Chapter 9.
The Absolute Galois Group of $C(t)$

Let C be an algebraically closed field of cardinality m, x an indeterminate, E a finite extension of $C(x)$ of genus g, and S a set of prime divisors of E/C. We denote the maximal extension of E ramified at most over S by E_S. If X is a smooth projective model of E/C, then we interpret S as a subset of $X(C)$, call $\mathrm{Gal}(E_S/E)$ the **fundamental group of** $X \smallsetminus S$, and denote it by $\pi_1(X \smallsetminus S)$. Starting from the fundamental group of the corresponding Riemann surface and applying the Riemann existence theorem, one proves that when $r = \mathrm{card}(S) < \infty$, $\mathrm{Gal}(E_S/E)$ is the free profinite group generated by $r + 2g$ elements $\sigma_1, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g'$ with the unique defining relation $\sigma_1 \cdots \sigma_r [\tau_1, \tau_1'] \cdots [\tau_g, \tau_g'] = 1$ (Proposition 9.1.2). Using Grothendieck's specialization theorem, we generalize that result to an arbitrary algebraically closed field C of characteristic 0 (Proposition 9.1.5). In particular, if $r \geq 1$, then $\mathrm{Gal}(E_S/E) \cong \hat{F}_{r+2g-1}$. When $m = \mathrm{card}(S)$ is infinite, we take the limit on all finite subsets of S to conclude that $\mathrm{Gal}(E_S/E) \cong \hat{F}_m$ (Corollary 9.1.9). In particular, if S is all of the prime divisors of E/C, then $\mathrm{card}(S) = \mathrm{card}(C)$ and we find that $\mathrm{Gal}(E) \cong \hat{F}_m$ (Corollary 9.1.10). In particular, $\mathrm{Gal}(E)$ is projective (Corollary 9.1.11).

The situation is quite different when $\mathrm{char}(C)$ is a positive prime number p. We can not use the Riemann existence theorem to determine the structure of $\mathrm{Gal}(E_S/E)$. Indeed, if S is nonempty and of cardinality less than that of C, then $\mathrm{Gal}(E_S/E)$ is even not a free profinite group (Proposition 9.9.4) as is the case in characteristic 0. What we do know is the structure of the Galois group $\mathrm{Gal}(E_{S,p'}/E)$, where $E_{S,p'}$ is the maximal Galois extension of E ramified at most over S and of degree not divisible by p. Using Grothendieck's lifting to characteristic 0, one proves that the latter group is just the maximal quotient of order not divisible by p of the corresponding group in characteristic 0 (Proposition 9.2.1). But, this does not help us to compute $\mathrm{Gal}(E)$. Instead, we prove by algebraic means that $\mathrm{Gal}(E)$ is a free profinite group of cardinality m. This proof works over every algebraically closed field and does not use the Riemann existence theorem.

The first step is to prove that $\mathrm{Gal}(E)$ is projective (Proposition 9.4.6). Our proof applies some basic properties of the cohomology of profinite groups. Then we use that every finite split embedding problem for $\mathrm{Gal}(E)$ has m solutions (Proposition 8.6.3) to conclude that $\mathrm{Gal}(E) \cong \hat{F}_m$ (Corollary 9.4.9).

Interesting enough, the same arguments work if E is a finite extension of $K(x)$, where K is a field of cardinality m of positive characteristic p and $\mathrm{Gal}(K)$ is a pro-p group. Thus, even in this case $\mathrm{Gal}(E) \cong \hat{F}_m$ (Theorem 9.4.8).

Next we prove for each nonempty set of prime divisors of E/C that $\mathrm{Gal}(E_S/E)$ is projective (Corollary 9.5.8). In addition to the projectivity of

M. Jarden, *Algebraic Patching*, Springer Monographs in Mathematics,
DOI 10.1007/978-3-642-15128-6_9,

$\mathrm{Gal}(E)$, the main tool used in the proof is the Jacobian variety of a smooth projective model Γ of E/C. The same tool helps us to prove that $\mathrm{Gal}(E_S/E)$ is not projective if S is empty (Proposition 9.6.1). The latter group can be interpreted as the fundamental group of Γ.

Finally we consider the case where $E = C(x)$ and apply algebraic patching to solve each split embedding problems m times in E_S, first in the case that C is complete under an ultrametric absolute value and then when C is an arbitrary algebraically closed field. This proves that $\mathrm{Gal}(E_S/E) \cong \hat{F}_m$ if $\mathrm{card}(S) = m$ (Theorem 9.8.5). This is an optimal result in characteristic p. In that case, $\mathrm{Gal}(E_S/E)$ is not free if $\mathrm{card}(S) < m$ (Proposition 9.9.4).

9.1. The Fundamental Group of a Riemann Surface

Algebraic topology teaches us that the fundamental group of a sphere punctured in r points is generated by r elements $\sigma_1, \ldots, \sigma_r$ with the single relation $\sigma_1 \cdots \sigma_r = 1$. The theory of Riemann surfaces and in particular Riemann existence theorem translates this result to a theorem about finite Galois groups over $\mathbb{C}(x)$ (Proposition 9.1.1) and more generally over algebraic function fields E of one variable over $\mathbb{C}$ (Proposition 9.1.2). Using Grothendieck's specialization theorem, it is possible to generalize these results to arbitrary algebraically closed field C of characteristic 0 (Proposition 9.1.5). Taking the limit over the sets of prime divisors that we allow to ramify in the extensions prove the main result of this section: Let S be a set of prime divisors of E/C of infinite cardinality m. Denote the maximal Galois extension of E ramified at most over S by E_S. Then $\mathrm{Gal}(E_S/E) \cong \hat{F}_m$ (Proposition 9.1.9). In particular, $\mathrm{Gal}(E)$ is the free profinite group of rank equal to $\mathrm{card}(C)$ (Corollary 9.1.10).

Proposition 9.1.1 ([Voe96, Thm. 2.13]):

(a) *Let F be a finite Galois extension of $\mathbb{C}(x)$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime divisors of $\mathbb{C}(x)$ which are ramified in F. Then there exist generators $\sigma_1, \ldots, \sigma_r$ of $\mathrm{Gal}(F/\mathbb{C}(x))$ with $\sigma_1 \cdots \sigma_r = 1$ such that σ_i generates an inertia group over $\mathfrak{p}_i$, $i = 1, \ldots, r$.*

(b) *If G is a finite group generated by $\sigma_1, \ldots, \sigma_r$ with $\sigma_1 \cdots \sigma_r = 1$, then $\mathbb{C}(x)$ has a finite Galois extension F ramified at most over $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that σ_i generates an inertia group over $\mathfrak{p}_i$, $i = 1, \ldots, r$.*

No algebraic proof is known to either parts of Proposition 9.1.1. It would be highly desirable to have one.

Similar transition from topology to complex analysis and then to algebra generalizes Proposition 9.1.1 to Galois extensions of function fields of one variable over $\mathbb{C}$. Following the usual convention of group theory, we set $[x, y] = x^{-1}y^{-1}xy$ for elements x, y of a group G.

Proposition 9.1.2 ([Ser92, Section 6.2]): *Let E be a finite extension of $\mathbb{C}(x)$ of genus g and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ a set of r prime divisors of $E/\mathbb{C}$.*

(a) *Let F be a finite Galois extension of E such that* $\mathrm{Ram}(F/E) \subseteq S$. *Then F has prime divisors $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ respectively lying over $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and there are elements $\sigma_1, \dots, \sigma_r, \tau_1, \tau_1', \dots, \tau_g, \tau_g'$ generating* $\mathrm{Gal}(F/E)$ *such that σ_i generates the decomposition group $D_{\mathfrak{P}_i/\mathfrak{p}_i}$ for $i = 1, \dots, r$ and*

$$\sigma_1 \cdots \sigma_r [\tau_1, \tau_1'] \cdots [\tau_g, \tau_g'] = 1. \tag{1}$$

(b) *Let G be a finite group generated by elements $\sigma_1, \dots, \sigma_r, \tau_1, \tau_1', \dots, \tau_g, \tau_g'$ satisfying relation (1). Then E has a Galois extension F such that* $\mathrm{Gal}(F/E) \cong G$ *and F has prime divisors $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ respectively lying over $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ such that σ_i generates $D_{\mathfrak{P}_i/\mathfrak{p}_i}$, $i = 1, \dots, r$.*

On the other hand, it is not difficult to replace $\mathbb{C}$ in Propositions 9.1.1 and 9.1.2 by an arbitrary algebraically closed field C of characteristic 0. This depends on the ability to descend from an algebraically closed field to an algebraically closed subfield.

Let E be a function field of one variable over an algebraically closed field K, S a set of prime divisors of E/K, and G a finite group. We denote the set of all Galois extensions F such that $\mathrm{Gal}(F/E) \cong G$ and $\mathrm{Ram}(F/E) \subseteq S$ by $\mathcal{F}(E, S, G)$. If $E = K(x)$ is a field of rational functions, we identify the set of prime divisors of E/K with the set $K \cup \{\infty\}$ and $\mathrm{Ram}(F/E)$ with $\mathrm{Branch}(F/E)$.

Lemma 9.1.3: *Let $K \subseteq L$ be an extension of algebraically closed fields, S a finite subset of $K \cup \{\infty\}$, G a finite group, and x an indeterminate. Suppose $\mathcal{F}(L(x), S, G)$ is a finite set. Then the map $F \mapsto FL$ maps $\mathcal{F}(K(x), S, G)$ bijectively onto $\mathcal{F}(L(x), S, G)$. In particular, $\mathcal{F}(K(x), S, G)$ is a finite set.*

Proof: If S is empty, then so is $\mathcal{F}(K(x), S, G)$ and $\mathcal{F}(L(x), S, G)$ (a consequence of the Riemann-Hurwitz formula (Remark 5.8.1(f)). Thus, we may assume that S is nonempty. Applying a Möbius transformation, we may assume that $\infty \in S$.

Since L/K is a regular extension, the map $F \mapsto FL$ maps $\mathcal{F}(K(x), S, G)$ injectively into the set $\mathcal{F}(L(x), S, G)$. The proof that the map is surjective breaks up into two parts.

Part A: *Suppose $\mathcal{F}(L(x), S, G)$ consists of only one field F.* We denote the set of zeros of a polynomials $h \in L[x]$ by $\mathrm{Zero}(h)$. By [Has80, p. 64], there are polynomials $f_1, \dots, f_m \in L[X, Y]$ monic in Y and primitive elements $y_1, \dots, y_m$ of $F/L(x)$ such that $f_i(x, Y)$ is irreducible in $L(x)[Y]$, $f_i(x, y_i) = 0$, and

$$\mathrm{Branch}(F/L(x)) \smallsetminus \{\infty\} = \bigcap_{i=1}^{m} \mathrm{Zero}(\mathrm{discr}(f_i(x, Y))). \tag{2}$$

There exist $u_1, \dots, u_n \in L$ and polynomials $g_i \in K[U_1, \dots, U_n, x, Y]$ such that $f_i(x, Y) = g_i(\mathbf{u}, x, Y)$, where $\mathbf{u} = (u_1, \dots, u_n)$, $F_{\mathbf{u}} = K(\mathbf{u}, x, y_i)$ is

a Galois extension of $K(\mathbf{u}, x)$ independent of i with Galois group G. Since L is algebraically closed, we may enlarge the set $\{u_1, \dots, u_n\}$ if necessary such that it contains $\mathrm{Zero}(\mathrm{discr}(f_i(x, Y)))$ for each i. The same reason implies that the polynomials $f_i(x, Y)$ are absolutely irreducible. Since K is algebraically closed, $\mathbf{u}$ generates an absolutely irreducible variety $U = \mathrm{Spec}(K[\mathbf{u}])$ in $\mathbb{A}^n_K$ defined over K.

By Hilbert [FrJ08, Lemma 13.1.1] and Bertini-Noether [FrJ08, Prop. 9.4.3], U has a nonempty Zariski-open subset U' such that for each $\mathbf{u}' \in U'(K)$ the K-specialization $\mathbf{u} \to \mathbf{u}'$ extends to a $K(x)$-place $'$ of the field $F_{\mathbf{u}}$ with residue field $F_{\mathbf{u}'}$ that has all the properties of the preceding paragraph with $\mathbf{u}'$ replacing $\mathbf{u}$.

Hilbert's Nullstellensatz gives a $\mathbf{u}' \in U'(K)$. Thus, $F_{\mathbf{u}'}$ is a Galois extension of $K(x)$ with Galois group G, $g_i(\mathbf{u}', x, Y)$ is absolutely irreducible (as a polynomial in x, Y), $g_i(\mathbf{u}', x, y_i') = 0$, and $F_{\mathbf{u}'} = K(x, y_i')$. Moreover, $\mathrm{discr}(f_i(x, Y))' = \mathrm{discr}(g_i(\mathbf{u}, x, Y)') = \mathrm{discr}(g_i(\mathbf{u}', x, Y))$ for each i. Hence, by (2),

$$\begin{aligned}\mathrm{Zero}(\mathrm{discr}(g_i(\mathbf{u}', x, Y))) &= \mathrm{Zero}(\mathrm{discr}(f_i(x, Y))') \\ &= \mathrm{Zero}(\mathrm{discr}(f_i(x, Y)))' \subseteq S' = S.\end{aligned}$$

The second equality holds because we assumed that $\mathrm{discr}(f_i(x, Y))$ decomposes into linear factors over $K(\mathbf{u})$.

Again, by [Has80, p. 64],

$$\mathrm{Branch}(F_{\mathbf{u}'}/K(x)) \setminus \{\infty\} \subseteq \bigcap_{i=1}^{m} \mathrm{Zero}(\mathrm{discr}(g_i(\mathbf{u}', x, Y))) \subseteq S.$$

It follows from $\infty \in S$ that $\mathrm{Branch}(F_{\mathbf{u}'}/K(x)) \subseteq S$, so $F_{\mathbf{u}'} \in \mathcal{F}(K(x), S, G)$. By the second paragraph of the proof, $F_{\mathbf{u}'}L \in \mathcal{F}(L(x), S, G) = \{F\}$. Consequently, $F_{\mathbf{u}'}L = F$.

Part B: *The general case.* We list the fields of $\mathcal{F}(L(x), S, G)$ as $F_1, \dots, F_s$ and set F to be their compositum. Then F is a finite Galois extension of K, say with Galois group H. Moreover, $\mathrm{Branch}(F/L(x)) \subseteq S$ and H is the compositum of all normal subgroups N with $H/N \cong G$. If F' is another field in $\mathcal{F}(L(x), S, H)$, then F' is a compositum of Galois extensions F_i', $i = 1, \dots, s$, that belong to $\mathcal{F}(L(x), S, G)$. Each of them must be contained in F, so $F' \subseteq F$. Since both fields have the same Galois group over $L(x)$, they coincide. It follows that $\mathcal{F}(L(x), S, H) = \{F\}$.

Part A gives a field $E \in \mathcal{F}(K(x), S, H)$ with $EL = F$. By the definition of H, E is the compositum of s distinct fields $E_1, \dots, E_s$ with Galois group G. The corresponding composita $E_1L, \dots, E_sL$ are s distinct fields in $\mathcal{F}(L(x), S, G)$ contained in F. Hence $\{E_1L, \dots, E_sL\} = \{F_1, \dots, F_s\}$. Consequently, the map $E \mapsto EL$ from $\mathcal{F}(K(x), S, G)$ to $\mathcal{F}(L(x), S, G)$ is surjective. □

We generalize Lemma 9.1.3 from rational function fields to algebraic function fields.

PROPOSITION 9.1.4: *Let $K \subseteq L$ be an extension of algebraically closed fields, E a function field of one variable over K algebraically independent from L over K, S a finite subset of prime divisors of E/K, and G a finite group. We identify S with a set of prime divisors of EL/L and suppose $\mathcal{F}(EL, S, G)$ is a finite set. Then the map λ: $\mathcal{F}(E, S, G) \to \mathcal{F}(EL, S, G)$ defined by $\lambda(F) = FL$ is bijective. In particular, $\mathcal{F}(E, S, G)$ is a finite set.*

Proof: The map λ is injective because the fields $\tilde{E}$ and L are linearly disjoint over K. The proof that λ is surjective applies Lemma 9.1.3.

Let x be a separating transcendental element for the extension E/K. Then x is also a separating transcendental element for EL/L. We choose a finite subset T of $K \cup \{\infty\}$ that contains $\mathrm{Ram}(E/K(x))$ and the restriction of S to $K(x)$. Now consider $F' \in \mathcal{F}(EL, S, G)$, let $\hat{F}'$ be the Galois closure of $F'/L(x)$, and set $H = \mathrm{Gal}(\hat{F}'/L(x))$. Then $\hat{F}' \in \mathcal{F}(L(x), T, H)$. By Lemma 9.1.3, there exists $\hat{F} \in \mathcal{F}(K(x), T, H)$ with $\hat{F}L = \hat{F}'$. By linear disjointness, the map res: $\mathrm{Gal}(\hat{F}'/L(x)) \to \mathrm{Gal}(\hat{F}/K(x))$ is an isomorphism. Hence, E has a Galois extension F in $\hat{F}$ satisfying $FL = F'$ and $\mathrm{Gal}(F/E) \cong G$. Finally consider $\mathfrak{p} \in \mathrm{Ram}(F/E)$. Then the unique extension of $\mathfrak{p}$ to a prime divisor of EL/L ramifies in F', so $\mathfrak{p} \in S$. Consequently, $F \in \mathcal{F}(E, S, G)$. □

PROPOSITION 9.1.5: *Let C be an algebraically closed field of characteristic 0, E a finite extension of $C(x)$ of genus g and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ a set of r prime divisors of E/C.*

(a) *Let F be a finite Galois extension of E with $\mathrm{Ram}(F/E) \subseteq S$. Then F has prime divisors $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ respectively lying over $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and there are elements $\sigma_1, \ldots, \sigma_r$, $\tau_1, \tau_1', \ldots, \tau_g, \tau_g'$ generating $\mathrm{Gal}(F/E)$ such that σ_i generates the decomposition group $D_{\mathfrak{P}_i/\mathfrak{p}_i}$, $i = 1, \ldots, r$, and*

$$\sigma_1 \cdots \sigma_r [\tau_1, \tau_1'] \cdots [\tau_g, \tau_g'] = 1. \tag{1}$$

(b) *Let G be a finite group generated by elements $\sigma_1, \ldots, \sigma_r$, $\tau_1, \tau_1', \ldots, \tau_g, \tau_g'$ satisfying relation (1). Then E has a Galois extension F such that $\mathrm{Gal}(F/E) \cong G$ and F has prime divisors $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ respectively lying over $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that σ_i generates $D_{\mathfrak{P}_i/\mathfrak{p}_i}$, $i = 1, \ldots, r$.*

Proof: First we consider the case where $C = \mathbb{C}$. Let E_S be the maximal extension of E that is ramified at most over S. Let Γ be the free profinite group with generators $\sigma_1, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g'$ and the unique defining relation (1). Then Γ is finitely generated and, by Lemma 9.1.2, has the same finite quotients as $\mathrm{Gal}(E_S/E)$. Hence, $\Gamma \cong \mathrm{Gal}(E_S/E)$ [FrJ08, Prop. 16.10.7(b)]. It follows from [FrJ08, Lemma 16.10.2] that $\mathcal{F}(E, S, G)$ is finite. Moreover, the cardinality $n(r, g, G)$ of $\mathcal{F}(E, S, G)$ depends only on r, g, and G.

Next we consider the case where $C \subseteq \mathbb{C}$. Without loss we may assume that E is algebraically independent from $\mathbb{C}$ over C and identify S with a

set of prime divisors of $E\mathbb{C}/E$ by extending the field of constants from C to $\mathbb{C}$. By the preceding paragraph, $\mathcal{F}(E\mathbb{C}, S, G)$ is finite. Hence, by Proposition 9.1.4, the map $F \mapsto F\mathbb{C}$ maps $\mathcal{F}(E, S, G)$ bijectively onto $\mathcal{F}(E\mathbb{C}, S, G)$. Moreover, $g = \text{genus}(E/C) = \text{genus}(E\mathbb{C}/\mathbb{C})$ [FrJ08, Prop. 3.4.2(b)]. Hence, by the first paragraph, $|\mathcal{F}(E, S, G)| = n(r, g, G)$. By linear disjointness, res: $\text{Gal}(F\mathbb{C}/E\mathbb{C}) \to \text{Gal}(F/E)$ is an isomorphism for each $F \in \mathcal{F}(E, S, G)$. Since res maps the decomposition group over $E\mathbb{C}$ of a prime divisor $\mathfrak{P}$ of $F\mathbb{C}/\mathbb{C}$ isomorphically onto the decomposition group of $\mathfrak{P}|_F$ over E, (a) and (b) of our proposition follow from (a) and (b) of Proposition 9.1.2.

In the general case we find an algebraically closed subfield C_0 of C with a finite transcendence degree over $\mathbb{Q}$, a function field E_0 of one variable over C_0 algebraically independent from C over C_0 with $E_0C = E$, and a set $S_0 = \{\mathfrak{p}_{0,1}, \ldots, \mathfrak{p}_{0,r}\}$ of prime divisors of E_0/C_0 that uniquely extends to S when C_0 extends to C. Without loss we may assume that $C_0 \subseteq \mathbb{C}$. Then, $g = \text{genus}(E/C) = \text{genus}(E_0/C_0) = \text{genus}(E_0\mathbb{C}/\mathbb{C})$. By the preceding paragraph, $|\mathcal{F}(E_0, S_0, G)| = n(r, g, G)$. Moreover, (a) and (b) hold for C_0, E_0, S_0 replacing C, E, S. If $\mathcal{F}(E, S, G)$ had more than $n(r, g, G)$ fields, then we could choose C_0 such that $\mathcal{F}(E_0, S_0, G)$ would also have more that $n(r, g, G)$ fields, in contrast to the previous conclusion. Therefore, $\mathcal{F}(E, S, G)$ is finite. We may therefore apply Proposition 9.1.4 again and conclude that the map $F_0 \mapsto F_0C$ maps the set $\mathcal{F}(E_0, S_0, G)$ bijectively onto the set $\mathcal{F}(E, S, G)$. This map is compatible with restriction of Galois groups and decomposition groups. Therefore, (a) and (b) hold also for C, E, S. □

Giving a function field E of one variable over a field K and a set S of prime divisors of E/K, we denote (as in the proof of Proposition 9.1.5) the compositum of all finite Galois extensions F of E with $\text{Ram}(F/E) \subseteq S$ by E_S. Thus, E_S is a Galois extension of E. If S' is another set of prime divisors of E/K and $S \subseteq S'$, then $E_S \subseteq E_{S'}$. If S is empty, then E_S is the compositum of all unramified finite Galois extensions of E. In this case we denote E_S also by E_{ur}.

PROPOSITION 9.1.6: *Let C be an algebraically closed field of characteristic 0, E a finite extension of $C(x)$ of genus g, and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ a set of r prime divisors of E/C. Then $\text{Gal}(E_S/E)$ is the free profinite group generated by elements $\sigma_1, \ldots, \sigma_r$, $\tau_1, \tau_1', \ldots, \tau_g, \tau_g'$ satisfying the relation (1) and each σ_i is a generator of the decomposition group of a prime divisor of E_S/C lying over $\mathfrak{p}_i$.*

Proof: We extend the argument of the first paragraph of the proof of Proposition 9.1.5. For each finite Galois extension F of E in E_S we consider the finite set $\mathcal{A}(F/E)$ of all $(2r + 2g)$-tuples

$$(\mathfrak{P}_1, \ldots, \mathfrak{P}_r, \sigma_1, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g') \tag{3}$$

such that $\mathfrak{P}_i$ is a prime divisor of F/C lying over $\mathfrak{p}_i$, σ_i is a generator of the decomposition group $D_{\mathfrak{P}_i/\mathfrak{p}_i}$, $i = 1, \ldots, r$, and $\sigma_1, \ldots, \sigma_r, \tau_1, \tau_1', \ldots, \tau_g, \tau_g'$

are generators of $\mathrm{Gal}(F/E)$ satisfying relation (1). If F' is a finite Galois extension of E in E_S that contains F and $\mathfrak{P}'_i$ is a prime divisor of F'/C lying over $\mathfrak{p}_i$, then $\mathfrak{P}_i = \mathfrak{P}'_i|_F$ is a prime divisor of F/C lying over $\mathfrak{p}_i$ and the epimorphism res: $\mathrm{Gal}(F'/E) \to \mathrm{Gal}(F/E)$ maps $D_{\mathfrak{P}'_i/\mathfrak{p}_i}$ onto $D_{\mathfrak{P}_i/\mathfrak{p}_i}$ [Ser79, Chap. 1, Prop. 22(b)]. Hence res induces a map of $\mathcal{A}(F'/E)$ into $\mathcal{A}(F/E)$. By Proposition 9.1.5(a), each $\mathcal{A}(F/E)$ is nonempty. Therefore, the inverse limit of the sets $\mathcal{A}(F/E)$ is nonempty [FrJ08, Lemma 1.1.3]. Each element of that inverse limit is an $(2r+2g)$-tuple (3) satisfying relation (1) such that $\mathfrak{P}_i$ is a prime divisor of E_S/C lying over $\mathfrak{p}_i$ and σ_i generates $D_{\mathfrak{P}_i/\mathfrak{p}_i}$.

Now, let Γ be the free profinite group on the generators $\sigma_1, \ldots, \sigma_r$, $\tau_1, \tau'_1, \ldots, \tau_g, \tau'_g$ satisfying relation (1). By Proposition 9.1.5, $\mathrm{Gal}(E_S/E)$ and Γ have the same finite quotients. Consequently, by [FrJ08, Prop. 16.10.7], $\mathrm{Gal}(E_S/E) \cong \Gamma$. □

Corollary 9.1.7: *In the notation of Proposition 9.1.6,*
(a) *If $g = 0$ and $r \geq 2$ or $g \geq 1$ and $r \geq 1$, then $\langle \sigma_i \rangle \cong \hat{\mathbb{Z}}$, $i = 1, \ldots, r$.*
(b) *If $r \geq 1$, then $\mathrm{Gal}(E_S/E) \cong \hat{F}_{r-1+2g}$.*

Proof of (a): In order to prove that $\langle \sigma_i \rangle \cong \hat{\mathbb{Z}}$, it suffices to prove that for each positive integer n the cyclic group C_n of order n is a quotient of $\langle \sigma_i \rangle$.

Let y be a generator of C_n. If $r \geq 2$, we choose $j \neq i$, $1 \leq j \leq r$. Then we map σ_i onto y, σ_j onto y^{-1} and all other generators to 1 to get an epimorphism $\mathrm{Gal}(E_S/E) \to C_n$ that maps $\langle \sigma_i \rangle$ onto C_n.

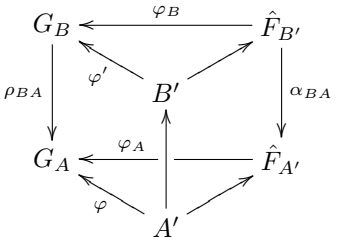
It remains to consider the case where $r = 1$ and $g \geq 1$. Let D_{2n} be the dihedral group of order $2n$ generated by elements x, y with the defining relations $x^{2n} = 1$, $y^2 = 1$, and $y^{-1}xy = x^{-1}$. Then $[x, y] = x^{-1}y^{-1}xy = x^{-2}$ has order n. Hence, the map $\sigma_1 \mapsto [x, y]^{-1}$, $\tau_1 \mapsto x$, $\tau'_1 \mapsto y$, $\tau_j \mapsto 1$, and $\tau'_j \mapsto 1$ for $j \geq 2$ extends to an epimorphism of $\mathrm{Gal}(E_S/E)$ onto D_{2n} mapping $\langle \sigma_1 \rangle$ onto the cyclic group of order n generated by $[x, y]$.

Proof of (b): By Proposition 9.1.6, $\mathrm{Gal}(E_S/E)$ is the free profinite group generated by the elements $\sigma_2, \ldots, \sigma_r$, $\tau_1, \tau'_1, \ldots, \tau_g, \tau'_g$. The extra generator σ_1 can be expressed in terms of the other generators via (1). □

Remark 9.1.8: Inverse limit of free profinite groups. One way to construct a free profinite group of arbitrary rank is to start from disjoint sets S, T such that T is finite. For each subset A of S we set $A' = A \cup T$ and consider the free profinite group $\hat{F}_{A'}$ with basis A'. If A, B are finite subsets of S and $A \subseteq B$, then the map $B' \to A'$ that maps each $a \in A'$ onto itself and each $b \in B \smallsetminus A$ onto 1 uniquely extends to an epimorphism $\alpha_{BA}\colon \hat{F}_{B'} \to \hat{F}_{A'}$. The inverse limit F of the groups $\hat{F}_{A'}$ and the maps α_{BA} is isomorphic to the free profinite group $\hat{F}_{S'}$ with basis $S' = S \cup T$. Indeed, for each A let α_{SA} be the limit of all maps α_{BA}, where B ranges over all finite subsets B of S that contain A. For each open normal subgroup N of F there exists a finite subset A of S such that $\mathrm{Ker}(\alpha_{SA}) \leq N$, so $S' \smallsetminus A' \subseteq N$. Thus, S' converges to 1 in the sense of [FrJ08, Section 17.1]. Moreover, if φ_0 is a map of S' into a finite group H that maps the complement of some A' onto 1, then φ_0 decomposes

through $\alpha_{SA}\colon S' \to A'$. Since A' is a basis of $\hat{F}_{A'}$, we may extend φ_0 to a continuous homomorphism $\varphi\colon F \to H$.

Using compactness, it is possible to relax the above rigid condition on the maps α_{BA}. Consider a projective limit $G = \varprojlim G_A$ of profinite groups, where A ranges over all finite subsets of S. Assume for each A the group G_A is isomorphic to $\hat{F}_{A'}$, and if $B \supseteq A$, then the associated homomorphism $\rho_{BA}\colon G_B \to G_A$ is surjective. Consider the compact space $(G_A)^{A'}$ (in the product topology) of all functions from A' into G_A. Let Φ_A be a closed subset of $(G_A)^{A'}$. Suppose each $\varphi \in \Phi_A$ satisfies $\langle \varphi(a) \mid a \in A' \rangle = G_A$. Suppose also that if $B \supseteq A$ and $\varphi' \in \Phi_B$, then $\varphi = \rho_{BA} \circ \varphi'|_{A'} \in \Phi_A$ and $\rho_{BA}(\varphi'(b)) = 1$ for each $b \in B \smallsetminus A$. Then φ (resp. φ') uniquely extends to an epimorphism $\varphi_A\colon \hat{F}_{A'} \to G_A$ (resp $\varphi_B\colon \hat{F}_{B'} \to G_B$) such that $\rho_{BA} \circ \varphi_B = \varphi_A \circ \alpha_{BA}$. By [FrJ08, Lemma 17.4.11], φ_A (resp. φ_B) is an isomorphism.



It follows that $\Phi = \varprojlim \Phi_A$ is nonempty [FrJ08, Lemma 1.1.3]. Each $\varphi \in \Phi$ gives an isomorphism of $\hat{F}_{S'}$ onto G. In particular, $\varphi(S')$ is a basis of G and for each A we have $\rho_{SA} \circ \varphi|_A \in \Phi_A$. □

PROPOSITION 9.1.9: *Let C be an algebraically closed field of characteristic 0, E a function field of one variable over C, S an infinite set of cardinality m of prime divisors of E/C. Then* $\mathrm{Gal}(E_S/E) \cong \hat{F}_m$.

Proof: We choose a prime divisor $\mathfrak{p}_1 \in S$ and denote the collection of all finite nonempty subsets of $S \smallsetminus \{\mathfrak{p}_1\}$ by $\mathcal{A}$. We also choose a set T disjoint from S of $2g$ elements, where $g = \mathrm{genus}(E/C)$. For each $A \in \mathcal{A}$ let $G_A = \mathrm{Gal}(E_{\{\mathfrak{p}_1\}\cup A}/E)$ and $A' = A \cup T$. By Corollary 9.1.7(b), $G_A \cong \hat{F}_{A'}$. Let Φ_A be the set of all functions $\varphi\colon A' \to G_A$ such that $G_A = \langle \varphi(a) \mid a \in A' \rangle$ and for each $\mathfrak{p} \in A$, $\varphi(\mathfrak{p})$ generates a decomposition group of a prime divisor of $E_{\{\mathfrak{p}_1\}\cup A}/C$ over $\mathfrak{p}$.

CLAIM: *Φ_A is closed in $G_A^{A'}$.* Indeed, suppose a function $\psi\colon A' \to G_A$ belongs to the closure of Φ_A. Then for each finite Galois extension F of E in $E_{\{\mathfrak{p}_1\}\cup A}$ there exists $\varphi \in \Phi_A$ such that $\psi(a)|_F = \varphi(a)|_F$ for each $a \in A'$. It follows that $\mathrm{Gal}(F/E) = \langle \psi(a)|_F \mid a \in A' \rangle$ and for each $\mathfrak{p} \in A$, $\psi(\mathfrak{p})|_F$ generates a decomposition group of a prime divisor of F/C lying over $\mathfrak{p}$. Taking the limit over all possible F, we find that $\psi \in \Phi_A$, as claimed.

Next note that if $B \in \mathcal{A}$ and $A \subseteq B$, then $E_{\{\mathfrak{p}_1\}\cup A} \subseteq E_{\{\mathfrak{p}_1\}\cup B}$. Let $\rho_{BA}\colon G_B \to G_A$ be the restriction map. Consider $\varphi_B \in \Phi_B$ and $\mathfrak{p} \in B \setminus A$. Then $\varphi_B(\mathfrak{p})$ generates the decomposition group of some prime divisor of $E_{\{\mathfrak{p}_1\}\cup B}/C$ lying over $\mathfrak{p}$. Therefore, $\varphi_B(\mathfrak{p})|_{E_{\{\mathfrak{p}_1\}\cup A}}$ generates the decomposition group of a prime divisor $\mathfrak{P}$ of $E_{\{\mathfrak{p}_1\}\cup A}/C$ lying over $\mathfrak{p}$. Since C is algebraically closed, $D_{\mathfrak{P}/\mathfrak{p}} = I_{\mathfrak{P}/\mathfrak{p}}$. However, $\mathfrak{p}$ is unramified in $E_{\{\mathfrak{p}_1\}\cup A}$, because $\mathfrak{p} \notin A$. Hence, $I_{\mathfrak{P}/\mathfrak{p}} = 1$, so $\rho_{BA}(\varphi_B(\mathfrak{p})) = \varphi_B(\mathfrak{p})|_{E_{\{\mathfrak{p}_1\}\cup A}} = 1$.

Finally observe that ρ_{BA} maps each set of generators of G_B onto a set of generators of G_A. Therefore, $\rho_{BA} \circ \varphi_B|_A \in \Phi_A$.

Consequently, by Remark 9.1.8, $\mathrm{Gal}(E_S/E) \cong \hat{F}_m$. □

If we take S in Proposition 9.1.9 to be the set of all prime divisors of E/C, then $E_S = \tilde{E}$. In this case the group $\mathrm{Gal}(E_S/E)$ becomes the absolute Galois group of E and $\mathrm{card}(S) = \mathrm{card}(C)$.

Corollary 9.1.10 ([Dou64, Théorème 2]): *Let C be an algebraically closed field of characteristic 0 and of cardinality m and E a function field of one variable over C. Then $\mathrm{Gal}(E) \cong \hat{F}_m$.*

Since each free profinite group is projective [FrJ08, Cor. 22.4.5], the combination of Corollary 9.1.7(b) and Proposition 9.1.9 gives the following result:

Corollary 9.1.11: *Let C be an algebraically closed field of characteristic 0 and S a nonempty set of prime divisors of E/C. Then $\mathrm{Gal}(E_S/E)$ is projective. In particular, $\mathrm{Gal}(E)$ is projective.*

Remark 9.1.12: Freeness and projectivity. The projectivity of $\mathrm{Gal}(E_S/E)$ obtained in Corollary 9.1.11 is a much weaker property than the freeness of the group. Yet we generalize it in Theorem 9.5.7 for an arbitrary characteristic by algebraic means and deduce the freeness of $\mathrm{Gal}(E_S/E)$ for infinite sets S (Theorem 9.8.5). If however, $\mathrm{char}(C) > 0$ and S is finite, then $\mathrm{Gal}(E_S/E)$ is not free (Proposition 9.9.4). □

9.2 Fundamental Groups in Positive Characteristic

We continue our survey of the theory of fundamental groups of curves over an algebraically closed fields and move to the case where the characteristic is a prime number p. The results obtained in characteristic 0 can be carried over as long as we "stay away" from p, but are completely different in the general case.

Proposition 9.2.1 ([SGA1, Exposé XIII, Cor. 2.12]): *Let C be an algebraically closed field of characteristic p, E a function field of one variable over C of genus g, and $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ a finite set of prime divisors of E/C.*

(a) *Let $E_{S,\mathrm{tr}}$ be the compositum of all finite Galois extensions F of E such that $\mathrm{Ram}(F/E) \subseteq S$ and each $\mathfrak{p} \in \mathrm{Ram}(F/E)$ is tamely ramified. Then*

$\mathrm{Gal}(E_{S,\mathrm{tr}}/E)$ *is generated by elements* $\sigma_1,\dots,\sigma_r,\ \tau_1,\tau_1',\dots,\tau_g,\tau_g'$ *satisfying the relation*

$$\sigma_1\cdots\sigma_r[\tau_1,\tau_1']\cdots[\tau_g,\tau_g']=1. \tag{1}$$

(b) *Let* $E_{S,p'}$ *be the compositum of all finite Galois extensions* F *of* E *of degree not divisible by* p *such that* $\mathrm{Ram}(F/E)\subseteq S$. *Then* $\mathrm{Gal}(E_{S,p'}/E)$ *is the free group generated by elements* $\sigma_1,\dots,\sigma_r,\ \tau_1,\tau_1',\dots,\tau_g,\tau_g'$ *with the defining relation (1) in the category of profinite groups with order not divisible by* p.

(c) *In both (a) and (b),* σ_i *can be chosen to generate a decomposition group of a prime divisor lying over* $\mathfrak{p}_i$, $i=1,\dots,r$.

Sketch of proof: One chooses a smooth projective model Γ for E/C. Then one finds a complete discrete valuation ring R, with residue field C, and an algebraically closed quotient field K of characteristic 0 and a projective connected smooth curve Δ over $S=\mathrm{Spec}(R)$ whose special fiber is $\Delta\times_S \mathrm{Spec}(C)\cong\Gamma$. Let Δ_K be the generic fiber of Δ. Then $\mathrm{genus}(\Delta_K)=g$. Let $\mathbf{p}_1,\dots,\mathbf{p}_r$ be the points of $\Gamma(C)$ corresponding to $\mathfrak{p}_1,\dots,\mathfrak{p}_r$. By Hensel's lemma, the points $\mathbf{p}_1,\dots,\mathbf{p}_r$ lift to points $\mathbf{q}_1,\dots,\mathbf{q}_r$ of $\Delta_K(R)$. Let F be the function field of Δ_K over K and $\mathfrak{q}_1,\dots,\mathfrak{q}_r$ the prime divisors corresponding to the points $\mathbf{q}_1,\dots,\mathbf{q}_r$. Let $T=\{\mathbf{q}_1,\dots,\mathbf{q}_r\}$. Using knowledge of the behavior of the tamely ramified covers of the curve, one proves that there is a surjective map $\mathrm{Gal}(F_T/F)\to\mathrm{Gal}(E_{S,\mathrm{tr}}/E)$ defining an isomorphism $\mathrm{Gal}(F_{T,p'}/F)\to\mathrm{Gal}(E_{S,p'}/E)$ compatible with decomposition groups. Using Proposition 9.1.6, this gives (a), (b), and (c). □

Remark 9.2.2: Abhyankar's conjecture. Let C be an algebraically closed field of positive characteristic p, E a function field of one variable of genus g, S a finite nonempty set of r prime divisors of E/C. Proposition 9.2.1 gives us information only on the maximal tamely ramified quotient and the maximal p'-quotient of $\mathrm{Gal}(E_S/E)$. The structure of $\mathrm{Gal}(E_S/E)$ is unknown, even in the case where $E=C(x)$ and S consists of one prime divisor. That is, we do not know the structure of the fundamental group of the affine line in characteristic p. What we do know is the set of finite quotients of $\mathrm{Gal}(E_S/E)$.

Consider a finite Galois extension F of E in E_S. Let $G=\mathrm{Gal}(F/E)$ and denote the normal subgroup of G generated by all p-Sylow subgroups of G by $G(p)$. Let F_0 be the fixed field of $G(p)$ in F. Then F_0 is a finite Galois extension of E in E_S of order not divisible by p. It follows from Proposition 9.2.1(b) that $G/G(p)\cong\mathrm{Gal}(F_0/E)$ is generated by elements $\sigma_1,\dots,\sigma_r,\tau_1,\tau_1',\dots,\tau_g,\tau_g'$ satisfying Relation (1). In particular, if E is a field of rational functions over C and $r=1$, then $g=0$, so $\sigma_1=1$ and $F_0=E$. This follows also from the Riemann-Hurwitz formula for tamely ramified extensions [FrJ05, Remark 3.6.2(d)]. Therefore, $G=G(p)$ is generated by its p-Sylow subgroups. A finite group having that property is said to be a **quasi-p group**.

This observation led Shreeram Abhyankar in [Abh57] to conjecture that each finite group G such that $G/G(p)$ is generated by $r+2g$ elements satisfying Relation (1) with $r \geq 1$ appears as a quotient of $\mathrm{Gal}(E_S/E)$. In the case $G(p)=1$, the conjecture follows from Proposition 9.2.1(b). Jean-Pierre Serre proved Abhyankar's conjecture for solvable groups G [Ser90] using class field theory. Raynaud proved Abhyankar's conjecture for an arbitrary quasi-p group over the affine line [Ray94], and David Harbater settled the general Abhyankar's conjecture [Hrb94a] by reducing it to the case of the affine line proved by Raynaud. Finally, [Pop95] proves that every finite split embedding problem for $\mathrm{Gal}(E_S/E)$ whose kernel is a finite quotient of the fundamental group of the affine line is solvable. If S is nonempty, then $\mathrm{Gal}(E_S/E)$ is a projective group (Corollary 9.5.8). Using Proposition 9.2.1 and Raynaud's result this gives an alternative proof of Abhyankar's conjecture.

Indeed, let G be a finite group such that $G/G(p)$ is generated by $r+2g$ elements satisfying Relation (1) with $r \geq 1$. By Proposition 9.2.1(b), there is an epimorphism $\varphi\colon \mathrm{Gal}(E_S/E) \to G/G(p)$. Let $\alpha\colon G \to G/G(p)$ be the quotient map. Since $\mathrm{Gal}(E_S/E)$ is projective, there is a homomorphism $\gamma\colon \mathrm{Gal}(E_S/E) \to G$ such that $\alpha\circ\gamma=\varphi$. Denote the fixed field of $\mathrm{Ker}(\gamma)$ by $\hat{E}$. Then there are epimorphisms $\hat{\varphi}\colon \mathrm{Gal}(E_S/E) \to \mathrm{Gal}(\hat{E}/E)$ and $\bar{\varphi}\colon \mathrm{Gal}(\hat{E}/E) \to G/G(p)$ such that $\varphi=\bar{\varphi}\circ\hat{\varphi}$. Moreover, there is an embedding $\bar{\gamma}\colon \mathrm{Gal}(\hat{E}/E) \to G$ such that $\gamma=\bar{\gamma}\circ\hat{\varphi}$ and $\alpha\circ\bar{\gamma}=\bar{\varphi}$. Let $\hat{G}=G\times_{G/G(p)}\mathrm{Gal}(\hat{E}/E)$ be the corresponding fiber product and let $\hat{\alpha}\colon \hat{G} \to \mathrm{Gal}(\hat{E}/E)$ be the projection on the second factor. Then ($\hat{\varphi}\colon \mathrm{Gal}(E_S/E) \to \mathrm{Gal}(\hat{E}/E)$, $\hat{\alpha}\colon \hat{G} \to \mathrm{Gal}(\hat{E}/E)$) is a finite split embedding problem for $\mathrm{Gal}(E_S/E)$ whose kernel is isomorphic to $G(p)$, so it is a finite quotient of the fundamental group of the affine line (by Raynaud). It follows from Pop's theorem that the embedding problem is solvable. In particular, G is a quotient of $\mathrm{Gal}(E_S/E)$, as claimed. □

Remark 9.2.3: Half Riemann existence theorem. One may refer to Proposition 9.2.1 as the **tame Riemann existence theorem**. The best known approximation to Proposition 9.1.1 is the so called **Half Riemann existence theorem**, due to Pop [Pop94]. It applies to an arbitrary Henselian field (K,v). For a positive integer r let $S=\{a_1,b_1,\ldots,a_r,b_r\}$ be a subset of K_s such that $a_i \neq b_i$, $v(a_i-b_i) > v(a_i-b_j)$ for all $i \neq j$, and both $\{a_1,\ldots,a_r\}$ and $\{b_1,\ldots,b_r\}$ are invariant under $\mathrm{Gal}(K)$. Let Π be $\hat{F}_r$ if $\mathrm{char}(K)=\mathrm{char}(\bar{K}_v)$ and the free product of r copies of $\hat{\mathbb{Z}}/\mathbb{Z}_p$ if $\mathrm{char}(K)=0$ and $\mathrm{char}(\bar{K}_v)=p>0$. Then the field $K(x)$ of rational functions in x over K has a Galois extension N with $\mathrm{Branch}(N/K(x))=S$ such that $\mathrm{Gal}(N/K_s(x)) \cong \Pi$ and $\mathrm{Gal}(N/K(x)) = \mathrm{Gal}(K) \ltimes \mathrm{Gal}(N/K_s(x))$. Moreover, one may choose generators $\sigma_1,\ldots,\sigma_r$ for Π such that σ_i generates an inertia group of both a_i and b_i, $i=1,\ldots,r$. See also [Hrb03, Thm. 4.3.3 and Remark 4.4.4(c)]. □

9.3 Cohomology of Groups

We survey in this section the basic notions and results of the cohomology of profinite groups needed in this book. Our basic references are [Rib70] and [Ser79]. In this Chapter we apply a small part of our survey to prove that $\mathrm{Gal}(E)$ is projective for each extension E of transcendence degree 1 over an algebraically closed field (Proposition 9.4.6). In Chapter 11 we build on our survey to prove local-global theorems for Brauer groups. This leads to fields of transcendence degree 1 over PAC fields with projective absolute Galois groups.

9.3.1 G-MODULES.

Let G be a profinite group and A a discrete Abelian (additive) group. We say that A is a **G-module** if G acts continuously on A from the left, that is there is a continuous map $G \times A \to A$ mapping a pair $(\sigma, a) \in G \times A$ onto the element σa of A such that

(1a) $(\sigma\tau a) = \sigma(\tau a)$,

(1b) $\sigma(a + b) = \sigma a + \sigma b$, and

(1c) $1a = a$

for all $a, b \in A$ and $\sigma, \tau \in G$. If $\sigma a = a$ for all $\sigma \in G$ and $a \in A$ we say that A is a **trivial G-module**. Our basic examples occur when $G = \mathrm{Gal}(L/K)$ is a Galois group and A is either the additive group L^+ or the multiplicative group $L^\times$ of L (where in the latter case we have to switch to a multiplicative module). We may also take A to be the group of all roots of unity belonging to L or the group $J(L)$, where J is an Abelian variety defined over K.

For each closed subgroup U of G we write A^U for the fixed module of A under U. For each $a \in A$ the equality $1a = a$ implies that there exists an open subgroup U of G such that $\sigma a = a$ for each $\sigma \in U$, i.e. $a \in A^U$. Thus

$$A = \bigcup A^U, \tag{2}$$

where U ranges on all open subgroups (or even open normal subgroups) U of G.

A map $\varphi\colon A \to B$ between G-modules is a **G-homomorphism** if φ is a group homomorphism that satisfies $\varphi(\sigma a) = \sigma\varphi(a)$ for all $\sigma \in G$ and $a \in A$.

9.3.2 DEFINITION OF THE COHOMOLOGY GROUPS.

Given a G-module A, we consider for each $q \geq 0$ the group $C^q(G, A)$ of all continuous maps $f\colon G^q \to A$ (called **non-homogeneous q-cochains**) and the homomorphisms $\partial_{q+1}\colon C^q(G, A) \to C^{q+1}(G, A)$ (called the **non-homogeneous coboundary operators**) defined by $(\partial_1 f)(\sigma) = \sigma f(1) - f(1)$ and for $q \geq 1$ by

$$\begin{aligned}(3)(\partial_{q+1}f)(\sigma_1, \ldots, \sigma_{q+1}) &= \sigma_1 f(\sigma_2, \ldots, \sigma_{q+1}) \\ &\quad + \sum_{i=1}^{q} (-1)^i f(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_{q+1}) \\ &\quad + (-1)^{q+1} f(\sigma_1, \ldots, \sigma_q).\end{aligned}$$

One proves that

$$\partial_{q+1} \circ \partial_q = 0, \tag{4}$$

so that

$$0 \to C^0(G,A) \xrightarrow{\partial_1} C^1(G,A) \xrightarrow{\partial_2} C^2(G,A) \xrightarrow{\partial_3} \dots$$

is a **complex**. Each element of the group $Z^q(G,A) = \mathrm{Ker}(\partial_{q+1})$ is a **q-cocycle** whereas each element of the group $B^q(G,A) = \mathrm{Im}(\partial_q)$ is a **q-coboundary**. By (4), $B^q(G,A) \le Z^q(G,A)$. This gives rise to the **q-th cohomology group with coefficients in** A:

$$H^q(G,A) = Z^q(G,A)/B^q(G,A).$$

Note that $C^0(G,A)$ is the set of all functions $f\colon \{1\} \to A$. Taking $\partial_0 = 0$, we get $B^0(G,A) = 0$ and $H^0(G,A) = Z^0(G,A) = A^G$. A 1-coboundary is a map $f_a\colon G \to A$ defined by $f_a(\sigma) = \sigma a - a$ for a fixed $a \in A$. A 1-cocycle is a **crossed homomorphism**, namely a map $f\colon G \to A$ satisfying $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$. Thus, an element of $H^1(G,A)$ is an equivalence class of crossed homomorphisms modulo coboundaries. If A is a trivial G-module, then each 1-coboundary is 0 and each crossed homomorphism is a homomorphism $G \to A$. Thus, in this case $H^1(G,A) = \mathrm{Hom}(G,A)$.

9.3.3 Functoriality of the Cohomology Groups.

The cohomology groups are functorial in both variables. Each G-homomorphism $\alpha\colon A \to B$ of G-modules induces a homomorphism $\alpha\colon C^q(G,A) \to C^q(G,B)$ of the corresponding cochain groups that commutes with the coboundary operator: $(\alpha f)(\sigma_1,\dots,\sigma_q) = \alpha(f(\sigma_1,\dots,\sigma_q))$. It follows that $\alpha(Z^q(G,A)) \le Z^q(G,B)$ and $\alpha(B^q(G,A)) \le B^q(G,B)$. Hence, α yields a homomorphism $\alpha\colon H^q(G,A) \to H^q(G,B)$. Each of the assignments $A \rightsquigarrow C^q(G,A)$, $A \rightsquigarrow Z^q(G,A)$, $A \rightsquigarrow B^q(G,A)$, and $A \rightsquigarrow H^q(G,A)$ is a covariant functor from the category of G-modules to the category of Abelian groups. This means that the composition $\beta \circ \alpha$ of homomorphisms of G-modules is assigned to the composition $\beta \circ \alpha$ of Abelian groups and the identity of G-modules is assigned to the corresponding identity of Abelian groups.

9.3.4 Short and Long Exact Sequences.

The most important feature of group cohomology is the theorem about the exact sequences: To each short exact sequence

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

of G-modules there corresponds a long exact sequence

$$\begin{aligned} 0 \to A^G &\xrightarrow{\alpha} B^G \xrightarrow{\beta} C^G \\ &\xrightarrow{\delta} H^1(G,A) \xrightarrow{\alpha} H^1(G,B) \xrightarrow{\beta} H^1(G,C) \\ &\xrightarrow{\delta} H^2(G,A) \xrightarrow{\alpha} H^2(G,B) \xrightarrow{\beta} H^2(G,C) \xrightarrow{\delta} \cdots, \end{aligned}$$

where the **connecting homomorphisms** δ are functorial [Rib70, p. 115, Prop. 4.4].

9.3.5 Compatible Homomorphisms.

Generalizing the functoriality of the cohomology to both variables, we consider a G-module A and an H-module B. A pair (φ, β) consisting of a homomorphism of profinite groups $\varphi\colon G \to H$ and a homomorphism $\beta\colon B \to A$ of H and G modules, respectively, is said to be **compatible** if $\sigma(\beta(b)) = \beta(\varphi(\sigma)b)$ for all $\sigma \in G$ and $b \in B$. In this case they define for each $q \geq 0$ a homomorphism $(\varphi, \beta)\colon C^q(H, B) \to C^q(G, A)$ by the formula: $((\varphi, \beta)g)(\sigma_1, \ldots, \sigma_q) = \beta(g(\varphi(\sigma_1), \ldots, \varphi(\sigma_q)))$ for $g \in C^q(H, B)$ and $\sigma_1, \ldots, \sigma_q \in G$. As in Subsection 9.3.3, (φ, β) commutes with the coboundary homomorphisms, so it induces natural homomorphisms

$$(\varphi, \beta)\colon H^q(H, B) \to H^q(G, A).$$

The maps (φ, β) behave functorially in the following sense. If I is a profinite group, C is an I-module, and $\psi\colon H \to I$ and $\gamma\colon C \to B$ are compatible homomorphisms, then $(\psi \circ \varphi, \beta \circ \gamma)$ is a pair of compatible homomorphisms from G to I and C to A and the following triangle is commutative:

(5)
$$\begin{array}{ccc} H^q(H, B) & \xleftarrow{\quad(\psi,\gamma)\quad} & H^q(I, C) \\ & {\scriptstyle(\varphi,\beta)}\searrow \quad \swarrow{\scriptstyle(\psi\circ\varphi,\beta\circ\gamma)} & \\ & H^q(G, A) & \end{array}$$

9.3.6 Inflation and Restriction.

An important example occurs when N is a closed normal subgroup of G. Let A be a G-module and denote the image of an element $\sigma \in G$ in G/N under the quotient map by $\bar{\sigma}$. Then G/N acts on A^N by $\bar{\sigma}a = \sigma a$ and this action is compatible with the inclusion $A^N \to A$. Thus, it induces for each $q \geq 0$ the **inflation homomorphism** $\inf\colon H^q(G/N, A^N) \to H^q(G, A)$. Similarly, the restriction of the action of G on A to N is compatible with the identity map $A \to A$, so it gives rise to the **restriction homomorphisms** $\mathrm{res}\colon H^q(G, A) \to H^q(N, A)$.

Lemma 9.3.7: *Let G be a profinite group, N a closed normal subgroup, A a G-module, and $q \geq 1$. Suppose $H^i(G, A) = 0$ for $1 \leq i \leq q-1$. Then the sequence*

(6)
$$0 \to H^q(G/N, A^N) \xrightarrow{\inf} H^q(G, A) \xrightarrow{\mathrm{res}} H^q(N, A)$$

is exact. In particular, if $H^1(G, A) = 0$, then the following sequence is exact:

(7)
$$0 \to H^2(G/N, A^N) \xrightarrow{\inf} H^2(G, A) \xrightarrow{\mathrm{res}} H^2(N, A).$$

The proof of the lemma for $q = 1$ is carried out by direct verification on cocycles. Then one applies "dimension shifting" to continue the proof for arbitrary q by induction. This is done in [CaF67, p. 100, Prop. 4] for abstract groups and in [Koc70, Sec. 3.7] for profinite groups. Note that the latter source adds two more groups to the sequence (6). The same five terms sequence is also proved to be exact in [Rib70, p. 177, Cor. 5.4] by application of spectral sequences.

9.3.8 Corestriction.

We consider an open subgroup U of a profinite group G and choose a set S of representatives for the left cosets of G modulo U, thus $G = \bigcup_{\sigma\in S} \sigma U$. Then we define for each G-module A a group homomorphism $N_{G/U}\colon A^U \to A^G$ by $N_{G/U}(a) = \sum_{\sigma\in S} \sigma a$. It can be uniquely extended to a natural transformation $\mathrm{cor}_G^U\colon H^q(U, A) \to H^q(G, A)$, called the **corestriction** [Rib70, p. 136]. Composing the corestriction with the restriction gives multiplication with the index of U in G:

$$\mathrm{cor}_G^U \circ \mathrm{res}_U^G = (G : U)\mathrm{id}. \tag{8}$$

In particular, if G is finite and we apply (8) to an element $x \in H^q(G, A)$ with $q \geq 1$, we find that $\mathrm{res}_1^G(x) \in H^q(1, A) = 0$, hence $|G|x = 0$. In other words, $H^q(G, A)$ is a torsion group and the order of each element of $H^q(G, A)$ divides the order of G.

9.3.9 Direct Systems.

In order to generalize the latter result to profinite groups, we have to be able to take direct limits of cohomology groups. To this end we consider a **direct system** $(A_i, \alpha_{ij})_{i,j\in I}$ of Abelian groups. Thus, I is a partially ordered nonempty set such that for all $i, j \in I$ there exists $k \in I$ with $i, j \leq k$. For all $i, j \in I$ with $i \leq j$ the system has a homomorphism $\alpha_{ij}\colon A_i \to A_j$ such that $\alpha_{jk} \circ \alpha_{ij} = \alpha_{ik}$ if $i \leq j \leq k$. Moreover, $\alpha_{ii} = \mathrm{id}_{A_i}$ for $i \in I$. Let R be the subgroup of $\bigoplus_{i\in I} A_i$ generated by all elements $a_i - a_j$ with $i, j \in I$, $a_i \in A_i$, $a_j \in A_j$ for which there exists $k \geq i, j$ such that $\alpha_{ik}(a_i) = \alpha_{jk}(a_j)$. The factor group $A = \varinjlim A_i = (\bigoplus_{i\in I} A_i)/R$ is called the **direct limit** of the system $(A_i, \alpha_{ij})_{i,j\in I}$. Viewing each A_i as a subgroup of $\bigoplus_{i\in I} A_i$, we may consider the homomorphism $\alpha_i\colon A_i \to \varinjlim A_i$ given by $\alpha_i(a_i) = a_i + R$. The homomorphisms α_i satisfy the compatibility condition $\alpha_j \circ \alpha_{ij} = \alpha_i$ if $i \leq j$. Moreover, given an Abelian group B and homomorphisms $\beta_i\colon A_i \to B$ such that $\beta_j \circ \alpha_{ij} = \beta_i$ whenever $i \leq j$, there is a unique homomorphism $\beta\colon A \to B$ such that $\beta \circ \alpha_i = \beta_i$ for all $i \in I$.

Each $a \in A$ can be written as $a = \sum_{i\in I_0} a_i + R$, where I_0 is a finite subset of I and $a_i \in A_i$ for each $i \in I_0$. We choose $j \in I$ with $i \leq j$ for all $i \in I_0$ and let $a_j = \sum_{i\in I_0} \alpha_{ij}(a_i)$. Then $a_j \in A_j$ and $a = a_j + R = \alpha_j(a_j)$. Consequently, $A = \bigcup_{i\in I} \alpha_i(A_i)$.

If $a_i \in A_i$ and $\alpha_i(a_i) = 0$, then a_i is a sum of elements $a_{ij} - a_{ik}$ in $\oplus_{r\in I} A_r$ with $a_{ij} \in A_j$, $a_{ik} \in A_k$, and there exists $l \geq j, k$ with $\alpha_{jl}(a_{ij}) = \alpha_{kl}(a_{ik})$.

Since in a direct sum equality holds if and only if it holds in each coordinate, we may assume that $a_{ij}, a_{ik} \in A_i$ for all j, k. We choose an $m \in I$ greater or equal to i and all of the l's occurring in the above conditions. Then $\alpha_{im}(a_i) = 0$. Of course, if the latter condition holds, then $\alpha_i(a_i) = 0$.

9.3.10 Cohomology Groups as Directed Limes.

Now we consider an inverse system $(G_i, \pi_{ji})_{i,j\in I}$ of profinite groups and a directed system $(A_i, \alpha_{ij})_{i,j\in I}$ of Abelian groups such that A_i is a G_i-module and for all $i \le j$ the pair (π_{ji}, α_{ij}) is compatible. Let $G = \varprojlim G_i$ and $A = \varinjlim A_i$. For each $i \in I$ let $\pi_i\colon G \to G_i$ be the projection on the ith component and $\alpha_i\colon A_i \to A$ the map defined by the embedding of A_i in $\bigoplus_{i\in I} A_i$. Then G is a profinite group, A is an Abelian group, and G acts on A in the following way: Given $\sigma \in G$ and $a \in A$, we choose $i \in I$ and $a_i \in A_i$ with $\alpha_i(a_i) = a$ and set $\sigma_i = \pi_i(\sigma)$. Then we define $\sigma a = \alpha_i(\sigma_i a_i)$. One checks that this definition is good and that the action of G on A is continuous, so that A becomes a G-module. For all $q \ge 0$ and $i \le j$ the compatibility condition yields a homomorphism $(\pi_{ij}, \alpha_{ij})\colon H^q(G_i, A_i) \to H^q(G_j, A_j)$. By the commutativity of the triangle (5), this leads to a directed system of cohomological groups $(H^q(G_i, A_i), (\pi_{ij}, \alpha_{ij}))_{i,j\in I}$. By [Rib70, p. 109, Prop. 4.1],

$$H^q(G, A) = \varinjlim H^q(G_i, A_i). \tag{9}$$

Starting from an arbitrary profinite group G and a G-module A, we present G as an inverse limit $G = \varprojlim G/U$, where U ranges over all open normal subgroups of G, and recall that $A = \bigcup A^U$. Note that if $U' \subseteq U$, then $A^U \le A^{U'}$. Let $\pi_{U',U}\colon G/U' \to G/U$ be the quotient map and let $\alpha_{U,U'}\colon A^U \to A^{U'}$ be the inclusion map. Then, (9) yields in this case an isomorphism

$$H^q(G, A) = \varinjlim H^q(G/U, A^U). \tag{10}$$

Given an Abelian group A and a positive integer n we set $A_n = \{a \in A \mid na = 0\}$. For each prime number p we let $A_{p^\infty} = \bigcup_{k=1}^{\infty} A_{p^k}$ be the **p-primary part** of A. If A is a torsion group, then $A = \bigoplus A_{p^\infty}$. It follows that if $\alpha\colon A \to B$ is a homomorphism of torsion Abelian groups, then $\alpha(A_{p^\infty}) \le B_{p^\infty}$ for each p. Hence, each exact sequence $A \to B \to C$ of torsion Abelian groups yields an exact sequence $A_{p^\infty} \to B_{p^\infty} \to C_{p^\infty}$ of their p-primary parts.

Since each of the groups G/U is finite, the order of each element of $H^q(G/U, A^U)$ is finite (Subsection 9.3.8). It follows that $H^q(G, A)$ is a torsion Abelian group. As such it has a presentation

$$H^q(G, A) = \bigoplus_p H^q(G, A)_{p^\infty}. \tag{11}$$

Lemma 9.3.11: *Let G be a profinite group acting on a vector space V over $\mathbb{Q}$. Then:*
(a) $H^q(G,V)=0$ *for each* $q\geq 1$.
(b) $H^{q-1}(G,\mathbb{Q}/\mathbb{Z})\cong H^q(G,\mathbb{Z})$ *for each* $q\geq 2$.

Proof of (a): First we suppose G is finite and consider the restriction map res: $H^q(G,V)\to H^q(1,V)$ and the corestriction map

$$\text{cor: } H^q(1,V)\to H^q(G,V).$$

Both maps are trivial, so $\alpha=\text{cor}\circ\text{res: } H^q(G,V)\to H^q(G,V)$ is also trivial. By (8), α is multiplication by the order n of G.

Now let $f\text{: } G^q\to V$ be a q-cocycle. Since V is divisible, there exists a function $g\text{: } G^q\to V$ such that $ng=f$. Since division by n is unique, g is a cocycle. It follows from the preceding paragraph that f is a coboundary. Consequently, $H^q(G,V)=0$.

In the general case we use the presentation (10). By the preceding paragraph, $H^q(G/U,V^U)=0$ for each U. Consequently, $H^q(G,V)=0$.

Proof of (b): The short exact sequence of trivial G-modules $0\to\mathbb{Z}\to\mathbb{Q}\to\mathbb{Q}/\mathbb{Z}\to 0$ induces for each $q\geq 1$ a four terms exact sequence

$$H^{q-1}(G,\mathbb{Q})\to H^{q-1}(G,\mathbb{Q}/\mathbb{Z})\to H^q(G,\mathbb{Z})\to H^q(G,\mathbb{Q}).$$

By (a), the first and the fourth terms of this sequence are 0 for each $q\geq 2$, so (b) holds. □

9.3.12 Induced Modules.

Let $H\leq G$ be profinite groups. For each H-module A we denote by $\text{Ind}_H^G(A)$ the Abelian group of all continuous maps $f\text{: } G\to A$ such that $f(\eta\sigma)=\eta f(\sigma)$ for all $\eta\in H$ and $\sigma\in G$. The action of G on $\text{Ind}_H^G(A)$ is defined by $(\sigma' f)(\sigma)=f(\sigma\sigma')$. This action is continuous [Rib70, p. 142, Prop. 7.1], so $\text{Ind}_H^G(A)$ is a G-module. Note that $\text{Ind}_H^G(A)$ is naturally isomorphic to the G-module $\prod_{\sigma\in S}A$, where S is a system of representatives for the right cosets of G modulo H. Indeed, each continuous map $f\text{: } S\to A$ uniquely extends to an element $\hat{f}$ of $\text{Ind}_H^G(H)$ by $\hat{f}(\eta\sigma)=\eta f(\sigma)$ for $\eta\in H$ and $\sigma\in S$.

Shapiro's lemma ensures that

$$H^q(G,\text{Ind}_H^G(A))\cong H^q(H,A) \tag{12}$$

for each $q\geq 0$ [Rib70, p. 145, Thm. 7.4].

In the special case where $H=1$, the right hand side of (12) is 0 for each $q\geq 1$. Hence, $H^q(G,\text{Ind}_1^G(A))=0$.

9.3.13 Cohomological Triviality.

Let G be a finite group and A a G-module. The norm map norm: $A\to A$ is defined by $\text{norm}(a)=\sum_{\sigma\in G}\sigma a$. By [CaF, p. 113, Thm. 9], $H^q(G,A)=0$ for each $q\geq 1$ if $A^G=\text{norm}(A)$ and $H^1(G,A)=0$.

9.3.14 Cohomological p-Dimension.

Let G be a profinite group, p a prime number, and $n \geq 0$ an integer. We write $n = \mathrm{cd}_p(G)$ if there exists a torsion G-module A such that $H^n(G, A)_{p^\infty} \neq 0$ but $H^q(G, B)_{p^\infty} = 0$ for each $q \geq n+1$ and every torsion G-module B. In that case $H^q(G, B)_{p^\infty} = 0$ for each $q \geq n+2$ and every G-module B [Rib70, p. 197, Prop. 1.4]. Finally we note that for the inequality $\mathrm{cd}_p(G) \leq n$ to hold it suffices that $H^{n+1}(G, A) = 0$ for all finite simple p-primary G-modules A [Rib70, p. 200, Prop.1.5]. Here we say that A is a **simple G-module** if the only G-submodules of A are 0 and A itself. In this case $A \cong (\mathbb{Z}/p\mathbb{Z})^r$ for some nonnegative number r.

9.3.15 Cohomological Dimension.

The **cohomological dimension**, $\mathrm{cd}(G)$ of a profinite group G is the supremum of $\mathrm{cd}_p(G)$, where p ranges on all prime numbers. Thus, if $n = \mathrm{cd}(G) < \infty$, then there exists a torsion G-module A with $H^n(G, A) \neq 0$ and for all $q \geq n+1$, all torsion G-modules B, and every prime number p we have $H^q(G, B)_{p^\infty} = 0$. By (11), $H^q(G, B) = 0$. Similarly, the latter equality holds if $q \geq n+2$ and B is an arbitrary G-module.

9.3.16 Group Extensions.

We consider an exact sequence

$$0 \to A \to E \xrightarrow{\pi} G \to 1 \tag{13}$$

of profinite groups, where A is an additive finite Abelian group, choose a continuous section $s\colon G \to E$ of π [FrJ08, Lemma 1.2.7], and define a continuous action of G on A by the formula $(\sigma, a) \mapsto s(\sigma)as(\sigma)^{-1}$. This action does not depend on s. We call (13) an **extension of A by G**. The extension (13) is **equivalent** to another extension $0 \to A \to E \xrightarrow{\pi} G \to 1$ if there exists a homomorphism $E \to E'$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

commutative. Given a profinite group G and a finite G-module A, there is a bijective correspondence between the equivalence classes of extensions of A by G with the given G-action and the elements of $H^2(G, A)$ [Rib70, p. 100, Thm. 3.1]. The class of split extensions corresponds under that correspondence to the 0 element of $H^2(G, A)$ [Rib70, p. 105]. By Subsection 9.3.14 we have for each prime number p that $\mathrm{cd}_p(G) \leq 1$ if and only if $H^2(G, A) = 0$ for all finite simple p-primary G-modules A. Hence, $\mathrm{cd}_p(G) \leq 1$ if and only if each exact sequence $0 \to (\mathbb{Z}/p\mathbb{Z})^r \to E \to G \to 1$ splits. Consequently, by [FrJ08, Cor. 22.4.3], G is projective if and only if $\mathrm{cd}(G) \leq 1$.

By [FrJ08, Prop. 22.10.4] (whose proof does not depend on cohomology), a profinite group G is projective if and only if each of its p-Sylow

groups (for all p) is a free pro-p group, alternatively a projective group [FrJ08, Prop. 22.7.6].

9.3.17 Galois Cohomology.

Let L/K be a Galois extension. By the normal basis theorem,

$$H^1(\mathrm{Gal}(L/K), L^+) = 0$$

[Rib70, p. 246, Prop. 1.1]. By the multiplicative form of Hilbert's Theorem 90,

$$H^1(\mathrm{Gal}(L/K), L^\times) = 1 \tag{14}$$

[Rib70, p. 246, Prop. 1.2]. If $p = \mathrm{char}(K) > 0$, then $\mathrm{cd}_p(\mathrm{Gal}(K)) \leq 1$ [Rib70, p. 256, Thm. 3.3]. Thus, by Subsection 9.3.16, every p-Sylow subgroup of $\mathrm{Gal}(K)$ is projective. It follows from the last paragraph of Subsection 9.3.16 that $\mathrm{Gal}(K)$ is projective if every l-Sylow subgroup of $\mathrm{Gal}(K)$, for each $l \neq p$, is projective.

9.3.18 Brauer Groups.

Let K be a field. A **central simple K-algebra** is an associative (but not necessarily commutative) K-algebra A whose center is K and with no nontrivial two sided ideals. If A is finitely generated, then by Wedderburn-Artin [Bou58, p. 51, Cor. 2] there exist a division ring D with center K and a positive integer n such that A is isomorphic to the algebra $M_n(D)$ of all $n \times n$ matrices with entries in D. Another finitely generated central simple K-algebra A' is **equivalent** to A if $A' \cong M_{n'}(D)$ for some positive integer n'. We denote the equivalence classes of A by $[A]$. Let $\mathrm{Br}(K)$ be the set of all equivalence classes of finitely generated central simple K-algebras. The operation $([A], [A']) \mapsto [A \otimes_K A']$ makes $\mathrm{Br}(K)$ a group whose unit element is the class of K [Bou58, p. 117]. If L is a field extension of K, then the map $[A] \to [A \otimes_K L]$ is a group homomorphism $\alpha\colon \mathrm{Br}(K) \to \mathrm{Br}(L)$ [Bou58, p. 118, Prop. 6]. The kernel of α consists of all classes $[A]$ such that A **splits** over L, i.e. $A \cong_L M_n(L)$ for some positive integer n. One denotes $\mathrm{Ker}(\alpha)$ by $\mathrm{Br}(L/K)$.

There is an isomorphism $H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathrm{Br}(L/K)$ [Jac96, Thm. 2.5.11] such that if $K \subseteq L \subseteq N$ is a tower of fields and N/K is Galois, then the following diagram is commutative [Lor08, p. 194]

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^2(\mathrm{Gal}(L/K), L^\times) & \xrightarrow{\inf} & H^2(\mathrm{Gal}(N/K), N^\times) & \xrightarrow{\mathrm{res}} & H^2(\mathrm{Gal}(N/L), N^\times) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Br}(L/K) & \longrightarrow & \mathrm{Br}(N/K) & \longrightarrow & \mathrm{Br}(N/L)
\end{array}$$

where the second arrow in the lower row is the inclusion map and the third one is $[A] \mapsto [A \otimes_K L]$. Since, by (14), $H^1(\mathrm{Gal}(N/K), N^\times) = 1$, Lemma 9.3.7 implies that the upper row is exact. Hence, so is the lower.

If $\mathrm{cd}_p(\mathrm{Gal}(K)) \leq 1$, then $\mathrm{Br}(K)_p = 0$ for each $p \neq \mathrm{char}(K)$ [Rib70, p. 262, Cor.3.7]. If $\mathrm{Br}(L) = 0$ for each finite separable extension L of K, then $\mathrm{cd}(\mathrm{Gal}(K)) \leq 1$ [Rib70, p. 263, Cor. 3.8], so $\mathrm{Gal}(K)$ is projective (Subsection 9.3.16). If $\mathrm{cd}(\mathrm{Gal}(K)) \leq 1$ and K is perfect, then $\mathrm{Br}(K) = 0$ [Rib70, p. 263, Prop. 3.9].

9.4 The Projectivity of Gal($C(t)$)

Our third main goal in these notes is to prove that for each algebraically closed field C, the group $\mathrm{Gal}(C(x))$ is free. It would then follow that $\mathrm{Gal}(C(x))$ is projective [FrJ08, Lemma 22.3.6]. However, the projectivity of $\mathrm{Gal}(C(x))$ is an essential step in our proof that $\mathrm{Gal}(C(x))$ is free. So, we first prove that $\mathrm{Gal}(C(x))$ is projective. Our proof uses Galois cohomology, but it replaces advanced tools by more basic ones.

Remark 9.4.1: C_i fields. A field K is said to be C_i if every form (i.e. homogeneous polynomial) $f \in K[X_0, \ldots, X_n]$ of positive degree d with $d^i \leq n$ has a nontrivial zero in K^{n+1}. Thus, for K to be C_0 means that every homogeneous polynomial in $K[X_0, X_1]$ has a nontrivial zero in K^2. In other words, K is algebraically closed. The field K is C_1 if and only if each homogeneous polynomial $f \in K[X_0, \ldots, X_n]$ with $\deg(f) \leq n$ has a nontrivial zero in K^{n+1}. For example, every finite field is C_1 (a theorem of Chevalley [FrJ08, Proposition 21.2.4]), every PAC field of characteristic 0 is C_1 [Kol07, Thm. 1], and every perfect PAC field of positive characteristic is C_2 [FrJ08, Thm. 21.3.6]. Moreover, if K is C_i and L is a field extension of K of transcendence degree j, then L is C_{i+j} [FrJ08, Prop. 21.2.12]. In particular, if K is algebraically closed and x is an indeterminate, then every algebraic extension of $K(x)$ is C_1. □

Lemma 9.4.2: *Let L/K be a finite Galois extension.*
(a) *If K is C_1, then* $\mathrm{norm}_{L/K} L^\times = K^\times$.
(b) *In the general case,* $\mathrm{trace}_{L/K} L = K$.

Proof of (a): Let $w_1, \ldots, w_d$ be a basis of L/K and set $G = \mathrm{Gal}(L/K)$. Then

$$f(X_1, \ldots, X_d) = \prod_{\sigma \in G} (X_1 w_1^\sigma + \cdots + X_d w_d^\sigma)$$

is a form of degree d with coefficients in K. If $x_1, \ldots, x_d \in K$ and $f(x_1, \ldots, x_d) = 0$, then there exists $\tau \in G$ such that $z = x_1 w_1^\tau + \cdots + x_d w_d^\tau = 0$. Hence, all conjugates of z over K are zero. Thus, $x_1 w_1^\sigma + \cdots + x_d w_d^\sigma = 0$ for all $\sigma \in G$. Since $\det(w_i^\sigma) \neq 0$ [Lan93, p. 266, Cor. 5.4], we have $x_1 = \cdots = x_d = 0$.

Let now $a \in K^\times$. Since K is C_1, there exist $y_0, y_1, \ldots, y_d \in K$, not all 0, such that $f(y_1, \ldots, y_d) = y_0^d a$. By the preceding paragraph, $y_0 \neq 0$. Hence, with $x_i = y_i/y_0$, $i = 1, \ldots, d$, and $b = x_1 w_1 + \cdots + x_d w_d$, we have $\mathrm{norm}_{L/K} b = a$.

Proof of (b): By Artin's theorem about the linear independence of characters [Lan93, p. 283, Thm. 4.1], there exists $x \in L$ with $a = \sum_{\sigma \in G} x^\sigma \neq 0$. Then, $a = \mathrm{trace}_{L/K} x$ and $a \in K$. Consequently, each $b \in K$ can now be written as $b = \mathrm{trace}_{L/K}\left(\frac{b}{a} x\right)$. □

LEMMA 9.4.3: *Let L/K be a finite cyclic field extension.*
(a) *If K is C_1, then every short exact sequence*

$$1 \longrightarrow L^\times \longrightarrow E \xrightarrow{h} \mathrm{Gal}(L/K) \longrightarrow 1 \tag{1}$$

of groups with the usual Galois action of $\mathrm{Gal}(L/K)$ on $L^\times$ splits. Thus, $H^2(\mathrm{Gal}(L/K), L^\times) = 1$.
(b) *In the general case, every short exact sequence*

$$0 \longrightarrow L^+ \longrightarrow E \xrightarrow{h} \mathrm{Gal}(L/K) \longrightarrow 1 \tag{2}$$

of groups with the usual Galois action of $\mathrm{Gal}(L/K)$ on L^+ splits. Thus, $H^2(\mathrm{Gal}(L/K), L^+) = 0$.

Proof: Let $n = [L : K]$ and let σ be a generator of $\mathrm{Gal}(L/K)$. We have to find $\varepsilon \in E$ such that $h(\varepsilon) = \sigma$ and $\varepsilon^n = 1$.

By assumption, there exists $\varepsilon \in E$ such that $h(\varepsilon) = \sigma$. For each $y \in L^\times$, we have $y^\varepsilon = y^\sigma$. Also, $\varepsilon^n \in L^\times$. Hence, $(\varepsilon^n)^\sigma = (\varepsilon^n)^\varepsilon = \varepsilon^n$, so $\varepsilon^n \in K^\times$.

By Lemma 9.4.2, there exists $x \in L^\times$ such that $\mathrm{norm}_{L/K} x = \varepsilon^{-n}$ in Case (a) and $\mathrm{trace}_{L/K} x = \varepsilon^{-n}$ in Case (b). For arbitrary elements x, ε of a group G, one proves by induction on n that

$$(x\varepsilon)^n = \varepsilon^n x^{\varepsilon^n} x^{\varepsilon^{n-1}} \cdots x^\varepsilon.$$

In Case (a), this formula gives

$$(x\varepsilon)^n = \varepsilon^n x^{\varepsilon^n} x^{\varepsilon^{n-1}} \cdots x^\varepsilon = \varepsilon^n x^{\sigma^n} x^{\sigma^{n-1}} \cdots x^\sigma = \varepsilon^n \mathrm{norm}_{L/K} x = 1. \tag{3}$$

Therefore, $x\varepsilon$ is the desired element of E.

In Case (b) the operation of L^+ is addition, so we have to replace (3) by

$$\begin{aligned}(x\varepsilon)^n &= \varepsilon^n (x^{\varepsilon^n} + x^{\varepsilon^{n-1}} + \cdots + x^\varepsilon) \\ &= \varepsilon^n (x^{\sigma^n} + x^{\sigma^{n-1}} + \cdots + x^\sigma) = \varepsilon^n \mathrm{trace}_{L/K} x = 1.\end{aligned}$$

Again, $x\varepsilon$ is the desired element of E.

The triviality of the second cohomology groups follows now from Subsection 9.3.16. □

LEMMA 9.4.4: *Let K be a C_1 field, p a prime number, and E a p-***Sylow extension of** *K (i.e. E is the fixed field in K_s of a p-Sylow subgroup of* Gal(K)*.) Then*
$H^2(\mathrm{Gal}(E), E_s^\times) = 1$.

Proof: By Subsection 9.3.10, $H^2(\mathrm{Gal}(E), E_s^\times) = \varinjlim H^2(\mathrm{Gal}(N/E), N^\times)$, where N ranges over all finite Galois extensions of E and the maps involved in the direct limit are inflations. We prove by induction on the degree, that for each finite Galois extension N/L with $E \subseteq L \subseteq N \subseteq K_s$ we have $H^2(\mathrm{Gal}(N/L), N^\times) = 1$.

Indeed, N/L is a p-extension. If this extension is nontrivial, it has a cyclic subextension M/L of degree p. By Remark 9.4.1, L is C_1, hence by Lemma 9.4.3(a), $H^2(\mathrm{Gal}(M/L), M^\times) = 1$. By induction, $H^2(\mathrm{Gal}(N/M), N^\times) = 1$. Finally we use the exactness of the inflation restriction sequence

$$1 \longrightarrow H^2(\mathrm{Gal}(M/L), M^\times) \xrightarrow{\inf} H^2(\mathrm{Gal}(N/L), N^\times) \xrightarrow{\mathrm{res}} H^2(\mathrm{Gal}(N/M), N^\times)$$

(Lemma 9.3.7) to conclude that $H^2(\mathrm{Gal}(N/L), N^\times) = 1$. □

LEMMA 9.4.5: *Let K be a C_1 field, p a prime number, and E a p-Sylow extension of K. Then,* Gal(E) *is projective, hence pro-p free.*

Proof: The statement holds for $p = \mathrm{char}(E)$ by [Rib70, p. 256]. So, we assume that $p \neq \mathrm{char}(E)$.

By Subsection 9.3.16, we have to prove that $H^2(\mathrm{Gal}(E), \mathbb{Z}/p\mathbb{Z}) = 0$. To this end consider the short exact sequence

$$1 \longrightarrow \mu_p \longrightarrow E_s^\times \xrightarrow{p} E_s^\times \longrightarrow 1, \tag{4}$$

where μ_p is the group of roots of unity of order p and the map from $E_s^\times$ to $E_s^\times$ is raising to the pth power. Since $[E(\mu_p) : E]$ divides $p - 1$ and Gal(E) is a pro-p group, $[E(\mu_p) : E] = 1$, so $\mu_p \subseteq E$ and the action of Gal(E) on μ_p is trivial. Hence, μ_p is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a Gal(E)-module. Now we consider the following segment of the long exact sequence derived from the exact sequence (4) (Subsection 9.3.4):

$$H^1(\mathrm{Gal}(E), E_s^\times) \longrightarrow H^2(\mathrm{Gal}(E), \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^2(\mathrm{Gal}(E), E_s^\times). \tag{5}$$

The left term of (5) is trivial, by Subsection 9.3.17. The right term of (5) is trivial, by Lemma 9.4.4. Hence, the middle term of (5) is also trivial. □

PROPOSITION 9.4.6 (Tsen):
(a) *Let E be a C_1 field. Then* Gal(E) *is projective.*
(b) *Let E be an extension of transcendence degree* 1 *over a separably closed field C. Then* Gal(E) *is projective.*

Proof of (a): By Lemma 9.4.5, each of the Sylow subgroups of Gal(E) is projective. It follows from [FrJ08, Prop. 22.10.4] that Gal(E) is projective. Note that the proof of the latter theorem is carried out without cohomology.

Proof of (b): First we note that $(E\tilde{C})_s/E_s\tilde{C}$ is both a separable extension and a purely inseparable extension, so it is a trivial extension. Thus, $E_s\tilde{C} = (E\tilde{C})_s$. In addition, $E_s \cap E\tilde{C} = E$, hence $\mathrm{Gal}(E) \cong \mathrm{Gal}(E\tilde{C})$. We may therefore assume that C is algebraically closed. By Remark 9.4.1, E is a C_1 field. Hence, by (a), $\mathrm{Gal}(E)$ is projective. □

Following [FrJ08, Remark 17.4.7], we denote the free profinite group of rank m by $\hat{F}_m$ and rephrase a special case of [FrJ08, Lemma 25.1.8]:

PROPOSITION 9.4.7: *Let m be an infinite cardinal and G a projective group of rank at most m. Suppose every finite split embedding problem for G with a nontrivial kernel has m solutions. Then $G \cong \hat{F}_m$.*

THEOREM 9.4.8: *Let K be a field of characteristic p and cardinality m and let E be a function field of one variable over K. Suppose* $\mathrm{Gal}(K)$ *is trivial if $p = 0$ or* $\mathrm{Gal}(K)$ *is a pro-p group if $p > 0$. Then* $\mathrm{Gal}(E) \cong \hat{F}_m$.

Proof: We choose a separating transcendental element x for E/K. Consider a prime number $l \neq p$ and let G_l be an l-Sylow subgroup of $\mathrm{Gal}(K(x))$. Since $\mathrm{Gal}(K_s(x)/K(x)) \cong \mathrm{Gal}(K)$ is trivial if $p = 0$ or a pro-p group if $p > 0$, G_l is an l-Sylow subgroup of $\mathrm{Gal}(K_s(x))$. By Proposition 9.4.6(b), $\mathrm{Gal}(K_s(x))$ is projective. Hence, by Subsection 9.3.16, G_l is projective. It follows from Subsection 9.3.17 that $\mathrm{Gal}(K(x))$ is projective.

By Theorem 5.8.3, K is ample. Hence, by Proposition 8.6.3, every finite split embedding problem for $\mathrm{Gal}(K(x))$ with a nontrivial kernel has m solutions. In particular, $m \geq \mathrm{rank}(\mathrm{Gal}(K(x))) \geq \aleph_0$. By Proposition 9.4.7, $\mathrm{Gal}(K(x)) \cong \hat{F}_m$. It follows from [FrJ08, Prop. 25.4.2] that $\mathrm{Gal}(E) \cong \hat{F}_m$. □

COROLLARY 9.4.9: *Let K be a separably closed field of cardinality m and let E be an algebraic function field of one variable over K. Then* $\mathrm{Gal}(E) \cong \hat{F}_m$.

Remark 9.4.10: An analog of Shafarevich's Conjecture. We denote the extension of a field K generated by all roots of unity by K_{cycl}. As mentioned in Example 5.10.5, Shafarevich's conjecture predicts that $\mathrm{Gal}(K_{\mathrm{cycl}}) \cong \hat{F}_\omega$ for each number field K.

As is the case with several other conjectures (e.g. the Riemann hypothesis), the analog of Shafarevich's conjecture for function fields K of one variable over finite fields is true. In this case $K_{\mathrm{cycl}} = \tilde{\mathbb{F}}_p K$, where $p = \mathrm{char}(K)$. Thus, if we choose a transcendental element x of K over $\mathbb{F}_p$, then K_{cycl} is a finite extension of $\tilde{\mathbb{F}}_p(x)$. Therefore, by Corollary 9.4.9, $\mathrm{Gal}(K_{\mathrm{cycl}}) \cong \hat{F}_\omega$, as claimed. □

9.5 Projectivity of Fundamental Groups

Let C be an algebraically closed field, E a function field of one variable over C, S a nonempty set of prime divisors of E/C, and E_S the maximal Galois extension of E ramified at most over S. The only known proof of the Riemann existence theorem uses complex analytic methods. It follows, as mentioned

in Remark 9.1.12, that the proof of the projectiveness of $\mathrm{Gal}(E_S/E)$ in the case $\mathrm{char}(C) = 0$, stated in Corollary 9.1.11, relies on analytic methods.

The aim of this section is to prove that $\mathrm{Gal}(E_S/E)$ is projective, without any restriction on the characteristic, by algebraic means. This will in particular reproves the projectivity of $\mathrm{Gal}(E_S/E)$ in characteristic 0.

As mentioned in the proof of Proposition 9.4.6, a profinite group G is projective if and only if for each prime number p each p-Sylow subgroup G_p of G is projective [FrJ08, Prop. 22.10.4]. We therefore say that G is **p-projective** if G_p is projective. We say that an embedding problem $(\varphi\colon H \to A,\ \alpha\colon B \to A)$ is **central** if $\mathrm{Ker}(\alpha)$ is contained in the center of B.

Lemma 9.5.1: *Let p be a prime number.*

(a) *Let G be a profinite group. Suppose for every open subgroup H, each finite nonsplit central embedding problem*

$$\begin{array}{ccccccccc} & & & & & & H & & \\ & & & & & & \downarrow{\scriptstyle\varphi} & & \\ 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow & 1 \end{array}$$

for which B is a p-group is solvable. Then G is p-projective.

(b) *Let N/E be a Galois extension. Suppose for each finite subextension K of N/E, for each finite p-subextension L/K of N/K, and every nonsplit central exact sequence of p-groups*

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow B \xrightarrow{\alpha} \mathrm{Gal}(L/K) \longrightarrow 1 \tag{1}$$

there exists a Galois extension $\hat{L}$ of K in N that contains L and there exists an isomorphism $\gamma\colon \mathrm{Gal}(\hat{L}/K) \to B$ such that $\alpha \circ \gamma = \mathrm{res}_L$. Then $\mathrm{Gal}(N/E)$ is p-projective.

Proof: Statement (b) is a reinterpretation of (a) for Galois groups, so we prove (a).

Let G_p be a p-Sylow subgroup of G. In order to prove that G_p is projective, it suffices to prove that each finite embedding problem

$$\begin{array}{ccccccccc} & & & & & & G_p & & \\ & & & & & & \downarrow{\scriptstyle\varphi_p} & & \\ 1 & \longrightarrow & B_0 & \longrightarrow & B & \xrightarrow{\alpha} & A & \longrightarrow & 1 \end{array} \tag{2}$$

in which B is a p-group and B_0 is a minimal normal subgroup of B is weakly solvable, that is there exists a homomorphism $\gamma\colon G_p \to B$ such that $\alpha \circ \gamma = \varphi_p$ [FrJ08, Lemma 22.3.4 and Lemma 22.4.1]. By elementary group theory, B_0 is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and lies in the center of B. This means that the short exact sequence in (2) is central.

If the short exact sequence in (2) splits, there exists a homomorphism $\alpha'\colon A \to B$ such that $\alpha \circ \alpha' = \mathrm{id}_A$. Then $\alpha' \circ \varphi_p$ weakly solves (2). Otherwise we choose an open normal subgroup N of G such that $G_p \cap N = \mathrm{Ker}(\varphi_p)$. Let $H = G_pN$. Then H is an open subgroup of G that contains G_p and φ_p extends to a homomorphism $\varphi\colon H \to A$. By assumption, there exists a homomorphism $\gamma\colon H \to B$ such that $\alpha \circ \gamma = \varphi$. The restriction of γ to G_p weakly solves embedding problem (2). Note that since we are now assuming that α does not split, $B_0 \cap \gamma(G_p) \neq 1$, so $B_0 \leq \gamma(G_p)$. Therefore, $\gamma|_{G_p}$ is even surjective. □

Lemma 9.5.2: *Let A be a finite group, p a prime number, and let*

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E_i \xrightarrow{\varepsilon_i} A \longrightarrow 1$$

$i = 1, 2$, be central group extensions. Then there exists an isomorphism $\varphi\colon E_1 \to E_2$ such that $\varepsilon_2 \circ \varphi = \varepsilon_1$ if and only if the two group extensions

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E_1 \times_A E_2 \xrightarrow{\pi_i} E_i \longrightarrow 1,$$

where $\pi_i\colon E_1 \times_A E_2 \to E_i$ is the projection onto E_i, split.

Proof: Suppose there exists an isomorphism $\varphi\colon E_1 \to E_2$ such that $\varepsilon_2 \circ \varphi = \varepsilon_1$. Then φ induces a homomorphism $\varphi'\colon E_1 \to E_1 \times_A E_2$ such that $\pi_1 \circ \varphi' = \mathrm{id}_{E_1}$ [FrJ08, Prop. 22.2.1]. Applying the same argument to φ^{-1} yields the splitting of π_2.

Conversely, suppose $\pi_1\colon E_1 \times_A E_2 \to E_1$ has a group theoretic section $\pi_1'\colon E_1 \to E_1 \times_A E_2$, that is $\pi_1 \circ \pi_1' = \mathrm{id}_{E_1}$. Let $\psi_2 = \pi_2 \circ \pi_1'$. Then, $\varepsilon_2 \circ \psi_2 = \varepsilon_2 \circ \pi_2 \circ \pi_1' = \varepsilon_1 \circ \pi_1 \circ \pi_1' = \varepsilon_1$, so $\mathrm{Ker}(\psi_2) \leq \mathrm{Ker}(\varepsilon_1)$. If $\mathrm{Ker}(\psi_2) = 1$, then $\psi_2\colon E_1 \to E_2$ is the desired isomorphism φ. Otherwise, since $\mathrm{Ker}(\varepsilon_1) = \mathbb{Z}/p\mathbb{Z}$, we have $\mathrm{Ker}(\psi_2) = \mathrm{Ker}(\varepsilon_1)$. Therefore, ψ_2 induces a monomorphism $\psi_2'\colon A \to E_2$ such that $\varepsilon_2 \circ \psi_2' = \mathrm{id}_A$. It follows that $E_2 = \mathbb{Z}/p\mathbb{Z} \times \psi_2'(A)$.

Arguing with π_2, we are reduced to the case where the latter consequence of the preceding paragraph holds and in addition $E_1 = \mathbb{Z}/p\mathbb{Z} \times \psi_1'(A)$, where $\psi_1'\colon A \to E_1$ is a group theoretic section of ε_1. Now we define a map $\varphi\colon E_1 \to E_2$ whose restriction to $\mathbb{Z}/p\mathbb{Z}$ is the identity map and $\varphi(\psi_1'(a)) = \psi_2'(a)$ for each $a \in A$. Then φ is an isomorphism such that $\varepsilon_2 \circ \varphi = \varepsilon_1$, as desired. □

Lemma 9.5.3: *Let L/K be a Galois extension, $p \neq \mathrm{char}(K)$ a prime number, and (1) a nonsplit central exact sequence of p-groups. Suppose K contains a root ζ of 1 of order p and let $L(x^{1/p})$ be a solution field of (1) with $x \in L^\times$. Then the set of solution fields of (1) coincides with the set of fields $L((ax)^{1/p})$, $a \in K^\times$.*

Proof: Set $x_1 = x$, $N_1 = L(x_1^{1/p})$, $E_1 = \mathrm{Gal}(N_1/K)$, and $A = \mathrm{Gal}(L/K)$. Let $\varepsilon_1\colon E_1 \to A$ be the restriction map. By assumption, N_1 is a solution field of (1). Hence, $0 \to \mathbb{Z}/p\mathbb{Z} \to E_1 \xrightarrow{\varepsilon_1} A \to 1$ is a nonsplit central extension (because (1) is).

Now consider an $a \in K^\times$. Set $x_2 = ax_1$, $N_2 = L(x_2^{1/p})$, and $N = N_1N_2$. Then $N = N_1K(a^{1/p})$ is a Galois extension of K. Moreover, if $\sigma \in \mathrm{Gal}(N/L)$, then $\sigma|_{N_1}$ is in the center of $\mathrm{Gal}(N_1/K)$ (by assumption) and $\sigma|_{L(a^{1/p})}$ is in $\mathrm{Gal}(L(a^{1/p})/L)$, hence is also in the center of $\mathrm{Gal}(L(a^{1/p})/K)$ (because $\mathrm{Gal}(L(a^{1/p})/K) = \mathrm{Gal}(L(a^{1/p})/L) \times \mathrm{Gal}(L(a^{1/p})/K(a^{1/p}))$ and $\mathrm{Gal}(L(a^{1/p})/L)$ is cyclic). Thus, $\mathrm{Gal}(N/L)$ is contained in the center of $\mathrm{Gal}(N/K)$. It follows that N_2 (that lies between L and N) is a Galois extension of K and $\mathrm{Gal}(N_2/L)$ is contained in the center of $\mathrm{Gal}(N_2/K)$.

Assuming $N_1 \neq N_2$, we set $E_2 = \mathrm{Gal}(N_2/K)$ and let $\varepsilon_2 \colon E_2 \to A$ be the restriction map. Then $\mathrm{Gal}(N_2/L) \cong \mathbb{Z}/p\mathbb{Z}$ (otherwise, $a^{1/p} \in N_1$, so the ε_1 splits) and $0 \to \mathbb{Z}/p\mathbb{Z} \to E_2 \xrightarrow{\varepsilon_2} A \to 1$ is a central exact sequence. Moreover,

$$\mathrm{Gal}(N/K) \cong E_1 \times_A E_2$$

[FrJ08, Example 22.2.7(a)] is a split extension of both E_1 and E_2. Hence, by Lemma 9.5.2, there exists an isomorphism $\varphi \colon E_1 \to E_2$ that commutes with restriction to L. Therefore, N_2 is also a solution field of (1).

Conversely, suppose $N_2 = L(x_2^{1/p})$ with $x_2 \in L^\times$ is a solution field of embedding problem (1) and $N_2 \neq N_1$ and let E_2 and ε_2 be as above. Then there exists an isomorphism $\varphi \colon E_1 \to E_2$ such that $\varepsilon_2 \circ \varphi = \varepsilon_1$. Then, with $N = N_1N_2$, $\mathrm{Gal}(N/K) \cong E_1 \times_A E_2$. By Lemma 9.5.2, the group extension $0 \to \mathbb{Z}/p\mathbb{Z} \to \mathrm{Gal}(N/K) \to \mathrm{Gal}(N_1/K) \to 1$ splits, which implies that $N = N_1(a^{1/p})$ with $a \in K^\times$. But $N = N_1(x_2^{1/p})$, so by Kummer theory, $x_2a^{-1} \in (N_1^\times)^p$ (replacing a by a power of a if necessary). Hence, $L((x_2a^{-1})^{1/p}) \subseteq N_1$. If equality holds, then by Kummer theory, $x_2a^{-1}x_1^{-1} \in (L^\times)^p$ (replacing x_1 by some power of itself if necessary), therefore $N_2 = L(x_2^{1/p}) = L((ax)^{1/p})$, as claimed.

Otherwise, $x_2a^{-1} \in (L^\times)^p$, so $N_2 = L(x_2^{1/p}) = L(a^{1/p})$. Hence, the short exact sequence $1 \to \mathrm{Gal}(N_2/L) \to \mathrm{Gal}(N_2/K) \to \mathrm{Gal}(L/K) \to 1$ splits. Therefore, also the short exact sequence $1 \to \mathrm{Gal}(N_1/L) \to \mathrm{Gal}(N_1/K) \to \mathrm{Gal}(L/K) \to 1$ splits (because both N_1 and N_2 are solution fields of (1)). This contradicts the assumption that embedding problem (1) does not split. □

Lemma 9.5.4: *Let K be a function field of one variable over an algebraically closed field C, S a finite nonempty set of prime divisors of K/C, $p \neq \mathrm{char}(K)$ a prime number, and L/K a finite Galois subextension of K_S/K. Suppose (1) is a nonsplit central p-embedding problem which is solvable in K_s. Then (1) has a solution field $\hat{L}$ in K_S.*

Proof: Let $L(x^{1/p})$ be a solution field of (1) in K_s. By Lemma 9.5.3, it suffices to find $a \in K^\times$ such that $L((ax)^{1/p}) \subseteq K_S$.

We extend each $\sigma \in \mathrm{Gal}(L/K)$ to an element σ of $\mathrm{Gal}(L(x^{1/p})/K)$. Then $L((x^{1/p})^\sigma) = L(x^{1/p})$. Hence, $(x^{1/p})^\sigma = x^{i/p}u$ for some $0 \leq i \leq p-1$ and $u \in$

$L^\times$ (by Kummer theory). Now we consider the element $\tau \in \mathrm{Gal}(L(x^{1/p})/L)$ defined by $(x^{1/p})^\tau = \zeta x^{1/p}$, where ζ is a root of unity of order p. Then $(x^{1/p})^{\tau\sigma} = (\zeta x^{1/p})^\sigma = \zeta x^{i/p} u$ and $(x^{1/p})^{\sigma\tau} = (x^{i/p}u)^\tau = \zeta^i x^{i/p} u$. Since (1) is central, $\tau\sigma = \sigma\tau$, so $i = 1$. It follows that $x^\sigma = xu^p$, so $\mathrm{div}(x^\sigma) \equiv \mathrm{div}(x) \mod p\mathrm{Div}(L/C)$. Hence, $v_{\mathfrak{P}}(x^\sigma) \equiv v_{\mathfrak{P}}(x) \mod p$ for each prime divisor $\mathfrak{P}$ of L/C. Since $v_{\mathfrak{P}}(x^\sigma) = v_{\mathfrak{P}^{\sigma^{-1}}}(x)$, this implies that $v_{\mathfrak{P}^\sigma}(x) \equiv v_{\mathfrak{P}}(x) \mod p$ for all $\mathfrak{P}$ and σ. Since the set of prime divisors of L/C lying over each prime divisor $\mathfrak{p}$ of K/C form a conjugacy class under the action of $\mathrm{Gal}(L/K)$, we may denote the common residue modulo p of $v_{\mathfrak{P}}(x)$ for all $\mathfrak{P}$ dividing $\mathfrak{p}$ by $n_{\mathfrak{p}}$ and write $\mathrm{div}(x) \equiv \sum_{\mathfrak{p}} n_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} \mod p\mathrm{Div}(L/C)$, where $\mathfrak{p}$ ranges over the prime divisors of K/C.

If $\mathfrak{p} \notin S$, then $\mathfrak{p}$ is unramified in L, so $\mathfrak{p} = \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$. Hence,

$$\begin{aligned}\mathrm{div}(x) &= \sum_{\mathfrak{p}\notin S} n_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} + \sum_{\mathfrak{p}\in S} n_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P} \mod p\mathrm{Div}(L/C)\\ &\equiv \mathfrak{a} + \mathfrak{B} \mod p\mathrm{Div}(L/C),\end{aligned}$$

where $\mathfrak{a} \in \mathrm{Div}(K/C)$ and $\mathfrak{B}$ is a divisor of L/C that involves only primes over S.

We choose $\mathfrak{o} \in S$. By Subsection 6.3.2, there exists $a \in K^\times$ with $\mathrm{div}(a) + \mathfrak{a} - \deg(\mathfrak{a})\mathfrak{o} \equiv 0 \mod p\mathrm{Div}(K/C)$. Therefore, $\mathrm{div}(ax) \equiv \deg(\mathfrak{a})\mathfrak{o} + \mathfrak{B} \mod p\mathrm{Div}(L/C)$. This implies that $v_{\mathfrak{P}}(ax) \equiv 0 \mod p$ for each $\mathfrak{P}$ which does not lie over S. Such $\mathfrak{P}$ is unramified in $L((ax)^{1/p})$ [FrJ08, Example 2.3.8]. Consequently, $L((ax)^{1/p}) \subseteq K_S$. □

In order to prove an analog of Lemma 9.5.3 also for $p = \mathrm{char}(C) > 0$, we have to replace Kummer theory in the above arguments by Artin-Schreier theory. To that end we consider till the end of the proof of Lemma 9.5.6 only fields of characteristic p. Let $\wp$ be the additive operator defined on fields of characteristic p by $\wp(x) = x^p - x$. Recall that if L/K is a cyclic extension of degree p, then $L = K(x)$, where $\wp(x) \in K \setminus \wp(K)$ [Lan93, p. 290, Thm. 6.4]. For each subgroup A of the additive group of K we have $[K(\wp^{-1}(A)) : K] = [A + \wp(K) : \wp(K)]$ [Lan93, p. 296, Thm. 8.3]. In particular, let $x, y, z \in K_s$ with $\wp(x), \wp(y), \wp(z) \in K$. Then

(3a) $K(x) = K$ if and only if $\wp(x) \in \wp(K)$.

(3b) If $K(x) = K(y)$, then there exist $k, l \in \mathbb{Z}$ not both divisible by p such that $\wp(kx) + \wp(ly) \equiv 0 \mod \wp(K)$. Conversely, if neither of k, l is divisible by p and $\wp(kx) + \wp(ly) \equiv 0 \mod \wp(K)$, then $K(x) = K(y)$.

(3c) If $x \notin K$ and $K(x) = K(y)$, then there exists $k \in \mathbb{Z}$ such that $p \nmid k$ and $\wp(y) \equiv \wp(kx) \mod \wp(K)$.

(3d) If $x_i \in K_s$, $a_i = \wp(x_i) \in K$ for $i = 1, \ldots, n$, and $a_1, \ldots, a_n$ are linearly independent over $\mathbb{F}_p$ modulo $\wp(K)$, then the fields $K(x_1), \ldots, K(x_n)$ are linearly disjoint cyclic extensions of K of degree p.

We use the rules (3) in the proof of the following additive analog of Lemma 9.5.3.

LEMMA 9.5.5: *Let L/K be a finite Galois extension of fields of positive characteristic p and let (1) be a nonsplit central exact sequence. Suppose $L(x)$ is a solution field of (1) and $\wp(x) \in L$. Then $\hat{L}$ is a solution field of (1) if and only if $\hat{L} = L(y)$ with $\wp(y) \in L$ and $\wp(y) \equiv \wp(x) \mod K + \wp(L)$.*

Proof: First suppose y is an element of K_s such that $\wp(y) \in L$ and $\wp(y) \equiv \wp(x) + a \mod \wp(L)$ with $a \in K$. Set $A = \mathrm{Gal}(L/K)$ and $N = L(x, y)$ and assume $L(x) \neq L(y)$. We choose $z \in K_s$ such that $\wp(z) = a$. Then $K(z)/K$ is a cyclic extension of degree 1 or p and $\wp(y) \equiv \wp(x + z) \mod \wp(L)$. Hence, $L(x, y) = N = L(x, x + z) = L(x)K(z)$ (by (3b)). Therefore, the extension

$$1 \longrightarrow \mathrm{Gal}(N/L(x)) \longrightarrow \mathrm{Gal}(N/K) \longrightarrow \mathrm{Gal}(L(x)/K) \longrightarrow 1 \tag{4}$$

splits. Next note that $\mathrm{Gal}(L(z)/K) = \mathrm{Gal}(L(z)/L) \times \mathrm{Gal}(L(z)/K(z))$ and $\mathrm{Gal}(L(z)/L)$ is cyclic. Hence, $\mathrm{Gal}(L(z)/L)$ is contained in the center of $\mathrm{Gal}(L(z)/K)$. In addition, by assumption, $\mathrm{Gal}(L(x)/L)$ is contained in the center of $\mathrm{Gal}(L(x)/K)$. Hence, $\mathrm{Gal}(N/L)$ is contained in the center of $\mathrm{Gal}(N/K)$. It follows that $L(y)/K$ is Galois and $1 \to \mathrm{Gal}(L(y)/L) \to \mathrm{Gal}(L(y)/K) \to \mathrm{Gal}(L/K) \to 1$ is a central exact sequence. Moreover, the relation $\wp(y - z) \equiv \wp(x) \mod \wp(L)$ implies that $L(y)K(z) = N$, so the extension

$$1 \longrightarrow \mathrm{Gal}(N/L(y)) \longrightarrow \mathrm{Gal}(N/K) \longrightarrow \mathrm{Gal}(L(y)/K) \longrightarrow 1 \tag{5}$$

splits. Then $\mathrm{Gal}(N/K) \cong \mathrm{Gal}(L(x)/K) \times_A \mathrm{Gal}(L(y)/K)$ and the restriction maps on $L(x)$ and $L(y)$ correspond to the projections on the groups $\mathrm{Gal}(L(x)/K)$ and $\mathrm{Gal}(L(y)/K)$. By Lemma 9.5.2 there exists an isomorphism φ: $\mathrm{Gal}(L(y)/K) \to \mathrm{Gal}(L(x)/K)$ that commutes with the restriction to L. It follows that $L(y)$ is a solution field of (1).

Conversely, suppose $\hat{L}$ is a solution field of (1). In particular, $\hat{L}$ is a cyclic extension of degree p of L. Hence $\hat{L} = L(y_0)$ with $\wp(y_0) \in L$ and there exists an isomorphism φ: $\mathrm{Gal}(L(y_0)/K) \to \mathrm{Gal}(L(x)/K)$ that commutes with the restriction to L. Hence, with y_0 replacing y, both extensions (4) and (5) split (Lemma 9.5.2). This implies that $N = L(x, z)$ with $\wp(z) \in K$. If $L(y_0) = L(x)$, then $\wp(ky_0) \equiv \wp(x) \mod \wp(L)$ for some $k \in \mathbb{Z}$ with $p \nmid k$ (by (3c)).

If $L(y_0) \neq L(x)$, then there exist $k, l \in \mathbb{Z}$ with $p \nmid k$ such that $\wp(ky_0) + \wp(lz) \equiv \wp(x) \mod \wp(L)$ (by (3d)), so $\wp(ky_0) \equiv \wp(x) \mod K + \wp(L)$. In both cases $y = ky_0$ satisfies the requirements of the lemma. □

LEMMA 9.5.6: *Let K be a function field of one variable over an algebraically closed field C of characteristic $p > 0$. Let S be a finite nonempty set of prime divisors of K/C. Let L/K be a finite Galois subextension of K_S/K. Suppose the central nonsplit embedding problem (1) has a solution. Then (1) has a solution field $\hat{L}$ in K_S.*

Proof: By assumption there exists $u \in L \setminus \wp(L)$ and there exists $x \in K_s$ such that $\wp(x) = u$ and $L(x)$ solves (1). If $\mathfrak{P}$ is a prime divisor of L/C that

does not lie over S, then $\mathfrak{P}$ is unramified over K. Moreover, the residue field of L at $\mathfrak{P}$ is C (because C is algebraically closed), hence equals to the residue field of K at $\mathfrak{P}|_K$. Therefore, K is $\mathfrak{P}$-dense in L. Since S is nonempty, the strong approximation theorem [FrJ08, Prop. 3.3.1] gives an $a \in K$ such that

$$\begin{aligned} v_{\mathfrak{P}}(a-u) \geq 0 \text{ if } \mathfrak{P}|_K \notin S \wedge v_{\mathfrak{P}}(u) < 0 \\ v_{\mathfrak{P}}(a) \geq 0 \text{ if } \mathfrak{P}|_K \notin S \wedge v_{\mathfrak{P}}(u) \geq 0. \end{aligned} \tag{6}$$

We choose $y \in K_s$ such that $\wp(y) = u-a$. By Lemma 9.5.5, $L(y)$ is a solution field of (1). By (6), $v_{\mathfrak{P}}(u-a) \geq 0$ for each $\mathfrak{P}$ that does not lie over S, hence by [FrJ08, Example 2.3.9], each such $\mathfrak{P}$ is unramified in $L(y)$. Consequently, $L(y) \subseteq K_S$, as desired. □

We combine Lemmas 9.5.4 and 9.5.6 with Lemma 9.5.1(b):

THEOREM 9.5.7: *Let E be a function field of one variable over an algebraically closed field C and S a finite nonempty set of prime divisors of E/C. Then $\mathrm{Gal}(E_S/E)$ is projective.*

Proof: Consider a finite extension K of E in E_S, a prime number p, a finite p-extension L of K in E_S, and a central nonsplit embedding problem (1). By Lemma 9.5.1(b) it suffices to solve (1) in E_S. Let S' be the set of prime divisors of K/C that lie over S. Then $K_{S'} = E_S$. Hence, without loss, we may assume that $K = E$ and $S' = S$. Therefore, by Lemmas 9.5.4 and 9.5.6, it suffices to solve embedding problem (1) in the separable closure K_s of K.

By Proposition 9.4.6(b), $\mathrm{Gal}(K)$ is projective. Hence, there exists a homomorphism $\gamma\colon \mathrm{Gal}(K) \to B$ with $\alpha \circ \gamma = \mathrm{res}_L$. In particular,

$$\alpha(\gamma(\mathrm{Gal}(K))) = \mathrm{Gal}(L/K).$$

If $\mathbb{Z}/p\mathbb{Z} \cap \gamma(\mathrm{Gal}(K))$ is trivial, then α has a group theoretic section, in contrast to our assumption. Therefore, $\mathbb{Z}/p\mathbb{Z} \subseteq \gamma(\mathrm{Gal}(K))$, so γ is surjective. The fixed field of $\mathrm{Ker}(\gamma)$ in K_s is the desired field $L(x)$. □

COROLLARY 9.5.8: *Let E be a function field of one variable over an algebraically closed field C and S a nonempty set of prime divisors of E/C. Then $\mathrm{Gal}(E_S/E)$ is projective.*

Proof: Every finite embedding problem for $\mathrm{Gal}(E_S/E)$ is equivalent to an embedding problem of the form

$$(\mathrm{res}\colon \mathrm{Gal}(E_S/E) \to \mathrm{Gal}(F/E),\ \alpha\colon B \to \mathrm{Gal}(F/E)), \tag{7}$$

where F is a finite Galois extension of E in E_S, B is a finite group, and α is an epimorphism. The case $F = E$ being trivial, we may assume that F is a proper extension of E. Then the set T of all prime divisors of E/C ramified in F is finite and we have $F \subseteq E_T \subseteq E_S$. Since S is nonempty, we may extend F in E_S, if necessary, to assume that T is nonempty. By Theorem 9.5.7, there is a homomorphism $\gamma\colon \mathrm{Gal}(E_T/E) \to B$ such that $\alpha \circ \gamma = \mathrm{res}_{E_T/F}$. It follows that the homomorphism $\gamma' = \gamma \circ \mathrm{res}_{E_S/E_T}$ weakly solves embedding problem (7). Consequently, $\mathrm{Gal}(E_S/E)$ is a projective group. □

9.6 Maximal Unramified Extensions

Let C be an algebraically closed field, E a function field of one variable over C, and S a set of prime divisors of E/C. Theorem 9.5.7 states that $\mathrm{Gal}(E_S/E)$ is projective if S is nonempty. In this section we consider the case when S is empty and redenote E_S by E_{ur}. Thus E_{ur} is the maximal unramified extension of E. In this case Theorem 9.5.7 is false, that is $\mathrm{Gal}(E_{\mathrm{ur}}/E)$ is not projective. We prove it in two ways. The first method uses Proposition 9.2.1, hence the Riemann existence theorem. The second method is algebraic and involves the Jacobian of E.

PROPOSITION 9.6.1: *Let E be a function field of one variable over an algebraically closed field C of positive genus g. Then $\mathrm{Gal}(E_{\mathrm{ur}}/E)$ is not projective.*

First proof: Let $p = \mathrm{char}(C)$ and choose a prime number $l \neq p$. We denote the compositum of all finite unramified Galois extensions of E of degree not divisible by p by E'_{ur} and of an l-power degree by $E^{(l)}_{\mathrm{ur}}$. Then $E \subseteq E^{(l)}_{\mathrm{ur}} \subseteq E'_{\mathrm{ur}} \subseteq E_{\mathrm{ur}}$. Assume $\mathrm{Gal}(E_{\mathrm{ur}}/E)$ is projective. Then $\mathrm{Gal}(E^{(l)}_{\mathrm{ur}}/E)$, being the maximal pro-$l$ quotient of $\mathrm{Gal}(E_{\mathrm{ur}}/E)$, is also projective [FrJ08, Prop. 22.4.8], hence pro-l free [FrJ08, Prop. 22.7.6]. On the other hand, by Proposition 9.2.1(b), $\mathrm{Gal}(E'_{\mathrm{ur}}/E)$ is the free group generated by elements $\tau_1, \tau'_1, \ldots, \tau_g, \tau'_g$ with the defining relation

$$[\tau_1, \tau'_1] \cdots [\tau_g, \tau'_g] = 1 \tag{1}$$

in the category of profinite groups with order not divisible by p. Since $\mathrm{Gal}(E^{(l)}_{\mathrm{ur}}/E)$ is also the maximal pro-l quotient of $\mathrm{Gal}(E'_{\mathrm{ur}}/E)$, it is the free pro-$l$ group generated by elements $\tau_1, \tau'_1, \ldots, \tau_g, \tau'_g$ with the defining relation (1). Now choose a basis $t_1, t'_1, \ldots, t_g, t'_g$ for the $\mathbb{F}_l$-vector space $\mathbb{F}_l^{2g}$. The map $\tau_i \mapsto t_i$ and $\tau'_i \mapsto t'_i$ for $i = 1, \ldots, g$ extends to an epimorphism of $\mathrm{Gal}(E^{(l)}_{\mathrm{ur}}/E)$ onto $\mathbb{F}_l^{2g}$. Since the rank of the latter group is $2g$ and that of the former one is at most $2g$, we deduce that $\mathrm{rank}(E^{(l)}_{\mathrm{ur}}/E) = 2g$. It follows from [FrJ08, Lemma 17.4.6(b)] that $\tau_1, \tau'_1, \ldots, \tau_g, \tau'_g$, viewed as generators of $\mathrm{Gal}(E^{(l)}_{\mathrm{ur}}/E)$ form a basis of that group. Thus, every map of the basis into an l-group A extends to a homomorphism of $\mathrm{Gal}(E^{(l)}_{\mathrm{ur}}/E)$ into A. In particular, this is the case if we choose A to be noncommutative and a_1, a'_1 elements of A with $[a_1, a'_1] \neq 1$. Then the map $\tau_1 \mapsto a_1$, $\tau'_1 \mapsto a'_1$, $\tau_i \mapsto 1$, and $\tau'_i \mapsto 1$ for $i \geq 2$ extends to a homomorphism into A. It follows from (1) that $[a_1, a'_1] = 1$. This contradiction proves that $\mathrm{Gal}(E_{\mathrm{ur}}/E)$ is not projective. □

The second proof of Proposition 9.6.1 depends on the following piece of information.

LEMMA 9.6.2: *Let E be a function field of one variable of genus g over an algebraically closed field C. Let $l \neq \mathrm{char}(C)$ be a prime number and A the*

subgroup of $E^\times/(E^\times)^l$ consisting of all cosets $x(E^\times)^l$ such that $l|v_\mathfrak{p}(x)$ for all prime divisors $\mathfrak{p}$ of E/C. Then, $A \cong (\mathbb{Z}/l\mathbb{Z})^{2g}$.

Proof: We distinguish between two cases.

Case A: $g = 0$. Then $E = C(t)$ is the field of rational functions over C in an indeterminate t [FrJ08, Example 3.2.4]. In this case, each finite prime divisor of E/C has a prime element of the form $t - a$ with some $a \in C$. Thus, if $x(E^\times)^l \in A$, then $x = c\prod_{a\in C}(t-a)^{lk(a)}$ with $c \in C^\times$ and with $k(a) \in \mathbb{Z}$ such that $k(a) = 0$ for all but finitely many a's. Moreover, since C is algebraically closed, c is an l-power in C. Hence, $x(E^\times)^l$ is the unit element of $E^\times/(E^\times)^l$. Consequently, A is trivial.

Case B: $g \geq 1$. We consider the group $\mathrm{Div}_0(E/C)$ of divisors of E/C of degree 0, its subgroup $\mathrm{div}(E^\times)$ of principal divisors, and the Jacobian variety J of E/C (which exists since $\mathrm{genus}(E/C) > 0$). For each $x(E^\times)^l \in A$ there exists a divisor $\mathfrak{a}$ of E/C such that $\mathrm{div}(x) = l\mathfrak{a}$. It satisfies $0 = l\deg(\mathfrak{a})$, so $\deg(\mathfrak{a}) = 0$. We map $x(E^\times)^l$ onto $\mathfrak{a} + \mathrm{div}(E^\times)$. If $y \in E^\times$, then $\mathrm{div}(xy^l) = l(\mathfrak{a} + \mathrm{div}(y))$, so our map defines a homomorphism $\alpha\colon A \to \mathrm{Div}_0(E/C)/\mathrm{div}(E^\times)$. If $x(E^\times)^l \in \mathrm{Ker}(\alpha)$, then $\mathfrak{a} = \mathrm{div}(z)$ for some $z \in E^\times$, so $\mathrm{div}(xz^{-l}) = 0$. Hence, $xz^{-l} \in C^\times$ [FrJ08, Sec. 3.1]. Since C is algebraically closed, there exists $c \in C^\times$ such that $x = (cz)^l$. It follows that α is injective. Note that since $l\mathfrak{a} = \mathrm{div}(x)$, we have $l(\mathfrak{a} + \mathrm{div}(E^\times)) = 0$. Thus, the image of α lies in the subgroup $\mathcal{D}$ of $\mathrm{Div}_0(E/C)/\mathrm{div}(E^\times)$ of all elements annihilated by l. Conversely, if $\mathfrak{a} + \mathrm{div}(E^\times) \in \mathcal{D}$, then there exists $x \in E^\times$ such that $l\mathfrak{a} = \mathrm{div}(x)$, so $\alpha(x(E^\times)^l) = \mathfrak{a} + \mathrm{div}(E^\times)$. It follows that $\mathrm{Im}(\alpha) = \mathcal{D}$. Hence $A \cong \mathcal{D}$.

As mentioned in Subsection 6.3.2, there is an isomorphism

$$\mathrm{Div}_0(E/C)/\mathrm{div}(E^\times) \cong J(C).$$

Hence, $\mathcal{D} \cong J(C)_l$. By Subsection 6.3.1, $J(C)_l \cong (\mathbb{Z}/l\mathbb{Z})^{2g}$. Consequently, $A \cong (\mathbb{Z}/l\mathbb{Z})^{2g}$. □

Next we apply Kummer theory.

Lemma 9.6.3: *Let E be a function field of one variable over an algebraically closed field C and let $l \neq \mathrm{char}(C)$ be a prime number. Denote the maximal unramified pro-l extension of E by $E_{\mathrm{ur}}^{(l)}$ and set $g = \mathrm{genus}(E/C)$. Then* $\mathrm{rank}(\mathrm{Gal}(E_{\mathrm{ur}}^{(l)}/E)) = 2g$.

Proof: Denote the compositum of all cyclic unramified extensions of E of degree l by F. By [FrJ08, Lemma 22.7.4], $\mathrm{Gal}(E_{\mathrm{ur}}^{(l)}/F)$ is the Frattini subgroup of $\mathrm{Gal}(E_{\mathrm{ur}}^{(l)}/E)$ and $\mathrm{Gal}(F/E) \cong (\mathbb{Z}/l\mathbb{Z})^r$, where $r = \mathrm{rank}(\mathrm{Gal}(E_{\mathrm{ur}}^{(l)}/E))$. On the other hand, since E contains a root of unity of order l, each cyclic extension of E of degree l has the form $E(x^{1/l})$ with $x \in E^\times$. That extension is unramified over E if and only if $l|v_\mathfrak{p}(x)$ for each prime divisor $\mathfrak{p}$

of E/C [FrJ08, Example 2.3.8]. Thus, by Kummer Theory [Lan93, p. 295, Thm. 8.2], $\mathrm{Gal}(F/E) \cong A$, where A is as in Lemma 9.6.2, hence by that lemma $\mathrm{Gal}(F/E) \cong (\mathbb{Z}/l\mathbb{Z})^{2g}$. Combining that with the opening statement of the proof, we conclude that $\mathrm{rank}(E_{\mathrm{ur}}^{(l)}/E) = 2g$. □

PROPOSITION 9.6.1: *Let E be a function field of one variable over an algebraically closed field C of positive genus g. Then $\mathrm{Gal}(E_{\mathrm{ur}}/E)$ is not projective.*

Second proof: Let $p = \mathrm{char}(C)$ and choose a prime number $l \neq p$. We denote the compositum of all finite unramified Galois extensions of E of degree not divisible by p by E'_{ur} and of an l-power degree by $E_{\mathrm{ur}}^{(l)}$. Then $E \subseteq E_{\mathrm{ur}}^{(l)} \subseteq E'_{\mathrm{ur}} \subseteq E_{\mathrm{ur}}$. Assume that $\mathrm{Gal}(E_{\mathrm{ur}}/E)$ is projective. Then $G = \mathrm{Gal}(E_{\mathrm{ur}}^{(l)}/E)$, being the maximal pro-$l$ quotient of $\mathrm{Gal}(E_{\mathrm{ur}}/E)$, is also projective [FrJ08, Prop. 22.4.8], hence pro-l free [FrJ08, Prop. 22.7.6]. By Lemma 9.6.3, $\mathrm{rank}(G) = 2g$.

Now we choose a proper finite extension F of E in $E_{\mathrm{ur}}^{(l)}$ and set $h = \mathrm{genus}(F/C)$. Since F is unramified over E, Riemann-Hurwitz genus formula simplifies to $2h - 2 = [F : E](2g - 2)$ (Remark 5.8.1(f)). hence

$$h - 1 = [F : E](g - 1). \tag{2}$$

On the other hand, $H = \mathrm{Gal}(E_{\mathrm{ur}}^{(l)}/F)$ is an open subgroup of G of index $[F : E]$. Hence, by Nielsen-Schreier [FrJ08, Prop. 17.5.7], $\mathrm{rank}(H) - 1 = [F : E](\mathrm{rank}(G) - 1)$. Note that $F_{\mathrm{ur}}^{(l)} = E_{\mathrm{ur}}^{(l)}$, so by Lemma 9.6.3, $\mathrm{rank}(H) = 2h$. Hence,

$$2h - 1 = [F : E](2g - 1) \tag{3}$$

Substituting the value of h from (2) in (3) leads to $[F : E] = 1$. This contradiction to our assumption proves that $\mathrm{Gal}(E_{\mathrm{ur}}/E)$ is not projective. □

9.7 Embedding Problems with Given Branching

We fix for the whole section a rational function field $E = C(x)$ over an algebraically closed field C. Assume that C is complete with respect to an ultrametric absolute value. We show in this section how to solve finite split embedding problems with an extra information on the branch points of the solution fields. This prepares the way in the next section to prove for general C that $\mathrm{Gal}(E_S/E)$ is free of rank m, if $|S| = m = \mathrm{card}(C)$.

LEMMA 9.7.1: *For each integer $n > 1$ there exists a cyclic extension F/E of degree n such that $\mathrm{Branch}(F/E) = \{1, \infty\}$.*

Proof: The lemma follows from Lemma 4.2.5 by applying a suitable Möbius transformation. Nevertheless, we supply a direct proof to the special case at hand.

If $\mathrm{char}(C) \nmid n$, let $F = E(y)$, where $y^n = x - 1$. If $n = p = \mathrm{char}(C) > 0$, let $F = E(y)$, where $y^p - y = \frac{x^2}{x-1}$. Then $\mathrm{Branch}(F/E) = \{1, \infty\}$ [FrJ08, Examples 2.3.8 and 2.3.9]. In each case F/E is a cyclic extension of degree n.

The rest of the proof reduces the general case to these two cases.

PART A: *Without loss of generality n is a prime power.* Indeed, if $n = \prod_{i=1}^m p_i^{r_i}$, where $p_1, \ldots, p_m$ are distinct primes, and for each $1 \le i \le m$ there is a cyclic extension F_i/E of degree $p_i^{r_i}$, ramified at $\{1, \infty\}$ and unramified elsewhere, then the compositum $F = \prod_{i=1}^m F_i$ has the required properties.

PART B: *Without loss of generality n is prime.* Indeed, assume that n is a power of a prime p and there is a cyclic extension F_1/E of degree p, whose branch points are $1, \infty$. Let $S = \{1, \infty\}$. By Theorem 9.5.7, the embedding problem

$$(\alpha\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathrm{Gal}(F_1/E),\ \mathrm{res}\colon \mathrm{Gal}(E_S/E) \to \mathrm{Gal}(F_1/E))$$

for $\mathrm{Gal}(E_S/E)$ has a weak solution, say, $\psi\colon \mathrm{Gal}(E_S/E) \to \mathbb{Z}/n\mathbb{Z}$. But ψ is surjective, because $\alpha(\psi(\mathrm{Gal}(E_S/E))) = \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ is the only subgroup H of $\mathbb{Z}/n\mathbb{Z}$ with $\alpha(H) = \mathbb{Z}/p\mathbb{Z}$. The fixed field F of $\mathrm{Ker}(\psi)$ has the required properties. □

LEMMA 9.7.2: *Suppose C is complete with respect to an ultrametric absolute value $|\ |$. Let $c \in C$, $r \in C^\times$, and set $w = \frac{r}{x-c}$. Let $n > 1$ be an integer. Then there exists $0 < \varepsilon < |r|$ such that for all distinct $b_1, b_2 \in C$ with $|b_1 - c|, |b_2 - c| \le \varepsilon$ there is a cyclic extension F/E of degree n, with $\mathrm{Branch}(F/E) = \{b_1, b_2\}$ and $F \subseteq \mathrm{Quot}(C\{w\})$.*

Proof: Lemma 9.7.1 gives a cyclic extension F_1/E of degree n with $\mathrm{Branch}(F_1/E) = \{1, \infty\}$. Since F_1/E is unramified at 0 and C is algebraically closed, we have $F_1 \subset C((x))$. Let y be a primitive element of F_1/E integral over $C[x]$. By Proposition 2.4.5, y converges at some point $b \in C$. Thus, if we write $y = \sum_{n=0}^\infty a_n x^n$, then the series $\sum_{n=0}^\infty a_n b^n$ converges. Set $\varepsilon = \min(1, |rb|, \frac{|r|}{2})$. Then for each $a \in C^\times$ with $|a| \le |rb|$ we have $\mu_a(y) = \sum_{n=0}^\infty a_n a^n x^n = \sum_{n=0}^\infty a_n \left(\frac{a}{r}\right)^n (rx)^n$, so the latter series in rx converges. This means that $\mu_a(y) \in C\{rx\}$ and $\mu_a(F_1) \subseteq \mathrm{Quot}(C\{rx\})$.

Let $b_1, b_2 \in C$ such that $|b_1 - c|, |b_2 - c| \le \varepsilon$. Set $a = b_2 - b_1$ and $F_2 = \mu_a(F_1)$. Then $|a| \le \varepsilon \le |rb|$, so $F_2 \subseteq \mathrm{Quot}(C\{rx\})$. By Remark 4.1.4,

$$\begin{aligned}\mathrm{Branch}(F_2/E) &= (\mu_a')^{-1}(\mathrm{Branch}(F_1/E)) \\ &= \frac{1}{a}\{1, \infty\} = \{\frac{1}{b_2 - b_1}, \infty\}.\end{aligned}$$

Let θ be the C-automorphism of E given by $\theta(x) = \frac{1}{x-c}$, so that $\theta(rx) = w$. Extend θ to an isomorphism of fields $\theta\colon F_2 \to F_3$. Then $F_3 \subseteq \mathrm{Quot}(C\{w\})$

and by Remark 4.1.4,

$$\begin{aligned}\mathrm{Branch}(F_3/E) &= (\theta')^{-1}(\mathrm{Branch}(F_2/E))\\ &= (\theta')^{-1}\{\frac{1}{b_2-b_1},\infty\} = \{c+b_2-b_1,c\}.\end{aligned}$$

Let $d = c - b_1$. Then $|d| \le \varepsilon \le 1$. Let λ be the automorphism of $C\{w\}$ that maps $f = \sum_{n=0}^{\infty} a_n w^n$ onto

$$\begin{aligned}\lambda(f) = \sum_{n=0}^{\infty} a_n(w+d)^n &= \sum_{n=0}^{\infty} a_n \sum_{k=0}^{n} \binom{n}{k} d^{n-k}w^k\\ &= \sum_{k=0}^{\infty}\Big(\sum_{n=k}^{\infty}\binom{n}{k}a_n d^{n-k}\Big)w^k.\end{aligned}$$

Then $\binom{n}{k}a_n d^{n-k} \to 0$ as $n \to \infty$, so the series $\sum_{n=k}^{\infty}\binom{n}{k}a_n d^{n-k}$ converges in C, hence λ is well defined. Moreover,

$$\Big|\sum_{n=k}^{\infty}\binom{n}{k}a_n d^{n-k}\Big| \le \max_{n\ge k}|a_n|.$$

We extend λ to an automorphism of $\mathrm{Quot}(C\{w\})$. The restriction of λ to E is the map $w \mapsto w + d$. Let $F = \lambda(F_3)$. Then $F \subseteq \mathrm{Quot}(C\{w\})$ and

$\mathrm{Branch}(F/E) = (\lambda')^{-1}(\mathrm{Branch}(F_3/E)) = \{c+b_2-b_1-d, c-d\} = \{b_2, b_1\}$. □

Remark 9.7.3: A **disk** in $C \cup \{\infty\}$ is a set of the form

$$D = \theta(\{a \in C \mid |a| \le \varepsilon\})$$

where $\varepsilon > 0$ and θ is a Möbius transformation over C. Thus, each set of the form $D = \{a \in C \mid |a-c| \le \varepsilon\}$ or $D = \{a \in C \mid |a| \ge \varepsilon\} \cup \{\infty\}$, where $c \in C$, is a disk. (In fact, each disk is of this form; but we shall not use this fact.) Note that the cardinality of a disk is the same as the cardinality of C. □

Lemma 9.7.4: *Assume C is complete with respect to an ultrametric absolute value. Let F_1/E be a finite Galois extension with group G_1 and*

$$\alpha\colon G = G_1 \ltimes H \to G_1 = \mathrm{Gal}(F_1/E) \tag{1}$$

a finite split embedding problem for $\mathrm{Gal}(E)$ with a nontrivial kernel H. Consider a finite set J that does not contain 1 and let $\{G_i\}_{i\in J}$ be a finite family of nontrivial cyclic subgroups of G that generate H. Then there exists a family of pairwise disjoint disks $\{D_i\}_{i\in J}$ in C such that for every $B \subset \bigcup_{i\in J} D_i$ with $\mathrm{card}(B \cap D_i) = 2$ for each $i \in J$, there exists a solution field F of (1) with $\mathrm{Branch}(F^{G_1}/E) = B$.

Proof: Let $I = J \cup \{1\}$. Then $G = \langle G_i \mid i \in I\rangle$. We choose distinct elements $c_i \in C$, $i \in I$, and an element $r \in C^\times$ with $|r| \le |c_i - c_j|$ for all distinct $i, j \in I$. Then let $w_i = \frac{r}{x-c_i}$, $P_i = \mathrm{Quot}(C\{w_j \mid j \ne i\})$ and $P_i' = \mathrm{Quot}(C\{w_i\})$.

CLAIM: *We may assume that* $F_1 \subseteq P_1'$. Indeed, since C is algebraically closed, every prime divisor of F_1/C is of degree 1. In particular, F_1/C has an unramified prime divisor of degree 1. By Lemma 4.3.7, there is a C-automorphism of E that extends to an embedding $\theta\colon F_1 \to P_1'$. Let $F_1' = \theta(F_1)$ and extend θ to an automorphism of E_s. Then θ defines isomorphisms $\theta_*\colon \mathrm{Gal}(F_1/E) \to \mathrm{Gal}(F_1'/E)$ and $\theta_*\colon \mathrm{Gal}(E) \to \mathrm{Gal}(E)$ such that the following diagram commutes

$$\begin{array}{ccccc} & & \mathrm{Gal}(E) & \xrightarrow{\theta_*} & \mathrm{Gal}(E) \\ & & \big\downarrow{\scriptstyle \mathrm{res}} & & \big\downarrow{\scriptstyle \mathrm{res}} \\ G & \xrightarrow{\alpha} & \mathrm{Gal}(F_1/E) & \xrightarrow{\theta_*} & \mathrm{Gal}(F_1'/E). \end{array}$$

Suppose that there is a family of disjoint disks $\{D_i'\}_{i\in J}$ in C such that for every $B' \subset \bigcup_{i\in J} D_i'$ with $\mathrm{card}(B' \cap D_i') = 2$, for each $i \in J$, the embedding problem

$$(\theta_* \circ \alpha\colon G \to \mathrm{Gal}(F_1'/E),\ \mathrm{res}\colon \mathrm{Gal}(E) \to \mathrm{Gal}(F_1'/E))$$

has a solution field F' with $\mathrm{Branch}(F'^{G_1}/E) = B'$. Let θ' be the permutation of $C \cup \{\infty\}$ induced by θ as in Remark 4.1.4. Then the disks $D_i = \theta'(D_i)$, for $i \in J$, have the required property.

Indeed, if $B \subset \bigcup_{i\in J} D_i$ and $\mathrm{card}(B \cap D_i) = 2$, for each $i \in J$, we put $B' = (\theta')^{-1}(B)$, let F' be as above, and extend θ to an automorphism of E_s. Then $F = \theta^{-1}(F')$ solves (1) and $\theta(F^{G_1}) = F'^{G_1}$. By Remark 4.1.4,

$$\theta'(\mathrm{Branch}(F'^{G_1}/E)) = \mathrm{Branch}(F^{G_1}/E).$$

Hence, $B = \mathrm{Branch}(F^{G_1}/E)$, as desired.

Thus, replacing F_1 by F_1' we may assume that $F_1 \subseteq P_1'$.

By Lemma 9.7.2, there is an $0 < \varepsilon < |r|$ such that the (necessarily disjoint) disks $D_i = \{a \in C \mid |a - c_i| \le \varepsilon\}$, for $i \in J$, have the following property: For every $B \subset \bigcup_{i\in J} D_i$ with $\mathrm{card}(B \cap D_i) = 2$, for each $i \in J$, there exist Galois extensions F_i/E with the cyclic Galois group G_i and $\mathrm{Branch}(F_i/E) = B \cap D_i$ and $F_i \subseteq \mathrm{Quot}(C\{w_i\}_{i\in I})$, for each $i \in J$. Let $P = \mathrm{Quot}(C\{w_i\}_{i\in I})$.

By Proposition 3.4.5, $\mathcal{E} = (E, F_i, P_i, Q; G_i, G)_{i\in I}$ is patching data. Its compound F is, by Lemma 1.3.1(c), a Galois extension of E that solves (1). By Lemma 7.2.3(c),

$$\mathrm{Branch}(F^{G_1}/E) = \bigcup_{i\in J} \mathrm{Branch}(F_i/E) = \bigcup_{i\in J} B \cap D_i = B. \qquad \square$$

9.8 Descent

We wish to apply Lemma 9.7.4 to a sufficiently large complete extension of a given algebraically closed field. Thus we consider the following situation. Let $C_1 \subseteq C_2$ be two algebraically closed fields and x an intermediate. We set $E_1 = C_1(x)$, $E_2 = C_2(x)$, and let

$$\rho\colon G = G_1 \ltimes H \to G_1 = \mathrm{Gal}(F_1/E_1) \tag{1}$$

be a finite split embedding problem for $\mathrm{Gal}(E_1)$ with a nontrivial kernel H. Let $F_2 = F_1E_2$. Then the restriction map $\mathrm{Gal}(F_2/E_2) \to \mathrm{Gal}(F_1/E_1)$ is an isomorphism. We identify $\mathrm{Gal}(F_2/E_2)$ with $G_1 = \mathrm{Gal}(F_1/E_1)$ via this map. Then (1) induces a finite split embedding problem

$$\rho\colon G = G_1 \ltimes H \to G_1 = \mathrm{Gal}(F_2/E_2) \tag{2}$$

for $\mathrm{Gal}(E_2)$ with a nontrivial kernel.

Before dealing with embedding problems let us notice a simple fact:

Remark 9.8.1: Let A be an infinite subset of a field K. Then every nonempty Zariski K-open subset of $\mathbb{A}^n$ meets A^n. Indeed, the only polynomial in n variables over K that vanishes on A^n is 0. □

Lemma 9.8.2: *Let A be an infinite subset of C_1. Suppose (2) has a solution field L_2 such that $\infty \notin \mathrm{Branch}(L_2^{G_1}/E_2)$ and the elements of $\mathrm{Branch}(L_2^{G_1}/E_2)$ are algebraically independent over C_1. Then (1) has a solution field L_1 with $\mathrm{Branch}(L_1^{G_1}/E_1) \subseteq A$.*

Proof: There is an irreducible monic polynomial $h \in C_2[x, Z]$ such that $L_2 = E_2(z)$, with $h(x, z) = 0$. Furthermore, there are irreducible polynomials $f_1, \ldots, f_r \in C_2[x, Z]$ such that a root z_j of f_j is a primitive element of $L_2^{G_1}/E_2$ (hence also of L_2/F_2), and

$$\mathrm{Branch}(L_2^{G_1}/E_2) = \bigcap_{j=1}^{r} \mathrm{Zero}(\mathrm{discr}(f_j)) \tag{3}$$

[Has80, p. 64].

We set $\mathrm{Branch}(L_2^{G_1}/E_2) = \{u_1, \ldots, u_k\}$ and choose $u_{k+1}, \ldots, u_l \in C_2$ such that $h, f_1, \ldots, f_r \in C_1[\mathbf{u}][x, Z]$. We also set $E_{\mathbf{u}} = C_1(\mathbf{u}, x)$, $F_{\mathbf{u}} = F_1(\mathbf{u})$ and add more elements of C_2 to $\{u_1, \ldots, u_l\}$, if necessary, such that $L_{\mathbf{u}} = E_{\mathbf{u}}(z)$ is a Galois extension of $E_{\mathbf{u}}$ that solves the embedding problem $G \to \mathrm{Gal}(F_{\mathbf{u}}/E_{\mathbf{u}})$ induced from (1), and $L_{\mathbf{u}}^{G_1} = E_{\mathbf{u}}(z_j)$, $j = 1, \ldots, r$.

Let $U = \mathrm{Spec}(C_1[\mathbf{u}])$ be the irreducible variety that $\mathbf{u}$ generates over C_1. For each $\mathbf{u}' \in U(C_1)$ the C_1-specialization $\mathbf{u} \to \mathbf{u}'$ first extends to an F_1-place $'\colon F_{\mathbf{u}} \to F_1 \cup \{\infty\}$, and then to a place $'\colon L_{\mathbf{u}} \to \tilde{E}_1 \cup \{\infty\}$. Let $B = \{u_1', \ldots, u_k'\} \subset C_1$ be the image of $\mathrm{Branch}(L_2^{G_1}/E_2) = \{u_1, \ldots, u_k\}$.

The variety U has a nonempty Zariski-open subset U' such that for all $\mathbf{u}' \in U'$ the following statements hold:

(4a) $h', f_1', \dots, f_r' \in C_1[x, Z]$ are irreducible over $C_1(x)$ [FrJ08, Prop. 9.4.3];
(4b) $L_1 = E_1(z')$ is Galois over E_1 and L_1 solves embedding problem (1) [FrJ08, Lemma 13.1.1];
(4c) the respective roots $z_1', \dots, z_r'$ of $f_1', \dots, f_r'$ are primitive elements for $L_1^{G_1}/E_1$.

From (3), $B = \bigcap_{j=1}^r \mathrm{Zero}(\mathrm{discr}(f_j'))$. Since $L_1^{G_1}/E_1$ is unramified at each point outside $\mathrm{Zero}(\mathrm{discr}(f_j'))$, $j = 1, \dots, r$ (by [Has80, p. 64]),

(4d) $\mathrm{Branch}(L_1^{G_1}/E_1) \subseteq B$.

By assumption, $u_1, \dots, u_k$ are algebraically independent over C_1. Therefore, the projection on the first k coordinates pr: $U \to \mathbb{A}^k$ is a dominant map, hence $\mathrm{pr}(U')$ contains a Zariski-open subset of $\mathbb{A}^k$ [Lan58, p. 88, Prop. 4]. By Remark 9.8.1, we may choose $\mathbf{u}' \in U'(C_1) \cap \mathrm{pr}^{-1}(A^k)$, so $B = \{u_1', \dots, u_k'\} \subset A$. Consequently, $\mathrm{Branch}(L_1^{G_1}/E_1) \subseteq A$. □

To achieve the algebraic independence in Lemma 9.8.2 we use:

LEMMA 9.8.3: *Let $C_1 \subset C_2$ be two algebraically closed fields such that $\mathrm{card}(C_1) < \mathrm{card}(C_2)$. Let $\{D_j\}_{j \in J}$ be a finite collection of pairwise disjoint subsets of C_2 of cardinality $\mathrm{card}(C_2)$. Then there exists a set $B \subseteq \bigcup_{j \in J} D_j$ such that $\mathrm{card}(B \cap D_j) = 2$ for each $j \in J$ and the elements of B are algebraically independent over C_1.*

Proof: Write J as $\{1, \dots, k\}$, and suppose, by induction, that we have already found $b_j, b_j' \in D_j$, for $j = 1, \dots, k-1$, such that $b_1, b_1', \dots, b_{k-1}, b_{k-1}'$ are algebraically independent over C_1. The cardinality of the algebraic closure C_1' of $C_1(b_1, b_1', \dots, b_{k-1}, b_{k-1}')$ in C_2 is $\mathrm{card}(C_1) < \mathrm{card}(C_2) = \mathrm{card}(D_k)$, so there exist $b_k, b_k' \in D_k$ algebraically independent over C_1'. Thus, $b_1, b_1', \dots, b_k, b_k'$ are algebraically independent over C_1. □

LEMMA 9.8.4: *Let G be a projective group of rank m. Set $m' = 1$ if $m = \aleph_0$ and $m' = m$ if $m > \aleph_0$. Suppose every finite split embedding problem for G with a nontrivial kernel has m' solutions. Then $G \cong \hat{F}_m$.*

Proof: The case where $m > \aleph_0$ is settled in [FrJ08, Lemma 21.5.8]. Consider the case where $m = \aleph_0$. By Iwasawa, it suffices to prove that every finite embedding problem

$$(\varphi\colon G \to A,\ \alpha\colon B \to A) \tag{5}$$

is solvable [FrJ08, Cor. 24.8.3]. Indeed, since G is projective, there exists a homomorphism $\gamma\colon G \to B$ with $\alpha \circ \gamma = \varphi$. Then $\mathrm{Ker}(\gamma)$ is an open normal subgroup of G, so $\hat{A} = G/\mathrm{Ker}(\gamma)$ is a finite group. Let $\hat{\varphi}\colon G \to \hat{A}$ be the quotient map and $\bar{\varphi}\colon \hat{A} \to A$ and $\hat{\gamma}\colon \hat{A} \to B$ the homomorphisms induced by φ and γ, respectively. In particular $\alpha \circ \hat{\gamma} = \bar{\varphi}$. Next consider the fiber product $\hat{B} = B \times_A \hat{A}$ with the corresponding projections $\beta\colon \hat{B} \to B$ and $\hat{\alpha}\colon \hat{B} \to \hat{A}$. The defining property of the fiber product gives a homomorphism $\hat{\alpha}'\colon \hat{A} \to \hat{B}$ such that $\hat{\alpha} \circ \hat{\alpha}' = \mathrm{id}_{\hat{A}}$. In other words, $\hat{\alpha}$ splits. By assumption there exists

an epimorphism $\delta\colon G \to \hat{B}$ such that $\hat{\alpha} \circ \delta = \hat{\varphi}$. Thus, $\beta \circ \delta$ solves embedding problem (5). Consequently, $G \cong \hat{F}_\omega$. □

The preceding lemmas yield the main result of this chapter:

THEOREM 9.8.5: *Let C be an algebraically closed field of cardinality m, $E = C(x)$ the field of rational functions over C, and S a subset of $C \cup \{\infty\}$ of cardinality m. Then $\mathrm{Gal}(E_S/E)$ is isomorphic to the free profinite group of rank m.*

Proof: Put $C_1 = C$ and $E_1 = E$. By Corollary 9.5.8, $\mathrm{Gal}(E_S/E)$ is projective. Therefore, by Lemma 9.8.4, it suffices to show that every finite split embedding problem (1) for $\mathrm{Gal}(E_S/E)$ with a nontrivial kernel has m' solution fields, where $m' = 1$ if $m = \aleph_0$, and $m' = m$ otherwise.

Let $\beta < m$ be an ordinal number. Suppose, by transfinite induction, that $\{N_\alpha\}_{\alpha<\beta}$ is a family of distinct solution fields of (1). For each α, the set $\mathrm{Branch}(N_\alpha/E)$ is finite. Hence, $A = S \setminus \bigcup_{\alpha<\beta} \mathrm{Branch}(N_\alpha/E)$ is infinite.

We choose an algebraically closed field C_2 that contains C and is complete with respect to a nontrivial ultrametric absolute value such that $\mathrm{card}(C) < \mathrm{card}(C_2)$. For instance, choose a field C' that contains C such that $\mathrm{card}(C) < \mathrm{card}(C')$, and let C_2 be the completion of the algebraic closure of $C'((t))$. We consider the induced embedding problem (2).

Let $\{G_j \mid j \in J\}$ be a nonempty set of nontrivial cyclic groups that generate H with $1 \notin J$. By Lemma 9.7.4, there exists a family of disks $\{D_j\}_{j\in J}$ in C_2 such that for every $B \subset \bigcup_{j\in J} D_j$ with $\mathrm{card}(B \cap D_j) = 2$ for each $j \in J$ there exists a solution field L_2 to (2) with $\mathrm{Branch}(L_2^{G_1}/C_2(x)) = B$. We choose such a set B. By Remark 9.7.3, $\mathrm{card}(D_j) = \mathrm{card}(C_2)$. By Lemma 9.8.3, we may assume that the elements of B are algebraically independent over C. Therefore, by Lemma 9.8.2, (1) has a solution field $N = N_\beta$ such that $\mathrm{Branch}(N^{G_1}/E) \subseteq A$.

Since $N = F_1 N^{G_1}$, we have

$$\mathrm{Branch}(N/E) = \mathrm{Branch}(F_1/E) \cup \mathrm{Branch}(N^{G_1}/E)$$

(Remark 4.1.1). Furthermore,

$$\mathrm{Branch}(F_1/E), \mathrm{Branch}(N^{G_1}/E) \subseteq S,$$

so $\mathrm{Branch}(N/E) \subseteq S$. Since $\mathrm{Branch}(N^{G_1}/E) \subseteq A$, we have

$$\mathrm{Branch}(N^{G_1}/E) \cap \mathrm{Branch}(N_\alpha/E) = \emptyset$$

for each $\alpha < \beta$. In addition, $[N^{G_1} : E] = |H| > 1$, so by the Riemann-Hurwitz genus formula (Remark 5.8.1(f)), $\mathrm{Branch}(N^{G_1}/E) \neq \emptyset$. Since

$$\mathrm{Branch}(N^{G_1}/E) \subset \mathrm{Branch}(N/E),$$

it follows that $\mathrm{Branch}(N/E) \neq \mathrm{Branch}(N_\alpha/E)$ for each $\alpha < \beta$. Consequently $N \neq N_\alpha$ for each $\alpha < \beta$. □

Remark 9.8.6: Fundamental groups. In the special case of Theorem 9.8.5, where S is the set of all prime divisors, $C(x)_S = C(x)_s$. Thus, $\mathrm{Gal}(C(x)) \cong \hat{F}_m$. If F is a finite extension of $C(x)$, then $\mathrm{Gal}(F)$ is isomorphic to an open subgroup of $\mathrm{Gal}(C(x))$, so $\mathrm{Gal}(F) \cong \hat{F}_m$ [FrJ08, Prop. 25.2.2]. It follows that Theorem 9.8.5 is essentially a generalization of Corollary 9.4.9.

One may try to generalize the latter observation to a proper finite extension F of $C(x)$ and a set S of prime divisors of F/C of cardinality $\mathrm{card}(C)$. Let T be the set of all prime divisors of $C(x)/C$ that lie under S and those that ramify in F. Then $F_S \subseteq C(x)_T$, so $\mathrm{Gal}(C(x)_T/F)$ is an open subgroup of $\mathrm{Gal}(C(x)_T/C(x))$. By Theorem 9.8.5 and [FrJ08, Prop. 25.2.2], $\mathrm{Gal}(C(x)_T/F) \cong \hat{F}_m$. However, $\mathrm{Gal}(F_S/F)$ might be a proper quotient of $\mathrm{Gal}(C(x)_T/F)$, so our methods fail to prove that the latter group is also isomorphic to $\hat{F}_m$.

Nevertheless, using formal patching, Harbater proved that $\mathrm{Gal}(F_S/F) \cong \hat{F}_m$ if the complement of S is finite [Hrb95, Thm. 4.4]. Using rigid analytic patching, Pop proved the latter isomorphism under the weaker condition that $\mathrm{card}(S) = m$ [Pop95, p. 556, Thm. A]. Note that both Harbater and Pop consider a smooth projective model X for F/C, reinterpret S as a subset of $X(C)$, call $\mathrm{Gal}(F_S/F)$ the **fundamental group of** $X \smallsetminus S$, and denote it by $\Pi(X \smallsetminus S)$. □

9.9 Fundamental Groups with S Finite

We consider again a function field E of one variable of genus g over an algebraically closed field C of characteristic p. Let S be a finite nonempty set of prime divisors of E/C. As before we denote the maximal Galois extension of E ramified at most over S by E_S. By Corollary 9.1.7, $\mathrm{Gal}(E_S/E)$ is a free profinite group if $p = 0$. We prove in this section that this is false if $p > 0$.

For each prime number l we denote the maximal pro-l extension of E which is ramified at most over S by $E_S^{(l)}$.

LEMMA 9.9.1: *Let E be a function field of one variable over an algebraically closed field C, S a finite nonempty set of prime divisors of E/C, and l a prime number. Then $\mathrm{Gal}(E_S^{(l)}/E)$ is a free pro-l group.*

Proof: The group $\mathrm{Gal}(E_S^{(l)}/E)$ is the maximal pro-l quotient of $\mathrm{Gal}(E_S/E)$. By Theorem 9.5.7, the latter group is projective. Hence, by [FrJ08, Prop. 22.4.8], so is the former. Alternatively, one may repeat the proof of Theorem 9.5.7. □

LEMMA 9.9.2: *Let C be an infinite field of positive characteristic p and cardinality m. Let E be a function field of one variable over C and S a nonempty set of prime divisors of E/C. Then $\mathrm{rank}(\mathrm{Gal}(E_S^{(p)}/E)) = m$.*

Proof: Since $\mathrm{card}(E) = m$, the field E has at most m finite extensions in $E_S^{(p)}$, hence $\mathrm{rank}(\mathrm{Gal}(E_S^{(p)}/E)) \leq m$ [FrJ08, Prop. 17.1.2]. Thus, it suffices to

prove that $\mathrm{rank}(\mathrm{Gal}(E_S^{(p)}/E)) \geq m$. The rest of the proof breaks up into two parts.

PART A: *Assume $E = C(x)$ with a transcendental element x over C.* Since $\mathrm{Gal}(C(x)_S^{(p)}/C(x))$ is a pro-p group, it suffices to construct m linearly disjoint cyclic extensions in $C(x)_S$ of degree p [FrJ08, Lemma 22.7.1].

We apply a Möbius transformation on $C(x)$, if necessary, to assume that the pole $\mathfrak{p}_{x,\infty}$ of x belongs to S. Then $C(x)^{(p)}_{\{\mathfrak{p}_{x,\infty}\}} \subseteq C(x)_S^{(p)}$. Therefore, we may further assume that $S = \{\mathfrak{p}_{x,\infty}\}$. Since C is infinite, the dimension of C as a vector space over $\mathbb{F}_p$ is m. Let B be a basis of C over $\mathbb{F}_p$. For each $b \in B$ let y_b be an element of $C(x)_s$ such that $y_b^p - y_b = bx$. Then $C(x, y_b)$ is a cyclic extension of degree p. Moreover, since $\mathfrak{p}_{x,\infty}$ is the only pole of bx, no prime divisor of $C(x)/C$ but $\mathfrak{p}_{x,\infty}$ is ramified in $C(x, y_b)$. This means that $C(x, y_b) \subseteq C(x)_S^{(p)}$. To conclude the proof we have now to prove that the elements of Bx are linearly independent over $\mathbb{F}_p$ modulo $\wp(C(x))$ (Statement (3d) of Section 9.5).

To that end consider distinct elements $b_1, \ldots, b_n$ of B and arbitrary elements $\beta_1, \ldots, \beta_n \in \mathbb{F}_p$. Assume there exists $u \in C(x)$ with

$$\sum_{i=1}^{n} \beta_i b_i x = u^p - u. \tag{1}$$

Then u is integral over $C[x]$, and because $C[x]$ is integrally closed, $u \in C[x]$. If $\deg(u) \geq 1$, then the degree of the right hand side of (1) is greater than 1 while the degree of the left hand side of (1) is 1. If $\deg(u) = 0$, then $\sum_{i=1}^{n} \beta_i b_i = 0$. Consequently, $\beta_i = 0$ for each i, as contended.

PART B: *The general case.* We choose a transcendental element x of E over C and denote the set of prime divisors of $C(x)/C$ lying under S by T. By Part A, $\mathrm{rank}(\mathrm{Gal}(C(x)_T^{(p)}/C(x))) = m$. Since E is a finite extension of $C(x)$, so is $E_0 = C(x)_T^{(p)} \cap E$, hence $\mathrm{Gal}(C(x)_T^{(p)}/E_0)$ is an open subgroup of $\mathrm{Gal}(C(x)_T^{(p)}/C(x))$, hence $\mathrm{rank}(\mathrm{Gal}(C(x)_T^{(p)}/E_0)) = m$ [FrJ08, Cor. 17.1.5]. Now observe that $C(x)_T^{(p)} \subseteq E_S^{(p)}$, so $\mathrm{Gal}(C(x)_T^{(p)}/E_0)$ is a quotient of the group $\mathrm{Gal}(E_S^{(p)}/E)$. Therefore, by [FrJ08, Cor. 17.1.4], $\mathrm{rank}(\mathrm{Gal}(E_S^{(p)}/E)) \geq m$, as contended. □

LEMMA 9.9.3: *Let C be an algebraically closed field, E a function field of one variable over C, S a finite set of prime divisors of E/C, and l a prime number that does not divide* $\mathrm{char}(C)$. *Then* $\mathrm{rank}(\mathrm{Gal}(E_S^{(l)}/E)) < \infty$.

Proof: Let E' be the compositum of all cyclic extensions of E of degree l in $E_S^{(l)}$. Since $\mathrm{Gal}(E_S^{(l)}/E')$ is a pro-l group and $\mathrm{Gal}(E_S^{(l)}/E')$ is the Frattini subgroup of $\mathrm{Gal}(E_S^{(l)}/E)$, the rank of $\mathrm{Gal}(E_S^{(l)}/E)$ is equal to that of

$\mathrm{Gal}(E'/E)$ [FrJ08, Lemma 22.7.4]. Thus, it suffices to prove that $\mathrm{Gal}(E'/E)$ is finite.

Let S' be the complement of S in the set of all prime divisors of E/C. Denote the subgroup of $E^\times$ consisting of all elements x satisfying $l|v_\mathfrak{p}(x)$ for all $\mathfrak{p} \in S'$ by B'. Then $E' = E(x^{1/l} \mid x \in B')$ [FrJ08, Example 2.3.8]. Let B be the subgroup of $E^\times/(E^\times)^l$ consisting of all $x(E^\times)^l$ with $x \in B'$. By Kummer theory [Lan93, p. 294, Thm. 8.1], $B \cong \mathrm{Gal}(E'/E)$. Thus, we have to prove that B is finite.

To that end consider the map $\nu\colon B \to (\mathbb{Z}/l\mathbb{Z})^S$ defined by

$$\nu(x(E^\times)^l) = (v_\mathfrak{p}(x) + l\mathbb{Z})_{\mathfrak{p}\in S}.$$

Then $\mathrm{Ker}(\nu)$ consists of all left classes $x(E^\times)^l$ such that $l|v_\mathfrak{p}(x)$ for all prime divisors of E/C. By Lemma 9.6.2, $\mathrm{Ker}(\nu)$ is finite. Since $(\mathbb{Z}/l\mathbb{Z})^S$ is finite, it follows that B is also finite. □

PROPOSITION 9.9.4: *Let C be an algebraically closed field of positive characteristic, E a function field of one variable over C, and S a set of prime divisors of E/C with $\mathrm{card}(S) < \mathrm{card}(C)$. Suppose that S is nonempty or E is not rational. Then $\mathrm{Gal}(E_S/E)$ is not a free profinite group.*

Proof: If S is empty, then $E_S = E_{\mathrm{ur}}$. By assumption, $\mathrm{genus}(E) > 0$, so $\mathrm{Gal}(E_S/E)$ is not projective (Proposition 9.6.1). It follows that $\mathrm{Gal}(E_S/E)$ is not free [FrJ08, Cor. 22.4.5].

Assume S is nonempty and $\mathrm{Gal}(E_S/E)$ is a free profinite group of rank m. Then, for each prime number l, the maximal pro-l quotient $\mathrm{Gal}(E_S^{(l)}/E)$ of $\mathrm{Gal}(E_S/E)$ is a free pro-l group of rank m [FrJ08, Lemma 17.4.10]. Applying Lemma 9.9.2 for the case $l = \mathrm{char}(C)$, we conclude that

$$m = \mathrm{rank}(\mathrm{Gal}(E_S^{(l)}/E)) = \mathrm{card}(C)$$

is infinite.

On the other hand consider the case $l \neq \mathrm{char}(C)$. If S is finite, then $\mathrm{rank}(\mathrm{Gal}(E_S^{(l)}/E)) < \infty$ (Lemma 9.9.3). This contradicts the conclusion of the preceding paragraph.

If S is infinite, then $\aleph_0 \leq \mathrm{card}(S) < m$. Let $\mathcal{A}$ be the collection of all finite subsets of S. Then $\mathrm{card}(\mathcal{A}) = \mathrm{card}(S)$ and $E_S^{(l)} = \bigcup_{A\in\mathcal{A}} E_A^{(l)}$. Since m is infinite, $\mathrm{rank}(\mathrm{Gal}(E_S^{(l)}/E))$ is equal to the cardinality of the set of all finite extensions of E in $E_S^{(l)}$ [FrJ08, Prop. 17.1.2]. Each of these extensions is contained in $E_A^{(l)}$ for some $A \in \mathcal{A}$. For each $A \in \mathcal{A}$, E has at most countably many finite extensions in $E_A^{(l)}$ (because $\mathrm{rank}(\mathrm{Gal}(E_A^{(l)}/E)) < \infty$). It follows that $\mathrm{rank}(\mathrm{Gal}(E_S/E)) \leq \mathrm{card}(\mathcal{A})\aleph_0 = \mathrm{card}(S)\aleph_0 < m$. Again, this is a contradiction to the conclusion of the second paragraph of the proof. We conclude from this contradiction that $\mathrm{Gal}(E_S/E)$ is not a free profinite group. □

Remark 9.9.5: Non-isomorphic fundamental groups. Let E be a function field of one variable of genus $g > 0$ over an algebraically closed field of characteristic p and let S be a finite set of prime divisors of r elements. By Proposition 9.1.6, $\mathrm{Gal}(E_S/E)$ is uniquely determined up to an isomorphism by r and g if $p = 0$. This is not the case if $p > 0$.

Indeed, for $p \neq 0, 2$ consider elements a and a' in $\tilde{\mathbb{F}}_p$ such that the elliptic curve Γ defined over $\tilde{\mathbb{F}}_p$ with j-invariant a is ordinary and the elliptic curve Γ' defined over $\tilde{\mathbb{F}}_p$ with j-invariant a' is supersingular. Let F (resp. F') be the function field of Γ (resp. Γ'). Then $\mathrm{Gal}(F_{\mathrm{ur}}/F) \ncong \mathrm{Gal}(F'_{\mathrm{ur}}/F')$ although $\mathrm{genus}(F/\tilde{\mathbb{F}}_p) = 1 = \mathrm{genus}(F'/\tilde{\mathbb{F}}_p)$. Indeed, F has a unique unramified $\mathbb{Z}/p\mathbb{Z}$-extension while F' has none [Hrb77, p. 338, Exercise 4.8].

Similarly, let $E = \tilde{\mathbb{F}}_p(x)$, $S = \{0, 1, \infty, a\}$ and $S' = \{0, 1, \infty, a'\}$ with distinct $a, a' \in \tilde{\mathbb{F}}_p$. By [Hrb94b, Thm. 1.8], $\mathrm{Gal}(E_S/E) \ncong \mathrm{Gal}(E_{S'}/E)$ although they have the same invariants, $r = 4$ and $g = 0$. □

Notes

The proof of Proposition 9.1.1 and its generalization, Proposition 9.1.2, uses non-algebraic tools such as algebraic topology and the theory of Riemann surfaces, so it goes beyond the scope of this book. For a complete detailed proof of Proposition 9.1.1 we refer the reader to Helmut Völklein's book [Voe96]. See also [MaM99, Chap. 1, Thms. 1.3 and 1.4]. A proof of Proposition 9.1.2 can be found in [Dou79], [Matz87, p. 30, Satz 1], and [Ser92, Section 6.2]. Proposition 9.1.5 is reduced to Proposition 9.1.2 via Proposition 9.1.4. This reduction goes also under the name of "Grothendieck specialization theorem". Standard projective limit argument allows us to deduce Proposition 9.1.6 from Proposition 9.1.5. This transition appears also in [Matz87, p. 37, Satz 3]. Corollary 9.1.10 is due to Douady. It is a special case of Proposition 9.1.9. The proof of the latter theorem applies Proposition 9.1.6 and a projective limit argument over all finite subsets of S. Although we do not include information about the decomposition groups in Proposition 9.1.9 that information enters into the limit argument in an essential way. We have borrowed that ingredient of the proof from the proof of [Rib70, p. 70, Thm. 8.1].

A survey of Abhyankar's conjecture, Raynaud's proof of the conjecture for the affine line, and Pop's reduction to Raynaud's result appears in [MaM99, Sections 5.2, 5.3, and 5.4].

Section 9.3 surveys the cohomology of groups and Galois cohomology to the extent needed in the book. Our main source is [Rib70].

Section 9.4 reproduces [Jar99, Sec. 1], which by itself puts together well known arguments. The standard proof of Lemma 9.4.4 uses a special case of cohomological triviality: Let G be a finite group and let A be a G-module. If $\hat{H}^0(G, A) = A^G/NA = 0$ (where $Na = \Sigma_{\sigma \in G} \sigma a$) and $H^1(G, A) = 0$, then $H^2(G, A) = 0$ [CaF67, p. 113, Thm. 9]. In our case, $G = \mathrm{Gal}(N/K)$, $A = N^\times$ and $A^G/NA = K^\times/\mathrm{norm}_{N/K} N^\times = 1$. Also, $H^1(G, N^\times) = 1$, by Hilbert's theorem 90. So, indeed, $H^2(G, A) = 1$. Replacing cohomological triviality in

the proof of Lemma 9.4.4 by the more elementary argument is due to Sigrid Böge (private communication).

Proposition 9.4.6 is usually referred to as **Tsen's theorem**, because Tsen proved the essential ingredient of its proof, namely that the field of ratioanl functions over an algebraically closed field is C_1 [Tse33].

The proof that $\mathrm{Gal}(E_S/E)$ is projective in Section 9.5 is based on tips of Heinrich Matzat.

Lemma 9.5.2 is a rewrite of [Son94, Lemma 2.6]. Lemma 9.5.3 is due to Shafarevich [Sha89, p. 109]. See also [Son94, Prop. 2.5]. The proof of Lemma 9.5.4 is a modification of the proof of [Son94, Prop. 3.2]. Theorem 9.5.7 is proved by Serre [Ser90, Prop. 1], using étale cohomology.

The second proof of Proposition 9.6.1 that do not use Riemann's existence theorem arose from discussions with Gerhard Frey. The same goes for the proof of Lemma 9.6.2.

Harbater proves Theorem 9.8.5 in the case where $C \cup \{\infty\} \smallsetminus S$ is finite by formal patching [Har95, Thm. 4.1]. Pop proves Theorem 9.8.5 in its full strength by rigid methods [Pop05, p. 556, Cor.]. We follow [HaJ00a]. Corollary 9.4.9 is a special case of Theorem 9.8.5 and Theorem 9.4.8 is a slight generalization of Corollary 9.4.9.

Shafarevich discussed his conjecture on the freeness of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}})$ during a talk in Oberwolfach in 1964. Latter it appeared in [Bey80].

A Galois theoretic version of Lemma 9.8.4 appears in [Matz87, p. 231, Lemma 1].