_i) \mid \mathrm{ind}(A)$$

since L_i is a maximal subfield of D_i and since the index of a base changed algebra is a divisor of the index of the original algebra (see Section 3).

By the condition on the n_i,

$$\deg(A) = |G| = \mathrm{lcm}(|G|/n_1, \dots, |G|/n_r) \mid \mathrm{ind}(A).$$

But for any central simple algebra, the index divides the degree, hence the index of A must equal the degree of A which is the order of G. Thus A is a division algebra, forcing E to be a field. □

Problems for Section 5

Problem 5.3. Show that the induced algebra $E = \mathrm{Ind}_H^G(L)$ is a commutative algebra which is independent of the choices made (e.g. the coset representatives). Also show that $E^G = F$. Do the explicit construction of Ind_H^G in the case when $G = S_3$, and H is either a cyclic subgroup of order two or A_3.

Problem 5.4. Consider the setup of Theorem 5.2.

(1) Use the hypothesis on $L_i \otimes_F F_\varnothing$ to define a patching problem which will yield a G-Galois F-algebra E with the required property. You will need to use an extra set U to cover $\mathbb{P}^1_k$ by patches, and a corresponding E_U and A_U. The latter should satisfy $A_U \otimes_{F_U} F_\varnothing \xrightarrow{\sim} \mathrm{Mat}_n(F_\varnothing)$.

(2) Now use the hypothesis again to show that there exist isomorphisms $A_i \otimes_{F_i} F_\varnothing \xrightarrow{\sim} \mathrm{Mat}_n(F_\varnothing)$ for all $i = 1, \dots, r$, where $n = |G|$.

(3) Use the Skolem-Noether Theorem to show that for each $i = 1, \ldots, r$, there is a commutative diagram

$$\begin{array}{ccc} A_i \otimes_{F_i} F_\varnothing & \longrightarrow & A_\varnothing \\ \uparrow & & \uparrow \\ E_i \otimes_{F_i} F_\varnothing & \longrightarrow & F_\varnothing^{\oplus |G|} \end{array}$$

(4) Combine the previous steps with a central simple algebra version of Theorem 2.8 to obtain a central simple algebra A that contains a G-Galois algebra E as a maximal subalgebra.

Problem 5.5. Let A be a central simple algebra over F, and let $F_\xi = F_{U_\xi}$ for a finite collection of subsets U_ξ of the projective line over k (as in Problem 5.4 above). Show by example that the index of the induced F_ξ-algebra A_ξ can be strictly less than that of A for some ξ. In fact, can it be strictly less for every ξ?

6 Building blocks for Sylow subgroups

Let F be as in the previous section. Let G be a finite group whose order is not divisible by the characteristic of the residue field k. Since k is algebraically closed, it contains a primitive $|G|$th root of unity. By a standard lifting argument involving Hensel's Lemma, K also contains a primitive $|G|$th root of unity (and hence so do all its overfields, in particular, the field F).

Proposition 6.1. *Let p be a prime unequal to the characteristic of k and let P be an abelian p-group of rank at most two. Then for each closed point Q of $\mathbb{P}^1_k$, P is admissible over $F_{\{Q\}}$. The corresponding field extension L and division algebra D can be chosen to satisfy $L \otimes_{F_{\{Q\}}} F_\varnothing \xrightarrow{\sim} F_\varnothing^{\oplus |P|}$ and $D \otimes_{F_{\{Q\}}} F_\varnothing \xrightarrow{\sim} \mathrm{Mat}_{|P|}(F_\varnothing)$.*

Proof. For simplicity of notation, we assume that Q is a finite place (which is the case after a suitable change of variables). By hypothesis, P is abelian of rank at most two, so let $P = C_q \times C_s$ where q and s are p-powers. The point Q is defined by $t = 0, x = c$ for some $c \in k$. Consider the elements $a := (x-c)/(x-c-t)$ and $b := (x-c-t^2)/(x-c-t-t^2)$. Let L be the extension of $F_{\{Q\}}$ defined by $y^q = a, z^s = b$. Neither a nor b is a dth power in $F_{\{Q\}}$, for any $d > 1$ (why?), so the two extensions defined by the individual equations are Galois with group C_q and C_s, respectively (by Kummer theory). The first extension is totally ramified over $(x-c)$, whereas the other extension is unramified there. Hence they are linearly disjoint over $F_{\{Q\}}$, and L has Galois group P as required.

By the discussion preceding the proposition, $F_{\{Q\}}$ contains a primitive $|P|$th root of unity ζ. We use the symbol algebra construction provided in Section 3: Let D be the central simple algebra generated by elements Y, Z subject to the relations $Y^s = y, Z^q = z$ and $YZ = \zeta ZY$. We leave it to the reader to check that D is a division algebra which contains L as a maximal subfield (see Problem 6.2).

Finally, we show the splitness assertion $L \otimes_{F_{\{Q\}}} F_\varnothing \xrightarrow{\sim} F_\varnothing^{\oplus |P|}$, which implies that $D \otimes_{F_{\{Q\}}} F_\varnothing \xrightarrow{\sim} \mathrm{Mat}_{|P|}(F_\varnothing)$. The elements a and b each lie in the valuation ring of the discretely valued field $F_\varnothing$ (see Problem 2.14.c), and in fact, each is congruent to 1 modulo t. The reductions of a and b are thus $|P|$th powers in k, and hence in $F_\varnothing$, by Hensel's Lemma and completeness. But this means the equations defining L define trivial extensions of $F_\varnothing$, hence the claim. $\square$

The proof of the converse direction of Theorem 4.12 is now done by combining Theorem 5.2 with Proposition 6.1. We leave it to the reader to work out the details.

Problems for Section 6

Problem 6.2. Complete the proof of Proposition 6.1: First, show that the symbol algebra D is equal to a cyclic algebra $(h, F_{\{Q\}}(y), \sigma)$ for some suitable $h \in F_{\{Q\}}$ and $\sigma \in \mathrm{Gal}(F_{\{Q\}}(y)/F_{\{Q\}})$. Then use the valuation theoretic criterion to show that D is a division algebra. Then show that y and z commute in D, and use this to define an embedding of L as a subfield of D. Finally, look at the degree of L to conclude it is a maximal subfield of D. Notice that this gives another proof of the fact that the symbol algebra D is a central simple algebra (more generally, one can use this type of calculation to relate symbol algebras and cyclic algebras).

Problem 6.3. Construct a division algebra over $F = \mathbb{C}((t))(x)$ that contains a maximal subfield that is Galois over F with group S_3.

Problem 6.4. Show by example what goes wrong if one patches together two division algebras over $F = \mathbb{C}((t))(x)$, each having maximal subfields with Galois group $C_2 \times C_2$, in an attempt to prove admissibility of C_2^4 over F.

Problem 6.5. Is every cyclic field extension of $\mathbb{C}((t))(x)$ a maximal subfield of an F-division algebra?

Problem 6.6. Are all cyclic groups admissible over the field of fractions $\mathbb{C}((x, y))$ of the power series ring $\mathbb{C}[[x, y]]$? You should be able to attack this question using methods similar to those used in the proof of Proposition 6.1.

Problem 6.7. What can be said about admissible groups over $F = k((t))(x)$ if k is not algebraically closed? What if k has positive characteristic? What if $k((t))$ is replaced by $\mathbb{Q}_p$? Try to formulate conjectures.

References

[BO] Grégory Berhuy, Frédérique Oggier. Introduction to central simple algebras and their applications to wireless communication. Available at `www-fourier.ujf-grenoble.fr/~berhuy/fichiers/BOCSA.pdf`.

[Bou72] Nicolas Bourbaki. Commutative Algebra. Addison-Wesley Publishing Co., 1972.

[DI71] Frank DeMeyer and Edward Ingraham. Separable algebras over commutative rings. Springer-Verlag, Berlin, 1971.

[HH10] David Harbater and Julia Hartmann. Patching over fields. Israel J. Math. **176** (2010), 61–107.

[HHK09] David Harbater, Julia Hartmann, and Daniel Krashen. Applications of Patching to Quadratic Forms and Central Simple Algebras. Invent. Math. **178** (2009), no.2, 231–263.

[Lie07] Max Lieblich. Period and index in the Brauer group of an arithmetic surface, with an appendix by Daniel Krashen. 2007 manuscript. To appear in Crelle. Also available at arXiv:math/0702240.

[Sch68] Murray M. Schacher. Subfields of division rings. I. J. Algebra **9** (1968), 451–477.

[Son83] Jack Sonn. $\mathbb{Q}$-admissibility of solvable groups. J. Algebra **84** (1983), 411–419.