W.-D. Geyer and M. Jarden
Nagoya Math. J.
Vol. 150 (1998), 13–62

BOUNDED REALIZATION OF l-GROUPS OVER GLOBAL FIELDS

The method of Scholz and Reichardt

WULF-DIETER GEYER AND MOSHE JARDEN[1]

Abstract. We use the method of Scholz and Reichardt and a transfer principle from finite fields to pseudo finite fields in order to prove the following result. THEOREM *Let G be a group of order l^n, where l is a prime number. Let K_0 be either a finite field with $|K_0| > l^{4n+4}$ or a pseudo finite field. Suppose that $l \neq \mathrm{char}(K_0)$ and that K_0 does not contain the root of unity ζ_l of order l. Let $K = K_0(t)$, with t transcendental over K_0. Then K has a Galois extension L with the following properties*: (a) $\mathcal{G}(L/K) \cong G$; (b) *L/K_0 is a regular extension*; (c) $\mathrm{genus}(L) < \frac{1}{2}nl^{2n}$; (d) *$K_0[t]$ has exactly n prime ideals which ramify in L; the degree of each of them is $[K_0(\zeta_{l^n}) : K_0]$*; (e) *$(t)_\infty$ totally decomposes in L*; (f) *$L = K(x)$, with $\mathrm{irr}(x, K) = X^{l^n} + a_1(t)X^{l^n-1} + \cdots + a_{l^n}(t)$, $0 < \deg(a_1(t)) \leq \frac{1}{2}nl^{2n}$ and $\deg(a_i(t)) < \deg(a_1(t))$ for $i = 1, \ldots, l^n$.*

Introduction

Scholz [Sch] proved that if l is an odd prime, then each l-group occurs as a Galois group over $\mathbb{Q}$. Here G is an **l-group** if the order of G is a power of l. Independently, Reichardt [Rei] gave a simpler and shorter proof to the same theorem. One can find a modern presentation of Reichardt's proof in Serre's course on Galois theory [Se1, §2.1].

The reason why the method of Scholz and Reichardt does not work for $l = 2$ is that the primitive root of unity of order 2, namely -1, belongs to $\mathbb{Q}$. The same reason forced Rzedowski-Calderón and Villa-Salvador [RCV] to exclude all primes l with $\zeta_l \in \mathbb{F}_q$, when they proved that each l-group occurs as a Galois group over $\mathbb{F}_q(t)$. Here q is a power of a prime $p \neq l$ and ζ_l is a primitive root of unity of order l.

Shafarevich [Sh1] has overcome this difficulty. He used refined combinatorial arguments to prove that for an arbitrary prime number l, for each number field K, and for each l-group G, there exists a Galois extension L

Received July 10, 1995.

[1] This research was supported by The Israel Science Foundation administered by The Israel Academy of Sciences and Humanities.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

of K such that $\mathcal{G}(L/K) \cong G$. In a later work [Sh2], Shafarevich pointed out how to correct an incomplete group theoretic argument in his earlier work for the case $l = 2$.

However, Shafarevich had to pay a price for his generalization. The combinatorial arguments forced him to allow an exponentially growing number of primes of K which may ramify in L. In contrast, as Serre [Se1, p. 9] emphasizes, the method of Scholz and Reichardt gives for a group G of order l^n, with l odd, a Galois extension L of $\mathbb{Q}$ in which only n primes ramify.

Although Rzedowski-Calderón and Villa-Salvador [RCV] use the method of Scholz and Reichardt they do not try to bound the number of ramified primes. Indeed for a given l-group G with $l \nmid q$ and $\zeta_l \notin \mathbb{F}_q$, they construct a Galois extension L of $\mathbb{F}_q(t)$ such that $\mathcal{G}(L/\mathbb{F}_q(t)) \cong G$ and the genus of L is large. Here and in the sequel, t is a transcendental element over the base field. By the Hurwitz-Riemann genus formula, this means that the number of primes of $\mathbb{F}_q(t)$ which ramify in L is also large.

The goal of this work is to use the method of Scholz and Reichardt to realize each l-group G over an arbitrary global field with bounded ramification.

THEOREM A. *Let K be a global field and let l be a prime number such that $l \neq \mathrm{char}(K)$ and $\zeta_l \notin K$. Then there exists a nonnegative integer $r = r(K)$ such that for each group G of order l^n there exists a Galois extension L of K with $\mathcal{G}(L/K) \cong G$ and $|\mathrm{Ram}(L/K)| \leq n + r$.*

Here $\mathrm{Ram}(L/K)$ denotes the set of primes of K which ramify in L. If $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$, then $r(K) = 0$. In the former case we therefore reproduce the result of [Se1]. In the latter case we improve the result of [RCV].

The extension L/K which Theorem A gives can actually be constructed to satisfy given 'local conditions'. See Theorem 7.4 for the exact formulation.

Serre uses cyclotomic fields in his proof. Rzedowski-Calderón and Villa-Salvador use Carlitz' analog of cyclotomic fields over $\mathbb{F}_q(t)$. Both type of fields are useless for the construction of l-extensions with bounded ramification over an arbitrary global field K. We replace their use by a systematic application of class field theory.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

In the function field case, we supplement Theorem A with bounds on various invariants of the extension L/K. We prove that for each large multiple k of $[\mathbb{F}_q(\zeta_{l^n}) : \mathbb{F}_q]$, the field L can be chosen such that $\deg(\mathfrak{p}) = k$ for each prime $\mathfrak{p} \in \mathrm{Ram}(L/K)$ and

$$2g_L - 2 \leq l^n(2g_K - 2 + (n + r(K))k). \tag{0.1}$$

Here g_K (resp., g_L) is the genus of K (resp., L). See Theorem 8.6 for more details.

The bounds of Theorem 9.6 become more explicit if $K = \mathbb{F}_q(t)$. For example, Theorem 9.1 improves (0.1) in this case to

$$2g_L - 2 \leq l^n(nk - 2).$$

Theorem 10.5 does even better under the assumption that $q > l^{4n+4}$. It produces absolutely irreducible polynomials $f,\ g \in \mathbb{F}_q(T, X)$ with coefficients of bounded degrees such that L is the splitting field over $K = \mathbb{F}_q(t)$ of both $f(t, X)$ and $g(t, X)$ and $\mathrm{Ram}(L/K)$ consists of those prime of K which divide the discriminants of both $f(t, X)$ and $g(t, X)$. Of course, $\mathcal{G}(L/K) \cong G$. Moreover, $(t)_\infty$ totally decomposes in L, $g_L \leq \frac{1}{2}nl^{2n}$, $|\mathrm{Ram}(L/K)| = n$, and $\deg(\mathfrak{p}) = [\mathbb{F}_q(\zeta_{l^n}) : \mathbb{F}_q]$ for each $\mathfrak{p} \in \mathrm{Ram}(L/K)$.

It is therefore possible to write down a sentence $\theta(l, n)$ in the first order language of the theory of fields, such that if $q > l^{4n+4}$, then $K = \mathbb{F}_q(t)$ has a Galois extension as in the preceding paragraph.

This has an immediate consequence for the infinite models of the theory of finite fields. They are called **pseudo finite fields**. For example, each nonprincipal ultraproduct of finite fields is pseudo finite. Also, if F is a countable Hilbertian field (e.g., $F = \mathbb{Q}$ or $F = \mathbb{F}_q(t)$), then $\tilde{F}(\sigma)$ is pseudo finite for almost all σ in the absolute Galois group $G(F)$ of F [Ja1, Thm. 3.5]. Here $\tilde{F}(\sigma)$ is the fixed field of σ in the algebraic closure $\tilde{F}$ of F.

THEOREM B. *Let K_0 be a pseudo finite field and let l be a prime number such that $l \nmid \mathrm{char}(K_0)$ and $\zeta_l \notin K_0$. Let G be a group of order l^n. Then $K = K_0(t)$ has a Galois extension L which is regular over K_0 such that $\mathcal{G}(L/K) \cong G$, $|\mathrm{Ram}(L/K)| = n$, $g_L \leq \frac{1}{2}nl^{2n}$, $(t)_\infty$ totally decomposes in L, and $\deg(\mathfrak{p}) = [K_0(\zeta_{l^n}) : K_0]$ for each $\mathfrak{p} \in \mathrm{Ram}(L/K)$.*

Note that each pseudo finite field K_0 is **PAC**. That is, each absolutely irreducible variety over K_0 has a K_0-rational point. It is known for an

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

arbitrary PAC field K_0 and for each finite group G that there exists a Galois extension L of $K_0(t)$ which is regular over K_0 such that $\mathcal{G}(L/K) \cong G$. This was first proved by Fried and Völklein [FrV] in characteristic 0. In the general case it follows from a theorem of Harbater [Ja2, Thm. 2.6] which has been recently reproved in an elementary way by Haran and Völklein [HaV]. However, none of the proofs of this theorem supplies a bound for $|\mathrm{Ram}(L/K)|$. Theorem B does it in a very special case.

§1. Global fields

Consider a global field K. Thus, K is either a **number field**, that is, a finite extension of $\mathbb{Q}$, or K is a **function field**, that is, K is a regular extension of transcendence degree 1 of a finite field $\mathbb{F}_q$ with q elements. We denote the set of primes of K by $\mathbb{P} = \mathbb{P}(K)$. In the number field case, $\mathbb{P}$ has a finite subset $\mathbb{P}_\infty$, the set of **archimedean primes**, which correspond to the embeddings of K into $\mathbb{C}$. Each archimedean prime $\mathfrak{p}$ is a divisor of the unique archimedean prime ∞ of $\mathbb{Q}$ and we write $\mathfrak{p}|\infty$. All other primes of K are **nonarchimedean**. In particular, if K is a function field, then K has only nonarchimedean primes and we let $\mathbb{P}_\infty = \emptyset$.

Fix a prime number l which does not divide $\mathrm{char}(K)$. For each n choose a root of unity ζ_{l^n} of order l^n. Most of our results will assume that $\zeta_l \notin K$. If K is a number field, we denote the finite subset of $\mathbb{P}$ that consists of all prime divisors of l by $\mathbb{P}_l$. If K is a function field, we let $\mathbb{P}_l = \emptyset$.

Denote the completion of K at a prime $\mathfrak{p}$ by $K_\mathfrak{p}$ and let $\bar{K}_\mathfrak{p}$ be its residue field. If $\mathfrak{p}$ is archimedean, then $K_\mathfrak{p}$ is either $\mathbb{R}$ ($\mathfrak{p}$ is **real**) or $\mathbb{C}$ ($\mathfrak{p}$ is **complex**). In each case we let $U_\mathfrak{p} = K_\mathfrak{p}^\times$ be the multiplicative group of $K_\mathfrak{p}$ and set $\pi_\mathfrak{p} = 1$. If $\mathfrak{p}$ is nonarchimedean, then $K_\mathfrak{p}$ is a complete discrete valuation field. We denote its normalized valuation by $v_\mathfrak{p}$ and choose a prime element $\pi_\mathfrak{p}$ in $K_\mathfrak{p}$, that is $v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. Let $U_\mathfrak{p}$ be the group of units of $K_\mathfrak{p}$ and $U_{\mathfrak{p},1}$ its group of 1-units. Then $K_\mathfrak{p}^\times \cong \langle\pi_\mathfrak{p}\rangle \times U_\mathfrak{p}$ and $U_\mathfrak{p}/U_{\mathfrak{p},1}$ is isomorphic to $\bar{K}_\mathfrak{p}^\times$. If K is a number field, then $\bar{K}_\mathfrak{p}$ is a finite extension of $\mathbb{F}_p$, where p is the rational prime that lies under $\mathfrak{p}$. If K is a function field, then $\bar{K}_\mathfrak{p}$ is a finite extension of $\mathbb{F}_q$ and $[\bar{K}_\mathfrak{p} : \mathbb{F}_q] = \deg(\mathfrak{p})$. In both cases $U_{\mathfrak{p},1}$ is a pro-p group, where $p = \mathrm{char}(\bar{K}_\mathfrak{p})$.

The group I_K of **ideles** of K is the restricted product of the multiplica-

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

tive groups $K_\mathfrak{p}^\times$ with respect to the subgroups $U_\mathfrak{p}$. Thus

$$I_K = \left\{ \alpha \in \prod_{\mathfrak{p}\in\mathbb{P}} K_\mathfrak{p}^\times \mid \alpha_\mathfrak{p} \in U_\mathfrak{p} \text{ for all but finitely many } \mathfrak{p} \in \mathbb{P} \right\}.$$

A basis for the topology of I_K consists of all sets $\prod V_\mathfrak{p}$ such that $V_\mathfrak{p}$ is open in $K_\mathfrak{p}^\times$ and $V_\mathfrak{p} = U_\mathfrak{p}$ for almost all $\mathfrak{p}$. In particular, the group of **unit ideles** is open in I_K:

$$U = \prod_{\mathfrak{p}\in\mathbb{P}} U_\mathfrak{p}.$$

This group is the kernel of the **divisor map** div: $I_K \to \mathrm{Div}(K) = \bigoplus_{\mathfrak{p}\nmid\infty} \mathbb{Z}\cdot\mathfrak{p}$ which is defined by $\mathrm{div}(\alpha) = \sum_{\mathfrak{p}\nmid\infty} v_\mathfrak{p}(\alpha_\mathfrak{p})\mathfrak{p}$. The image of the divisor map is the **group of divisors** $\mathrm{Div}(K)$ of K.

One embeds $K^\times$ diagonally in I_K and calls $C_K = I_K/K^\times$ the **idele class group** of K. Its factor by $UK^\times/K^\times$ is the **ideal class group** of K:

$$\mathrm{Cl}(K) = I_K/UK^\times = \mathrm{Div}(K)/\mathrm{div}(K^\times). \tag{1.1}$$

If K is a number field, then $\mathrm{Cl}(K)$ is a finite abelian group, whose order h_K is the **class number** of K. If K is a function field, then we define the **degree function** for ideles deg: $I_K \to \mathbb{Z}$ by $\deg(\alpha) = \sum_{\mathfrak{p}\in\mathbb{P}} v_\mathfrak{p}(\alpha_\mathfrak{p})\deg(\mathfrak{p})$ and consider the group of ideles of **degree** 0:

$$I_K^0 = \{\alpha \in I_K \mid \deg(\alpha) = 0\}$$

The product formula implies that $K^\times \le I_K^0$. Also, $U \le I_K^0$. So, we may consider the **group of idele classes of degree** 0: $\mathrm{Cl}_0(K) = I_K^0/UK^\times$. Then $\mathrm{Cl}(K)/\mathrm{Cl}_0(K) \cong \mathbb{Z}$, but $\mathrm{Cl}_0(K)$ is a finite abelian group whose order h_K is the **class number** of K. More important for us is the l-**class rank** of K:

$$\mathrm{rank}_l(K) = \dim_{\mathbb{F}_l} \mathrm{Cl}(K)_l$$

Here $\mathrm{Cl}(K)_l$ is the l-torsion part of the finite abelian group $\mathrm{Cl}(K)$.

To each finite nonempty subset S of $\mathbb{P}$ that contains $\mathbb{P}_\infty$ one associates the group K_S of S-**units**. Thus K_S consists of all elements $x \in K$ such that $v_\mathfrak{p}(x) = 0$ for all $\mathfrak{p} \notin S \cup \mathbb{P}_\infty$. By Dirichlet's unit theorem, $K_S \cong \mu_K \times \mathbb{Z}^{|S|-1}$ where μ_K is the finite cyclic group of roots of unity of K [CaF, p. 72]. If K is a function field, then $\mu_K = \mathbb{F}_q^\times$. If K is a number field and $S = \mathbb{P}_\infty$, we

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

call $\mathrm{rank}_\infty(K) = |\mathbb{P}_\infty| - 1$ the **unit rank** of K and $E_K = K_{\mathbb{P}_\infty}$ is the **group of units** of K. If K is a function field, we let $E_K = \mu_K$ and $\mathrm{rank}_\infty(K) = 0$.

The group of S-**ideles** of K is the direct product

$$I_{K,S} = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}. \tag{1.2}$$

It contains U and satisfies

$$K_S = I_{K,S} \cap K^\times. \tag{1.3}$$

The restricted topology of I_K induces the usual direct product topology on $I_{K,S}$. In particular, if h is a homomorphism of $I_{K,S}$ into a finite group C such that h is continuous on $K_\mathfrak{p}^\times$ for each $\mathfrak{p} \in S$ and $h(\prod_{\mathfrak{p}\notin S} U_\mathfrak{p}) = 1$, then h is continuous.

Data 1.1. (Basic set) If K is a number field, choose ideles $\alpha_1, \ldots, \alpha_{h_K}$ which represent I_K modulo $UK^\times$. Let S_0 be the set of archimedean primes and those nonarchimedean primes $\mathfrak{p}$ for which $v_\mathfrak{p}(\alpha_{i,\mathfrak{p}}) \neq 0$ for at least one i. Then S_0 is a finite set and each set of primes S which contains S_0 satisfies

$$I_K = I_{K,S}K^\times. \tag{1.4}$$

If K is a function field, then we choose $\alpha_0 \in I_K$ of degree 1 and $\alpha_1, \ldots, \alpha_{h_K}$ which represent I_K^0 modulo $UK^\times$. Let S_0 be the set of primes $\mathfrak{p}$ such that $v_\mathfrak{p}(\alpha_i) \neq 0$ for at least one i. Again, S_0 is a finite subset of $\mathbb{P}$ and each set $S_0 \subseteq S \subseteq \mathbb{P}$ satisfies (1.4). It follows from (1.3) and (1.4) that

$$C_K = I_{K,S}/K_S \tag{1.5}$$

We increase S_0 now by adding $\mathbb{P}_l$ to it, if K is a number field, and possibly finitely many additional primes which we choose at will. Then we call S_0 a **basic set** and fix it for the rest of this work.

Example 1.2. (The cases $K = \mathbb{Q}$ and $K = \mathbb{F}_q(t)$) For $K = \mathbb{Q}$ the unique factorization in $\mathbb{Z}$ implies that $I_\mathbb{Q} = U\mathbb{Q}^\times$ and therefore $h_\mathbb{Q} = 1$. We may therefore choose $\alpha_1 = 1$ and S_0 to be any finite set of primes that contains $\{\infty, l\}$.

For $K = \mathbb{F}_q(t)$ we may choose α_0 as the idele whose component at the pole of t (which we denote by $(t)_\infty$) is t^{-1} and otherwise is 1. Again, the unique factorization in $\mathbb{F}_q[t]$ implies that $I_K^0 = UK^\times$ and $h_K = 1$. We may therefore choose S_0 to be any finite set of primes of K that contains $(t)_\infty$.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

§2. Class field theory

Class field theory teaches us that the idele class group C_K controls the abelian extensions of K. Specifically, for each finite abelian extension L/K the **reciprocity law** gives a continuous epimorphism

$$\psi\colon C_K \longrightarrow \mathcal{G}(L/K), \tag{2.1}$$

whose kernel is $N_{L/K}C_L$ and which is functorial in L. For details, we refer the reader to chapters 4 (Serre: local class field theory) and 5 (Tate: global class field theory) of [CaF] and also to [Neu] (which however handles only the class field theory of number fields).

For each prime $\mathfrak{p}$ of K we consider $K_\mathfrak{p}^\times$ as the subgroup of I_K which consists of all ideles whose $\mathfrak{q}$ coordinate is 1 for each $\mathfrak{q} \neq \mathfrak{p}$. Under this identification $K_\mathfrak{p}^\times \cap K^\times = 1$. So, we may and we will consider $K_\mathfrak{p}^\times$ also as a subgroup of C_K. The restriction of ψ to $K_\mathfrak{p}^\times$ gives a continuous epimorphism

$$\psi_\mathfrak{p}\colon K_\mathfrak{p}^\times \longrightarrow D_\mathfrak{p}(L/K) \tag{2.2}$$

whose kernel is $N_{L_\mathfrak{p}/K_\mathfrak{p}}L_\mathfrak{p}^\times$. Here, $L_\mathfrak{p}$ is the completion of L with respect to a prime $\mathfrak{p}'$ of L which lies over $\mathfrak{p}$ and $D_\mathfrak{p}(L/K)$ is the **decomposition group** of $\mathfrak{p}$ in L. Since L/K is abelian, both the norm group and the decomposition group do not depend on $\mathfrak{p}'$. The fixed field of $D_\mathfrak{p}(L/K)$ is $L \cap K_\mathfrak{p}$. It is the maximal subfield of L/K in which $\mathfrak{p}$ completely decomposes. In particular $\mathfrak{p}$ completely decomposes in L if and only if $D_\mathfrak{p}(L/K) = 1$. The homomorphism $\psi_\mathfrak{p}$ maps $U_\mathfrak{p}$ onto the **inertia group** $I_\mathfrak{p}(L/K)$ of L/K whose fixed field is the maximal subfield of L/K in which $\mathfrak{p}$ is unramified. Thus $I_\mathfrak{p}(L/K) = 1$ if and only if $\mathfrak{p}$ is unramified in L. If φ is unramified at $\mathfrak{p}$, then $\psi_\mathfrak{p}(\pi_\mathfrak{p}) = \left(\frac{L/K}{\mathfrak{p}}\right)$ is the Frobenius automorphism of L/K at $\mathfrak{p}$. Finally, the condition $D_\mathfrak{p}(L/K) = I_\mathfrak{p}(L/K)$ is equivalent for nonarchimedean $\mathfrak{p}$ to $\bar{L}_\mathfrak{p} = \bar{K}_\mathfrak{p}$.

Let $\tilde{K}$ (resp., K_s) be the algebraic (resp., separable) closure of K and let $G(K) = \mathcal{G}(K_s/K)$ be the absolute Galois group of K. We embed $\tilde{K}$ into $\tilde{K}_\mathfrak{p}$, thereby extending $\mathfrak{p}$ to $\tilde{K}$. Then $\tilde{K} \cap K_\mathfrak{p} = K_{\mathfrak{p},\mathrm{alg}}$ is a Henselian closure (resp., real closure) of K with respect to $\mathfrak{p}$ if $\mathfrak{p}$ is nonarchimedean (resp., archimedean). Its absolute Galois group $G(K_{\mathfrak{p},\mathrm{alg}})$ is the **absolute decomposition group** of $\mathfrak{p}$. We denote it by $D_\mathfrak{p}$. By Krasner's lemma, $K_sK_\mathfrak{p} = K_{\mathfrak{p},s}$. Hence, $\mathrm{res}_{K_s}\colon G(K_\mathfrak{p}) \to D_\mathfrak{p}$ is an isomorphism. We identify $G(K_\mathfrak{p})$ with $D_\mathfrak{p}$ under this map. We denote the maximal unramified

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

extension of $K_\mathfrak{p}$ by $K_{\mathfrak{p},\mathrm{ur}}$ (if $\mathfrak{p}$ is archimedean, we set $K_{\mathfrak{p},\mathrm{ur}} = K_\mathfrak{p}$) and let $I_\mathfrak{p} = \mathrm{res}_{K_s}(G(K_{\mathfrak{p},\mathrm{ur}}))$. This is the **absolute inertia group** of $\mathfrak{p}$. If $\mathfrak{p}$ is nonarchimedean, then the quotient group $D_\mathfrak{p}/I_\mathfrak{p} \cong \mathcal{G}(K_{\mathfrak{p},\mathrm{ur}}/K_\mathfrak{p})$ is isomorphic to $\hat{\mathbb{Z}}$ and the Frobenius automorphism $\mathrm{Frob}_\mathfrak{p}$ is a canonical generator of this group.

Whenever we consider a homomorphism $\varphi: G(K) \to G$ into a finite (not necessarily abelian) group G, we assume that φ is continuous. Then, the fixed field L of $\mathrm{Ker}(\varphi)$ in K_s is a finite extension of K. The prime $\mathfrak{p}$ totally decomposes in L if and only if $\varphi(D_\mathfrak{p}) = 1$, i.e., $L \subseteq K_\mathfrak{p}$. We then say that φ **totally decomposes** at $\mathfrak{p}$. Similarly, we say that φ is **unramified** at $\mathfrak{p}$ if $\mathfrak{p}$ is unramified in L, that is, if $\varphi(I_\mathfrak{p}) = 1$. In this case φ induces a homomorphism of $\mathcal{G}(K_{\mathfrak{p},\mathrm{ur}})$ onto $\mathcal{G}(L/K)$ which maps $\mathrm{Frob}_\mathfrak{p}$ onto the Frobenius element $[\frac{L/K}{\mathfrak{p}'}]$ of $\mathcal{G}(L/K)$, where $\mathfrak{p}'$ is the prime of L which is determined by the embedding of L into $\tilde{K}_\mathfrak{p}$. If $\mathfrak{p}$ is nonarchimedean and $|I_\mathfrak{p}|$ is relatively prime to $\mathrm{char}(\bar{K}_\mathfrak{p})$, then φ is **tamely ramified** at $\mathfrak{p}$. We denote the finite set of primes at which φ ramifies by $\mathrm{Ram}(\varphi)$ and also by $\mathrm{Ram}(L/K)$. Finally, $\varphi(I_\mathfrak{p}) = \varphi(D_\mathfrak{p})$ if and only if $\bar{L}_\mathfrak{p} = \bar{K}_\mathfrak{p}$. Note that all these concepts are independent of the embedding of $\tilde{K}$ into $\tilde{K}_\mathfrak{p}$.

We choose a multiplicative copy C_l of the cyclic group of order l. Let Hom be the functor of continuous homomorphisms. Then the reciprocity law gives a commutative diagram

$$\begin{tikzcd}
\mathrm{Hom}(G(K), C_l) \arrow[r, "\Psi"] \arrow[d] & \mathrm{Hom}(C_K, C_l) \arrow[d] \\
\mathrm{Hom}(D_\mathfrak{p}, C_l) \arrow[r, "\Psi_\mathfrak{p}"] \arrow[d] & \mathrm{Hom}(K_\mathfrak{p}^\times, C_l) \arrow[d] \\
\mathrm{Hom}(I_\mathfrak{p}, C_l) \arrow[r, "\Psi_\mathfrak{p}"] & \mathrm{Hom}(U_\mathfrak{p}, C_l)
\end{tikzcd} \tag{2.3}$$

in which the horizontal maps are isomorphisms and the vertical maps are the natural restriction maps. Both Ψ and $\Psi_\mathfrak{p}$ map epimorphisms onto epimorphisms. If $h \in \mathrm{Hom}(D_\mathfrak{p}, C_l)$ is trivial on $I_\mathfrak{p}$ and $\eta = \Psi_\mathfrak{p}(h)$, then η is trivial on $U_\mathfrak{p}$. In this case h induces a homomorphism $\bar{h}: \mathcal{G}(K_{\mathfrak{p},\mathrm{ur}}/K_\mathfrak{p}) \to C_l$ such that $\bar{h}(\mathrm{Frob}_\mathfrak{p}) = \eta(\pi_\mathfrak{p})$.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

§3. Embedding problems; Scholz extensions

An l-**group** is a group G whose order is a power of l. Such a group has a central sequence all of its factors are of order l. We consider **central embedding problems** for $G(K)$ of the following type:

(3.1)
$$\begin{tikzcd} & & & G(K) \arrow[d, "\rho"] & \\ 1 \arrow[r] & C_l \arrow[r] & G \arrow[r, "\alpha"] & \bar{G} \arrow[r] & 1 \end{tikzcd}$$

Here the lower sequence is exact, ρ is surjective, and C_l is contained in the center of G. A **weak solution** to (3.1) is a homomorphism $\varphi\colon G(K) \to G$ such that $\alpha \circ \varphi = \rho$. If φ is in addition surjective, we call φ a **solution**. In this case let L (resp., L') be the fixed field in K_s of $\mathrm{Ker}(\rho)$ (resp., $\mathrm{Ker}(\varphi)$). Then ρ (resp., φ) induces an isomorphism $\bar{\rho}\colon \mathcal{G}(L/K) \to \bar{G}$ (resp., $\bar{\varphi}\colon \mathcal{G}(L'/K) \to G$) such that $\bar{\rho} \circ \mathrm{res}_L = \alpha \circ \bar{\varphi}$. The embedding problem **splits** if the short exact sequence splits. This is the case if and only if $G \cong C_l \times \bar{G}$ and α is the projection onto the second factor. Each epimorphism from $G(K)$ onto C_l can then be multiplied with ρ to yield a solution to (3.1) and each solution of (3.1) is of this type. In the general case, if φ is a weak solution to (3.1), then $C_l \cdot \varphi(G(K)) = G$ and hence the index of $\varphi(G(K))$ in G divides l. Since G is an l-group, $\varphi(G(K))$ is normal in G. Hence, if (3.1) does not split, then $C_l \leq \varphi(G(K))$ and therefore φ is a solution to (3.1). In this case, if $\eta\colon G(K) \to C_l$ is a homomorphism, than the map $\varphi'\colon G(K) \to G$ defined by $\varphi'(\sigma) = \eta(\sigma)\varphi(\sigma)$ for $\sigma \in G(K)$ is also a solution to (3.1). Moreover, each solution to (3.1) is obtained in this way. We write $\varphi' = \eta \cdot \varphi$.

For each prime $\mathfrak{p}$ of K, (3.1) gives rise to a **local embedding problem**:

(3.2)
$$\begin{tikzcd} & & & D_{\mathfrak{p}} \arrow[d, "\rho_{\mathfrak{p}}"] & \\ 1 \arrow[r] & C_l \arrow[r] & G_{\mathfrak{p}} \arrow[r, "\alpha_{\mathfrak{p}}"] & \bar{G}_{\mathfrak{p}} \arrow[r] & 1 \end{tikzcd}$$

Here $D_{\mathfrak{p}}$ is the absolute decomposition group of $\mathfrak{p}$ (Section 2), $\rho_{\mathfrak{p}} = \rho|_{D_{\mathfrak{p}}}$, $\bar{G}_{\mathfrak{p}} = \rho(D_{\mathfrak{p}})$, $G_{\mathfrak{p}} = \alpha^{-1}(\bar{G}_{\mathfrak{p}})$ and $\alpha_{\mathfrak{p}} = \alpha|_{G_{\mathfrak{p}}}$. If (3.1) is central, then so is (3.2). However, even if (3.1) does not split, (3.2) may split.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Class field theory reduces the solvability of the global embedding problem (3.1) to the solvability of all local embedding problems induced by (3.1) (as we shall see in the proof of Lemma 4.3). This led Scholz to try to construct the map $\rho\colon G(K) \to \bar{G}$ with conditions that will impose the solvability of all local embedding problems (3.2). Before we reformulate Scholz's conditions we fix some 'local data' which we would like to impose on φ.

Local data 3.1. A set $\{\varphi_\mathfrak{p}\colon D_\mathfrak{p} \to G \mid \mathfrak{p} \in S_0\}$ of homomorphisms is a **local data** for an l-group G and a positive integer n if it satisfies the following conditions:

(3.3a) $\varphi_\mathfrak{p}(I_\mathfrak{p}) = 1$ for each $\mathfrak{p} \in \mathbb{P}_l$,

(3.3b) if $\mathfrak{p} \in S_0$ and $\varphi_\mathfrak{p}(I_\mathfrak{p}) \neq 1$, then $\zeta_{l^n} \in K_\mathfrak{p}$ and $\varphi_\mathfrak{p}(I_\mathfrak{p}) = \varphi_\mathfrak{p}(D_\mathfrak{p})$.

We fix the local data for G for the rest of this work.

Our definition of a Scholz extension depends on a finite set S_1 of $\mathrm{rank}_l(K) + \mathrm{rank}_\infty(K)$ 'exceptional primes' of K which is disjoint from S_0. We choose such a set in §5. It depends on K and on l but not on G.

DEFINITION 3.2. (Scholz extension) Let n be a positive integer and let φ be an epimorphism of $G(K)$ onto an l-group G equipped with a local data as in Local data 3.1. We say that φ is n-**Scholz** if

(3.4a) $\zeta_{l^n} \in K_\mathfrak{p}$, for each $\mathfrak{p} \in \mathrm{Ram}(\varphi)$,

(3.4b) $\varphi(I_\mathfrak{p}) = \varphi(D_\mathfrak{p})$ for each $\mathfrak{p} \in \mathrm{Ram}(\varphi)$, and

(3.4c) $\varphi|_{D_\mathfrak{p}} = \varphi_\mathfrak{p}$ for each $\mathfrak{p} \in S_0$ (Thus, φ **respects** the **local data**.)

(3.4d) $\varphi(I_\mathfrak{p}) = \varphi(D_\mathfrak{p})$ for each $\mathfrak{p} \in S_1$.

We say that a finite Galois extension L/K is an l-**extension**, if $\mathcal{G}(L/K)$ is an l-group. In this case L/K is n-**Scholz** if $\mathrm{res}_L\colon G(K) \to \mathcal{G}(L/K)$ is an n-Scholz epimorphism.

By (3.3a), φ ramifies at no $\mathfrak{p} \in \mathbb{P}_l$. In other words, if $\mathfrak{p} \in \mathrm{Ram}(\varphi)$, then φ is tamely ramified at $\mathfrak{p}$. By (3.3b), φ is unramified at each archimedean prime if $l^n \neq 2$. Condition (3.4a) then means that $\mathfrak{p}$ totally decomposes in $K(\zeta_{l^n})$. By Hensel's lemma, it is also equivalent to $\zeta_{l^n} \in \bar{K}_\mathfrak{p}$ and also to $N\mathfrak{p} \equiv 1 \bmod l^n$ (Recall that $N\mathfrak{p}$ is the cardinality of $\bar{K}_{\mathfrak{p}}$). Condition (3.4b) means that the inertia group of each prime of L which ramifies over K coincides with its decomposition group. If $\varphi_{\mathfrak{p}} = 1$ for some $\mathfrak{p} \in S_0$, then Condition (3.4c) means that $\mathfrak{p}$ totally decomposes in L. If on the other hand, $\varphi_{\mathfrak{p}}(I_{\mathfrak{p}}) \neq 1$, then Condition (3.4c) implies that $\mathfrak{p} \in \mathrm{Ram}(\varphi)$. Thus, $\mathrm{Ram}(\varphi) \cap S_0$ is a priori determined by the local data. Note that all conditions are independent of the particular embedding we have chosen for $\tilde{K}$ into $\tilde{K}_{\mathfrak{p}}$.

In the notation of (3.1), the local data for G induces a local data for $\bar{G}$. This is the set $\{\rho_{\mathfrak{p}} = \alpha \circ \varphi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$. (Note that Condition (3.3) is satified for the $\rho_{\mathfrak{p}}$'s.) If φ is a solution for the embedding problem (3.1) and φ is n-Scholz, then ρ is n-Scholz. But even if ρ is n-Scholz, φ need not be n-Scholz itself. So, in order to continue the induction on the order of G, we multiply φ by an appropriate homomorphism $\eta\colon G(K) \to C_l$ such that it will be n-Scholz. We do it in two steps. First we change φ in this way such that $\mathrm{Ram}(\varphi) \cup S_1 = \mathrm{Ram}(\rho) \cup S_1$. Then we change the resulting φ such that $\mathrm{Ram}(\varphi) \cup S_0 \cup S_1 = \mathrm{Ram}(\rho) \cup \{\mathfrak{q}\} \cup S_0 \cup S_1$ where $\mathfrak{q}$ is an additional new ramified prime which arises from an application of the Chebotarev density theorem. At this step we use the assumption $\zeta_l \notin K$. Thus, if the order of G is l^n, then we finally realize G as the Galois group of a Galois extension L/K with $|\mathrm{Ram}(L/K) \smallsetminus (S_0 \cup S_1)| = n$.

Note the difference between the roles of the finite sets S_0 and S_1. The set S_0 must contain some basic primes but otherwise we are free to make it arbitrarily large and we are completely free to determine $\varphi|_{D_{\mathfrak{p}}}$ for each $\mathfrak{p} \in S_0$. In particular, we can assume that $\varphi(I_{\mathfrak{p}}) = 1$ for each $\mathfrak{p} \in S_0$ and then φ will be unramified at each $\mathfrak{p} \in S_0$. The behaviour of φ at $\mathfrak{p} \in S_1$ on the other hand is out of our control. In particular we can not determine whether or not φ is ramified at a given $\mathfrak{p} \in S_1$. However, $|S_1| = \mathrm{rank}_l(K) + \mathrm{rank}_\infty(K)$ does not depend on G.

§4. Existence of a solution

The first step toward an n-Scholz solution of embedding problem (3.1) is to find a solution which need not be n-Scholz. The easier case is when (3.1) splits. In this case (Lemma 4.2) we need to make no assumptions on ρ. In the more difficult case (Lemma 4.3) we have to assume that ρ is an n-Scholz epimorphism.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

LEMMA 4.1. *Let $\mathfrak{q}$ be a prime of K which does not belong to $\mathbb{P}_l \cup \mathbb{P}_\infty$. Suppose that $\zeta_l \in K_\mathfrak{q}$. Then $U_\mathfrak{q}/U_\mathfrak{q}^l \cong C_l$.*

Proof. We have assumed in the function field case that $l \neq \mathrm{char}(K)$. Hence, in both cases $l \neq \mathrm{char}(\bar{K}_\mathfrak{q})$. Hence $\zeta_l \in \bar{K}_\mathfrak{q}$. By Hensel's Lemma $U_{\mathfrak{q},1} \leq U_\mathfrak{q}^l$. Hence $U_\mathfrak{q}/U_\mathfrak{q}^l \cong \bar{K}_\mathfrak{q}^\times/(\bar{K}_\mathfrak{q}^\times)^l \cong C_l$. □

LEMMA 4.2. *Suppose that embedding problem* (3.1) *splits. Then it has a solution.*

Proof. Denote the fixed field of $\mathrm{Ker}(\rho)$ by L. Then assume without loss that $\bar{G} = \mathcal{G}(L/K)$, $G = C_l \times \mathcal{G}(L/K)$, $\rho = \mathrm{res}_L$, and α is the projection on the second factor.

As K is Hilbertian [FrJ, Cor. 12.8], every finite abelian group is realizable over K [FrJ, Thm. 24.48]. In particular suppose that C_l^m is the maximal l-elementary abelian quotient of $\mathcal{G}(L/K)$. Let N be a Galois extension of K with $\mathcal{G}(N/K) \cong C_l^{m+1}$. Then N has a subfield M which is linearly disjoint from L over K and $\mathcal{G}(M/K) \cong C_l$. So, $L' = LM$ satisfies $\mathcal{G}(L'/K) \cong \mathcal{G}(M/K) \times \mathcal{G}(L/K)$ and $\mathrm{res}_{L'}\colon G(K) \to \mathcal{G}(L'/K)$ gives a solution to (3.1).

Alternatively, let $S = \mathrm{Ram}(L/K) \cup S_0 \cup S_1$. Choose generators $a_1, \ldots, a_s$ for K_S modulo K_S^l and consider the Galois extension $N = K(\zeta_l, \sqrt[l]{a_1}, \ldots, \sqrt[l]{a_s})$ of K. Apply the Chebotarev density theorem to choose a prime $\mathfrak{q} \notin S$ such that $\left(\frac{N/K}{\mathfrak{q}}\right) = 1$, i.e., $N \subset K_\mathfrak{q}$. In particular, $v_\mathfrak{q}(a_i) = 0$ and $a_i \in U_\mathfrak{q}^l$, $i = 1, \ldots, s$. Also, $\mathfrak{q} \nmid l$. Hence, by Lemma 4.1, there exists a continuous epimorphism $h_\mathfrak{q}\colon U_\mathfrak{q} \to C_l$. Define a continuous homomorphism

$$h\colon I_{K,S} = \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^\times \times U_\mathfrak{q} \times \prod_{\mathfrak{p} \notin S \cup \{\mathfrak{q}\}} U_\mathfrak{p} \longrightarrow C_l$$

by $h(K_\mathfrak{p}^\times) = 1$ for $\mathfrak{p} \in S$, $h|_{U_\mathfrak{q}} = h_\mathfrak{q}$, and $h(U_\mathfrak{p}) = 1$ for $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$. Since $a_i \in U_\mathfrak{q}^l$, $i = 1, \ldots, s$, $h(K_S) = 1$. Hence, h induces an epimorphism $\bar{h}\colon C_K \cong I_{K,S}/K_S \to C_l$ which satisfies $\bar{h}(K_\mathfrak{p}^\times) = 1$ for $\mathfrak{p} \in S$, $\bar{h}(U_\mathfrak{q}) = C_l$, and $h(U_\mathfrak{p}) = 1$ for $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$.

The reciprocity law (2.3) transfers $\bar{h}$ to an epimorphism $\eta\colon G(K) \to C_l$ such that $\eta(I_\mathfrak{q}) = C_l$. Let M be the fixed field of $\mathrm{Ker}(\eta)$ in K_s. Then $\mathcal{G}(M/K) \cong C_l$ and $\mathfrak{q}$ is ramified in M. Since $\mathfrak{q}$ is unramified in L, we have $M \cap L = K$. Conclude the proof as in the second paragraph. □

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

The following local global principle is implicit in [Rei], [Ko, p. 35], and [Se, Lemma 2.1.5]. We include a proof of this principle for the convenience of the reader.

LEMMA 4.3. *If each of the embedding problems* (3.2) *has a weak solution, then the embedding problem* (3.1) *has a solution.*

Proof. By lemma 4.2 we may assume that (3.1) does not split. So, by the discussion in the first paragraph of §3, we have to prove that (3.1) has a weak solution.

To this end let $K' = K(\zeta_l)$ and apply class field theory to write a commutative diagram of cohomology groups:

$$\begin{tikzcd} H^2(\bar{G}, C_l) \arrow[r, "\rho^*"] \arrow[d, "\mathrm{res}"] & H^2(G(K), C_l) \arrow[r, "\mathrm{res}"] \arrow[d, "\mathrm{res}"] & H^2(G(K'), C_l) \arrow[d, "\mathrm{res}"] \\ \prod_{\mathfrak{p}} H^2(\bar{G}_{\mathfrak{p}}, C_l) \arrow[r, "\rho^*_{\mathfrak{p}}"] & \prod_{\mathfrak{p}} H^2(G(\bar{K}_{\mathfrak{p}}), C_l) \arrow[r, "\mathrm{res}"] & \prod_{\mathfrak{p}} H^2(G(\bar{K}'_{\mathfrak{p}}), C_l) \end{tikzcd} \tag{4.1}$$

The Brauer-Hasse-Noether theorem for Brauer groups [CaF, p. 185] implies that the right vertical map in (4.1) is injective. Since $[K' : K]$ is relatively prime to l, the upper res map in (4.1) is injective [CaF, p. 105]. Hence, the middle vertical map in (4.1) is injective.

Denote now the element of $H^2(\bar{G}, C_l)$ (resp., $H^2(\bar{G}_{\mathfrak{p}}, C_l)$) which corresponds to the short exact sequence by ε (resp., $\varepsilon_{\mathfrak{p}}$). A necessary and sufficient condition for (3.1) (resp., (3.2)) to be weakly solvable is that $\rho^*(\varepsilon) = 1$ (resp., $\rho^*_{\mathfrak{p}}(\varepsilon_{\mathfrak{p}}) = 1$) [Hoe, Lemma 1.1] (Note that C_l is a multiplicative group).

It follows from the preceding paragraph and from the weak solvability of each of the local embedding problems that (3.1) is weakly solvable. □

LEMMA 4.4. *Let L/K be an n-Scholz extension with $\bar{G} = \mathcal{G}(L/K)$. Suppose that the central embedding problem* (3.1) *does not split and that the exponent of G is at most l^n. Then* (3.1) *has a solution.*

Proof. By Lemma 4.3, it suffices to prove that each of the local embedding problems (3.2) that (3.1) induces is solvable. To this end we put $L_{\mathfrak{p}} = LK_{\mathfrak{p}}$, replace $\bar{G}_{\mathfrak{p}}$ by the group $\mathcal{G}(L_{\mathfrak{p}}/K_{\mathfrak{p}})$, $D_{\mathfrak{p}}$ by $G(K_{\mathfrak{p}})$, and $\rho_{\mathfrak{p}}$ by $\mathrm{res}_{L_{\mathfrak{p}}}$.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

If $L_\mathfrak{p}/K_\mathfrak{p}$ is an unramified extension, then $\rho_\mathfrak{p}$ decomposes through a map $\bar{\rho}_\mathfrak{p}: \hat{\mathbb{Z}} = \mathcal{G}(K_{\mathfrak{p},\mathrm{ur}}/K_\mathfrak{p}) \to \mathcal{G}(L_\mathfrak{p}/K_\mathfrak{p})$ and therefore (3.2) is weakly solvable.

If $L_\mathfrak{p}/K_\mathfrak{p}$ is ramified, then by (3.4b) and (3.4a), it is totally ramified and $\zeta_{l^n} \in K_\mathfrak{p}$. By (3.3a) $l \neq \mathrm{char}(\bar{K}_\mathfrak{p})$ and therefore the ramification is tame. Hence $L_\mathfrak{p}$ is a cyclic Kummer extension. Since $\mathcal{G}(L_\mathfrak{p}/K_\mathfrak{p})$ is isomorphic to a subgroup of $\bar{G}$ and since the exponent of $\bar{G}$ is at most l^{n-1}, the order of $\mathcal{G}(L_\mathfrak{p}/K_\mathfrak{p})$ is at most l^{n-1}. Thus $L_\mathfrak{p} = K_\mathfrak{p}(\sqrt[l^{m-1}]{a})$ for some $m \leq n$ and $a \in K_\mathfrak{p}$ with $v_\mathfrak{p}(a) = 0$ [CaF, p. 32]. If (3.2) splits, then it certainly has a weak solution. If (3.2) does not split, then $G_\mathfrak{p}$ is a cyclic group of order l^m. Then $L'_\mathfrak{p} = K_\mathfrak{p}(\sqrt[l^m]{a})$ is a cyclic extension of $K_\mathfrak{p}$ of degree l^m which contains $L_\mathfrak{p}$. The composition of $\mathrm{res}: G(K_\mathfrak{p}) \to \mathcal{G}(L'_\mathfrak{p}/K_\mathfrak{p})$ with an isomorphism $\mathcal{G}(L'_\mathfrak{p}/K_\mathfrak{p}) \to G_\mathfrak{p}$ which maps generators of both groups to the same generator of $\mathcal{G}(L_\mathfrak{p}/K_\mathfrak{p})$ solves the local embedding problem (3.2). □

§5. Linearly disjoint fields; an exceptional set of primes

The condition that Lemma 5.1 imposes on the subgroup A of $\mathbb{F}_l^\times$ to be nontrivial is translated in Lemma 5.2 to $\zeta_l \notin K$. This condition restricts the Scholz-Reichardt method of realizing l-groups over K to the case where $\zeta_l \notin K$. In particular, as $\zeta_2 = -1$ belongs to every field, the method fails for $l = 2$.

The introduction of an 'exceptional set of primes' (Definition 5.4, Lemma 5.5, and Data 5.6) allow us to handle number fields and the case $l | h_K$. To find such a set and also for further applications we construct a special Galois extension N^* of K. Then we use the Chebotarev density theorem and find primes of K whose Artin symbol is the conjugacy class of a given element of $\mathcal{G}(N^*/K)$ and therefore have specific decomposition behaviour in N^*.

LEMMA 5.1. *Let A be a nontrivial subgroup of $\mathbb{F}_l^\times$ which acts on the direct product $C = C_l^m$ in a natural way: $(c_1, \ldots, c_m)^\alpha = (c_1^\alpha, \ldots, c_m^\alpha)$. Then the semidirect product $G = C \rtimes A$ has no nontrivial quotients of order l.*

Proof. Let $h: G \to C_l$ be a homomorphism. Then the order of $h(A)$ divides both l and $l-1$, and therefore $h(A) = 1$. Let now $1 \neq \alpha \in A$ and $c \in C$. Then $h(c)^\alpha = h(c^\alpha) = h(\alpha^{-1}c\alpha) = h(\alpha)^{-1}h(c)h(\alpha) = h(c)$ and hence $h(c) = 1$. Conclude that $h = 1$. □

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Let S be a finite set of primes of K and consider elements $a_1, \dots, a_s$ of K_S. We say that $a_1, \dots, a_s$ are **multiplicatively independent modulo** K_S^l if each relation

$$a_1^{l_1} \cdots a_s^{l_s} = b^l. \tag{5.1}$$

with $l_1, \dots, l_s \in \mathbb{Z}$ and $b \in K_S$ implies that $l | l_i$, $i = 1, \dots, s$. Replace '$b \in K_S$' by '$b \in K^\times$' to define the expression **multiplicatively independent modulo** $(K^\times)^l$.

LEMMA 5.2. *Let S be a finite set of primes of K. Let $a_1, \dots, a_s$ be multiplicatively independent elements of K_S modulo K_S^l. Then the fields $K(\zeta_l, \sqrt[l]{a_1}), \dots, K(\zeta_l, \sqrt[l]{a_s})$ are linearly disjoint and of degree l over $K(\zeta_l)$.*

Further, suppose that $\zeta_l \notin K$. Let L be an l-extension of K and let n be a positive integer. Then, the fields $L(\zeta_{l^n}, \sqrt[l]{a_1}), \dots, L(\zeta_{l^n}, \sqrt[l]{a_s})$ are linearly disjoint and of degree l over $L(\zeta_{l^n})$. In particular, $[L(\zeta_{l^n}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s}) : L(\zeta_{l^n})] = l^s$.

Proof. Observe that $a_1, \dots, a_s$ are even multiplicatively independent modulo $(K^\times)^l$. Indeed, let $l_1, \dots, l_s \in \mathbb{Z}$ and $b \in K^\times$ such that (5.1) holds. Then $l v_\mathfrak{p}(b) = 0$ and therefore $v_\mathfrak{p}(b) = 0$ for each $\mathfrak{p} \notin S$. So, $b \in K_S$. Hence l divides $l_1, \dots, l_s$, as desired.

It follows that $a_1, \dots, a_s$ are also multiplicatively independent modulo $(K(\zeta_l)^\times)^l$. Indeed, $k = [K(\zeta_l) : K]$ divides $l - 1$ and is therefore relatively prime to l. If in (5.1) $b \in K(\zeta_l)$, we take the norm of both sides to obtain

$$a_1^{kl_1} \cdots a_s^{kl_s} = (N_{K(\zeta_l)/K} b)^l.$$

By the preceding paragraph $l | kl_i$. Hence $l | l_i$ for $i = 1 \dots, s$, as desired.

By Kummer theory [Lan, p. 220, Thm. 14], the fields $K(\zeta_l, \sqrt[l]{a_1}), \dots, K(\zeta_l, \sqrt[l]{a_s})$ are linearly disjoint and of degree l over $K(\zeta_l)$. Hence $M = K(\zeta_l, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s})$ is a Galois extension of K and $\mathcal{G}(M/K)$ is the semidirect product of $\mathcal{G}(M/K(\sqrt[l]{a_1}, \dots, \sqrt[l]{a_s}))$ with $\mathcal{G}(M/K(\zeta_l)) \cong \mathbb{F}_l^s$. The former group is isomorphic to $\mathcal{G}(K(\zeta_l)/K)$ and therefore to a subgroup of $\mathbb{F}_l^\times$ which acts on the latter group by scalar multiplication. Indeed, if $\sigma \in \mathcal{G}(M/K(\sqrt[l]{a_1}, \dots, \sqrt[l]{a_s}))$ satisfies $\zeta_l^\sigma = \zeta_l^s$ for some $s \in \mathbb{F}_l^\times$ and $\tau \in \mathcal{G}(M/K(\zeta_l))$, then $\sigma^{-1}\tau\sigma = \tau^s$.

We may write $K(\zeta_{l^n}) = K(\zeta_l)K'$ where K' is a cyclic extension of K of degree l^m with $m \leq n - 1$. So, LK' is an l-extension of K. Since, by

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

assumption, $\mathcal{G}(K(\zeta_l)/K)$ is nontrivial, M/K has no Galois subextension of degree l (Lemma 5.1). Hence $M \cap LK' = K$ and therefore $M \cap L(\zeta_{l^n}) = K(\zeta_l)$. Let $N = L(\zeta_{l^n}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s})$. Then $\mathcal{G}(N/L(\zeta_{l^n})) \cong \mathcal{G}(M/K(\zeta_l))$. In particular $L(\zeta_{l^n}, \sqrt[l]{a_1}), \dots, L(\zeta_{l^n}, \sqrt[l]{a_s})$ are linearly disjoint and of degree l over $L(\zeta_{l^n})$.

$$\begin{tikzcd}
M \arrow[rr, dash] \arrow[d, dash] & & N \arrow[d, dash] \\
K(\zeta_l, \sqrt[l]{a_i}) \arrow[rr, dash] \arrow[d, dash] & & L(\zeta_{l^n}, \sqrt[l]{a_i}) \arrow[d, dash] \\
K(\zeta_l) \arrow[r, dash] \arrow[d, dash] & L(\zeta_l) \arrow[r, dash] \arrow[d, dash] & L(\zeta_{l^n}) \arrow[d, dash] \\
K \arrow[r, dash] & L \arrow[r, dash] & LK'
\end{tikzcd}$$

□

Remark 5.3. Under the assumption of Lemma 5.2 suppose that L is a function field over a finite field K_0. Then $N = L(\zeta_{l^n}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s})$ is a regular extension of $K_0(\zeta_{l^n})$

Indeed, let $L(\zeta_{l^\infty}) = L(\zeta_l, \zeta_{l^2}, \zeta_{l^3}, \dots)$. Since n is arbitrary in the last paragraph of the proof of Lemma 5.2, we have that $M \cap L(\zeta_{l^\infty}) = K(\zeta_l)$. Since $K_0(\zeta_{l^\infty})$ has no l-extensions and $M/K(\zeta_l)$ is an l-extension, this implies that $M \cap L\tilde{K}_0 = K(\zeta_l)$. Hence $N \cap L\tilde{K}_0 = L(\zeta_{l^n})$. Since L/K_0 is regular, $L(\zeta_{l^n}) \cap \tilde{K}_0 = K_0(\zeta_{l^n})$. Conclude that $N \cap \tilde{K}_0 = K_0(\zeta_{l^n})$, that is $N/K_0(\zeta_{l^n})$ is regular.

Definition 5.4. (Exceptional set of primes) Let $r = \mathrm{rank}_l(K)$ and choose $\alpha_1, \dots, \alpha_r$ in I_K (resp., I_K^0) which represent a multiplicative basis over $\mathbb{F}_l$ for $\mathrm{Cl}(K)_l$ (resp., $\mathrm{Cl}_0(K)_l$) if K is a number field (resp., function field). By definition there exist $\mu_i \in U$ and $a_i^* \in K^\times$ such that

$$\alpha_i^l = \mu_i a_i^*, \qquad i = 1, \dots, r. \tag{5.2}$$

We call $a_1^*, \dots, a_r^*$ an l-**basis** for K and fix it for the whole work. We also choose fundamental units of K. These are elements $w_1, \dots, w_s \in E_K$, with $s = \mathrm{rank}_\infty(K)$, which generate E_K modulo μ_K. We fix them too for the whole work. We also fix the following **basic** Galois extension of K:

$$N^* = K(\zeta_{l^n}, \sqrt[l]{a_1^*}, \dots, \sqrt[l]{a_r^*}, \sqrt[l]{w_1}, \dots, \sqrt[l]{w_s}).$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

By (5.2), $\mathrm{Ram}(N^*/K) \subseteq \mathbb{P}_l \cup \mathbb{P}_\infty$.

An n**-exceptional set** of primes of K is a set of finite primes

$$S_1 = \{\mathfrak{p}_1^*, \dots, \mathfrak{p}_r^*, \mathfrak{q}_1^*, \dots, \mathfrak{q}_s^*\} \tag{5.3}$$

which is disjoint from S_0 such that for all $i, i' \in \{1, \dots, r\}$ and all $j, j' \in \{1, \dots, s\}$ we have

$$\begin{aligned} &a_i^* \in K_{\mathfrak{p}_{i'}^*}^l \iff i \neq i'; \qquad a_i^* \in K_{\mathfrak{q}_j^*}^l, \\ &w_j \in K_{\mathfrak{p}_i^*}^l; \qquad w_j \in K_{\mathfrak{q}_{j'}^*}^l \iff j \neq j', \text{ and} \\ &\zeta_{l^n} \in K_{\mathfrak{p}_i^*}, \ \zeta_{l^n} \in K_{\mathfrak{q}_j^*}. \end{aligned} \tag{5.4}$$

Lemma 5.5. (Characterization of exceptional set) *Let*

$$N_i = K(\zeta_{l^n}, \sqrt[l]{a_1^*}, \dots, \sqrt[l]{a_{i-1}^*}, \sqrt[l]{a_{i+1}^*}, \dots, \sqrt[l]{a_r^*}, \sqrt[l]{w_1}, \dots, \sqrt[l]{w_s}), \qquad i = 1, \dots, r$$

$$N_j' = K(\zeta_{l^n}, \sqrt[l]{a_1^*}, \dots, \sqrt[l]{a_r^*}, \sqrt[l]{w_1}, \dots, \sqrt[l]{w_{j-1}}, \sqrt[l]{w_{j+1}}, \dots, \sqrt[l]{w_s}), \qquad j = 1, \dots, s$$

Then

(a) *N^*/N_i and N^*/N_j' are cyclic extensions of degree l, N^*/K is a Galois extension of degree $[K(\zeta_l^n) : K]l^{r+s}$, N_i/K and N_j'/K are Galois extensions, and*

(b) *the set S_1 (of (5.3)) is exceptional if and only if it is disjoint from S_0, and*

$$D_{\mathfrak{p}_i^*}(N^*/K) = \mathcal{G}(N^*/N_i) \text{ and } D_{\mathfrak{q}_j^*}(N^*/K) = \mathcal{G}(N^*/N_j'), \tag{5.5}$$

for $i = 1, \dots, r$ and $j = 1, \dots, s$.

Proof. Let $S = \mathbb{P}_\infty$. Once we prove that $a_1^*, \dots, a_r^*, w_1, \dots, w_s$ are multiplicatively independent modulo $K^\times$, (a) will follow from Lemma 5.2 with $L = K$. Since the fixed field of the decomposition group of a prime $\mathfrak{p}$ in N^* is $N^* \cap K_\mathfrak{p}$, statement (b) will then also hold. Note that since $\mathcal{G}(N^*/N_i)$ and $\mathcal{G}(N^*/N_j')$ are normal subgroups of $\mathcal{G}(N^*/K)$, (5.5) is independent of the embedding we have chosen for $\tilde{K}$ in $\tilde{K}_{\mathfrak{p}_i^*}$.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Suppose therefore that $k_1, \dots, k_r, l_1, \dots, l_s$ are integers and $b \in K^\times$ such that

$$(5.6) \qquad (a_1^*)^{k_1} \cdots (a_r^*)^{k_r} w_1^{l_1} \cdots w_s^{l_s} = b^l.$$

Then, by (5.2),

$$(5.7) \qquad \mu_1^{-k_1} \cdots \mu_r^{-k_r} w_1^{l_1} \cdots w_s^{l_s} = (\alpha_1^{-k_1} \cdots \alpha_r^{-k_r} b)^l.$$

Since the left hand side of (5.7) belongs to U, so is its right hand side and therefore $\alpha_1^{k_1} \cdots \alpha_r^{k_r} b^{-1} \in U$. Hence $\alpha_1^{k_1} \cdots \alpha_r^{k_r} \in UK^\times$. By the choice of $\alpha_1, \dots, \alpha_r$ each k_i is a multiple of l.

It follows from (5.6) that there exists $c \in K^\times$ such that $w_1^{l_1} \cdots w_s^{l_s} = c^l$. Hence $c \in E_K$ and since $w_1, \dots, w_s$ are multiplicatively independent over $\mathbb{Z}$ and generate E_K modulo μ_K, each l_j is a multiple of l. Conclude that $a_1^* \dots, a_r^*, w_1, \dots, w_s$ are multiplicatively independent modulo $(K^\times)^l$. □

Data 5.6. (Exceptional set of primes) Choose a generator σ_i^* for $\mathcal{G}(N^*/N_i)$, let $\mathrm{Con}(\sigma_i^*)$ be the conjugacy class of σ_i^* in $\mathcal{G}(N^*/K)$ and apply the Chebotarev density theorem to choose $\mathfrak{p}_i^* \in \mathbb{P} \smallsetminus S_0$ such that $\left(\frac{N^*/K}{\mathfrak{p}_i^*}\right) = \mathrm{Con}(\sigma_i^*)$, $i = 1, \dots, r$. Similarly, choose a generator τ_j^* for $\mathcal{G}(N^*/N_j')$ and $\mathfrak{q}_j^* \in \mathbb{P} \smallsetminus S_0$ such that $\left(\frac{N^*/K}{\mathfrak{q}_j^*}\right) = \mathrm{Con}(\tau_j^*)$, $j = 1, \dots, s$. Since the Artin symbol of a prime generates its decomposition group in N^*, (5.5) holds and therefore, by Lemma 5.5, the set S_1 of (5.3), chosen in this way is exceptional. We fix it for the rest of this work and note that $|S_1| = \mathrm{rank}_\infty(K) + \mathrm{rank}_l(K)$.

Note that if K is a number field, then S_1 is empty exactly if either $K = \mathbb{Q}$ and $l \neq 2$, $K = \mathbb{Q}(\sqrt{-3})$ and $l \neq 2, 3$, or K is another imaginary quadratic field with $l \neq 2$ and $l \nmid h_K$. If K is a function field, then $\mathrm{rank}_\infty(K) = 0$ and $|S_1| = \mathrm{rank}_l(K)$. In this case $S_1 = \emptyset$ is equivalent to $l \nmid h_K$.

§6. Getting rid of extra ramification

The second step in the solution of embedding problem (3.1) is to change the solution ψ_0 we have found in Lemma 4.4 such that in addition to the primes of $\mathrm{Ram}(\rho)$ the only primes of K at which the solution ramifies belong to the exceptional set S_1 which we have chosen in Data 5.6.

LEMMA 6.1. *Let S be a finite set of primes which is disjoint from the exceptional set S_1. For each prime $\mathfrak{p} \in S$ let $h_\mathfrak{p}: U_\mathfrak{p} \to C_l$ be a continuous*

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

homomorphism. Suppose that $\zeta_l \notin K$. Then there exists a continuous homomorphism $h: C_K \to C_l$ such that $h|_{U_\mathfrak{p}} = h_\mathfrak{p}$ for each $\mathfrak{p} \in S$ and $h(U_\mathfrak{p}) = 1$ for each prime $\mathfrak{p} \notin S \cup S_1$

Proof. We break the proof into five parts.

Part A. (*Definition of $h_\mathfrak{p}$ for $\mathfrak{p} \in S_1$*)

By (5.4), $\zeta_l \in U_\mathfrak{p}$. Hence, by Lemma 4.1, $U_\mathfrak{p}/U_\mathfrak{p}^l \cong C_l$. Hence, for each $u \in U_\mathfrak{p} \smallsetminus U_\mathfrak{p}^l$ and each $c \in C_l$ there exists a continuous homomorphism $h': U_\mathfrak{p} \to C_l$ such that $h'(u) = c$.

By (5.2) and (5.4), $\mu_i \in U_{\mathfrak{p}_i^*} \smallsetminus U_{\mathfrak{p}_i^*}^l$. Hence, there exists a continuous homomorphism $h_{\mathfrak{p}_i^*}: U_{\mathfrak{p}_i^*} \to C_l$ such that

$$(6.1) \qquad \left(\prod_{\mathfrak{p}\in S} h_\mathfrak{p}(\mu_{i,\mathfrak{p}})\right) \cdot h_{\mathfrak{p}_i^*}(\mu_{i,\mathfrak{p}_i^*}) = 1, \qquad i = 1, \ldots, r.$$

Here, $\mu_{i,\mathfrak{p}}$ is the $\mathfrak{p}$-th component of μ_i. For the same reason, there exists a continuous homomorphism $h_{\mathfrak{q}_j^*}: U_{\mathfrak{q}_j^*} \to C_l$ such that

$$(6.2) \qquad \left(\prod_{\mathfrak{p}\in S} h_\mathfrak{p}(w_j)\right) \cdot h_{\mathfrak{q}_j^*}(w_j) = 1, \qquad j = 1, \ldots, s.$$

This completes the definition of $h_\mathfrak{p}$ for each $\mathfrak{p} \in S_1$.

By (5.2) and (5.4), $\mu_i \in U_\mathfrak{p}^l$ and therefore

$$(6.3) \qquad h_\mathfrak{p}(\mu_{i,\mathfrak{p}}) = 1 \text{ for each } \mathfrak{p} \in S_1 \smallsetminus \{\mathfrak{p}_i^*\}$$

By (5.4), $w_j \in U_\mathfrak{p}^l$ and therefore

$$(6.4) \qquad h_\mathfrak{p}(w_j) = 1 \text{ for each } \mathfrak{p} \in S_1 \smallsetminus \{\mathfrak{q}_j^*\}$$

Part B. (*Definition of f' on $UK^\times/K^\times$*)

The formula

$$(6.5) \qquad f(\mu) = \prod_{\mathfrak{p}\in S\cup S_1} h_\mathfrak{p}(\mu_\mathfrak{p})$$

defines a continuous homomorphism f from the open subgroup U of I_K into C_l that is trivial on $U_\mathfrak{p}$ for each $\mathfrak{p} \notin S \cup S_1$ and coincides with $h_\mathfrak{p}$ on $U_\mathfrak{p}$ for each $\mathfrak{p} \in S \cup S_1$. By (6.2) and (6.4), $f(w_j) = 1$ for $j = 1, \ldots, s$. Since $|\mu_K|$ is relatively prime to l, f is trivial on μ_K. It follows that f is trivial on $E_K = U \cap K^\times$. So, f defines a homomorphism $\bar{f}: U/E_K \to C_l$ which we compose with the isomorphism $UK^\times/K^\times \cong U/E_K$ to get a continuous homomorphism $f': UK^\times/K^\times \to C_l$.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Part C. (*Claim:* $I_K^l K^\times \cap UK^\times = U^l K^\times \cdot \prod_{i=1}^r \langle \mu_i \rangle$)

Indeed, as $\mu_i = \alpha_i^l (a_i^*)^{-1}$, by (5.2), the right hand side is contained in the left hand side. Each element of the left hand side has the form $\xi = \alpha^l a = \mu b$ with $\alpha \in I_K$, $a, b \in K^\times$, and $\mu \in U$. Thus $\alpha^l = \mu b a^{-1} \in UK^\times$. If K is a function field, then $l \deg(\alpha) = \deg(\mu) + \deg(ba^{-1}) = 0$ and hence $\deg(\alpha) = 0$, so that $\alpha \in I_K^0$. So, in any case $\alpha = \nu c \prod_{i=1}^r \alpha_i^{k_i}$ for some $\nu \in U$, $c \in K^\times$, and $k_i \in \mathbb{Z}$, $i = 1, \ldots, r$. It follows from (5.2) that $\xi = \nu^l (c^l \prod_{i=1}^r (a_i^*)^{k_i}) \prod_{i=1}^r \mu_i^{k_i}$ belongs to the right hand side. This concludes the proof of the claim.

Part D. (*Definition of* g *on* $I_K^l UK^\times / K^\times$)

By (6.1) and (6.3), $f(\mu_i) = 1$, $i = 1, \ldots, r$. Hence, by Part C, f' is trivial on $(I_K^l K^\times \cap UK^\times)/K^\times$. So, f' extends to a continuous homomorphism $g\colon I_K^l UK^\times / K^\times \to C_l$ which is trivial on $I_K^l K^\times / K^\times$, coincides with $h_\mathfrak{p}$ on $U_\mathfrak{p}$ for each $\mathfrak{p} \in S \cup S_1$, and is trivial $U_\mathfrak{p}$ for each $\mathfrak{p} \notin S \cap S_1$.

$$\begin{tikzcd}
I_K^l K^\times \arrow[r, dash] \arrow[d, dash] & I_K^l UK^\times \arrow[d, dash] \\
I_K^l K^\times \cap UK^\times \arrow[r, dash] & UK^\times
\end{tikzcd}$$

Part E. (*Conclusion of the proof*)

Finally observe that $I_K/UK^\times$ is a finitely generated abelian profinite group (Section 1). Hence, $I_K^l UK^\times / I_K^l K^\times$ is an open subgroup of C_K/C_K^l. The latter group may be considered as a vector space over $\mathbb{F}_l$ and $I_K^l UK^\times / K^\times$ has a closed complement in it. So, g extends to a continuous homomorphism $h\colon C_K \to C_l$. □

LEMMA 6.2. *Suppose that the central embedding problem* (3.1) *does not split. Assume that* $\zeta_l \notin K$. *If the central embedding problem* (3.1) *has a solution* ψ_0, *then* (3.1) *also has a solution* $\psi\colon G(K) \to G$ *for which* $\mathrm{Ram}(\psi) \subseteq \mathrm{Ram}(\rho) \cup S_1$.

Proof. Let $S = \mathrm{Ram}(\psi_0) \smallsetminus (S_1 \cup \mathrm{Ram}(\rho))$. If $\mathfrak{p} \in S$, then $\rho(I_\mathfrak{p}) = 1$ and therefore $\psi_0(I_\mathfrak{p}) \le C_l$. (Actually, as $\mathfrak{p} \in \mathrm{Ram}(\psi_0)$, we have $\psi_0(I_\mathfrak{p}) \neq 1$ and therefore $\psi_0(I_\mathfrak{p}) = C_l$.) The reciprocity law (2.3) associates with $\psi_0|_{I_\mathfrak{p}}$ a continuous homomorphism $h_\mathfrak{p}\colon U_\mathfrak{p} \to C_l$. By Lemma 6.1 there exists a continuous homomorphism $h\colon C_K \to C_l$ such that $h|_{U_\mathfrak{p}} = h_\mathfrak{p}$ for each $\mathfrak{p} \in S$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

and $h(U_\mathfrak{p}) = 1$ for each $\mathfrak{p} \notin S \cup S_1$. Apply again the reciprocity law to obtain a continuous homomorphism $\eta\colon G(K) \to C_l$ such that $\eta|_{I_\mathfrak{p}} = \psi_0|_{I_\mathfrak{p}}$ for each $\mathfrak{p} \in S$ and $\eta(I_\mathfrak{p}) = 1$ for each $\mathfrak{p} \notin S \cup S_1$. Consider the solution $\psi = \eta^{-1} \cdot \psi_0$ to (3.1). Then, $\psi(I_\mathfrak{p}) = 1$ for each $\mathfrak{p} \in S \cup [\mathbb{P} \smallsetminus (\mathrm{Ram}(\psi_0 \cup S_1))]$. Hence, $\mathrm{Ram}(\psi) \subseteq (\mathbb{P} \smallsetminus S) \cap [\mathrm{Ram}(\psi_0) \cup S_1] \subseteq \mathrm{Ram}(\rho) \cup S_1$, as desired. □

§7. Scholz solution of a nonsplitting embedding problem

The last step in the solution of embedding problem (3.1) is to multiply the solution which Lemma 6.2 gives with a homomorphism $\eta\colon G(G) \to C_l$ such that the resulting solution will be n-Scholz.

LEMMA 7.1. *Let S be a finite set of primes of K which contains S_0. Let L be a finite l-extension of K and let n be a positive integer. For each $\mathfrak{p} \in S$ let $h_\mathfrak{p}\colon K_\mathfrak{p}^\times \to C_l$ be a homomorphism. Suppose that $\zeta_l \notin K$.*

Then there exists a prime $\mathfrak{q}$ of K and there exists a continuous homomorphism $h\colon C_K \to C_l$ such that

(a) *$\mathfrak{q} \notin S$ and $L(\zeta_{l^n}) \subseteq K_\mathfrak{q}$,*

(b) *$h|_{K_\mathfrak{p}^\times} = h_\mathfrak{p}$ for each $\mathfrak{p} \in S$,*

(c) *$h(U_\mathfrak{q}) = C_l$,*

(d) *$h(U_\mathfrak{p}) = 1$ for each $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$.*

Proof. We break the proof into five parts.

Part A. (*Reduction of the lemma to constructing a homomorphism $g\colon \bar{I}_{K,S}/\bar{K}_S \to C_l$*)

Let $(K_S : K_S^l) = l^s$. Choose generators $a_1, \dots, a_s$ for K_S modulo K_S^l. For each $\mathfrak{q} \notin S$ we can decompose $I_{K,S}$ as

$$I_{K,S} = \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^\times \times U_\mathfrak{q} \times \prod_{\mathfrak{p} \notin S \cup \{\mathfrak{q}\}} U_\mathfrak{p}.$$

Use a bar to denote the reduction of elements and subgroups of $I_{K,S}$ modulo $I_{K,S}^l$. In particular[1]

$$\bar{I}_{K,S} = \prod_{\mathfrak{p} \in S} \overline{K_\mathfrak{p}^\times} \times \bar{U}_\mathfrak{q} \times \prod_{\mathfrak{p} \notin S \cup \{\mathfrak{q}\}} \bar{U}_\mathfrak{p}. \tag{7.1}$$

[1] Do not confuse $\overline{K_\mathfrak{p}^\times} \cong K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^l$ with the multiplicative group of the $\bar{K}_\mathfrak{p}^\times$ of the residue field $\bar{K}_\mathfrak{p}$, for $\mathfrak{p} \notin \mathbb{P}_\infty$.

and

$$\bar K_S = \langle \bar a_1, \dots, \bar a_s \rangle \tag{7.2}$$

Also, $h_\mathfrak{p}\colon K_\mathfrak{p}^\times \to C_l$ induces a homomorphism $\bar h_\mathfrak{p}\colon \overline{K_\mathfrak{p}^\times} \to C_l$. Then $\bar I_{K,S}/\bar K_S = (I_{K,S}/I_{K,S}^l)/(K_S I_{K,S}^l/I_{K,S}^l)$ is a quotient of $C_K = I_{K,S}/K_S$ (See (1.5)). Hence, it suffices to find a prime $\mathfrak{q}$ of K which satisfies (a) and to construct a homomorphism $g\colon \bar I_{K,S} \to C_l$ such that

$$g|_{\overline{K_\mathfrak{p}^\times}} = \bar h_\mathfrak{p} \quad \text{for each } \mathfrak{p} \in S, \tag{7.3a}$$

$$g(\bar U_\mathfrak{q}) = C_l, \tag{7.3b}$$

$$g(\bar U_\mathfrak{p}) = 1 \quad \text{for each } \mathfrak{p} \notin S \cup \{\mathfrak{q}\}. \tag{7.3c}$$

$$g(\bar a_i) = 1 \quad \text{for } i = 1, \dots, s. \tag{7.3d}$$

By (7.1) and (7.3), g will induce a homomorphism $\bar g\colon \bar I_{K,S}/\bar K_S \to C_l$ which will compose with the canonical homomorphism $C_K \to \bar I_{K,S}/\bar K_S$ to the desired homomorphism h.

Part B. (*Presentation of $\bar a_i$ as an idele*)

For each i between 1 and s and each $\mathfrak{p}$ let $a_{i\mathfrak{p}}$ be a_i considered as an element of $K_\mathfrak{p}$ and let

$$\delta_i = \prod_{\mathfrak{p} \in S} h_\mathfrak{p}(a_{i\mathfrak{p}}) \tag{7.6}$$

If $\mathfrak{q}$ satisfies (a), then $a_1, \dots, a_s, \zeta_l \in U_\mathfrak{q}$ and $\bar U_\mathfrak{q} \cong C_l$ (Lemma 4.1). Choose a generator $\bar u_\mathfrak{q}$ of $\bar U_\mathfrak{q}$. For each i there exists then $0 \le \beta_i < l$ such that $\bar a_{i\mathfrak{q}} = \bar u_\mathfrak{q}^{\beta_i}$. The representation of $\bar a_i$ as an idele will therefore take the form:

$$\bar a_i = \prod_{\mathfrak{p} \in S} \bar a_{i\mathfrak{p}} \cdot \bar u_\mathfrak{q}^{\beta_i} \cdot \prod_{\mathfrak{p} \notin S \cup \{\mathfrak{p}\}} \bar a_{i\mathfrak{p}}. \tag{7.7}$$

Conditions (7.3a) and (7.3c) force that $g(\bar a_{i\mathfrak{p}}) = h(\bar a_{i\mathfrak{p}})$ for $\mathfrak{p} \in S$ and $g(\bar a_{i\mathfrak{p}}) = 1$ for $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$. Condition (7.3b) is equivalent to $g(\bar u_\mathfrak{q}) \neq 1$. We have therefore to choose $\mathfrak{q}$ such that (a) will hold and to define $g(\bar u_\mathfrak{q})$ as a nonzero element of C_l such that (7.3d) will be satisfied.

If $\delta_i = 1$ for $i = 1, \dots, r$ we may use the Chebotarev density theorem to choose $\mathfrak{q} \notin S$ such that

$$N = L(\zeta_{l^n}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s}) \subseteq K_\mathfrak{q}. \tag{7.8}$$

In particular (a) holds and $a_{i\mathfrak{q}} \in U_{\mathfrak{q}}^l$ so that $\beta_i = 0$ for $i = 1, \dots, s$. We therefore define $g(\bar{u}_{\mathfrak{q}})$ to be a generator of C_l and derive from (7.7) that $g(\bar{a}_i) = \delta_i \cdot g(\bar{u}_{\mathfrak{q}})^{\beta_i} = 1$, so that (7.3d) holds.

Part C. (*The main case*)

We may and we will from now assume that

$$(7.9) \qquad \delta_1 \neq 1$$

Under this assumption there exists $0 \leq \varepsilon_i < l$ such that in C_l

$$(7.10) \qquad \delta_1^{\varepsilon_i} = \delta_i, \qquad i = 1, 2, \dots, s.$$

In particular $\varepsilon_1 = 1$. Define

$$(7.11) \qquad b_1 = a_1 \text{ and } b_i = a_i / a_1^{\varepsilon_i}, \text{ for } i = 2, \dots, s.$$

As $a_1, \dots, a_s$ are multiplicatively independent modulo K_S^l, so are $b_1, \dots, b_s$. By Lemma 5.2, $L(\zeta_{l^n}, \sqrt[l]{b_1}), \dots, L(\zeta_{l^n}, \sqrt[l]{b_s})$ are linearly disjoint fields of degree l over $L(\zeta_{l^n})$.

Part D. (*Choosing* $\mathfrak{q}$)

Part C allows us to choose $\sigma \in \mathcal{G}(N/L(\zeta_{l^n}))$ with $\sigma\sqrt[l]{a_1} = \zeta_l\sqrt[l]{a_1}$ and $\sigma\sqrt[l]{b_i} = \sqrt[l]{b_i}$, $i = 2, \dots, s$.

Chebotarev density theorem gives a prime $\mathfrak{q} \notin S$ such that $\left(\frac{N/K}{\mathfrak{q}}\right) = \mathrm{Con}(\sigma)$. Thus, $L(\zeta_{l^n}) \subseteq K_{\mathfrak{q}}$ but $K_{\mathfrak{q}}(\zeta_{l^n}, \sqrt[l]{a_1})$ is an unramified extension of $K_{\mathfrak{q}}$ of degree l. In particular $a_1 \in U_{\mathfrak{q}} \smallsetminus U_{\mathfrak{q}}^l$. On the other hand $b_i \in U_{\mathfrak{q}}^l$ and therefore, by (7.11)

$$(7.12) \qquad \bar{a}_{i\mathfrak{q}} = \bar{a}_{1\mathfrak{q}}^{\varepsilon_i} \qquad i = 2, \dots, s.$$

Part E. (*Definition of* g)

By Part B, $\bar{a}_{1\mathfrak{q}} = \bar{u}_{1\mathfrak{q}}^{\beta}$ with $0 < \beta < l$. We may therefore define $g(\bar{u}_{\mathfrak{q}})$ as the element of C_l that satisfies

$$(7.13) \qquad g(\bar{u}_{\mathfrak{q}})^{\beta} = \delta_1^{-1}$$

In particular $g(\bar{u}_{\mathfrak{q}}) \neq 1$. By (7.12), $\bar{a}_{i\mathfrak{q}} = \bar{u}_{\mathfrak{q}}^{\beta\varepsilon_i}$, $i = 2, \dots, s$. As $\varepsilon_1 = 1$ the latter equality also holds for $i = 1$. This gives (7.7) the following form:

$$(7.14) \qquad \bar{a}_i = \prod_{\mathfrak{p} \in S} \bar{a}_{i\mathfrak{p}} \cdot \bar{u}_{\mathfrak{q}}^{\beta\varepsilon_i} \prod_{\mathfrak{p} \notin S \cup \{\mathfrak{q}\}} \bar{a}_{i\mathfrak{p}}.$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Apply g on (7.14) and use (7.3a), (7.3c), (7.6), (7.13), and (7.10) to get that

$$g(\bar{a}_i) = \left(\prod_{\mathfrak{p}\in S} g(\bar{a}_{i\mathfrak{p}})\right) \cdot g(\bar{u}_{\mathfrak{q}})^{\beta\varepsilon_i} = \delta_i\delta_1^{-\varepsilon_i} = 1.$$

So (7.3d) holds and the proof is complete. □

LEMMA 7.2. *Suppose that* (3.1) *is a central embedding problem such that ρ is an n-Scholz epimorphism which respects the local data $\{\rho_{\mathfrak{p}} = \alpha\circ\varphi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$. Suppose further that $\zeta_l \notin K$ and that* (3.1) *has a solution ψ such that* $\mathrm{Ram}(\psi) \cup S_1 = \mathrm{Ram}(\rho) \cup S_1$. *Then there exists a prime $\mathfrak{q} \notin$* $\mathrm{Ram}(\psi)\cup S_0\cup S_1$ *at which ρ totally decomposes and there exists an n-Scholz solution $\varphi\colon G(K) \to G$ to* (3.1) *which respects the local data $\{\varphi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$ such that* $\mathrm{Ram}(\varphi) \cup S_0 = \mathrm{Ram}(\psi) \cup \{\mathfrak{q}\} \cup S_0$.

Proof. Let L (resp., L') be the fixed field of $\mathrm{Ker}(\rho)$ (resp., $\mathrm{Ker}(\psi)$) in K_s. For each $\mathfrak{p} \in S = \mathrm{Ram}(\psi) \cup S_0 \cup S_1$ we define a homomorphism $\eta_{\mathfrak{p}}\colon D_{\mathfrak{p}} \to C_l$ as follows:

If $\mathfrak{p} \in (\mathrm{Ram}(\psi) \smallsetminus S_0) \cup S_1$, then $\mathfrak{p} \in \mathrm{Ram}(\rho) \cup S_1$. Choose a lifting of $\mathrm{Frob}_{\mathfrak{p}}$ to an element $\sigma_{\mathfrak{p}}$ of $D_{\mathfrak{p}}$. Since ρ is n-Scholz, we have $\alpha \circ \psi(\sigma_{\mathfrak{p}}) = \rho(\sigma_{\mathfrak{p}}) \in \rho(D_{\mathfrak{p}}) = \rho(I_{\mathfrak{p}}) = \alpha \circ \psi(I_{\mathfrak{p}})$. Hence, there exists $\tau \in I_{\mathfrak{p}}$ and $\gamma_{\mathfrak{p}} \in C_l$ such that $\psi(\sigma_{\mathfrak{p}}) = \gamma_{\mathfrak{p}}\psi(\tau)$. Replace $\sigma_{\mathfrak{p}}$ by $\sigma_{\mathfrak{p}}\tau^{-1}$, if necessary, to assume that $\psi(\sigma_{\mathfrak{p}}) = \gamma_{\mathfrak{p}}$. Now define a homomorphism $\bar{\eta}_{\mathfrak{p}}$ from $\langle\mathrm{Frob}_{\mathfrak{p}}\rangle = D_{\mathfrak{p}}/I_{\mathfrak{p}} \cong \hat{\mathbb{Z}}$ to C_l by $\bar{\eta}(\mathrm{Frob}_{\mathfrak{p}}) = \gamma_{\mathfrak{p}}^{-1}$. Then compose $\bar{\eta}_{\mathfrak{p}}$ with the canonical map $D_{\mathfrak{p}} \to D_{\mathfrak{p}}/I_{\mathfrak{p}}$ to a homomorphism $\eta_{\mathfrak{p}}\colon D_{\mathfrak{p}} \to C_l$. It satisfies

$$\eta_{\mathfrak{p}}(I_{\mathfrak{p}}) = 1 \text{ and } \eta_{\mathfrak{p}}(\sigma_{\mathfrak{p}}) = \psi(\sigma_{\mathfrak{p}})^{-1}. \tag{7.15}$$

If $\mathfrak{p} \in S_0$, then $\alpha \circ \psi|_{D_{\mathfrak{p}}} = \rho_{\mathfrak{p}} = \alpha \circ \varphi_{\mathfrak{p}}$. Hence $\varphi_{\mathfrak{p}} = \eta_{\mathfrak{p}} \cdot \psi|_{D_{\mathfrak{p}}}$ with a map $\eta_{\mathfrak{p}}\colon D_{\mathfrak{p}} \to C_l$. Since C_l is contained in the center of G, $\eta_{\mathfrak{p}}$ is a homomorphism.

Lemma 7.1, applied to L' instead of to L and the reciprocity law (2.3) supply a prime $\mathfrak{q} \in \mathbb{P}$ and a continuous epimorphism $\eta\colon G(K) \to C_l$ such that

(7.16a) $\mathfrak{q} \notin S$ and $L'(\zeta_{l^n}) \subseteq K_{\mathfrak{q}}$; in particular $\psi(D_q) = 1$,

(7.16b) $\eta|_{D_{\mathfrak{p}}} = \eta_{\mathfrak{p}}$ for each $\mathfrak{p} \in S$,

(7.16c) $\eta(I_{\mathfrak{q}}) = C_l$, and

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

(7.16d) $\eta(I_{\mathfrak{p}}) = 1$ for each $\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$.

We prove that $\varphi = \eta \cdot \psi : G(K) \to G$ satisfies the requirements of the lemma. To this end, let $\mathfrak{p}$ be a prime of K. We have to prove that if $\mathfrak{p} \notin S_0$, then $\varphi(I_{\mathfrak{p}}) \neq 1$ if and only if $\psi(I_{\mathfrak{p}}) \neq 1$ or $\mathfrak{p} = \mathfrak{q}$. In addition, if $\varphi(I_{\mathfrak{p}}) \neq 1$ or $\mathfrak{p} \in S_1$, then $\varphi(I_{\mathfrak{p}}) = \varphi(D_{\mathfrak{p}})$ should hold. Finally, we have to prove that $\varphi|_{D_{\mathfrak{p}}} = \varphi_{\mathfrak{p}}$ for each $\mathfrak{p} \in S_0$. We distinguish between several cases:

Case A. ($\mathfrak{p} \in (\mathrm{Ram}(\psi) \smallsetminus S_0) \cup S_1$)

Then, by (7.15), $\varphi|_{I_{\mathfrak{p}}} = \eta|_{I_{\mathfrak{p}}} \cdot \psi|_{I_{\mathfrak{p}}} = \psi|_{I_{\mathfrak{p}}}$. So, $\psi(I_{\mathfrak{p}}) \neq 1$ if and only if $\varphi(I_{\mathfrak{p}}) \neq 1$. Also, by (7.15) and (7.16b) $\varphi(\sigma_{\mathfrak{p}}) = \eta_{\mathfrak{p}}(\sigma_{\mathfrak{p}})\psi(\sigma_{\mathfrak{p}}) = 1$. Hence, $\varphi(D_{\mathfrak{p}}) = \varphi(\langle \sigma_{\mathfrak{p}}, I_{\mathfrak{p}} \rangle) = \varphi(I_{\mathfrak{p}})$.

Case B. ($\mathfrak{p} \in S_0$)

By (7.16b), $\varphi|_{D_{\mathfrak{p}}} = \eta_{\mathfrak{p}} \cdot \psi|_{D_{\mathfrak{p}}} = \varphi_{\mathfrak{p}}$. So, φ respects the given local data.

Case C. ($\mathfrak{p} = \mathfrak{q}$)

By (7.16a), $\psi(D_{\mathfrak{q}}) = 1$ and hence, by (7.16c), $\varphi(I_{\mathfrak{q}}) = C_l$. Also, for each $\sigma \in D_{\mathfrak{q}}$ we have $\varphi(\sigma) = \eta(\sigma) \cdot 1 \in C_l$. Hence $C_l = \varphi(I_{\mathfrak{q}}) \leq \varphi(D_{\mathfrak{q}}) \leq C_l$. So, $\varphi(I_{\mathfrak{q}}) = \varphi(D_{\mathfrak{q}})$.

Case D. ($\mathfrak{p} \notin S \cup \{\mathfrak{q}\}$)

Then $\varphi|_{I_{\mathfrak{p}}} = \eta|_{I_{\mathfrak{p}}} \cdot \psi|_{I_{\mathfrak{p}}} = 1$.

In each case all the requirements are fulfilled. □

We combine Lemmas 4.2, 4.3, 6.2, and 7.2:

PROPOSITION 7.3. (Solution of an embedding problem) *Let K be a global field and let $l \neq$ char(K) be a prime such that $\zeta_l \notin K$. Let S_0 be a basic set of primes* (*Data* 1.1), *let n be a positive integer, and let S_1 be an n-exeptional set of primes* (*Data* 5.6). *Consider an embedding problem* (3.1) *for $G(K)$ for which G is an l-group of exponent l^n. Let $\{\varphi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$ be a local data for G and n. Suppose that ρ is an n-Scholz epimorphism which respects the local data $\{\alpha \circ \varphi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$. Then there exists a prime $\mathfrak{q} \notin$ Ram$(\rho) \cup S_0 \cup S_1$ and there exists an n-Scholz solution φ for* (3.1) *which respects the local data $\{\varphi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$ such that*

$$\mathrm{Ram}(\varphi) \cup S_0 \cup S_1 = \mathrm{Ram}(\rho) \cup \{\mathfrak{q}\} \cup S_0 \cup S_1 \tag{7.17}$$

THEOREM 7.4. (Realization of l-groups) *Let K be a global field and let $l \neq$ char(K) be a prime such that $\zeta_l \notin K$. Let S_0 be a basic set of*

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

primes (Data 1.1*), let $m \leq n$ be positive integers, and let S_1 be an n-exeptional set of primes (Data* 5.6*). Consider a group G of order l^m and a local data $\{\varphi_{\mathfrak{p}}: D_{\mathfrak{p}} \to G \mid \mathfrak{p} \in S_0\}$ for G. Then K has a finite Galois extension L which is n-Scholz such that $\mathcal{G}(L/K) \cong G$, for each $\mathfrak{p} \in S_0$ the map* $\mathrm{res}: D_{\mathfrak{p}} \to D_{\mathfrak{p}}(L/K)$ *coincides with $\varphi_{\mathfrak{p}}$, and there exist m primes $\mathfrak{q}_1, \ldots, \mathfrak{q}_m \in \mathbb{P} \smallsetminus (S_0 \cup S_1)$ such that*

$$\mathrm{Ram}(L/K) \cup S_0 \cup S_1 = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\} \mathbin{\dot\cup} S_0 \mathbin{\dot\cup} S_1. \tag{3.18}$$

In particular, if each $\mathfrak{p} \in S_0$ completely decomposes in L, then

$$m \leq |\mathrm{Ram}(L/K)| \leq m + \mathrm{rank}_l(K) + \mathrm{rank}_\infty(K). \tag{3.19}$$

Proof. Suppose without loss that $m \geq 1$ and embed C_l in the center of G, let $\bar{G} = G/C_l$, and let $\alpha: G \to \bar{G}$ be the canonical map. Induction on the order of the group gives an n-Scholz epimorphism $\rho: G(K) \to \bar{G}$ which respects the local data $\{\alpha \circ \varphi_{\mathfrak{p}} \mid \mathfrak{p} \in S_0\}$ such that $|\mathrm{Ram}(\rho) \smallsetminus (S_0 \cup S_1)| = m - 1$. This creates an embedding problem (3.1). Proposition 7.3 supplies an n-Scholz solution of this problem such that (7.17) holds. Conclude that (7.18) is true. As $|S_1| = \mathrm{rank}_l(K) + \mathrm{rank}_\infty(K)$, this gives the estimates (7.19). □

Example 7.5. (Necessity of many ramified primes) We prove in this example that if L/K is an l-elementary abelian extension, then $\mathrm{Ram}(L/K)$ must be 'big'. More precisely, we compute a constant r_0 such that if $[L:K] = l^r$ and l is unramified in L, then $|\mathrm{Ram}(L/K)| \geq r - r_0$.

Indeed, let T be a finite set of m primes which is disjoint from $\mathbb{P}_l \cup \mathbb{P}_\infty$ and let $S = \mathbb{P}_l \cup \mathbb{P}_\infty \cup T$. Let r be the maximal integer for which K admits a Galois extension N which is unramified outside S such that $\mathcal{G}(N/K) \cong C_l^r$. Class field theory suggests a bound on r which does not depend on T.

Claim. *The following inequalities hold for a number field K:*

(7.20a) $r \leq [K:\mathbb{Q}] + |\mathbb{P}_l| + \mathrm{rank}_l(K) + m$, *if $l \neq 2$;*

(7.20b) $r \leq [K:\mathbb{Q}] + |\mathbb{P}_2| + \#$*real archimedean primes* $+ \mathrm{rank}_2(K) + m$, *if $l = 2$*

(7.20c) $r \leq 1 + m$, *if $K = \mathbb{Q}$ and $l \neq 2$,*

(7.20d) $r = 2 + m$, *if $K = \mathbb{Q}$ and $l = 2$,* *The following inequalities hold for a function field K:*

(7.20e) $r \leq 1 + \mathrm{rank}_l(K) + m$, *if K is a function field,*

(7.20f) $r \leq 1 + m$, *if $K = \mathbb{F}_q(t)$.*

Indeed, let $V = \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$. By the reciprocity law (2.3), r is the maximal integer for which there exists a homomorphism $h\colon I_K \to C_l^r$ which is trivial on $VK^\times$. As $V \leq U$ (in the notation of Section 1), we have the following short exact sequence

$$1 \longrightarrow UK^\times/VK^\times \longrightarrow I_K/VK^\times \longrightarrow \mathrm{Cl}(K) \longrightarrow 1.$$

Observe that $UK^\times/VK^\times$ is a homomorphic image of $U/V \cong \prod_{\mathfrak{p} \in S} U_{\mathfrak{p}}$. Hence

$$\begin{aligned} r &= \dim_{\mathbb{F}_l}(I_K/VK^\times)/(I_K/VK^\times)^l \\ &\leq \dim_{\mathbb{F}_l}(UK^\times/VK^\times)/(UK^\times/VK^\times)^l + \dim_{\mathbb{F}_l}\mathrm{Cl}(K)/\mathrm{Cl}(K)^l \\ &\leq \sum_{\mathfrak{p}\in S}\dim_{\mathbb{F}_l} U_{\mathfrak{p}}/U_{\mathfrak{p}}^l + \dim_{\mathbb{F}_l}\mathrm{Cl}(K)/\mathrm{Cl}(K)^l. \end{aligned} \tag{7.21}$$

For each $\mathfrak{p} \in \mathbb{P}_l$ the dimension of $U_{\mathfrak{p}}/U_{\mathfrak{p}}^l$ over $\mathbb{F}_l$ is $[K_{\mathfrak{p}} : \mathbb{Q}_l] + 1$ if $\zeta_l \in K_{\mathfrak{p}}$ and $[K_{\mathfrak{p}} : \mathbb{Q}_l]$ if $\zeta_l \notin K_{\mathfrak{p}}$. If $\mathfrak{p} \in \mathbb{P}_\infty$, then $U_{\mathfrak{p}} = U_{\mathfrak{p}}^l$ unless $l = 2$ and $\mathfrak{p}$ is real. In the latter case $U_{\mathfrak{p}} = \mathbb{R}^\times$ and so $\dim_{\mathbb{F}_2} U_{\mathfrak{p}}/U_{\mathfrak{p}}^2 = 1$. If $\mathfrak{p} \notin \mathbb{P}_l \cup \mathbb{P}_\infty$, then $U_{\mathfrak{p}} = U_{\mathfrak{p}}^l$ unless $\zeta_l \in U_{\mathfrak{p}}$, in which case $\dim_{\mathbb{F}_l} U_{\mathfrak{p}}/U_{\mathfrak{p}}^l = 1$. Thus

$$r \leq \sum_{\mathfrak{p}\in\mathbb{P}_l}([K_{\mathfrak{p}} : \mathbb{Q}_l] + 1) + \Big(\sum_{\mathfrak{p}\text{ real}} 1\Big) + m + \dim_{\mathbb{F}_l}\mathrm{Cl}(K)/\mathrm{Cl}(K)^l \tag{7.22a}$$

$$\leq [K : \mathbb{Q}] + |\mathbb{P}_l| + \#\text{real archimedean primes} + \dim_{\mathbb{F}_l}\mathrm{Cl}(K)/\mathrm{Cl}(K)^l + m \tag{7.22b}$$

where the term '#real archimedean primes' appears only if $l = 2$.

If K is a number field, then $\dim_{\mathbb{F}_l}\mathrm{Cl}(K)/\mathrm{Cl}(K)^l = \mathrm{rank}_l(K)$. If $l \neq 2$, then we can drop $\sum_{\mathfrak{p}\text{ real}} 1$ from (7.22b). So, (7.20a) and (7.20b) hold.

If $K = \mathbb{Q}$, then $\mathrm{Cl}(K) = 1$ and therefore $\dim_{\mathbb{F}_l}\mathrm{Cl}(K)/\mathrm{Cl}(K)^l = 0$. If in addition, $l \neq 2$, that $\zeta_l \notin \mathbb{Q}_l$ and therefore $\mathbb{P}_l = \{l\}$ contributes 1 to the sum $\sum_{\mathfrak{p}\in S}\dim_{\mathbb{F}_l} U_{\mathfrak{p}}/U_{\mathfrak{p}}^l$. If instead, $l = 2$, then #real archimedean primes $= 1$. This gives (7.20c) and (7.20d).

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

If K is a function field, then $|\mathbb{P}_l| = |\mathbb{P}_\infty| = 0$ but

$$\dim_{\mathbb{F}_l} \mathrm{Cl}(K)/\mathrm{Cl}(K)^l = \mathrm{rank}_l(K) + 1.$$

This gives (7.20e). Finally, if $K = \mathbb{F}_q(t)$, then $\mathrm{rank}_l(K) = 0$ and so (7.20f) is true.

Thus, in each case, there exists a constant r_0 that does not depend on m such that $r \leq r_0 + m$. If L/K is a Galois extension with $\mathcal{G}(L/K) \cong C_l^r$ and we take $T = \mathrm{Ram}(L/K) \smallsetminus \mathbb{P}_l$, then we find that $r - r_0 \leq |T|$, which is somewhat stronger than claimed.

Consider now the case in which $l \neq 2$ and $K = \mathbb{Q}$. Then $r_0 = 1$ and $\mathbb{Q}$ has a unique extension L_0 of degree l in which l ramifies. It is the unique extension of degree l which is contained in $\mathbb{Q}(\zeta_{l^2})$. No other prime execpt l is ramified in L_0. If L is a Galois extension of $\mathbb{Q}$ with $\mathcal{G}(L/\mathbb{Q}) \cong C_l^r$ which does not contain L_0, then $\mathcal{G}(LL_0/\mathbb{Q}) \cong C_l^{r+1}$. Hence, by the preceding paragraph $|\mathrm{Ram}(LL_0/\mathbb{Q}) \smallsetminus \mathbb{P}_l| \geq r$. Since $\mathrm{Ram}(L/\mathbb{Q})$ and $\mathrm{Ram}(L_0/\mathbb{Q}) = \{l\}$ are disjoint, we conclude that $\mathrm{Ram}(L/\mathbb{Q})$ contains at least r elements.

Similarly, let L be a Galois extension of $\mathbb{F}_q(t)$ with Galois group isomorphic to C_l^r which is regular over $\mathbb{F}_q$. Then L is disjoint from the unique unramified extension $\mathbb{F}_{q^l}$ of degree l of $\mathbb{F}_q(t)$. As in the preceding paragraph, $|\mathrm{Ram}(L/\mathbb{F}_q(t))| \geq r$.

Thus, if $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$, Theorem 7.4 gives the most economic realization of C_l^r in terms of number of ramified primes. □

§8. Estimates

In this section we consider the case where K is a function field of one variable over the field $K_0 = \mathbb{F}_q$, where q is a prime power. Our goal is to estimate some of the invariants of the field L of Theorem 7.4.

Data 8.1. *We fix the following notation for the whole section:*

$t =$ *transcendental element*
over K which we also consider as a variable
$K =$ *finite separable extension of $K_0(t)$ which is regular over K_0*
$g_K =$ *the genus of K*
$d = [K : K_0(t)]$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

$l =$ *prime element* $\neq \mathrm{char}(K)$
$n =$ *positive integer*
$d_n = [K_0(\zeta_{l^n}) : K_0]$
$S_0 =$ *basic set for* K (*Data* 1.1); *put* $s_0 = |S_0|$;
$N^* =$ *basic extension of* K (*Definition* 5.4)
$S_1 =$ *exceptional set of primes for* K.

Note that $s_1 = |S_1| = \mathrm{rank}_l K$ (*Data* 5.6).

LEMMA 8.2. *Let* N *be a finite Galois extension of* K. *Denote the algebraic closure of* K_0 *in* N *by* K_0'. *Let* $\mathcal{C}$ *be a conjugacy class in* $\mathcal{G}(N/K)$, *and let* $c = |\mathcal{C}|$. *Let* k *be a multiple of* $[K_0' : K_0]$. *Denote the number of primes* $\mathfrak{q}$ *of* K *which do not ramify over* $K_0(t)$ *nor in* N, *are of degree* k, *and such that* $\left(\frac{N/K}{\mathfrak{q}}\right) = \mathcal{C}$ *by* ν. *Let* ν_0 *be a positive integer and suppose that*

$$(8.1)\qquad k\log q \geq \max\Big\{2\log(2g_N + (d+1)[N:K'] + 3),\ 4\log(3g_K+1), 2\log\Big(\frac{\nu_0 k}{c}[N:K']\Big)\Big\}$$

then $\nu > \nu_0$.

Proof. Let $K' = KK_0'$ and let $m = [N : K']$. By (8.1), $q^{k/2} \geq \nu_0 km/c$ and $q^{k/2} \geq 2g_N + 2m + 3$. Also, (13.1) holds with K and N, respectively instead of E and F. Hence, by Corollary 13.5

$$\begin{aligned}\nu &> \frac{c}{km}\cdot q^k - \frac{2c}{km}\cdot(m + g_N + 1)\cdot q^{k/2}\\ &= \frac{c}{km}q^{k/2}\cdot\Big(q^{k/2} - 2(g_N + m + 1)\Big)\\ &\geq \nu_0 \cdot 1 = \nu_0.\end{aligned}$$

This proves our claim. □

For a finite set T of primes of a function field K/K_0 we write

$$\deg(T) = \sum_{\mathfrak{p}\in T}\deg(\mathfrak{p})$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

LEMMA 8.3. *Let L/K be a finite tamely ramified extension of function fields of one variable over the same constant field. Then their genera satisfy the following inequality:*

$$\frac{2g_L - 2}{[L:K]} \leq (2g_K - 2) + \deg(\mathrm{Ram}(L/K)) \tag{8.3}$$

Proof. The Riemann-Hurwitz genus formula for L/K is

$$2g_L - 2 = [L:K](2g_K - 2) + \sum_{\mathfrak{p}\in\mathrm{Ram}(L/K)} \sum_{\mathfrak{P}|\mathfrak{p}} (e(\mathfrak{P}/\mathfrak{p}) - 1)\deg(\mathfrak{P}) \tag{8.4}$$

[FrJ, p. 24]. In the second sum $\mathfrak{P}$ ranges over all prime divisors of L which lie over $\mathfrak{p}$ and $e(\mathfrak{P}/\mathfrak{p})$ denotes the relative ramification index. We also denote the relative residue degree of $\mathfrak{P}/\mathfrak{p}$ by $f(\mathfrak{P}/\mathfrak{p})$. Then

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathrm{Ram}(L/K)} \sum_{\mathfrak{P}|\mathfrak{p}} (e(\mathfrak{P}/\mathfrak{p}) - 1)\deg(\mathfrak{P}) & \\ &\leq \sum_{\mathfrak{p}\in\mathrm{Ram}(L/K)} \Big(\sum_{\mathfrak{P}/\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p})\Big)\deg(\mathfrak{p}) \\ &= \sum_{\mathfrak{p}\in\mathrm{Ram}(L/K)} [L:K]\deg(\mathfrak{p}) \\ &= [L:K]\deg(\mathrm{Ram}(L/K))\end{aligned}$$

Hence, inequality (8.3) follows from (8.4). □

LEMMA 8.4. *Let T be a finite set of primes of K. Suppose that $\zeta_l \notin K$. Let L/K be a finite l-extension such that L is regular over K_0 and let $S = \mathrm{Ram}(L/K) \cup T$. Consider elements $a_1, \dots, a_r$ of K_S which are multiplicatively independent modulo K_S^l and let $N = L(\zeta_{l^n}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_r})$. Then*

$$\frac{2g_N - 1}{l^r[L:K]} \leq 2g_K - 2 + \deg(S). \tag{8.5}$$

Proof. We apply Lemma 8.3 to $N/K(\zeta_{l^n})$ instead of to L/K.

Let $K_0' = K_0(\zeta_{l^n})$, $K' = K(\zeta_{l^n})$, and $L' = L(\zeta_{l^n})$. Then K'/K_0' is a regular extension which is obtained from the function field K/K_0 by a finite separable extension of the field of constants. Hence $g_{K'} = g_K$ [Deu, p. 132]. Let S' be the set of primes of K'/K_0' which lie over S. Since each prime of K' is unramified over K_0', we have $\deg(S') = \deg(S)$ [Deu, 132].

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

By Remark 5.3, N is a regular extension of K_0' and by Lemma 5.2, $[N : K'] = l^r[L : K]$. Since l is relatively prime to $\mathrm{char}(K)$, the extension N/K' is tamely ramified. If a prime $\mathfrak{p}$ of K'/K_0' does not belong to S and $\mathfrak{P}$ is an extension of $\mathfrak{p}$ to L', then $v_{\mathfrak{P}}(a_i) = v_{\mathfrak{p}}(a_i) = 0$. Hence, $\mathfrak{P}$ is unramified in $L'(\sqrt[l]{a_i})$ (a consequence of [CaF, p. 32, Prop. 1]) and therefore $\mathfrak{p}$ is unramified in N. Thus, $\mathrm{Ram}(N/K') \subseteq S'$.

It follows that (8.5) is a consequence of (8.3). □

LEMMA 8.5. *Let T be a finite set of primes of K. Suppose that $\zeta_l \notin K$. Let L/K be a Galois extension of degree l^m such that L is regular over K_0 and let $S = \mathrm{Ram}(L/K) \cup T$. Consider elements $a_1, \dots, a_s$ of K_S which are multiplicatively independent modulo K_S^l and let $N = L(\zeta_{l^n}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s})$. Suppose that k is a multiple of d_n such that* $\deg(\mathfrak{p}) \le k$ *for each $\mathfrak{p} \in S$. Let*

$$\mu = 3g_K + d + 1 + |S| \tag{8.6}$$

and let $\mathcal{C}$ be a conjugacy class in $\mathcal{G}(N/K(\zeta_{l^n}))$. Suppose that

$$k \log q \ge 4 \log 8 + 4(m+s) \log l + 4 \log \mu. \tag{8.7}$$

Then there exists $\mathfrak{q} \in \mathbb{P} \smallsetminus S$ such that $\deg(\mathfrak{q}) = k$ *and* $\left(\frac{N/K}{\mathfrak{q}}\right) = \mathcal{C}$.

Proof. Let $K_0' = K_0(\zeta_{l^n})$ and $K' = K(\zeta_{l^n})$. By Lemma 5.2, $[N : K'] = l^{m+s}$. If $m+s = 0$, then $N = K(\zeta_{l^n})$. Then $g_N = g_K$ and the constant m of Lemma 8.2 becomes 1. Let ν be the number of $\mathfrak{q} \in \mathbb{P}$ such that $\deg(\mathfrak{q}) = k$ and $\left(\frac{N/K}{\mathfrak{q}}\right) = \mathcal{C}$. We have to prove that $\nu > |S|$. Indeed, the inequality of Lemma 8.2 simplifies to $\nu > \frac{q^{k/2}}{k}(q^{k/2} - 2g_K - 2)$. Since $q^{k/2} \ge 2^{k/2} \ge k$ and $q^{k/2} \ge \mu^2$ (by (8.7)), we have $\nu > \mu^2 - \nu > |S|$.

So, assume from now on that $m + s \ge 1$. By Lemma 8.2, it suffices to prove (8.1) with $\nu_0 = |S|$.

The inequality $k \log q \ge 4 \log(2g_K + 1)$ follows from (8.6) and (8.7). Hence, it suffices to prove

$$\frac{k}{2} \log q \ge \log(2g_N + (d+1)l^{m+s} + 3) \tag{8.8}$$

$$\frac{k}{2} \log q \ge \log(kl^{m+s}|S|). \tag{8.9}$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

By Lemma 8.4 and by the assumption 'deg($\mathfrak{p}$) $\leq k$ for each $\mathfrak{p} \in S$' we have

$$(8.10) \qquad 2g_N - 2 \leq l^{m+s}(2g_K - 2 + \deg(S)) \leq l^{m+s}(2g_K - 2 + k|S|).$$

Since $5 \leq 2l^{m+s}$, (8.10) gives

$$(8.11) \qquad 2g_N + (d+1)l^{m+s} + 3 \leq l^{m+s}(2g_K + k|S| + d + 1).$$

Nest observe that $\frac{\log x}{x}$ is a decreasing function for $x \geq e$ and that $\frac{\log 16}{16} = \frac{\log 2}{4}$. Hence, for $k \geq 16$, $\log k \leq \frac{k}{4}\log 2 \leq \frac{k}{4}\log q$. If $k \leq 16$, then by (8.6), $\mu \geq 2$ and then by (8.7), $k \log q \geq 4\log(8\mu) \geq 4 \log k$. Thus, in each case $\log k \leq \frac{k}{4}\log q$. It follows from (8.7) that

$$(8.12) \qquad \begin{aligned} \log k + (m+s)\log l + \log\mu &\leq \frac{k}{4}\log q + (m+s)\log l + \log\mu \\ &\leq \frac{k}{4}\log q + \frac{k}{4}\log q = \frac{k}{2}\log q. \end{aligned}$$

Hence, by (8.11)

$$\begin{aligned} &\log(2g_N + (d+1)l^{m+s} + 3) \\ &\qquad \leq (m+s)\log l + \log k + \log(2g_K + |S| + d + 1) \\ &\qquad = \log k + (m+s)\log l + \log\mu \leq \frac{k}{2}\log q, \end{aligned}$$

which proves (8.8). Finally, (8.9) follows from (8.13) and the inequality $|S| \leq \mu$. □

THEOREM 8.6. *Let K be a function field of one variable over $\mathbb{F}_q$ and let S_0 and S_1 be sets of primes as in Data 8.1. Let G be a group of order l^m and let $n \geq m$. Suppose that $\zeta_l \notin K$. Then K has an n-Scholz extension L which is regular over $\mathbb{F}_q$ such that $\mathcal{G}(L/K) \cong G$, $|\mathrm{Ram}(L/K) \cup S_1| = m + \mathrm{rank}_l K$, and each $\mathfrak{p} \in S_0$ totally decomposes in L.*

Moreover, let $\mu = 3g_K + d + m + s_0 + \mathrm{rank}_l K + 1$ and let k be a multiple of d_n such that

$$(8.13) \qquad k \log q \geq 4\log 8 + 4(m + \mathrm{rank}_l K)\log l + 4\log\mu.$$

Then we can choose S_1 and L such that $\deg(\mathfrak{p}) = k$ *for each* $\mathfrak{p} \in \mathrm{Ram}(L/K) \cup S_1$. *The genus of L is estimated by*

$$(8.14) \qquad 2g_L - 2 \leq l^m(2g_K - 2 + (m + \mathrm{rank}_l(K))k).$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Proof. Denote $\mathbb{F}_q$ by K_0. Assume without loss that $m \geq 1$. Embed C_l in the center of G and let $\bar{G} = G/C_l$. By induction, K has an n-Scholz extension L which is regular over K_0 such that $\mathcal{G}(L/K) \cong \bar{G}$, and the above conditions are satisfied for $m-1$ instead of for m. Now consider the following central embedding problem

(8.15)
$$\begin{tikzcd} & & & G(K) \arrow[d, "\mathrm{res}"] & \\ 1 \arrow[r] & C_l \arrow[r] & G \arrow[r, "\alpha"] & \mathcal{G}(L/K) \arrow[r] & 1 \end{tikzcd}$$

Lemmas 4.2 and 4.4 give a solution ψ to (8.15), which however, need not be n-Scholz. Use Lemma 6.2 to replace ψ by another solution, if necessary, to assume that $\mathrm{Ram}(\psi) \subseteq \mathrm{Ram}(L/K) \cup S_1$. Then Lemma 7.2 gives a prime $\mathfrak{q} \notin S_0 \cup S_1 \cup \mathrm{Ram}(L/K)$ and an n-Scholz solution ψ to (8.15) such that $\mathrm{Ram}(\varphi) = \mathrm{Ram}(\psi) \cup \{\mathfrak{q}\}$. The fixed field L^* of $\mathrm{Ker}(\varphi)$ is an n-Scholz extension of K with $\mathcal{G}(L^*/L) \cong G$ and $\mathrm{Ram}(L^*/K) = \mathrm{Ram}(\psi) \cup \{\mathfrak{q}\}$. In particular L^*/L ramifies. Hence, as L is regular over K_0, so is L^*.

Now suppose that (8.13) holds. Then apply Lemma 8.5 to choose the exceptional set S_1 with primes of degree k. Here we follow the construction of Data 5.6 with $r = \mathrm{rank}_l(K)$ and $s = \mathrm{rank}_\infty(K) = 0$. Let N^* and w_i be as in Lemma 5.5. Then we choose a generator τ_i for $\mathcal{G}(N^*/N_i)$ and apply Lemma 8.5 to choose $\mathfrak{p}_i^* \in \mathbb{P} \smallsetminus \mathrm{Ram}(N^*/K) \cup S_0$ such that $\left(\frac{N^*/K}{\mathfrak{p}_i^*}\right) = \mathrm{Con}(\sigma_i)$, $i = 1, \dots, r$.

In order to choose $\mathfrak{q} \notin S_0 \cup S_1 \cup \mathrm{Ram}(L/K)$ as in Lemma 7.2 we have to apply Lemma 7.1. The latter Lemma chooses generators $a_1, \dots, a_s$ for K_S modulo K_S^l, puts $N = L(\zeta_{l^n}, \sqrt[l]{a_1}, \dots, \sqrt[l]{a_s})$ and chooses $\sigma \in \mathcal{G}(N/L(\zeta_{l^n}))$ in a special way (Part D, after the proof). Then it applies the Chebotarev density theorem to choose $\mathfrak{q} \in \mathbb{P} \smallsetminus S$ such that either $\left(\frac{N/K}{\mathfrak{q}}\right) = 1$ (in Part B) or $\left(\frac{N/K}{\mathfrak{q}}\right) = \mathrm{Con}(\sigma)$ (in Part D). Since (8.13) holds, we may apply Lemma 8.5, which is an effective version of the Chebotarev density theorem, and choose $\mathfrak{q}$ such that in addition to the above, $\deg(\mathfrak{q}) = k$.

Finally, (8.14) follows from Lemma 8.3. □

§9. Field of rational function

The case where $K = \mathbb{F}_q(t)$ is simpler than the general one. In this case, in the notation of Data 8.1, we have

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

(9.1) $d = 1$, $h_K = 1$, $N^* = \mathbb{F}_q(t, \zeta_{l^n})$, $\mathrm{Ram}(N^*/K) = \emptyset$, $\mathrm{rank}_l(K) = 0$, $S_1 = \emptyset$, and $g_K = 0$. We take S_0 as a finite set of primes of $K/\mathbb{F}_q$ which contains $(t)_\infty$.

Note that $\zeta_l \notin K$ is equivalent to $l \nmid q-1$ and $l \neq \mathrm{char}(K)$ is equivalent to $l \nmid q$. Thus Theorem 8.6 specializes in this case to the following result:

THEOREM 9.1. *Let q be a prime power and let l be a prime such that $l \nmid (q-1)q$. Let G be a group of order l^n and let S_0 be a finite set of primes of $\mathbb{F}_q(t)$ which contains $(t)_\infty$. Then $\mathbb{F}_q(t)$ has an n-Scholz extension L which is regular over $\mathbb{F}_q$ such that $\mathcal{G}(L/\mathbb{F}_q(t)) \cong G$, $|\mathrm{Ram}(L/\mathbb{F}_q(t))| = n$, and such that each $\mathfrak{p} \in S_0$ totally decomposes in L. Moreover, let k be a multiple of d_n such that $k \log q \geq 4 \log(8l^n(1 + n + |S_0|))$. Then we can choose L such that $\deg(\mathfrak{p}) = k$ for each $\mathfrak{p} \in \mathrm{Ram}(L/K)$ and $2g_L - 2 \leq l^n(nk-2)$.*

By the primitive element theorem, there exists a Galois polynomial $f \in \mathbb{F}_q[t, X]$ such that $\mathcal{G}(f(t,X), \mathbb{F}_q(t)) \cong G$. The degree of f in X is of course l^n. The following result will enable us to choose f with bounded degree in t.

LEMMA 9.2. *Let K_0 be an arbitrary field and consider a Galois extension L of $K = K_0(t)$ of degree d which is regular over K_0.*

(a) *Suppose that $(t)_\infty$ totally decomposes in L. Let $\mathfrak{p}$ be a prime divisor of L/K_0 which divides $(t)_\infty$ and let x be an element of L such that $(x)_\infty = k\mathfrak{p}$ for some positive integer k. Then x is integral over $K_0[t]$, $L = K(x)$ and $f = \mathrm{irr}(x, K(t))$ has the form*

$$f(t,X) = X^d + a_1(t)X^{d-1} + \cdots + a_d(t). \tag{9.1}$$

with $a_i \in K_0[t]$ and $\deg(a_i(t)) \leq \deg(a_1(t)) = k$, $i = 1, \ldots, d$.

(b) *Conversely, suppose that $x \in L$ and that $f = \mathrm{irr}(x, K(t))$ is given by (9.1) such that $a_i(t) \in K_0[t]$, $\deg(a_1(t)) > 0$, and $\deg(a_i(t)) \leq \deg(a_1(t))$, $i = 1, \ldots, d$. Then $(t)_\infty$ totally decomposes in L.*

Proof of (a). Denote the normalized valuation of L/K_0 that corresponds to $\mathfrak{p}$ by v. Then $v(x) = -k$ and $w(x) \geq 0$ for each other valuation w of L/K_0. In particular, since $v^\sigma \neq v$, we have $v(x^{\sigma^{-1}}) = v^\sigma(x) \geq 0$ for each $\sigma \in \mathcal{G}(L/K)$, $\sigma \neq 1$. Hence $x^{\sigma^{-1}} \neq x$ for each $\sigma \neq 1$, and therefore $L = K(t,x)$.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

In addition $w(x) \geq 0$ if $w(t) \geq 0$. Hence x is integral over $K_0[t]$. In particular $f(t,X) = \mathrm{irr}(x, K(t)) \in K_0[t,X]$ is a monic polynomial in X. Since L/K is a Galois extension, $f(t,X)$ decomposes into distinct linear factors over L:

$$f(t,X) = \prod_{\sigma\in G}(X - x^\sigma). \tag{9.2}$$

A comparison of (9.1) and (9.2) gives:

$$a_i(t) = (-1)^i \sum_{S\in\mathcal{P}_i}\prod_{\sigma\in S} x^\sigma \tag{9.3}$$

where $\mathcal{P}_i$ is the collection of all subsets of G of cardinality i. Note that v is unramified over K. Hence the restriction of v to K coincides with the valuation v_∞ that corresponds to $(t)_\infty$. Since $\sigma = 1$ appears at most once in each of the summands $\prod_{\sigma\in S} x^\sigma$, and since $v(x^\sigma) = 0$ for $\sigma \neq 1$, this gives

$$-\deg(a_i(t)) = v_\infty(a_i(t)) = v(a_i(t)) \geq \min_{S\in\mathcal{P}_i}\sum_{\sigma\in S} v(x^\sigma) = -k.$$

Also, $-\deg(a_1(t)) = v_\infty(a_1(t)) = v(-x - \sum_{\sigma\neq 1} x^\sigma) = v(x) = -k$, as desired.

Proof of (b). Let $k = \deg(a_1(t))$. Then $z = x/t^k$ satisfies

$$z^d + b_1(t)z^{d-1} + b_2(t)z^{d-2} + \cdots + b_d(t) = 0, \tag{9.4}$$

where $b_i(t) = a_i(t)/t^{ik}$. As in (a), choose an extension v of v_∞ to a valuation of L, let $e = e(v/v_\infty)$ and let $\mathfrak{p}$ be a prime divsior of L/K_0 that corresponds to v. Then $v(b_1(t)) = 0$ and $v(b_i(t)) = e(ik - \deg(a_i(t))) > 0$ for $i = 2,\dots,d$. Hence reduction of (9.4) modulo $\mathfrak{p}$ gives $\bar{z}^{d-1}(\bar{z}+b) = 0$ for some $0 \neq b \in K_0$. By Hensel's Lemma, $h(Z) = Z^d + b_1(t)Z^{d-1} + \cdots + b_n(t)$ has a root in the completion $K_0((t^{-1}))$ of K with respect to $(t)_\infty$. Since $L = K(z)$ is Galois over K, all roots of $h(Z)$ are in $K_0((t^{-1}))$. Conclude that $(t)_\infty$ totally decomposes in L. □

LEMMA 9.3. *Let K_0 be an arbitrary field and consider a Galois extension L of $K = K_0(t)$ of degree d which is regular over K_0. Suppose that $(t)_\infty$ totally decomposes in L. Then there exists $x \in L$ which is integral over $K_0[t]$ such that $L = K(x)$ and $f = \mathrm{irr}(x, K(t)) = X^d + a_1(t)X^{d-1} + \cdots + a_d(t)$ with $a_i \in K_0[t]$ such that $0 < \deg(a_1(t)) \leq g_L + 1$ and $\deg(a_i(t)) \leq \deg(a_1(t))$, $i = 1,\dots,d$.*

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Proof. Let $G = \mathcal{G}(L/K)$. By assumption $(t)_\infty = \sum_{\sigma \in G} \mathfrak{p}^\sigma$ for some prime divisor $\mathfrak{p}$ of L and $\mathfrak{p}^\sigma \neq \mathfrak{p}^\tau$ if $\sigma \neq \tau$. In particular $\deg(\mathfrak{p}) = 1$. For each k consider the vector space $\mathcal{L}(k\mathfrak{p}) = \{x \in L \mid (x) + k\mathfrak{p} \geq 0\}$ over K. We have $\dim \mathcal{L}(0 \cdot \mathfrak{p}) = 1$ and $\dim \mathcal{L}((2g_L - 1)\mathfrak{p}) = g$ [FrJ, p. 20], $\mathcal{L}((k-1)\mathfrak{p}) \subseteq \mathcal{L}(k\mathfrak{p})$ and $\dim \mathcal{L}(l\mathfrak{p}) - \dim \mathcal{L}(k\mathfrak{p}) \leq l-k$ if $l \geq k$ [FrJ, Chap. 2, Exer. 12]. In particular, $\dim \mathcal{L}(k\mathfrak{p}) = 1$ implies $k \leq g$. Hence, the first k for which $\dim \mathcal{L}(k\mathfrak{p}) = 2$ satisfies $k \leq g+1$. For this k there exists $x \in L$ such that $(x)_\infty = k\mathfrak{p}$. By Lemma 9.2, x satisfies the requirements of the present lemma. □

§10. Bounds

The goal of this section is to realize a given l-group G over $\mathbb{F}_q(t)$ with q large with a bound on all parameters involved in the realization. This will enable us to use model theory and to realize G over $K_0(t)$ for any pseudo finite field K_0. In order to do this, we need to speak about the set of ramified primes in the first order language of fields. So, we have to express discriminants of field extensions in an elementary way.

Let R be a Dedekind domain with a quotient field K, let L be a finite Galois extension of K with Galois group $G = \{\sigma_1, \ldots, \sigma_d\}$, and let S be the integral closure of R in L. The **discriminant** of S/R is the ideal $\mathrm{Disc}(S/R)$ of R which is generated by all determinants $\mathrm{Det}(\sigma_i w_j)^2$ where $w_1, \ldots, w_d \in S$ are linearly independent over K. If $\mathfrak{p}$ is a prime ideal of R, we can compute the $\mathfrak{p}$-component of the discriminant by localizing at $\mathfrak{p}$. That is $\mathrm{Disc}(S/R)R_\mathfrak{p} = \mathrm{Disc}(S_\mathfrak{p}/R_\mathfrak{p})$ [La2, p. 65]. The set of prime ideals of R which ramify in L coincides with the set of prime divisors of $\mathrm{Disc}(S/R)$ [CaF, p. 22]. In particular, if $R = K_0[t]$ for some field K_0, and $(t)_\infty$ is unramified in L, then $\mathrm{Ram}(L/K)$ consists of the prime divisors of $\mathrm{Disc}(S/R)$.

The **discriminant** of a monic polynomial $f \in R[X]$ is given in terms of its roots $x_1, \ldots, x_n$ by the formula $\mathrm{Disc}(f) = (-1)^{d(d-1)/2} \prod_{i \neq j}(x_i - x_j)$. It is an element of R and equals $(-1)^{d(d-1)/2} N_{L/K} f'(x_1)$. One can compute $\mathrm{Disc}(f)$ in terms of the resultant of f and its derivative by the formula $\mathrm{Resultant}(f, f') = (-1)^{d(d-1)/2}\mathrm{Disc}(f)$ [La4, p. 211]. $\mathrm{Resultant}(f, f')$ is a $(2d-1) \times (2d-1)$ determinant whose entries are the coefficients of f and f'. The only nonzero entries in the first column of this determinant are the leading coefficients of f and f'. In the case where $R = K_0[t]$, this leads to an estimate on the degree of $\mathrm{Disc}(f)$:

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

(10.1) Suppose that $R = K_0[t]$ and $\mathrm{char}(K_0) \nmid d$. If $f \in K_0[t, X]$ is a monic polynomial of degree d in X and $\deg_t(f) \leq m$, then $\deg(\mathrm{Disc}(f)) \leq m^{2d-2}$.

If x is integral over K, $L = K(x)$, and $f = \mathrm{irr}(x, K)$, then $\mathrm{Disc}(f)$ is a multiple of $\mathrm{Disc}(S/R)$. If in addition $S = R[x]$, then $\mathrm{Disc}(S/R) = \mathrm{Disc}(f)R$ [CaF, p. 17]. This situation occurs often in the local case as Lemma 10.1 reveals. Together with the local nature of the discriminant, this gives us a tool to handle disciminants.

LEMMA 10.1. *Let R be a discrete valuation ring of a field K with a maximal ideal $\mathfrak{p}$ and a perfect residue field $\bar{K}$. Let L be a finite Galois extension of K with $|\bar{K}| \geq [L : K]$. Denote the integral closure of R in L by S. Then there exists $x \in S$, such that $S = R[x]$. Moreover, S has only finitely many nonzero prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. If $x' \in S$ satisfies $x' \equiv x \bmod \mathfrak{q}_i^2$, $i = 1, \ldots, r$, then $S = R[x']$.*

Proof. Denote the valuation of K that corresponds to R by v. The ring S is a finitely generated R-module [La2, p. 6] and has only finitely many prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$. They correspond to the extensions $v_1, \ldots, v_r$ of v to L. In particular each $\mathfrak{q}_i$ is a principal ideal [La2, p. 15].

For each i let K_i be the decomposition field of $\mathfrak{q}_i$ over K and let L_i be its inertia field. Since $\bar{K}$ is perfect, the residue fields satisfy $\bar{K}_i = \bar{K} = R/\mathfrak{p}$, $\bar{L}_i = S/\mathfrak{q}_i$, and $[\bar{L}_i : \bar{K}] = [L_i : K_i]$ [Ser, p. 32]. For the same reason there exists $y_i \in S \cap L_i$ with $\bar{L}_i = \bar{K}[\bar{y}_i]$. Then $g_i = \mathrm{irr}(y_i, K_i)$ satisfies $\bar{g}_i = \mathrm{irr}(\bar{y}_i, \bar{K})$ and in particular $\bar{g}_i{}'(\bar{y}_i) \neq 0$. Observe that $g_i \in (S \cap L_i)[X]$.

We may replace each y_i by $y_i + a$ with $a \in R$. Since $\bar{y}_i$ has $[L_i : K_i]$ conjugates over $\bar{K}$ and since $\sum_{i=1}^r [L_i : K_i] \leq [L : K] \leq |\bar{K}|$, we may assume, without loss, that $\bar{y}_1, \ldots, \bar{y}_r$ are pairwise nonconjugate over $\bar{K}$. In other words, $\bar{g}_1, \ldots, \bar{g}_r$ are distinct.

Choose now $\pi_i \in S$ such that $v_i(\pi_i) = 1$ and let $x_i = y_i + \pi_i$. Then $g_i(x_i) = g_i'(y_i)\pi_i + c_i$ for some $c_i \in S$ with $v_i(c_i) > 1$. Hence $v_i(g_i(x_i)) = 1$. Since R is v_i-dense in $S \cap L_i$, there exists $h_i \in R[X]$ such that $v_i(h_i - g_i) > 1$. Then $v_i(h_i(x_i)) = 1$.

Use the chinese remainder theorem to choose $x \in S$ such that $v_i(x - x_i) > 1$, $i = 1, \ldots, r$. Then x modulo $\mathfrak{p}_i = \mathfrak{q}_i \cap R[x]$ generates $\bar{L}_i$. Also, with $\pi_i' = h_i(x) \in R[x]$ we have $v_i(\pi_i') = 1$. It follows that $\mathfrak{q}_i = \pi_i' S = \mathfrak{p}_i S$ and hence $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are distinct. Since $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ are the only nonzero prime

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

ideals of S and $\mathfrak{q}_i \cap R[x] = \mathfrak{p}_i$, $\mathfrak{q}_i$ is the only prime ideal of S which lies over $\mathfrak{p}_i$. Also, as $S/R[x]$ is an integral extension, each nonzero prime ideal of $R[x]$ lies under some $\mathfrak{q}_i$. Thus $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are all nonzero prime ideals of $R[x]$.

It suffices now to prove that $S = R[x]$. To this end consider the local rings $R[x]_i = R[x]_{\mathfrak{p}_i}$ and $S_i = S_{\mathfrak{q}_i}$. Then S_i is the unique valuation ring of L that contains $R[x]_i$. It follows that S_i is the integral closure of $R[x]_i$ in L [La3, p. 14]. Hence S_i is a finitely generated $R[x]_i$-Modul. Also, π_i' generates the maximal ideal of S_i and $\pi_i' \in R[x]_i$. By construction, $S_i/\pi_i' S_i = \bar{L}_i = R[x]_i/\mathfrak{p}_i R[x]_i$. It follows that $S_i = R[x]_i + \pi_i' S_i$. By Nakayama's Lemma, $S_i = R[x]_i$. Conclude that $S = \bigcap_{i=1}^r S_i = \bigcap_{i=1}^r R[x]_i = R[x]$. □

LEMMA 10.2. (Strong approximation theorem) *Let L be a function field of one variable over a field K_0. Let Q be a finite set of primes of L/K_0 and let $\mathfrak{q}_\infty$ be a prime of L/K_0 which does not belong to Q. Suppose that for each $\mathfrak{q} \in Q$ we are given an element $y_\mathfrak{q} \in L$ and a positive integer $m_\mathfrak{q}$. Suppose also that m satisfies*

$$m \cdot \deg(\mathfrak{q}_\infty) > 2g_L - 2 + \sum_{\mathfrak{q} \in Q} m_\mathfrak{q} \deg(\mathfrak{q}). \tag{10.2}$$

Then there exists $y \in L$ such that $v_\mathfrak{q}(y - y_\mathfrak{q}) \geq m_\mathfrak{q}$ for each $\mathfrak{q} \in Q$, $v_{\mathfrak{q}_\infty}(y) \geq -m$, and $v_\mathfrak{p}(y) \geq 0$ for each prime $\mathfrak{p} \notin S \cup \{\mathfrak{q}_\infty\}$.

Proof. Consider the divisor $\mathfrak{a} = m\mathfrak{q}_\infty - \sum_{\mathfrak{q} \in Q} m_\mathfrak{q} \mathfrak{q}$ of L/K_0. In the adele ring $\mathbb{A}$ of L/K_0 consider the vector space

$$\Lambda(\mathfrak{a}) = \{\alpha \in \mathbb{A} \mid v_\mathfrak{p}(\alpha) + v_\mathfrak{p}(\mathfrak{a}) \geq 0 \text{ for every } \mathfrak{p}\}.$$

By (10.2), $\deg(\mathfrak{a}) > 2g_L - 2$. Hence, by the Riemann-Roch theorem, $\dim(\mathbb{A}/(\Lambda(\mathfrak{a}) + L)) = 0$ [FrJ, Sec. 2.6]. It follows that $\mathbb{A} = \Lambda(\mathfrak{a}) + L$. Define $\eta \in \mathbb{A}$ by $\eta_\mathfrak{q} = y_\mathfrak{q}$ for $\mathfrak{q} \in Q$ and $\eta_\mathfrak{p} = 0$ for $\mathfrak{p} \notin Q$. Then there exists $y \in L$ such that $y - \eta \in \Lambda(\mathfrak{a})$. This y satisfies the requirements of the Lemma. □

NOTATION 10.3. (The set $\mathcal{F}_k(L/K)$) Let K_0 be a field, let $K = K_0(t)$, let L be a Galois extension of K of degree d, and let k be a positive integer. We define $\mathcal{F}_k(L/K_0)$ to be the set of all absolutely irreducible polynomials

$$h(T, X) = X^d + c_1(T)X^{d-1} + \cdots + c_d(T)$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

with $c_i(T) \in K_0[T]$ such that $0 < \deg(c_1(T)) \leq (k+d)^{2d}$, $\deg(c_i(T)) \leq \deg(c_1(T))$, $i = 1, \dots, d$, and $L = K(z)$ with $h(t,z) = 0$.

LEMMA 10.4. *Let K_0 be a perfect field, $R = K_0[t]$, and $K = K_0(t)$. Consider a Galois extension L of K of degree $d > 1$ which is regular over K_0 and let S be the integral closure of R in L.*

Suppose that $(t)_\infty$ totally decomposes in L, $\mathrm{char}(K_0) \nmid d$, and $|K_0| \geq d$. Suppose that $\mathcal{F}_k(L/K)$ contains a polynomial $f(T,X) = X^d + a_1(T)X^{d-1} + \cdots + a_d(T)$ with $\deg(a_1(T)) = k > 0$. Then the following two statements hold:

(a) *There exists $g \in \mathcal{F}_k(L/K)$ such that*

$$\mathrm{Disc}(S/R) = \gcd(\mathrm{Disc}(f(t,X)), \mathrm{Disc}(g(t,X)))R. \tag{10.3}$$

(b) *Let $f_1, g_1 \in \mathcal{F}_k(L/K)$ be polynomials such that*

$$d_1(t) = \gcd(\mathrm{Disc}(f_1(t,X)), \mathrm{Disc}(g_1(t,X)))$$

divides $\mathrm{Disc}(h(t,X))$ *for each* $h \in \mathcal{F}_k(L/K)$. *Then* $\mathrm{Disc}(S/R) = d_1(t)R$.

Proof of (a). The total degree of $f(T,X)$ is $k+d-1$. Hence, by [FrJ, Cor. 4.8]

$$g_L \leq \frac{1}{2}(k+d-2)(k+d-3) < \frac{1}{2}(k+d)^2. \tag{10.4}$$

Denote the set of prime divisors of K/K_0 which correspond to the irrreducible factors of $\mathrm{Disc}(f(t,X))$ by P and note that $(t)_\infty \notin P$. By (10.1)

$$\sum_{\mathfrak{p} \in P} \deg(\mathfrak{p}) \leq \deg(\mathrm{Disc}(f(t,X))) \leq k^{2d-2}. \tag{10.5}$$

For each $\mathfrak{p} \in P$ consider the localization $R_\mathfrak{p}$ and $S_\mathfrak{p}$ of R and S, respectively, at $\mathfrak{p}$. Then $R_\mathfrak{p}$ is a discrete valuation ring with residue field which contains K_0, and therefore of cardinality at least d, and $S_\mathfrak{p}$ is its integral closure in L. By Lemma 10.1 there exists $y_\mathfrak{p} \in S_\mathfrak{p}$ such that $S_\mathfrak{p} = R_\mathfrak{p}[y_\mathfrak{p}]$. Moreover, let $Q_\mathfrak{p}$ be the set of prime divisors of $\mathfrak{p}$ in L. Then, $S_\mathfrak{p} = R_\mathfrak{p}[y]$ for each $y \in S_\mathfrak{p}$ which satisfies $v_\mathfrak{q}(y - y_\mathfrak{p}) > 1$ for each $\mathfrak{q} \in Q_\mathfrak{p}$. Since $\mathfrak{p} = \sum_{\mathfrak{q} \in Q_\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p})\mathfrak{q}$, we have

$$\sum_{\mathfrak{q} \in Q_\mathfrak{p}} \deg(\mathfrak{q}) \leq \sum_{\mathfrak{q} \in Q_\mathfrak{p}} e(\mathfrak{q}/\mathfrak{p}) \deg(\mathfrak{q}) = \deg(\mathfrak{p}). \tag{10.6}$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Choose now a prime divsor $\mathfrak{q}_\infty$ of L which divides $(t)_\infty$ and let $m = 2g_L - 1 + \sum_{\mathfrak{p}\in P}\sum_{\mathfrak{q}\in Q_\mathfrak{p}} 2\deg(\mathfrak{q})$. By (10.4), (10.5), and (10.6)

$$(10.7) \qquad m \le (k+d)^2 + 2k^{2d-2} \le 3(k+d)^{2d-2} \le (k+d)^{2d}$$

By assumption, $\deg(\mathfrak{q}_\infty) = 1$. Hence, by Lemma 10.2 with $Q = \bigcup_{\mathfrak{p}\in P} Q_\mathfrak{p}$ and $m_\mathfrak{q} = 2$, there exists $y \in L$ such that $v_\mathfrak{q}(y - y_\mathfrak{p}) \ge 2$ for each $\mathfrak{p} \in P$ and each $\mathfrak{q} \in Q_\mathfrak{p}$, $v_{\mathfrak{q}_\infty}(y) \ge -m$, and $v_\mathfrak{q}(y) \ge 0$ for each $\mathfrak{q} \notin Q \cup \{\mathfrak{q}_\infty\}$. Since $v_\mathfrak{q}(y_\mathfrak{p}) \ge 0$ for each $\mathfrak{p} \in P$ and each $\mathfrak{q} \in Q_\mathfrak{p}$, we have $v_\mathfrak{q}(y) \ge 0$ for each prime of $\mathfrak{q} \ne \mathfrak{q}_\infty$. Hence $y \in S$. Also, $S_\mathfrak{p} = R_\mathfrak{p}[y]$ for each $\mathfrak{p} \in P$. In particular $L = K(y)$. Hence $y \notin K_0$ and therefore there exists a positive integer $k_0 \le m$ such that $(y)_\infty = k_0\mathfrak{q}_\infty$.

Let $g = \mathrm{irr}(y, K) \in R[X]$. Then $g(t, X)$ is monic and Galois in X, and since L/K_0 is regular, $g(T, X)$ is absolutely irreducible. By Lemma 10.2(a) applied to y, g, and k_0 instead of to x, f, and k and by (10.7), $g(T, X) = X^d + b_1(T)X^{d-1} + \cdots + b_d(T)$ with $b_i(T) \in K_0[T]$ and $\deg(b_i(T)) \le \deg(b_1(T)) = k_0 \le m \le (k+d)^{2d}$. Hence $g \in \mathcal{F}_k(L/K)$.

In order to conclude the proof of (a) recall first that the left hand side of (10.3) divides its right hand side. To prove the other direction consider a prime divisor $\mathfrak{p} \ne (t)_\infty$ of K/K_0. Then we may identify $\mathfrak{p}$ with a nonzero prime ideal of R. If $\mathfrak{p} \in P$, then $\mathrm{Disc}(S/R)R_\mathfrak{p} = \mathrm{Disc}(S_\mathfrak{p}/R_\mathfrak{p}) = \mathrm{Disc}(R_\mathfrak{p}[y]/R_\mathfrak{p}) = \mathrm{Disc}(g(t, X))R_\mathfrak{p}$. If $\mathfrak{p} \notin P$, then $v_\mathfrak{p}(\mathrm{Disc}(f(t, X))) = 0$ and therefore $v_\mathfrak{p}(\mathrm{Disc}(S/R)) = 0$. Thus, in each case the value of $v_\mathfrak{p}$ at both sides of (10.3) is the same. So, (a) holds.

Proof of (b). Again, $\mathrm{Disc}(S/R)$ divides both $\mathrm{Disc}(f_1(t, X))$ and $\mathrm{Disc}(g_1(t, X))$ and therefore also $d_1(t)$. Conversely, by assumption, $d_1(t)$ divides both $\mathrm{Disc}(f(t, X))$ and $\mathrm{Disc}(g(t, X))$. Hence, by (10.3), $d_1(t)|$ $\mathrm{Disc}(S/R)$. Conclude that $\mathrm{Disc}(S/R) = d_1(t)R$, as desired. □

THEOREM 10.5. *Let q be a prime power, let G be a group of order l^n with l a prime, and let t be a transcendental element over $\mathbb{F}_q$. Suppose that $l \ne \mathrm{char}(\mathbb{F}_q)$, $\zeta_l \notin \mathbb{F}_q$, and $q > l^{4n+4}$. Then there exist absolutely irreducible polynomials f, $g \in \mathbb{F}_q[T, X]$ which are monic and Galois in X such that*

(a) $f(T, X) = X^{l^n} + a_1(T)X^{l^n-1} + \cdots + a_{l^n}(T)$, $0 < \deg(a_1(T)) \le \frac{1}{2}nl^{2n}$, *and* $\deg(a_i(T)) \le \deg(a_1(T))$, $i = 1, \ldots, l^n$,

(b) *$f(t, X)$ and $g(t, X)$ have the same splitting field L over $K = \mathbb{F}_q(t)$; L is obtained by adjoining one root of $f(t, X)$ or of $g(t, X)$ to K,*

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

(c) *L is a regular extension of $\mathbb{F}_q$ and $\mathcal{G}(L/K) \cong G$,*

(d) *$g \in \mathcal{F}_k(L/K)$, where $k = \deg(a_1(T))$,*

(e) *$(t)_\infty$ totally decomposes in L; in particular, L has l^n prime divisors of degree 1,*

(f) *$g_L < \frac{1}{2}nl^{2n}$,*

(g) *$|\mathrm{Ram}(L/K)| = n$ and $\deg(\mathfrak{p}) = [\mathbb{F}_q(\zeta_{l^n}) : \mathbb{F}_q]$ for each $\mathfrak{p} \in \mathrm{Ram}(L/K)$,*

(h) *Let $R = K_0[t]$ and let S be the integral closure of R in L. Then $\mathrm{Disc}(S/R) = \gcd(\mathrm{Disc}(f(t,X)), \mathrm{Disc}(g(t,X)))R$. Thus $\mathrm{Ram}(L/K)$ consists of those primes $\neq (t)_\infty$ of K/K_0 that divide both $\mathrm{Disc}(f(t,X))$ and $\mathrm{Disc}(g(t,X))$.*

Proof. Assume without loss that $n \geq 1$. Since $\zeta_l \notin \mathbb{F}_q$, we have $l \geq 3$ and $2 \leq d_n = [\mathbb{F}_q(\zeta_{l^n}) : \mathbb{F}_q] \leq l^n$. Then $q^{d_n/4} \geq q^{1/2} > l^{2+2n} > 8l^n(2+n)$. Hence, Theorem 9.1 with $k = d_n$ and $S_0 = \{(t)_\infty\}$ gives a Galois extension L of K with $\mathcal{G}(L/K) \cong G$ which is regular over $\mathbb{F}_q$ such that $2g_L - 2 \leq l^n(nd_n - 2)$, $|\mathrm{Ram}(L/K)| = n$, $\deg(\mathfrak{p}) = d_n$ for each $\mathfrak{p} \in \mathrm{Ram}(L/K)$ and $(t)_\infty$ totally decomposes in L. Hence $g_L < \frac{1}{2}nl^{2n}$ and so (f) is true. By Lemma 9.3, there exists $x \in L$ which is integral over $\mathbb{F}_q[t]$ such that $L = \mathbb{F}_q(t,x)$ and $f(t,X) = \mathrm{irr}(x,K)$ satisfies (a). In particular $f(t,X)$ is monic and Galois in X. Since $L/\mathbb{F}_q$ is regular, $f(T,X)$ is absolutely irreducible.

Since $q > l^{4n+4} > l^n = [L : K]$, Lemma 10.4, with $d = l^n$ gives an absolutely irreducible polynomial $g \in \mathcal{F}_k(L/K)$ such that $\mathrm{Disc}(S/R)$ is the greatest common divisor of the ideal of $\mathbb{F}_q[t]$ generated by $\mathrm{Disc}(f(t,X))$ and $\mathrm{Disc}(g(t,X))$. Since $(t)_\infty$ is unramified in L this gives (h) and concludes the proof of the theorem. □

§11. Pseudo finite fields

A field K_0 is **pseudo finite** it satisfies one of the following equivalent conditions [Ax, Thm. 9]:

(11.1a) K_0 is a perfect, $G(K_0) \cong \hat{\mathbb{Z}}$, and each nonempty absolutely irreducible variety which is defined over K_0 has a K_0-rational point (Thus, in the terminology of [FrJ], K_0 is a perfect, 1-free **PAC field**.)

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

(11.1b) Every elementary statement about fields which is true in all but finitely many finite fields is true in K_0.

(11.1c) K_0 is an infinite model of the theory of finite fields.

Fried and Völklein [FrV] prove that if K_0 is a PAC field of characteristic 0 and G is a finite group, then $K = K_0(t)$ has a Galois extension L which is regular over K_0 such that $\mathcal{G}(L/K) \cong G$. The same result without any restriction on the characteristic follows from a theorem of Harbater [Har] (see, [Ja2, Thm 2.6]). However, in none of these results there is a bound on the cardinality of $\mathrm{Ram}(L/K)$ in terms of G. The following result suggests such a bound in the case where K_0 is pseudo finite and G is an l-group such that $l \nmid \mathrm{char}(K_0)$ and $\zeta_l \notin K_0$.

THEOREM 11.1. *Let K_0 be a pseudo finite field and let G be a group of order l^n with a prime l. Suppose that $l \neq \mathrm{char}(K_0)$ and $\zeta_l \notin K_0$. Let $d_n = [K_0(\zeta_{l^n}) : K_0]$. Then there exist absolutely irreducible polynomials f, $g \in K_0[T, X]$ which are monic and Galois in X such that*

(a) $f(T,X) = X^{l^n} + a_1(T)X^{l^n-1} + \cdots + a_{l^n}(T)$, *with* $0 < \deg(a_1(T)) \leq \frac{1}{2}nl^{2n}$, *and* $\deg(a_i(T)) \leq \deg(a_1(T))$, $i = 1, \ldots, l^n$;

(b) $f(t,X)$ *and* $g(t,X)$ *have the same splitting field L over* $K = K_0(t)$;

(c) *L is a regular extension of K_0 and* $\mathcal{G}(L/K) \cong G$;

(d) $g \in \mathcal{F}_k(L/K)$ *where* $k = \deg(a_1(T))$ *(Notation 11.3) and* $\deg_T g \leq (\frac{1}{2}nl^{2n} + l^n)^{2l^n}$;

(e) $g_L < \frac{1}{2}nl^{2n}$;

(f) $(t)_\infty$ *totally decomposes in L*;

(g) $|\mathrm{Ram}(L/K)| = n$ *and* $\deg(\mathfrak{p}) = [K_0(\zeta_{l^n}) : K_0]$ *for each* $\mathfrak{p} \in \mathrm{Ram}(L/K)$;

(h) *Let* $R = K_0[t]$ *and let S be the integral closure of R in L. Then* $\mathrm{Disc}(S/R) = \gcd(\mathrm{Disc}(f(t,X)), \mathrm{Disc}(g(t,X)))$. *In particular* $\mathrm{Ram}(L/K)$ *consists of the primes* $\neq (t)_\infty$ *of* L/K_0 *that divides both* $\mathrm{Disc}(f(t,X))$ *and* $\mathrm{Disc}(g(t,X))$.

Proof. Let d_n be a divisor of $(l-1)l^{n-1}$ and let $2 \leq k \leq \frac{1}{2}nl^{2n}$. Denote the conjunction of the following elementary statements on K_0 by $\theta(d_n, k)$ (see [FrJ, proof of Lemma 10.8] for the absolute irreduciblity and [FrJ, Prop. 18.2] for the statement about the Galois group):

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

(11.2a) $l \neq \mathrm{char}(K_0)$, $\zeta_l \notin K_0$, and $d_n = [K_0(\zeta_{l^n}) : K_0]$.

(11.2b) There exist absolutely irreducible polynomials $f, g \in K_0[T, X]$ which are monic and Galois in X such that $f(T, X) = X^{l^n} + a_1(T)X^{l^n-1} + \cdots + a_{l^n}(T)$ with $\deg(a_i(T)) \leq \deg(a_1(T)) = k$, $i = 1, \ldots, l^n$, $f(t, X)$ and $g(t, X)$ have the same splitting field L over $K = K_0(t)$ with $\mathcal{G}(L/K) \cong G$, $g \in \mathcal{F}_k(L/K)$, and $d(t) = \gcd(\mathrm{Disc}(f(t, X)), \mathrm{Disc}(g(t, X)))$ divides $\mathrm{Disc}(h(t, X))$ for each $h \in \mathcal{F}_k(L/K)$, and $d(t)$ has exactly n distinct irreducible divisors, each of them of degree d_n.

Let θ be the disjunction of all the above $\theta(d_n, k)$'s. By Theorem 10.5, for all but finitely many prime powers q the statement θ, with K_0 replaced by $\mathbb{F}_q$, is true in $\mathbb{F}_q$. Hence, by (11.1b), θ is true in K_0. So, there exist d_n and k such that $\theta(d_n, k)$ is true in K_0. In particular (a), (b), (c), and (d) are true. By Lemma 9.2 (b), $(t)_\infty$ totally decomposes in L. Hence, by Lemma (10.4a), and with the notation of (11.2b), $\mathrm{Disc}(S/R) = d(t)R$. In particular the primes in $\mathrm{Ram}(L/K)$ correspond to the irreducible divisors of $d(t)$. Hence (g) is true. Finally, by Lemma 8.3, $2g_L - 2 \leq [L : K](-2 + \deg(\mathrm{Ram}(L/K)) = l^n(-2 + nd_n) \leq nl^{2n}$. So, (e) is also true. □

The absolute Galois group $G(F)$ of a field F admits a unique normalized Haar measure. In the following Corollary we use the expression "almost all" with respect to this measure. For each $\sigma \in G(F)$ we denote the fixed field of the unique extension of σ to $\tilde{F}$ by $\tilde{F}(\sigma)$.

COROLLARY 11.2. *Let F be a countable Hilbertian field. Then for almost all $\sigma \in G(F)$, the field $K_0 = \tilde{F}(\sigma)$ satisfies the conclusion of Theorem 11.1.*

Proof. By [FrJ, Thm. 18.14], $\tilde{F}(\sigma)$ is a pseudo finite field for almost all $\sigma \in G(F)$. Now apply Theorem 11.1. □

§12. $\mathbb{Z}_l$-extensions

We have proved that if K_0 is a finite field or if $K_0 = \tilde{F}(\sigma)$ where F is a global field, $\sigma \in G(F)$ is taken at random, and $\zeta_l \notin K_0$, then for each l-group G there exists a Galois extension L of $K = K_0(t)$ which is regular over K_0 such that $\mathcal{G}(L/K) \cong G$. We then say that G is **regular** over K_0.

If K is a function field of one variable over a finite field K_0 with $l \nmid \mathrm{char}(K_0)$, then it has no Galois extension L which is regular over K_0 such that $\mathcal{G}(L/K) \cong \mathbb{Z}_l$ [GeJ, Thm. 1.1]. In particular, $\mathbb{Z}_l$ is not regular over K_0. Since K_0 has a unique extension with Galois group $\mathbb{Z}_l$, K has a unique $\mathbb{Z}_l$-extension.

Iwasaswa proves [Iwa, Thm. 2] that a number field K has at most $n = [K : \mathbb{Q}]$ linearly independent $\mathbb{Z}_l$ extensions. In particular, $\mathbb{Z}_l^{n+1}$ is not realizable over K. For a finitely generated field K of positive characteristic [GeJ, Thm. 1.1] says that K has exactly one $\mathbb{Z}_l$ extension. Thus the realization results of finite l-groups do not generalize to pro-l groups.

The goal of this section is to prove an analog of these results for almost all field $\tilde{F}(\sigma)$, where F is a global field.

LEMMA 12.1. *Let K be a function field of one variable over a field K_0 with $\mathrm{char}(K_0) \neq l$. Let L_1/K be a cyclic extension of degree l such that L_1 is regular over K_0. Suppose that L_1 is contained in a cyclic extension L_n of K of degree l^n. Suppose that $\mathfrak{p}$ is a prime of K/K_0 which ramifies in L_1. Then $\mathfrak{p}$ totally ramifies in L_n and its residue field contains $K_0(\zeta_{l^n})$. In particular $|\mathrm{Ram}(L_1\tilde{K}_0/K\tilde{K}_0)| \geq [K_0(\zeta_{l^n}) : K_0]$.*

Proof. Denote L_n by L. The inertia group $I_{\mathfrak{p}}(L_1/K)$ of $\mathfrak{p}$ coincides with $\mathcal{G}(L_1/K)$. Since $\mathrm{res}_{L_1}: \mathcal{G}(L/K) \to \mathcal{G}(L_1/K)$ maps $I_{\mathfrak{p}}(L/K)$ onto $I_{\mathfrak{p}}(L_1/K)$, we have $I_{\mathfrak{p}}(L/K) = \mathcal{G}(L/K)$. In other words, $\mathfrak{p}$ totally ramifies in L.

Let $\hat{K}_{\mathfrak{p}}$ be the completion of K at $\mathfrak{p}$ and let $\hat{L}_{\mathfrak{p}} = L\hat{K}_{\mathfrak{p}}$. Then $\hat{L}_{\mathfrak{p}}/\hat{K}_{\mathfrak{p}}$ is a cyclic totally and tamely ramified extension of complete discrete valuation fields. Hence $\zeta_{l^n} \in \hat{K}_{\mathfrak{p}}$ [CaF, p. 32] and therefore $\zeta_{l^n} \in \bar{K}_{\mathfrak{p}}$. It follows that there are at least $[K_0(\zeta_{l^n}) : K_0]$ distinct primes $\tilde{\mathfrak{p}}$ of $K\tilde{K}_0$ which lie over $\mathfrak{p}$. Each of them totally ramifies in $L\tilde{K}_0$ and therefore also in $L_1\tilde{K}_0$. Thus $|\mathrm{Ram}(L_1\tilde{K}_0/K\tilde{K}_0)| \geq [K_0(\zeta_{l^n}) : K_0]$. □

PROPOSITION 12.2. *Let K be a function field of one variable over a field K_0 of characteristic $\neq l$ such that $[K_0(\zeta_{l^n}) : K_0]$ is unbounded. Then K has no ramified Galois extension L which is regular over K_0 such that $\mathcal{G}(L/K) \cong \mathbb{Z}_l$. In particular, $\mathbb{Z}_l$ is not regular over K_0.*

Proof. Assume that there exists L as above. Then L is the ascending union of Galois extensions L_n of K with $\mathcal{G}(L_n/K) \cong \mathbb{Z}/l^n\mathbb{Z}$. Each L_n is a regular extension of K and for large m, L_{m+1}/L_m is ramified. Replace K

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

by such L_m, if necessary to assume that L_1/K is ramified. By Lemma 12.1, $[K_0(\zeta_{l^n}) : K_0] \leq |\mathrm{Ram}(L_1\tilde{K}_0/K\tilde{K}_0)|$, a contradiction.

Finally recall that if $K = K_0(t)$, then L_1/K is ramified [FrJ, Prop. 2.15]. Hence, K admits no $\mathbb{Z}_l$-extension L which is regular over K_0. □

PROPOSITION 12.3. *Let F be a global field of characteristic $\neq l$. Then for almost all $\sigma \in G(F)$, the group $\mathbb{Z}_l$ is not regular over $\tilde{F}(\sigma)$.*

Proof. Let $N = F(\zeta_l, \zeta_{l^2}, \zeta_{l^3}, \ldots)$. Then $N = KL$ with $K \cap L = F$, $\mathcal{G}(K/F) \cong \mathbb{Z}_l$, and $\mathcal{G}(L/F) = A$ is a finite group. Thus $\mathcal{G}(N/F) = \mathcal{G}(N/K) \times \mathcal{G}(N/L)$. If H is a finite subgroup of $\mathcal{G}(N/F)$, then its projection on $\mathcal{G}(N/L)$ is also finite and therefore trivial. Thus $H \leq \mathcal{G}(N/K)$. It follows that if for some $\sigma \in G(F)$ the degree $[\tilde{F}(\sigma)(\zeta_{l^n}) : \tilde{F}(\sigma)]$ is bounded, then $\mathcal{G}(N/N \cap \tilde{F}(\sigma))$ is finite and therefore $K \subseteq \tilde{F}(\sigma)$. Since K/F is infinite, almost no $\sigma \in G(F)$ satisfies the latter condition. Hence, for almost all $\sigma \in G(F)$, $[\tilde{F}(\sigma)(\zeta_{l^n}) : \tilde{F}(\sigma)]$ is unbounded. For each of these σ, Proposition 12.2, asserts that $\mathbb{Z}_l$ is not regular over K_0. □

Appendix. Effective form of the Chebotarev density theorem

Lemma 5.2 uses an effective form of the Chebotarev density theorem for function fields. One may find such a form in [FrJ, §5.4] and in [HKo]. Unfortunately, the proof of [FrJ, Prop 5.16] applies [FrJ, Lemma 5.14] in a faulty way. Indeed, on [FrJ, page 63, line -3] d should be replaced by md. The same mistake occurs in [HKo]. We therefore take this opportunity to correct the mistake and at the same time to improve the estimate of [FrJ, Prop 5.16].

Data 13.1. We fix the following notation for the whole section.

$$\begin{aligned}
q &= \text{a power of a prime number}\\
t &= \text{a transcendental element over } \mathbb{F}_q\\
K &= \text{a finite separable extension over } \mathbb{F}_q(t)\\
&\qquad\qquad\qquad\qquad \text{which is regular over } \mathbb{F}_q\\
d &= [K : \mathbb{F}_q(t)]\\
L &= \text{a finite Galois extension of } K\\
\mathbb{F}_{q^n} &\quad \text{the algebraic closure of } \mathbb{F}_q \text{ in } L\\
\mathbb{P}(K) &= \text{the set of all prime divisors of } K/\mathbb{F}_q
\end{aligned}$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

$$\begin{aligned}
\mathbb{P}'(K) &= \{\mathfrak{p} \in \mathbb{P}(K) \mid \mathfrak{p} \text{ is unramified over } \mathbb{F}_q(t) \text{ or in } L\}\\
\mathbb{P}_k(K) &= \{\mathfrak{p} \in \mathbb{P}(K) \mid \deg(\mathfrak{p}) = k\}\\
\mathbb{P}'_k(K) &= \{\mathfrak{p} \in \mathbb{P}'(K) \mid \deg(\mathfrak{p}) = k\}\\
\mathcal{C} &= \text{a conjugacy class in } \mathcal{G}(L/K);\ c = |\mathcal{C}|\\
C_k(L/K,\mathcal{C}) &= \{\mathfrak{p} \in \mathbb{P}'_k(K) \mid \left(\frac{L/K}{\mathfrak{p}}\right) = \mathcal{C}\}
\end{aligned}$$

Our first result improves [FrJ, Lemma 5.14].

LEMMA 13.2. *Suppose that $L = K\mathbb{F}_{q^n}$, $\mathcal{C} = \{\tau\}$, and $\tau|_{\mathbb{F}_{q^n}} = \varphi$. Then*

$$|\#C_1(L/K,\mathcal{C}) - q| < 2(g_L\sqrt{q} + g_L + d). \tag{13.1}$$

Proof. Note first that $C_1(L/K,\mathcal{C}) = \mathbb{P}'_1(K)$ and that each $\mathfrak{p} \in \mathbb{P}(K)$ is unramified in L. Thus, $\mathbb{P}_1(K) \smallsetminus C_1(L/K,\mathcal{C})$ consists exactly of all prime divisors of Different$(K/\mathbb{F}_q(t))$. By the Riemann-Hurwitz genus formula, deg(Different$(K/\mathbb{F}_q(t)) = 2(g_K + d - 1)$ [FrJ, P. 24]. By Weil's theorem $|\#\mathbb{P}_1(K) - (q+1)| \le 2g_K\sqrt{q}$ [FrJ, Thm. 3.14]. Hence, $|\#C_1(L/K,\mathcal{C}) - q| \le 2g_K\sqrt{q} + 1 + 2(g_K + d - 1)$. Since $g_K = g_L$, this proves (13.1). □

Next we improve [FrJ, Lemma 5.15]. Here we use the notation 'a pd b' to mean 'a **properly divides** b'.

LEMMA 13.3. *Let K' be an extension of K of degree km which contains $\mathbb{F}_{q^k}$. For each $\mathfrak{q} \in \mathbb{P}(K')$ we denote the prime of K which lies under $\mathfrak{q}$ by $\mathfrak{q}_K$. Then*

$$\#\{\mathfrak{q} \in \mathbb{P}(K') \mid \deg(\mathfrak{q}_K) \text{ pd } k\} \le m(q^{k/2} + (3g_K + 1)q^{k/4}). \tag{13.2}$$

Proof. If $j|k$ and $\mathfrak{p} \in \mathbb{P}(K)$, then $\mathbb{F}_{q^j} \subseteq \mathbb{F}_{q^k}$ and therefore $\mathfrak{p}$ decomposes in $K\mathbb{F}_{q^j}$ into j prime divisors of degree 1. Each of them has exactly one extension to $K\mathbb{F}_{q^k}$ and the latter decomposes in K' into at most m prime divisors. Hence, by Weil's theorem

$$\begin{aligned}
\#\{\mathfrak{q} \in \mathbb{P}(K') \mid \deg(\mathfrak{q}_K) \text{ pd } k\} &\le m \sum_{j \le k/2} \frac{1}{j} |\mathbb{P}_1(K\mathbb{F}_{q^j})|\\
&\le m \sum_{j \le k/2} \frac{1}{j}(q^j + 2g_K q^{j/2} + 1).
\end{aligned} \tag{13.3}$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Induction on k shows that for $q \geq 2$

$$\sum_{j \leq k/2} \frac{q^j}{j} \leq q^{k/2}. \tag{13.4}$$

A direct check for $k \leq 5$ and an induction for $k \geq 6$ shows that for $q \geq \frac{9}{7}$

$$\sum_{j \leq k/2} \frac{q^j}{j} \leq \frac{3}{2} q^{k/2}. \tag{13.5}$$

If q is a power of a prime, then $q^{1/2} \geq \sqrt{2} \geq 9/7$. Hence, (13.2) is a consequence of (13.3), (13.4), and (13.5). □

Finally we improve [FrJ, Prop. 5.16].

PROPOSITION 13.4. *In the notation of Data* 13.1 *let a be a positive integer and let τ be an element of $\mathcal{C}$ such that $\tau|_{\mathbb{F}_{q^n}} = \varphi^a$. Let k be a positive integer such that $k \equiv a \bmod n$. Then*

$$\begin{aligned} (13.6) \quad & |\#C_k(L/K, \mathcal{C}) - \frac{c}{km} q^k| \\ & < \frac{c}{km}[(m + 2g_L)q^{k/2} + m(3g_K + 1)q^{k/4} + 2(g_L + dm)]. \end{aligned}$$

Proof. Let $n' = nk \cdot \mathrm{ord}(\tau)$ and extend L to $L' = L\mathbb{F}_{q^{n'}}$. Then $[L' : K\mathbb{F}_{q^{n'}}] = [L : K\mathbb{F}_{q^n}] = m$. Since $k \equiv a \bmod n$ there exists $\tau' \in \mathcal{G}(L'/K)$ such that $\tau'|_L = \tau$ and $\tau'|_{\mathbb{F}_{q^{n'}}} = \varphi^k$. Then $\mathrm{ord}(\tau') = \mathrm{lcm}(\mathrm{ord}(\tau), \mathrm{ord}(\varphi^k)) = \mathrm{lcm}(\mathrm{ord}(\tau), [\mathbb{F}_{q^{n'}} : \mathbb{F}_{q^k}]) = \mathrm{lcm}(\mathrm{ord}(\tau), n \cdot \mathrm{ord}(\tau)) = n \cdot \mathrm{ord}(\tau)$. Denote the conjugacy class of τ' in $\mathcal{G}(L'/K)$ by $\mathcal{C}'$. By [FrJ, Lemma 5.12(c)], $C_k(L'/K, \mathcal{C}') = C_k(L/K, \mathcal{C})$.

Denote the fixed field of τ' in L' by K'. Then $K' \cap \mathbb{F}_{q^{n'}} = K' \cap \tilde{\mathbb{F}}_q = \mathbb{F}_{q^k}$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

and $K'\mathbb{F}_{q^{n'}} = L'$.

$$\begin{tikzcd}
 & K' \arrow[r, dash, "\mathrm{ord}(\tau')"] \arrow[d, dash, "m"'] & L' \arrow[d, dash, "m"'] \\
K \arrow[r, dash] \arrow[d, dash, "d"'] & K\mathbb{F}_{q^k} \arrow[r, dash] \arrow[d, dash, "d"'] & K\mathbb{F}_{q^{n'}} \arrow[d, dash] \\
\mathbb{F}_q(t) \arrow[r, dash] \arrow[d, dash] & \mathbb{F}_{q^k}(t) \arrow[r, dash] \arrow[d, dash] & \mathbb{F}_{q^{n'}}(t) \arrow[d, dash] \\
\mathbb{F}_q \arrow[r, dash] & \mathbb{F}_{q^k} \arrow[r, dash] & \mathbb{F}_{q^{n'}}
\end{tikzcd}$$

Then $[K' : K\mathbb{F}_{q^k}] = [L : K\mathbb{F}_{q^{n'}}] = m$ and therefore $[K' : \mathbb{F}_{q^k}(t)] = dm$. By [FrJ, Cor. 5.11] applied to L', K, $\mathcal{C}'$, $\{\tau'\}$, k instead of F, E, $\mathcal{C}$, $\mathcal{C}'$, r,

$$|C_k(L'/K, \mathcal{C}')| = \frac{c}{[K' : K]} |C_1(L'/K', \{\tau'\}) \smallsetminus \{\mathfrak{q} \in \mathbb{P}(K') \mid \deg(\mathfrak{q}_K) \text{ pd } k\}|.$$

Since $[K' : K] = km$, we have by Lemma 13.3,

$$\begin{aligned}(13.7) \qquad |\#C_k(L'/K, \mathcal{C}') - \frac{c}{km}\#C_1(L'/K', \{\tau'\})| &\\ \le \frac{c}{km}\#\{\mathfrak{q} \in \mathbb{P}(K') \mid \deg(\mathfrak{q}_K) \text{ pd } k\}& \\ \le \frac{c}{km} \cdot m(q^{k/2} + (3g_K + 1)q^{k/4})&\end{aligned}$$

By Lemma 13.2 applied to K', L', n', τ', q^k instead of to K, L, n, τ, q

$$(13.8) \qquad |\#C_1(L'/K', \{\tau'\}) - q^k| < 2(g_{L'}q^{k/2} + g_{L'} + dm).$$

Multiply (13.8) by $\frac{c}{km}$ and replace $g_{L'}$ by g_L. Then replace $C_K(L'/K, \mathcal{C}')$ in (13.7) by $C_k(L/K, \mathcal{C})$. Finally combine the two inequalities obtained in this way to (13.6). $\square$

Corollary 13.5. *If in the situation of Proposition* 13.4

$$(13.9) \qquad k \log q \ge \max\{2\log(g_L + dm), 4\log(3g_K + 1)\},$$

then

$$(13.10) \qquad |\#C_k(L/K, \mathcal{C}) - \frac{c}{km}q^k| < \frac{2c}{km}(m + g_L + 1)q^{k/2}.$$

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

Proof. By (13.9), $3g_K + 1 \le q^{k/4}$ and $g_L + dm \le q^{k/2}$. Hence

$$(m + 2g_L)q^{k/2} + m(3g_K + 1)q^{k/4} + 2(g_L + dm) \le (m + 2g_L + m + 2)q^{k/2}.$$

Now combine this inequality with (13.6) to get (13.10). □

References

[Ax] J. Ax, *The elementary theory of finite fields*, Annals of Mathematics, **88** (1968), 239–271.

[CaF] J. W. S. Cassels and A. Fröhlich, Algebraic Number Theory, Academic Press, London, 1967.

[FrJ] M. D. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik (3), 11, Springer, Heidelberg (1986).

[FrV] M. D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Mathematische Annalen **290** (1991), 771–800.

[GeJ] W.-D. Geyer and C. U. Jensen, *Extension prodiédrales*, C. R. Acad. Sci. Paris Sér. I, **319** (1994), 1241–1244.

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

[Hoe] Klaus Hoechsmann, *Zum Einbettungsproblem*, Journal für die reine und ungewandte Mathematik, **229** (1968), 81–106.

[HKo] F. Halter-Koch, *Der Čebotarev'sche Dichtigkeitsatz und ein analogon zum Dirichlet'schen Primzahlsatz für algebraische Funktionenkörper*, manuscripta mathematica, **72** (1991), 205–211.

[Ja1] M. Jarden, *Elementary statements over large algebraic fields*, Transactions of AMS, **164** (1972), 67–91.

[Ja2] M. Jarden, *The inverse Galois problem over formal power series fields,*, Israel Journal of Mathematics, **85** (1994), 263–275.

[Koc] H. Koch, *l-Erweiterungen mit vorgegebener Verzweigunsstellen*, Journal für die reine und angewandte Mathematik, **219** (1965), 30–61.

[Lan] S. Lang, Algebra, Addison-Wesley, Reading, 1970.

[La2] S. Lang, Algebraic Number Theory, Addison-Wesley, Reading, 1970.

[La3] S. Lang, Introduction to algebraic geometry, Interscience Publishers, New York, 1958.

[La4] S. Lang, Algebra, Second Edition, Addison-Wesley, Menlo Park, 1984.

[Neu] J. Neukirch, *Class field theory*, Grundlehren der mathematischen Wissenschaften, **280** (1985), Springer, Berlin.

[RCV] Rzedowski-Calderón and Villa-Salvador, *Automorphisms of congruence function fields*, Pacific Journal of Mathematics, **150** (1991), 167-178.

[Rei] H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, Journal für die reine und angewandte Mathematik, **177** (1937), 1–5.

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press

[Sch] Arnold Scholz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I*, Mathematische Zeitschrift, **42** (1936), 161–188.

[Se1] J.-P. Serre,, Topics in Galois Theory, Jones and Barlett, Boston, 1992.

[Se2] J.-P. Serre, Corps Locaux, Hermann, Paris, 1962.

[Sh1] I. R. Shafarevich, *On the construction of fields with a given Galois group of order l^a*, Izv. Akad. Nauk, **18** (1954), 261–296, = Collected Mathematical Papers 69–97, Springer, Berlin, 1989.

[Sh2] I. R. Shafarevich, *Factors of descending central series*, Mathematical Notes, **45** (1989), 262–264.

Wulf-Dieter Geyer
Mathematisches Institut, Universität Erlangen
Bismarckstraße $1\frac{1}{2}$, *91054, Germany*
geyer@mi.uni-erlangen.de

Moshe Jarden
School of Mathematical Sciences, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
jarden@math.tau.ac.il

https://doi.org/10.1017/S0027763000025046 Published online by Cambridge University Press