Abstract. We give an intrinsic parametrisation of the set of tamely ramified extensions of a local field and bring to the fore the role played by group cohomology. We show that two natural definitions of the cohomology class of a tamely ramified finite galoisian extension coincide, and can be recovered from the parameter. We also give an elementary proof of Serre’s mass formula in the tame case and in the simplest wild case, and we classify galoisian extensions of degree the cube of a prime (different from the residual characteristic).

Let $p$ be a prime number, and let $K$ be a local field with finite residue field $k$ of characteristic $p$ and cardinality $q$ (a power of $p$), so $K$ is either a finite extension of $\mathbb{Q}_p$ or isomorphic to $k((\pi))$. Let $e > 0$ be an integer such that $\gcd(e, p) = 1$ and let $f > 0$ be an arbitrary integer. Consider the set $\mathcal{T}_{e,f}(K)$ of $K$-isomorphism classes of finite (separable) extensions of $K$ of ramification index $e$ and residual degree $f$. This set was investigated by Hasse in Chapter 16 of his treatise [8] which was completed in 1938 but published only after the War of 39–45, and by Albert in [1] (who confined himself to the characteristic-0 case, but the arguments in the characteristic-$p$ case are similar).

Our purpose here is to give a more intrinsic parametrisation of this set, and to bring to the fore the role played by group cohomology, a theory which had not yet been fully formalised at the time of Hasse and Albert,
although only the first few cohomology groups (which were known under different names) are needed.

We are able to recover properties of $L \in \mathcal{T}_{e,f}(K)$ directly from its parameter. These properties include those of being galoisian, or abelian, or cyclic over $K$. For $L$ which are not galoisian over $K$, the parameter determines the smallest extension $\tilde{K}$ of $K$ such that $L \mid \tilde{K}$ is galoisian over $K$. When $L \mid K$ is galoisian, it determines the class of $\text{Gal}(L \mid K)$ as an extension of $\text{Gal}(K_f \mid K)$ by $\text{Gal}(L \mid K_f)$, where $K_f$ is the maximal unramified extension of $K$ in $L$; it also determines the smallest extension $K_f$ of $K$ such that the extension of groups corresponding to the tower $L \mid K$ splits.

We also give an easy elementary proof of Serre’s mass formula [12] in the tame case (and in the case when the degree is divisible by $p$ but not by $p^2$), analogous to the recent proof [3] in the prime degree $l$ (in both the cases $l \neq p$ and $l = p$). We explicitly work out all galoisian extensions of $K$ of degree $l^3$ (for every prime $l \neq p$), including the case $l = 2$ of octic dihedral or quaternionic extensions.

Let $K_f$ be the degree-$f$ unramified extension of $K$ (so that $K_1 = K$), $w_f : K_f^\times \to \mathbb{Z}$ its normalised valuation, $k_f$ the residue field of $K_f$, and $G_f = \text{Gal}(K_f \mid K) = \text{Gal}(k_f \mid k)$. We shall show that $\mathcal{T}_{e,f}(K)$ is in canonical bijection with the set of orbits for the action of $G_f$ on set of what we call ramified lines $D \subset K_f^\times / K_f^{\times e}$ or equivalently on the set of sections of $\bar{w}_f : K_f^\times / K_f^{\times e} \to \mathbb{Z}/e\mathbb{Z}$; ramified lines are precisely images of sections of $\bar{w}_f$. We show how properties of $L \in \mathcal{T}_{e,f}(K)$ (such as being galoisian or abelian or cyclic over $K$) can be read off from its parameter, the corresponding $G_f$-orbit in the set $\mathcal{R}_e(K_f)$ of ramified lines in $K_f^\times / K_f^{\times e}$.

We begin by recalling some basic facts about cohomology of groups in §1 and apply them to the cohomology of finite fields in §2, where we verify an important compatibility between two different definitions of the cohomology class of an extension of a cyclic group by a cyclic group. We then recall in §3 some basic properties of the Kummer pairing such as its equivariance. The fundamental notion of ramified lines is introduced in §4. In §5 we parametrise the set $\mathcal{T}_{e,1}(K)$ and give a proof in the spirit of [3] of Serre’s mass formula in degree $e$ (and also in degree $ep$ when combined with the results of [3]). We then provide in §6 an analogue in degree $e$ (prime to $p$) of the orthogonality relation in prime degree [3]. In §7, we give the parametrisation of $\mathcal{T}_{e,f}(K)$ and show how the various invariants of an $L \in \mathcal{T}_{e,f}(K)$ can be recovered from its parameter, and work out a number of instructive examples.

Our main contribution has thus been an intrinsic presentation of the
material, without making any choices of uniformisers or roots of unity. This text may also serve to illustrate the general problem of classification or parametrisation of all finite separable extensions of a given local field by showing how it can be solved in the simple case of tame ramification.

1 Cohomology of groups

For a group $G$ and a $G$-module $C$ with action $\theta : G \to \text{Aut}(C)$, we recall the definitions and some functorial properties of the groups $H^1(G, C)_\theta$ and $H^2(G, C)_\theta$; the first one classifies sections of the twisted product $C \to C \times_\theta G \to G$ up to $C$-conjugacy and the second one classifies extensions of $G$ by $C$. We also recall how these groups are computed when $G$ is cyclic, and give a presentation of every extension of $G$ by $C$ when moreover $C$ is also cyclic. For an account of group cohomology by one of its creators, see [4].

So most readers can skip this $\S$, except perhaps (1.8) where we compute the number of $G$-orbits in $C$ (when both groups are cyclic) — this is the key to Roquette’s determination of the cardinality of the set $\mathcal{T}_{e,f}(K)$ of tamely ramified extensions of $K$ with given ramification index $e$ and given residual degree $f$ (§7).

1.1 The group $H^2(G, C)_\theta$

Let $G$ be a group and $C$ a $G$-module, both written multiplicatively, and $\theta : G \to \text{Aut}(C)$ the action of $G$ on $C$; one often writes $\theta(g)(c) = g.c$ for $g \in G$ and $c \in C$. An extension of $G$ by $C$ is a short exact sequence $1 \to C \to \Gamma \to G \to 1$ such that the resulting conjugation action of $G$ on $C$ is equal to the given action $\theta$. Two extensions $\Gamma, \Gamma'$ of $G$ by $C$ are isomorphic if there is an isomorphism of groups $\Gamma \to \Gamma'$ inducing $\text{Id}_C$ on the common subgroup $C$ and $\text{Id}_G$ on the common quotient $G$. Isomorphism classes of extensions of $G$ by $C$ are classified by the group $H^2(G, C)_\theta$. The class $[\Gamma] \in H^2(G, C)_\theta$ vanishes if and only if the extension $\Gamma$ is split in the sense that the projection $\Gamma \to G$ admits a section. Recall that an extension is split if and only if it is isomorphic to the twisted product $C \times_\theta G$, the product set $C \times G$ with the law of composition

$$(c, g)(d, h) = (c\theta(g)(d), gh) = (c(g,d), gh),$$

so that $1 = (1, 1)$ and $(c, g)^{-1} = (\theta(g^{-1})(c^{-1}), g^{-1}) = (g^{-1}.c^{-1}, g^{-1})$.

1.2 The group $H^1(G, C)_\theta$

The group $H^1(G, C)_\theta$ can be identified with the group of outer automorphisms of any extension $\Gamma$ of $G$ by $C$ (the group of automorphisms
of the extension $\Gamma$ modulo the subgroup of inner automorphisms by an element of $C$. If the action $\theta$ is trivial, then $H^1(G, C)_\theta = \text{Hom}(G, C)$. When $\Gamma = C \times G$, the group $H^1(G, C)_\theta$ can be identified with the set of sections of the projection $\Gamma \to G$ up to $C$-conjugacy, which in turn can be identified with the set of supplements of $C$ in $\Gamma$ (subgroups $D \subset C \times G$ such that $C \cap D = 1$, $CD = \Gamma$) up to $\Gamma$-conjugacy (or $C$-conjugacy, which comes to the same).

1.3 The restriction map in general

Let $G$ be a group and $C$ a $G$-module. Let $\varphi : G' \to G$ be a morphism of groups; it allows us to view the $G$-module $C$ as a $G'$-module via $g'.c = \varphi(g').c$ for every $g' \in G'$ and every $c \in C$. Let $C'$ be a $G'$-module (with action $\theta'$), and let $\psi : C \to C'$ be a morphism of $G'$-modules. The pair $(\varphi, \psi)$ induces a map $H^1(G, C)_\theta \to H^1(G', C'_\theta)$ on cohomology called the restriction map.

For $i = 1$, it sends the class in $H^1(G, C)_\theta$ of a section $g \mapsto (\sigma(g), g)$ of the projection $C \times G \to G$ to the class in $H^1(G', C'_{\theta'})$ of the section $g' \mapsto (\psi(\sigma(\varphi(g'))), g')$ of the projection $C' \times G' \to G'$.

For $i = 2$, the restriction map $H^2(G, C)_\theta \to H^2(G', C'_{\theta'})$ coming from the pair $(\varphi, \text{Id}_C)$ (where $\varphi$ is a morphism $G' \to G$ of groups) sends the class of the extension $1 \to C \to \Gamma \to G \to 1$ to the class of the extension $\Gamma_{\varphi}$ of $G'$ by $C$ consisting of those $(\gamma, g') \in \Gamma \times G'$ such that $\bar{\gamma} = \varphi(g')$ in $G$.

When $C, C'$ are $G'$-modules (with actions $\theta, \theta'$) and $\psi : C \to C'$ is a morphism of $G'$-modules, the restriction map $H^2(G', C'_{\theta'}) \to H^2(G', C'_{\theta'})$ coming from the pair $(\text{Id}_{G'}, \psi)$ sends the class of an extension $\Gamma'$ of $G'$ by $C$ to the class of the extension $\psi \Gamma' = (C' \times \Gamma')/\psi'(C)$ of $G'$ by $C'$, where $\psi'(c) = (\psi(c), c^{-1})$.

The general case reduces to these two special cases, and is illustrated
by the diagram

\[
\begin{array}{c}
1 \to C \longrightarrow \Gamma \longrightarrow G \to 1 \\
\uparrow \quad \uparrow \quad \uparrow \varphi \\
1 \to C \longrightarrow \Gamma_{\varphi} \longrightarrow G' \to 1 \\
\psi \downarrow \quad \downarrow \quad \downarrow = \\
1 \to C' \longrightarrow \psi(\Gamma_{\varphi}) \longrightarrow G' \to 1.
\end{array}
\]

In the special case when \( \varphi : G' \to G \) is surjective and \( C' = C \), the restriction map is called the \textit{inflation map}.

\[\text{1.4 The case of cyclic groups}\]

Recall how the groups \( H^1(G, C)_{\theta} \) and \( H^2(G, C)_{\theta} \) can be computed when \( G \) is cyclic of order \( n > 0 \). Let \( \sigma \) be a generator of \( G \), and denote the automorphism \( \theta(\sigma) \) of \( C \) simply by \( \sigma \). Define the element \( N_{\sigma} = 1 + \sigma + \cdots + \sigma^{n-1} \) in the group ring \( \mathbb{Z}[G] \) (over which \( C \) is a left module via \( \theta \)), so that \( N_{\sigma}(\sigma - 1) = 0 \) and \( (\sigma - 1)N_{\sigma} = 0 \) (since \( \sigma^n = 1 \)), and we have the complex

\[\text{(1.4.1)}\]

\[
\begin{array}{c}
C \overset{\sigma - 1}{\longrightarrow} C \overset{N_{\sigma}}{\longrightarrow} C \overset{\sigma - 1}{\longrightarrow} C.
\end{array}
\]

The cohomology groups of this complex are canonically isomorphic to \( H^1(G, C)_{\theta} \) and \( H^2(G, C)_{\theta} \) respectively. In other words, the kernels and the images of the maps in (1.4.1) are independent of the choice of \( \sigma \) and

\[
\begin{array}{c}
H^1(G, C)_{\theta} = \text{Ker}(N_{\sigma})/\text{Im}(\sigma - 1), \\
H^2(G, C)_{\theta} = \text{Ker}(\sigma - 1)/\text{Im}(N_{\sigma}),
\end{array}
\]

(with a slight abuse of notation). In particular, if the action is trivial \( (\theta(\sigma) = \text{Id}_C) \), then \( H^1(G, C)_1 = \text{Hom}(G, C) = nC \) and \( H^2(G, C)_1 = C/C^n \).

Let \( G' \) be another cyclic group, \( \varphi : G' \to G \) a \textit{surjective} morphism of groups, and \( \sigma' \) a generator of \( G' \) such that \( \varphi(\sigma') = \sigma \). Let \( C' \) be a \( G' \)-module and \( \psi : C \to C' \) a morphism of \( G' \)-modules. Then the restriction map \( H^1(G, C)_{\theta} \to H^1(G', C')_{\theta'} \) is simply given by restriction to subgroups and passage to the quotient from the map \( \psi : C \to C' \).
1.5 The case of cyclic modules

Specialise further to the case when \( C \) is also cyclic, of some order \( m > 0 \), and let \( a > 0 \) be such that \( \theta(\sigma) = \bar{a} \) in \( (\mathbb{Z}/m\mathbb{Z})^\times \) (so that \( a^n \equiv 1 \) (mod. \( m \)) or equivalently \( m \mid a^n - 1 \)). The orders of the cyclic groups \( H^1(G, C)_a \) and \( H^2(G, C)_a \) can then be computed in terms of \( a, m \) and \( n \) because for every \( r \in \mathbb{N} \), the order of the kernel \( rC \) (resp. the image \( C^r \)) of the endomorphism \( (\cdot)^r \) of \( C \) is \( \gcd(m, r) \) (resp. \( m/\gcd(m, r) \)). Taking \( r = a - 1 \) and \( r = 1 + a + \cdots + a^{n-1} \) respectively gives the result.

To get a presentation of the extension \( \Gamma \) of \( G \) by \( C \) corresponding to a given class in \( H^2(G, C)_a \), choose generators \( \tau \in C, \sigma \in G \) (using which identify the given class as the class of an element \( s \in \mathbb{Z}/m\mathbb{Z} \) such that \( (a - 1)s \equiv 0 \) (mod. \( m \)) (modulo those which are \( \equiv (1 + a + \cdots + a^{n-1})t \) for some \( t \in \mathbb{Z}/m\mathbb{Z} \)). For a suitable lift \( \tilde{\sigma} \in \Gamma \) of \( \sigma \), we then have

\[
\Gamma = \langle \tau, \tilde{\sigma} \mid \tau^m = 1, \tilde{\sigma}^n = \tau^s, \tilde{\sigma} \tau \tilde{\sigma}^{-1} = \tau^a \rangle.
\]

For a direct derivation of this presentation, and an elementary proof of the fact that the extensions of \( G \) by the \( G \)-module \( C \) corresponding to \( s, s' \in \mathbb{Z}/m\mathbb{Z} \) (such that \( (a - 1)s \equiv 0 \) (mod. \( m \)) and \( (a - 1)s' \equiv 0 \) (mod. \( m \))) are isomorphic if and only if \( s \) and \( s' \) have the same class in the sense that \( s' - s \equiv (1 + a + \cdots + a^{n-1})t \) for some \( t \in \mathbb{Z}/m\mathbb{Z} \), see for example [10, 9.4].

Remark 1.5.2 In particular, the extension \( 1 \to C \to \Gamma \to G \to 1 \) (1.5.1) splits if and only if \( s \equiv (1 + a + \cdots + a^{n-1})t \) (mod. \( m \)) for some \( t \in \mathbb{Z}/m\mathbb{Z} \).

Example 1.5.3 Take \( n = 2 \) and \( m = 4 \). The possibilities for \( a \) (mod. \( 4 \)) are 1 and 3. When \( a = 1 \), we have \( H^2(G, C)_1 = C/C^2 \), and the two extensions \( \Gamma \) (1.5.1) are the direct product \( C \times G \) and the one in which the group \( \Gamma \) is cyclic (of order 8). When \( a = 3 \), we have \( H^2(G, C)_3 = 2C \), the split extension is the twisted product \( C \times_3 G \) (1.1) and called the dihedral group \( D_8 \) of order 8, while the one which is not split is called the quaternionic group \( \mathcal{H}_8 \).

Remark 1.5.4 In the presentation (1.5.1) for \( \mathcal{H}_8 \), one has \( m = 4 \), \( s = n = 2 \) and \( a = 3 \). The centre \( Z \) of \( \mathcal{H}_8 \) is generated by the involution \( \tilde{\sigma}^2 = \tau^2 \), and the quotient \( \mathcal{H}_8/Z \) is an elementary abelian 2-group (an \( \mathbb{F}_2 \)-space) of rank 2, so \( \mathcal{H}_8 \) also represents a class in \( H^2(\mathcal{H}_8/Z, Z)_1 \). As the extension \( 1 \to Z \to \mathcal{H}_8 \to \mathcal{H}_8/Z \to 1 \) is not split, the said class does not vanish.

1.6 Commutativity and cyclicity of the extension
Let us determine the order of \( \tilde{\sigma} \) in \( \Gamma \) (1.5.1), and the conditions for \( \Gamma \) to be commutative, or the direct product of \( C \) and \( G \), or cyclic. The ideas are as in [1] but our presentation is simpler and shows that the proofs are applicable to all extensions \( \Gamma \) (and not just to those coming from tamely ramified galoisian extensions of local fields).

**Remark 1.6.1** Although \( s \) is not uniquely determined as a number, \( r = \gcd(m, s) \) is uniquely determined; \( m/r \) is the order of \( \tau^s \) in the group \( \Gamma \). We claim that the order of the element \( \tilde{\sigma} \in \Gamma \) (1.5.1) is \( mn/r \). Indeed, the order of \( \tilde{\sigma} \) is a multiple \( dn \) of the order \( n \) of its image \( \sigma \in G \); we have to show that \( d = m/r \). Now, from the relation \( \tilde{\sigma}^n = \tau^s \), it follows that \( \tilde{\sigma}^{dn} = \tau^{ds} = 1 \), so \( d \) is a multiple of the order of \( m/r \) of \( \tau^s \). But conversely, it follows from \( \tilde{\sigma}^{mn/r} = \tau^{ms/r} = 1 \) that \( dn \) divides \( mn/r \) and therefore \( d \) divides \( m/r \). Hence \( d = m/r \), and the order of \( \tilde{\sigma} \) is \( mn/r \).

**Remark 1.6.2** Note that the group \( \Gamma \) (1.5.1) is commutative if and only if \( \tau \) and \( \tilde{\sigma} \) commute, which happens precisely when \( a \equiv 1 \pmod{m} \), in view of the relations \( \tau^m = 1 \), \( \tilde{\sigma} \tau \tilde{\sigma}^{-1} = \tau^a \).

**Remark 1.6.3** Suppose that \( a \equiv 1 \pmod{m} \), so that \( \Gamma \) is commutative. In this commutative case, the extension (1.5.1) has a section \( G \to \Gamma \) (and consequently \( \Gamma \) is the internal direct product of \( C \) and the image of the section) if and only if \( s \equiv 0 \pmod{\gcd(m, n)} \). Indeed, this condition is equivalent to the existence of a \( t \in \mathbb{Z}/m\mathbb{Z} \) such that \( nt \equiv s \pmod{m} \), which is equivalent to \( s \equiv (1 + a + \cdots + a^{n-1})t \pmod{m} \) in view of \( a \equiv 1 \pmod{m} \), which is equivalent to the existence of a section \( G \to \Gamma \) by (1.5.2).

For every prime \( l \) and every integer \( x \neq 0 \), we denote by \( v_l(x) \) the exponent of \( l \) in the prime decomposition of \( x \); for a fixed \( x \), we have \( v_l(x) = 0 \) for almost all \( l \). We have remarked (1.6.1) that the \( s \) in (1.5.1) is not uniquely determined as a number, but some properties such as being prime to \( \gcd(m, n) \) are independent of any particular number representing \( s \). One may wish to fix some such representative. The following proposition has been extracted from [1, Theorem 13] and the proof has been simplified.

**Proposition 1.6.4.** — Suppose that \( a \equiv 1 \pmod{m} \). The (commutative) group \( \Gamma \) is cyclic if and only if \( s \) is prime to \( \gcd(m, n) \).

**Proof.** Suppose first that \( s \) is prime to \( \gcd(m, n) \); we have to find an element of order \( mn \) in \( \Gamma \). The idea is to find an element \( \gamma_l \in \Gamma \) of order \( l^{v_l(mn)} \) for every prime \( l \) in each of the three (exhaustive) cases \( v_l(m)v_l(n) > 0, v_l(m) = 0, \text{ and } v_l(n) = 0 \).

If \( v_l(m)v_l(n) > 0 \), then \( l \mid \gcd(m, n) \) and is prime to \( s \), so \( \gcd(m, s) \)
is prime to $l$ and $m/\gcd(m, s)$ is divisible by $l^{v_l(m)}$. Consequently, $mn/\gcd(m, s)$ is divisible by $l^{v_l(mn)}$, and hence there is an element $\gamma_l \in \Gamma$ of order $l^{v_l(mn)}$, in view of the fact that the order of $\bar{\sigma} \in \Gamma$ is $mn/\gcd(m, s)$ by (1.6.1). Even if $v_l(m) = 0$ (so that $v_l(mn) = v_l(n)$), the subgroup (of order a multiple of $n$) generated by $\bar{\sigma}$ has an element $\gamma_l$ of order $l^{v_l(mn)}$. Finally, if $v_l(n) = 0$, then the subgroup (of order $m$) generated by $\tau$ has an element $\gamma_l$ of order $l^{v_l(m)} = l^{v_l(mn)}$. These $\gamma_l$ are trivial for almost all $l$ (because $v_l(mn) = 0$ for almost all $l$), so their product over all $l$ exists, is independent of the sequence of the factors because $\Gamma$ is commutative by (1.6.2), and has order $mn$.

Conversely, suppose that the group $\Gamma$ is cyclic, so that $\Gamma_l = \Gamma/\Gamma^{v_l(mn)} (= \Gamma \otimes \mathbb{Z}_l)$ is also cyclic and has order $l^{v_l(mn)}$ for every prime $l$. Suppose (if possible) that there is a prime $l$ dividing all three numbers $m, s, n$; we shall get a contradiction by showing that $\Gamma_l$ would then have order $< l^{v_l(mn)}$. This follows from the fact that it is generated by the pair $\bar{\tau}, \bar{\sigma} \in \Gamma_l$ (images of $\tau$ and $\bar{\sigma}$ respectively) each of which has order $< l^{v_l(mn)}$, because

$$v_l(m) < v_l(mn), \quad v_l(mn/\gcd(m, s)) < v_l(mn)$$

by hypothesis (recall that the order of $\bar{\sigma}$ is $mn/\gcd(m, s)$ by (1.6.1)). □

### 1.7 The inflation map in the bicyclic case

Let $G$ be a cyclic group of order $n$ with generator $\sigma$, and make it act on a cyclic group $C$ of order $m$ and generator $\tau$ by $\sigma \mapsto (\cdot)^a$ for some $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $a^n \equiv 1. We have seen that the group $H^2(G, C)_a$ can be identified with the kernel $a^{-1}C$ of $(\cdot)^a : C \rightarrow C$ modulo the image of $(\cdot)^{1+a+\cdots+a^{n-1}} : C \rightarrow C$ (1.4).

Let $G'$ be another cyclic group, of order $cn$ for some $c > 0$, let $\sigma'$ be a generator of $G'$, and let $\varphi : G' \rightarrow G$ be the surjection such that $\varphi(\sigma') = \sigma$. Regard $C$ as a $G'$-module via $\sigma' \mapsto \sigma \mapsto (\cdot)^a$. As before, the group $H^2(G', C)_a$ can be identified with the kernel $a^{-1}C$ of $(\cdot)^a : C \rightarrow C$ modulo the image of $(\cdot)^{1+a+\cdots+a^{n-1}} : C \rightarrow C$. Notice that, when $a > 1$,

$$\frac{1 + a + \cdots + a^{cn-1}}{1 + a + \cdots + a^{n-1}} = \frac{a^{cn} - 1}{a^n - 1} = a^{(c-1)n} + \cdots + a^n + 1 \equiv c \pmod{m},$$

so $1 + a + \cdots + a^{cn-1} \equiv (1 + a + \cdots + a^{n-1})c \pmod{m}$, which holds trivially.
for $a = 1$ as well. Hence there is a commutative diagram

$$
\begin{array}{ccc}
\mathbb{H}^2(G, C) & \xrightarrow{(1.7.1)} & \mathbb{H}^2(G', C) \\
\downarrow & & \downarrow \\
\mathbb{H}^2(G, C) & \xrightarrow{(a-1)c} & \mathbb{H}^2(G', C)
\end{array}
$$

in which the vertical arrows are the passage to the quotient. We claim that the lower horizontal arrow is the restriction map (1.3) coming from the pair $(\varphi, \text{Id}_C)$.

**Proposition 1.7.2.** — The map $\mathbb{H}^2(G, C) \to \mathbb{H}^2(G', C)$ in the above diagram is the inflation map corresponding to the quotient $\varphi : G' \to G$.

**Proof.** Let a class in $\mathbb{H}^2(G, C)$ be represented by an extension $\Gamma$ of $G$ by $C$ having the presentation $\langle \tau, \tilde{\sigma} \mid \tau^m = 1, \tilde{\sigma}^n = \tau^s, \tilde{\sigma}^a = \tau^a \rangle$ for some $s \in \mathbb{Z}/m\mathbb{Z}$ such that $(a-1)s \equiv 0 \pmod{m}$, where $\tilde{\sigma} \in \Gamma$ lifts the generator $\sigma$ of $G$.

The inflated extension $\Gamma'$ of $G'$ by $C$ consists of $(\alpha, \beta) \in \Gamma \times G'$ such that $\bar{\alpha} = \varphi(\beta)$ in $G$. As a lift $\tilde{\sigma}' \in \Gamma'$ of the generator $\sigma' \in G'$, we choose $\tilde{\sigma}' = (\tilde{\sigma}, \sigma')$. We then have $\tilde{\sigma}'^{cn} = (\tilde{\sigma}^{cn}, \sigma'^{cn}) = (\tau^{cs}, 1) = \tau^{cs}$ and we are done, because $\Gamma'$ admits the desired presentation

$$\Gamma' = \langle \tau, \tilde{\sigma} \mid \tau^m = 1, \tilde{\sigma}^{cn} = \tau^{cs}, \tilde{\sigma}^a = \tau^a \rangle$$

with $cs$ as the exponent of $\tau$ in the second relation where the presentation (1.5.1) for $\Gamma$ had $s$. (The exponent $cn$ of $\tilde{\sigma}'$ in the said relation is the order of $G'$, just as the exponent $n$ of $\tilde{\sigma}$ in (1.5.1) was the order of $G$.)$\Box$

**Remark 1.7.3** When we take $c$ to be the order of a class in $\mathbb{H}^2(G, C)$, the corresponding extension of $G'$ by $C$ splits. When we take $c$ to be the order of the group $\mathbb{H}^2(G, C)$, the inflation map is trivial.

### 1.8 The number of orbits

The following lemma captures one of the basic ingredients in Roquette’s computation [8, ch. 16] of the number of tamely ramified extensions of a given ramification index and a given residual degree (7.2.4).
LEMMA 1.8.1. — Let \( C \) be a cyclic group of order \( m \), written multiplicatively. Let \( a > 0 \) be prime to \( m \), and make \( \mathbb{Z} \) act on \( C \) by \( 1 \mapsto (\cdot)^a \). Then the number of orbits is \( \sum_{t \mid m} \phi(t)/\chi_a(t) \), where \( \chi_a(t) \) denotes the order of \( \bar{a} \) in the group \( (\mathbb{Z}/t\mathbb{Z})^\times \) of order \( \phi(t) \).

Proof. Notice that if \( x, y \in C \) are in the same orbit, then they have the same order in \( C \). The possible orders are the divisors of \( m \); for each divisor \( t \) of \( m \), there are \( \phi(t) \) elements of order \( t \). It is therefore sufficient to show that the orbit of an order-\( t \) element has \( \chi_a(t) \) elements.

Indeed, if \( x \) has order \( t \) in \( C \), and if its orbit consists of the \( r \) elements \( x, xa, \ldots, xa^{r-1} \), then \( r \) is the smallest integer \( > 0 \) such that \( xa^r = x \), which is the same as saying that \( r \) is the smallest integer \( > 0 \) such that \( a^r \equiv 1 \) (mod \( t \)), so \( r \) equals the order \( \chi_a(t) \) of \( \bar{a} \) in \( (\mathbb{Z}/t\mathbb{Z})^\times \).

2 Cohomology of finite fields

The purpose of this \( \S \) is to apply the results of \( \S 1 \) to some galoisian modules arising from finite fields. The main result here is the compatibility (2.3.1) between two different ways of defining the cohomology class of an extension of a cyclic group by a cyclic group; it could have been included in \( \S 1 \) but the formulation here is what will be needed later.

Let \( p \) be a prime number, \( k \) a finite extension of \( \mathbb{F}_p \) with \( q \) elements, and \( k_f \) the degree-\( f \) extension of \( k \) (for every \( f > 0 \)); it is galoisian over \( k \), and the group \( G_f = \text{Gal}(k_f/k) \) is cyclic of order \( f \), with a canonical generator \( \sigma \) which acts on the the cyclic group \( k_f^\times \) of order \( q_f - 1 \) by the automorphism \( (\cdot)^a \). From the fact that \( c k_f^\times = k_f^\times d \) whenever \( cd = q_f - 1 \) and the discussion in (1.4) it follows, upon taking \( d = q - 1 \) and \( c = q - 1 \) respectively, that \( H^1(G_f, k_f^\times)_q = 0 \) (Satz 90) and \( H^2(G_f, k_f^\times)_q = 0 \).

Let \( e > 0 \) be an integer which divides \( q_f - 1 \) (and which is therefore prime to \( p \)). We are interested in the groups \( H^2(G_f, k_f^\times/k_f^{\times e})_q \) and \( H^2(G_f, e k_f^\times)_q \), where \( e k_f^\times \) is the group of \( e \)-th roots of 1 in \( k_f^\times \). We observe (2.2) that every \( \xi \in k_f^\times \) such that \( \xi^{q-1} \in k_f^{\times e} \) gives rise to a class in the \( H^2 \) of each of these \( G_f \)-modules and prove the compatibility of these classes under the natural isomorphism \( k_f^\times/k_f^{\times e} \rightarrow e k_f^\times \) of \( G_f \)-modules (2.3). For a given class in \( H^2(G_f, k_f^\times/k_f^{\times e})_q \), we also determine (2.4.4) the smallest multiple \( \hat{f} \) of \( f \) such that the inflated class vanishes in \( H^2(G_f, k_f^{\times e})_q \).

2.1 The number of orbits

For the time being, let \( e > 0 \) be any integer prime to \( p \), and recall
that the group \( k_f^x/k_f^xe \) is cyclic of order \( g_f = \gcd(q^f - 1, e) \). Let us first compute the number of orbits for the galoisian action of \( G_f \) on this group.

**Remark** 2.1.1 As an immediate consequence of lemma 1.8.1, the number of orbits for the \( G_f \)-action on \( k_f^x/k_f^xe \) is \( \sum_{t|g_f} \phi(t)/\chi_q(t) \).

### 2.2 The classes in \( H^2(G_f, k_f^x/k_f^xe)_q \) and \( H^2(G_f, e k_f^x)_q \)

Let \( \xi \in k_f^x \). If the image \( \tilde{\xi} \in k_f^x/k_f^xe \) is such that \( \tilde{\xi}^{q-1} = \tilde{1} \), then it has a class \( [\tilde{\xi}] \in H^2(G_f, k_f^x/k_f^xe)_q \). But there is also a way to attach a class in \( H^2(G_f, e k_f^x)_q \) to such \( \tilde{\xi} \) which was inspired by [7, 6.1]

Suppose that \( \xi^{q-1} = \alpha^e \) for some \( \alpha \in k_f^x \), and put \( \zeta = N_f(\alpha) \), where \( N_f : k_f^x \to k^x \) is the norm map, so that \( \zeta = \alpha^{1+q+\cdots+q^{f-1}} \). We then have

\[
\zeta^e = N_f(\alpha^e) = N_f(\xi^{q-1}) = 1,
\]

so \( \zeta \in e k_f^x \). At the same time \( \zeta \in k^x \) (being the \( N_f \) of something in \( k_f^x \)), so \( \zeta^{q-1} = 1 \). In other words, \( \zeta \) is in the kernel of \( \chi^e : e k_f^x \to e k_f^x \), and so has a class \( [\zeta] \in H^2(G_f, e k_f^x)_q \). If now we replace \( \alpha \) by \( e \alpha \) for some \( e \in e k_f^x \), then \( \zeta \) gets replaced by \( N_f(e)\zeta \). As \( N_f(e) = e^{1+q+\cdots+q^{f-1}} \), the class \( [\tilde{\zeta}] \in H^2(G, e k_f^x)_q \) is uniquely determined by \( \tilde{\zeta} \) and does not depend on the choice of \( \alpha \).

### 2.3 The compatibility of the two classes

Suppose that \( e \mid q^f - 1 \). Observe that the two groups \( k_f^x/k_f^xe \), \( e k_f^x \) are cyclic of the same order \( e \) and they are canonically isomorphic as \( G_f \)-modules by \( \xi \mapsto \xi^{(q^f-1)/e} \). Therefore we get a canonical isomorphism

\[
H^2(G, k_f^x/k_f^xe)_q \to H^2(G, e k_f^x)_q.
\]

**Proposition 2.3.1.** — Under this isomorphism, the class \( [\tilde{\xi}] \) of any \( \xi \in k_f^x \) such that \( \xi^{q-1} \in k_f^xe \) gets mapped to the class \( [\zeta] \) of \( \zeta = N_f(\alpha) \) for any \( \alpha \in k_f^x \) such that \( \xi^{q-1} = \alpha^e \).

**Proof.** Put \( S = 1 + q + \cdots + q^{f-1} \). Notice first that the condition \( \xi^{q-1} \in k_f^xe \) is equivalent to \( \xi^{(q^f-1)/e} \in k^x \), because \( k_f^xe \) (resp. \( k^x = k_f^x S \)) is the subgroup of order \( (q^f - 1)/e \) (resp. \( q - 1 \)) of the cyclic group \( k_f^x \) of order \( q^f - 1 \). Indeed, if \( \omega \) is a generator of \( k_f^x \) and if \( \xi = \omega^x \), then
the condition \( \xi^{q-1} \in k_f^\times \) is equivalent to \( x(q - 1) \equiv 0 \pmod{e} \), and
the condition \( \xi^{(q^f - 1)/e} \in k^\times \) is equivalent to \( x(q^f - 1)/e \equiv 0 \pmod{S} \).
But these two congruences are equivalent (and are clearly satisfied when \( \xi \in k^\times \); they might sometimes be satisfied even by some \( \xi \notin k^\times \)).

Now let \( \xi \in k_f^\times \) be such that \( \xi^{q-1} = \alpha^e \) for some \( \alpha \in k_f^\times \), or equivalently,
as we’ve seen, \( \xi^{(q^f - 1)/e} = \beta^S \) for some \( \beta \in k_f^\times \). We have to show that
\( N_f(\alpha) = \alpha^S \) and \( \beta^S \), which are both in the kernel of the endomorphism
\( q^{-1} \) of \( e\kappa_f^\times \), define the same class in \( H^2(G, e\kappa_f^\times) \) or equivalently that
\( (\beta\alpha^{-1})^S = \eta^S \) for some \( \eta \in e\kappa_f^\times \).

Choose a generator \( \omega \) of \( k_f^\times \) and write \( \xi = \omega^x \), \( \alpha = \omega^a \), \( \beta = \omega^b \) with \( x, a, b \in \mathbb{Z} \), so that
\[
(q - 1)x = ae + (q^f - 1)c, \quad \left( \frac{q^f - 1}{e} \right) x = bS + (q^f - 1)d
\]
for some \( c, d \in \mathbb{Z} \). We then have \( (b - a)S = \left( \frac{q^f - 1}{e} \right) (cS - de) \), so if we take
\( \eta = \omega \left( \frac{q^f - 1}{e} \right)^c \), then \( \eta \in e\kappa_f^\times \) and \( \eta^S = (\beta\alpha^{-1})^S \), hence \( \alpha^S \) has the same class as \( \beta^S \) in \( H^2(G_f, e\kappa_f^\times) \), which was to be proved. \hfill \Box

2.4 The inflation map

Continue to suppose that \( e \mid q^f - 1 \). Let \( f' > 0 \) be a multiple of \( f \), so that \( e \mid q^{f'} - 1 \). By our notational convention, \( k_{f'} \) is the degree-\( f' \)
extension of \( k \); it is cyclic over \( k \) of group \( G_{f'} = \text{Gal}(k_{f'}|k) \), and it is
cyclic of degree \( f'/f \) over \( k_f \). The inclusion \( k_f^\times \to k_{f'}^\times \) induces a map on
the quotients \( k_f^\times/k_f^{xe} \to k_{f'}^{\times}/k_{f'}^{xe} \).

The reader may wish to compare the following lemma with [6, Satz 3.6].

**Lemma 2.4.1.** — For a given \( \xi \in k_f^\times \), the smallest multiple \( f' \) of \( f \) such
that \( \xi^{q-1} = 1 \) in \( k_f^{\times}/k_f^{xe} \) is \( f' = df \), where \( d \) is the order of \( \xi^{q-1} \) in
\( k_f^{\times}/k_f^{xe} \).

**Proof.** Clearly, \( f' \) being a multiple of \( f \), the relation \( \xi^{q-1} = 1 \) holds in
\( k_f^{\times}/k_f^{xe} \) if and only if \( \xi^{q-1} \in k_f^{xe} \). The result follows from the fact that
the degree of the extension \( k_f(\sqrt[q^{q-1}]{\xi^{q-1}}) \) over \( k_f \) equals \( d \). \hfill \Box

Next, it is clear that the map \( k_f^{\times}/k_f^{xe} \to k_{ef}^{\times}/k_{ef}^{xe} \) is trivial because
we have \( k_{ef} = k_f(\sqrt[q]{k_f^{\times}}) \) and hence \( k_f^{\times} \subset k_{ef}^{xe} \). More generally, for
every divisor $c$ of $e$, we have $k_{cf} = k_f\left(\sqrt[k]{k_f^c}\right)$ and the natural map

\[ \iota : k_f^x/k_f^{xe} \to k_{cf}^x/k_{cf}^{xe} \]

(induced by the inclusion $k_f^x \to k_{cf}^x$) is “raising to the exponent $c$” in the sense that if we choose a generator $\omega_c \in k_{cf}^x$ and put $\omega = \omega_c^{q^{cf-1}}$ (which is a generator of $k_f^x$), then the resulting diagram

\[
\begin{array}{ccc}
k_f^x/k_f^{xe} & \xrightarrow{L} & k_{cf}^x/k_{cf}^{xe} \\
\sim & & \sim \\
Z/eZ & \xrightarrow{\cdot c} & Z/eZ
\end{array}
\]

(in which the vertical arrows identify the $G_{cf}$-modules in question with $Z/eZ$ using the generators $\bar{\omega}$, $\bar{\omega}_c$, and where the canonical generator $(\cdot)^q$ of $G_{cf}$ acts on $Z/eZ$ as “multiplication by $q$”) is commutative. Indeed, since $q^e \equiv 1 \pmod{e}$, we have

\[
\frac{q^{cf} - 1}{q^f - 1} = q^{(c-1)f} + \cdots + q^f + 1 \equiv c \pmod{e}.
\]

Now, the map $\iota : k_f^x/k_f^{xe} \to k_{cf}^x/k_{cf}^{xe}$ is $G_{cf}$-equivariant (when we view $k_f^x/k_f^{xe}$ as a $G_{cf}$-module via its quotient $G_f$), and hence induces the inflation map

\[
(2.4.3) \quad H^2(G_f, k_f^x/k_f^{xe})_q \longrightarrow H^2(G_{cf}, k_{cf}^x/k_{cf}^{xe})_q.
\]

It is clear that if we take $c = e$, then this map is 0; indeed the map $k_f^x/k_f^{xe} \to k_{cf}^x/k_{cf}^{xe}$ is trivial, as we have just remarked.

**Lemma 2.4.4.** — For a given $\xi \in k_f^x$ such that $\bar{\xi}^{q-1} = 1$ in $k_f^x/k_f^{xe}$, the smallest multiple $\hat{f}$ of $f$ such that $[\hat{\xi}] = 0$ in $H^2(G_f, k_f^x/k_f^{xe})_q$ is $\hat{f} = \hat{c}f$, where $\hat{c}$ is the order of $[\hat{\xi}]$ in $H^2(G_f, k_f^x/k_f^{xe})_q$.

**Proof.** This follows from the fact that for every divisor $c$ of $e$, the map $\iota : k_f^x/k_f^{xe} \to k_{cf}^x/k_{cf}^{xe}$ of $G_{cf}$-modules can be identified (2.4.2) with $\cdot c : Z/eZ \to Z/eZ$, which is compatible with the inflation map (2.4.3) by prop. 1.7.2. \qed
3 Kummerian extensions

We need to recall some basic facts about abelian extensions of exponent dividing $d$ of a field $F$ which contains a primitive $d$-th root of 1 and which is finite galoisian over some other field $F'$.

3.1 Background

Let $F$ be a field and $d > 0$ an integer such that the group $\mu_d \subset F^\times$ of $d$-th roots of 1 is (cyclic) of order $d$ (so in particular $d \neq 0$ in $F$). Essentially as a consequence of the Hilbert-Noether vanishing theorem for a certain $H^1$ (Satz 90), the maximal abelian extension of $F$ of exponent dividing $d$ is $M = F(\sqrt[d]{F^\times})$, and there is a perfect pairing

\[(3.1.1) \quad \text{Gal}(M|F) \times (F^\times/F^\times d) \longrightarrow \mu_d, \quad (\sigma, \bar{x}) = \frac{\sigma(y)}{y} (y^d = x)\]

between the profinite group $\text{Gal}(M|F)$ and the discrete group $F^\times/F^\times d$. For any closed subgroup $H \subset \text{Gal}(M|F)$, we have $M^H = F(\sqrt[d]{\bar{D}})$ where $D \subset F^\times/F^\times d$ is the orthogonal complement of $H$ for the above pairing. Conversely, for every subgroup $D \subset F^\times/F^\times d$, the orthogonal complement $H \subset \text{Gal}(M|F)$ is a closed subgroup and $M^H = F(\sqrt[d]{D})$. Also, for every subgroup $D \subset F^\times/F^\times d$, the pairing (3.1.1) gives an isomorphism of (profinite) groups $\text{Gal}(F(\sqrt[d]{D})|F) \rightarrow \text{Hom}(D, \mu_d)$.

3.2 Equivariant pairings

Now suppose that $F$ is itself a finite galoisian extension of some field $F'$, of group $G = \text{Gal}(F|F')$. For which finite subgroups $D \subset F^\times/F^\times d$ is $F(\sqrt[d]{D})$ galoisian over $F'$? If it is, the group $\text{Gal}(F(\sqrt[d]{D})|F)$ may be considered as a $G$-module for the conjugation action coming from the short exact sequence

\[(3.2.1) \quad 1 \rightarrow \text{Gal}(F(\sqrt[d]{D})|F) \rightarrow \text{Gal}(F(\sqrt[d]{D})|F') \rightarrow G \rightarrow 1.\]

**Proposition 3.2.2.** — The extension $F(\sqrt[d]{D})$ is galoisian over $F'$ if and only if the subgroup $D \subset F^\times/F^\times d$ is $G$-stable. If so, the isomorphism of groups $\text{Gal}(F(\sqrt[d]{D})|F) \rightarrow \text{Hom}(D, \mu_d)$ is $G$-equivariant.

**Proof.** Suppose first that $D$ is $G$-stable. We have to show that $F(\sqrt[d]{\bar{D}})$, which is clearly separable over $F'$, coincides with all its $F'$-conjugates. The notation $F(\sqrt[d]{\bar{D}})$ stands for $F((\sqrt[d]{x})_{x \in \bar{D}})$, where $\bar{D} \subset F^\times$ is the preimage of $D$. For $\sigma \in G$, we have $\sigma(x) = y^d x'$ for some $x' \in \bar{D}$ and some $y \in F^\times$ (because $D$ is $G$-stable), and therefore $\sqrt[d]{\sigma(x)} = y^{d/2} x'$ is in $F(\sqrt[d]{D})$, so this extension is galoisian over $F'$. 
Conversely, suppose that $F(\sqrt[d]{D})$ is galoisian over $F'$, and let $\tilde{\sigma}$ be an extension of some $\sigma \in G$ to an $F'$-automorphism of $F(\sqrt[d]{D})$. For every $x \in \tilde{D}$, we have $\tilde{\sigma}(\sqrt[d]{x}) = \tilde{\sigma}(x) = \sigma(x)$, so $\sigma(x) \in \tilde{D}$ (because it has the $d$-th root $\tilde{\sigma}(\sqrt[d]{x})$ in $F(\sqrt[d]{D})$), and hence $D$ is $G$-stable.

Finally, to check that the isomorphism $\text{Gal}(F(\sqrt[d]{D})|F) \to \text{Hom}(D, \mu_d)$ (when $D$ is $G$-stable) is $G$-equivariant, it is enough to check that the pairing $\varphi: \text{Gal}(F(\sqrt[d]{D})|F) \times D \to \mu_d$ (3.1.1) is $G$-equivariant in the sense that $\varphi(\sigma, \tau, \sigma, x) = \sigma(\varphi(\tau, x))$. Indeed, for every lift $\tilde{\sigma} \in \text{Gal}(F(\sqrt[d]{D})|F')$ of a $\sigma \in G$, we have $\tilde{\sigma}(\sqrt[d]{x}) = \tilde{\sigma}(x) = \sigma(x)$ and

$$\varphi(\sigma, \tau, \sigma, x) = \tilde{\sigma}\tilde{\tau}^{-1}(\tilde{\sigma}(\sqrt[d]{x})) = \tilde{\tau}(\sqrt[d]{x}) = \sigma(\varphi(\tau, x))$$

for every $\tau \in \text{Gal}(F(\sqrt[d]{D})|F)$ and every $x \in \tilde{D}$. \hfill \Box

Remark 3.2.3 For some examples where the class in $H^2$ of the extension (3.2.1) can be explicitly computed, see [13]. At least when $F'$ is a local field, $F$ is unramified over $F'$, and $d$ is prime to the residual characteristic, we will see (§7) how to recover this class from the $G$-module $D$.

3.3 Orbits and equivalence

As before, let $F'$ be a field, $F$ a finite galoisian extension of $F'$ of group $G = \text{Gal}(F|F')$, and $d > 0$ an integer such that $\mu_d \subset F^\times$ has order $d$. Although it may very well be that the set of abelian extensions of $F$ of exponent dividing $d$ up to $F'$-isomorphisms is in natural bijection with the set of orbits for the action of $G$ on the set of subgroups of $F^\times/F^\times d$, we prove it only for cyclic extensions because this is the case which has the same flavour as (7.1.2).

**Proposition 3.3.1.** — The set of cyclic extensions of $F$ of degree $d$ up to $F'$-isomorphisms is in natural bijection with the set of orbits for the action of $G$ on the set of cyclic subgroups of $F^\times/F^\times d$ of order $d$.

**Proof.** Suppose first that the order-$d$ cyclic subgroups $D_1, D_2 \subset F^\times/F^\times d$ are in the same $G$-orbit, so that $D_2 = \sigma(D_1)$ for some $\sigma \in G$, and let $L_1 = F(\sqrt[d]{D_1}), L_2 = F(\sqrt[d]{D_2})$. Let $D_1$ be generated by the image of $x \in F^\times$, so that $D_2$ is generated by the image of $\sigma(x)$; we have

$$L_1 = F[T]/(T^d - x), \quad L_2 = F[T]/(T^d - \sigma(x)).$$

Consider the (unique) $F'$-automorphism $\tilde{\sigma}$ of $F[T]$ such that $\tilde{\sigma}(a) = \sigma(a)$ for every $a \in F$ and $\tilde{\sigma}(T) = T$. Composing it with the projection
F[T] → L_1 induces a F'-morphism L_1 → L_2 which is an F'-isomorphism because L_1 and L_2 have the same degree over F'.

Conversely, if L_i = F(√x_i) for some x_i ∈ F^× whose images in F^×/F^×_d have order d, and if we have an F'-isomorphism ˜σ : L_1 → L_2, we have to show that D_2 = σ(D_1) for some σ ∈ G, where D_i ⊂ F^×/F^×_d is the subgroup generated by the image of x_i. Now, ˜σ(F) = F because F is galoisian over F', and hence ˜σ|_F = σ for some σ ∈ G. Also, σ(x_1) has a d-th root in L_2 (namely ˜σ(√x_1)) and its image has order d in F^×/F^×_d, so it generates the same subgroup as the image of x_2. In other words, D_2 = σ(D_1), and we are done.

4.1 The definition of ramified lines

A subgroup D ⊂ K^×/K^×_e is called a ramified line if the restriction of ˜w to D → Z/eZ is an isomorphism; ramified lines are precisely the images of sections of ˜w. Equivalently, they are the subgroups D ⊂ K^×/K^×_e such that (k^×/k^×_e) ∩ D = {1} and (k^×/k^×_e).D = K^×/K^×_e. Still equivalently, every ramified line is generated by the image of a uniformiser of K and conversely.

As the group K^×/K^×_e is commutative, the conjugation action of Z/eZ on k^×/k^×_e resulting from the above exact sequence is trivial, so the number of ramified lines is equal to the order of

H^1(Z/eZ, k^×/k^×_e)_1 = Hom(Z/eZ, k^×/k^×_e) = k^×/k^×_e,
namely \( g = \gcd(q - 1, e) \). The set of ramified lines in \( \mathbb{K}^\times/\mathbb{K}^{x_e} \) is denoted by \( \mathcal{R}_e(K) \).

Every uniformiser \( \pi \) of \( K \) gives a bijection of the set \( \mathcal{R}_e(K) \) of ramified lines in \( \mathbb{K}^\times/\mathbb{K}^{x_e} \) with the group \( \mathbb{K}^\times/\mathbb{K}^{x_e} \) of order \( g = \gcd(q - 1, e) \); to the class \( \bar{u} \in \mathbb{K}^\times/\mathbb{K}^{x_e} \) of \( u \in \mathbb{K}^\times \) corresponds the ramified line generated by the image of \( u\pi \) in \( \mathbb{K}^\times/\mathbb{K}^{x_e} \). Notice that the map \( x \mapsto x^{q-1} \) identifies the group \( \mathbb{K}^\times/\mathbb{K}^{x_e} \) with the kernel \( e \mathbb{K}^\times \) of \( \cdot : \mathbb{K}^\times \to \mathbb{K}^\times \). With this identification, \( \xi \in e \mathbb{K}^\times \) corresponds the ramified line generated by \( u\pi \) for any \( u \in \mathbb{K}^\times \) such that \( u^{q-1} = \xi \).

4.2 The galoisian action on the set of ramified lines

For every \( f > 0 \), let \( K_f \) be the unramified extension of \( K \) of degree \( f \), \( k_f \) its residue field, and \( \mathbb{G}_f = \text{Gal}(K_f|K) = \text{Gal}(k_f|k) \). The group \( \mathbb{G}_f \) acts on the set \( \mathcal{R}_e(K_f) \) of ramified lines in \( \mathbb{K}_f^\times/\mathbb{K}_f^{x_e} \). Indeed, if \( D \) is generated by the image of a uniformiser \( \varpi \) of \( K_f \), then \( \sigma(D) \) is generated by the image of the uniformiser \( \sigma(\varpi) \) and hence \( \sigma(D) \) is a ramified line. Also, \( \text{Card} \mathcal{R}_e(K_f) = g_f \), where \( g_f = \gcd(q^f - 1, e) \).

Every uniformiser \( \pi \) of \( K \) can be viewed as a uniformiser of \( K_f \); for such uniformisers, the bijection \( k_f^\times/k_f^{x_e} \to \mathcal{R}_e(K_f) \) (4.1) is \( \mathbb{G}_f \)-equivariant. We have \( \text{Card} \mathcal{R}_e(K_f)^{\mathbb{G}_f} = g_f \), where \( g_f = \gcd(q^f - 1, e) \).

Let us compute the number of orbits for this action of \( \mathbb{G}_f \) on \( \mathcal{R}_e(K_f) \). For a divisor \( t \) of \( g_f = \gcd(q^f - 1, e) \), let \( \chi_q(t) \) denote the order of \( q \) in the group \( (\mathbb{Z}/t\mathbb{Z})^\times \) of order \( \phi(t) \); we have \( \chi_q(t) | \phi(t) \).

**Proposition 4.2.1.** — The number of orbits for the \( \mathbb{G}_f \)-action on \( \mathcal{R}_e(K_f) \) is \( \sum t | g_f \phi(t)/\chi_q(t) \).

**Proof.** By using the \( \mathbb{G}_f \)-equivariant bijection furnished by a uniformiser of \( K \), we translate the problem into that of computing the number of orbits for the action of \( \mathbb{G}_f \) on \( k_f^\times/k_f^{x_e} \). As the canonical generator of \( \mathbb{G}_f \) acts on the cyclic group \( k_f^\times/k_f^{x_e} \) of order \( g_f \) by the automorphism \( (\cdot)^q \), the result follows from (2.1.1).

4.3 The cohomology class of a stable ramified line, first definition

Denote the canonical generator of \( \mathbb{G}_f \) by \( \sigma \); it acts on \( k_f^\times \) by the automorphism \( (\cdot)^q \). Let \( \pi \) be a uniformiser of \( K \) and, viewing it as a uniformiser of \( K_f \), let \( D \subset \mathbb{K}_f^\times/\mathbb{K}_f^{x_e} \) be the ramified line generated by the image of \( \xi \pi \) for some \( \xi \in k_f^\times \). If \( D \) is \( \mathbb{G}_f \)-stable, which amounts to \( \sigma(D) = D \), then \( (\xi^q \pi)(\xi \pi)^{-1} \in k_f^{x_e} \) or equivalently \( \xi^{q-1} = \bar{1} \) in \( k_f^\times/k_f^{x_e} \).
If we replace $\pi$ by some other uniformiser $\pi' = u\pi$ of $K$ with $u \in k^\times$, then $\xi$ gets replaced by $\xi' = \bar{\xi}u$. But, as the norm map $N_f : k_f^\times \to k^\times$ is surjective, so $u = a^{1+q+\cdots+q^{f-1}}$ for some $a \in k_f^\times$, and hence $[\xi] = [\xi']$ in $H^2(G_f, k_f^\times/k_f^{\times e})_q$. It follows that the map $\mathcal{R}e(K_f)^{G_f} \to H^2(G_f, k_f^\times/k_f^{\times e})_q$ from the set of $G_f$-stable ramified lines does not depend on the choice of the uniformiser $\pi$ of $K$ used in its definition.

It is clear that this map is surjective: the class $[\xi] \in H^2(G_f, k_f^\times/k_f^{\times e})_q$ (with $\xi \in k_f^\times$ such that $\xi^{q-1} \in k_f^{\times e}$) is the class of the $G_f$-stable ramified line $D \in \mathcal{R}e(K_f)^{G_f}$ generated by (the image of) the uniformiser $\xi\pi$ of $K_f$, where $\pi$ is any uniformiser of $K$.

### 4.4 The cohomology class of a stable ramified line, second definition

This definition is inspired by [7, 6.1] and assigns a class in $H^2(G_f, e k_f^\times)_q$ to every $G_f$-stable ramified line $D \subset K_f^\times/K_f^{\times e}$. If $D$ is generated by (the image of) $\xi\pi$ as before, then $\xi^{q-1} = \alpha e$ for some $\alpha \in k_f^\times$, as we have seen; put $\zeta = N_f(\alpha)$. We have seen (2.2) that $\zeta$ defines a class in $H^2(G_f, e k_f^\times)_q$ which does not depend on the choice of $\alpha$. Moreover, if we replace $\pi$ by some other uniformiser $\pi' = u\pi$ ($u \in k^\times$) of $K$, then $\xi$ gets replaced by $\xi' = \bar{\xi}u^{-1}$, and then $\xi'^{q-1} = \xi^{q-1}(u^{-1})^{q-1} = \alpha e$, so we may use the same $\alpha$ for $\pi'$ as for $\pi$. In other words, the class $[\zeta]$ depends only on the $G_f$-stable ramified line $D$ generated by $\xi\pi$, not the choice of the uniformiser $\pi$ of $K$ using which we attached $\xi$ to $D$. We thus get a similar map $\mathcal{R}e(K_f)^{G_f} \to H^2(G_f, e k_f)_q$.

### 4.5 The compatibility of the two definitions

Observe that the two groups $k_f^\times/k_f^{\times e}$, $e k_f^\times$ are cyclic of the same order $g_f = \gcd(q^f - 1, e)$ and they are canonically isomorphic to each other under the $G_f$-equivariant map $\bar{\xi} \mapsto \xi^{(q^f-1)/g_f}$. This gives an isomorphism $H^2(G_f, k_f^\times/k_f^{\times e})_q \to H^2(G_f, e k_f)_q$; let us show that it is compatible with the two maps from $\mathcal{R}e(K_f)^{G_f}$, at least when $e \mid q^f - 1$, in which case $g_f = e$.

**Proposition 4.5.1.** When $e \mid q^f - 1$, the two definitions of the cohomology class of a $G_f$-stable ramified line $D \in \mathcal{R}e(K_f)^{G_f}$ are compatible with the isomorphism $k_f^\times/k_f^{\times e} \to e k_f^\times$ of $G_f$-modules.

**Proof.** This follows from the preceding constructions and prop. 2.3.1. □

### 4.6 The restriction map
Let $f' > 0$ be a multiple of $f$. By our notational convention, $K_{f'}$ is the degree-$f'$ unramified extension of $K$ (of group $G_f = \text{Gal}(K_{f'}|K)$ and residue field $k_{f'}$), so it is unramified of degree $f'/f$ over $K_f$. If $D \in R_e(K_f)$ is a ramified line, generated by the image of some uniformiser $\varpi$ of $K_f$, then its image in $K_{f'}^\times/K_{f'}^{x_e}$ is also generated by the image of $\varpi$, which continues to be a uniformiser of $K_{f'}$. So we have a natural map $R_e(K_f) \to R_e(K_{f'})$.

Under this map, the image of a $G_f$-stable ramified line is $G_{f'}$-stable. Indeed, $\sigma'(\varpi) = \sigma(\varpi)$ for every $\sigma' \in G_{f'}$ (with image $\sigma \in G_f$) and every uniformiser $\varpi$ of $K_f$. So we have a natural map $R_e(K_f)^{G_f} \to R_e(K_{f'})^{G_{f'}}$, restriction of the preceding one.

Also, the inclusion $k_f^\times \to k_{f'}^\times$ is a morphism of $G_{f'}$-modules, as is the induced map on the quotients $k_f^\times/k_{f}^{x_e} \to k_{f'}^\times/k_{f'}^{x_e}$, and hence the (lower horizontal) restriction map (2.4.3) in the diagram

$$
\begin{array}{c}
R_e(K_f)^{G_f} \longrightarrow R_e(K_{f'})^{G_{f'}} \\
\downarrow \quad \downarrow \\
H^2(G_f, k_f^\times/k_{f}^{x_e})_q \longrightarrow H^2(G_{f'}, k_{f'}^\times/k_{f'}^{x_e})_q.
\end{array}
$$

**Proposition 4.6.2.** — At least when $e \mid q^f - 1$, the diagram (4.6.1) is commutative.

**Proof.** Write $f' = cf$. We have seen that when we choose a uniformiser $\pi$ of $K$, the set $R_e(K_f)$ gets indentified with the group $k_f^\times/k_f^{x_e}$ and the subset $R_e(K_f)^{G_f}$ with the subgroup $q^{-1}(k_f^\times/k_f^{x_e})$ — the kernel of $(\ )^{q-1}$. The same holds for at the level of $K_{cf}$ in place of $K_f$.

When we choose a generator $\omega_c$ of $k_{cf}^\times$, the the map $k_{f}^\times/k_{f}^{x_e} \to k_{cf}^\times/k_{cf}^{x_e}$ of $G_{f'}$-modules can be identified (2.4.2) with $c : \mathbb{Z}/c\mathbb{Z} \to \mathbb{Z}/e\mathbb{Z}$. With these identifications, the result follows from prop. 1.7.2.

5 Totally tamely ramified extensions.

Let us first study the set $T_{e,1}(K)$ of (K-isomorphism classes of) totally ramified extensions of $K$ of degree $e$ (prime to $p$).

5.1 The parametrisation of $T_{e,1}(K)$
Proposition 5.1.1. — The set $\mathcal{T}_{e,1}(K)$ of totally ramified extensions of $K$ of degree $e$ is in canonical bijection with the set $\mathcal{R}_e(K)$ of ramified lines in $K^\times/K^{\times e}$. In particular, the cardinality of $\mathcal{T}_{e,1}(K)$ is $g = \gcd(q - 1, e)$.

Proof. For every uniformiser $\pi$ of $K$, the polynomial $T^e - \pi$ is irreducible (Eisenstein’s criterion) and the extension $F(\sqrt{\pi})$ is totally ramified of degree $e$. Conversely, let $L|K$ be a totally ramified extension of degree $e$ (so that the residue field of $L$ is $k$), let $\pi$ be a uniformiser of $K$, and write $\pi = u\xi\varpi^e$, where $u$ (resp. $\varpi$) is a 1-unit (resp. uniformiser) in $L$, and $\xi \in k^\times$. Since the group of 1-units of $L$ is a $\mathbb{Z}_p$-module and $e \in \mathbb{Z}_p^\times$, there is a (unique) 1-unit $v$ of $L$ such that $u = v^e$, so the uniformiser $\xi^{-1}\pi$ of $K$ has the $e$-th root $v\varpi$ in $L$ and therefore $L = K(\sqrt[1/e]{\xi^{-1}\pi})$.

For any two uniformisers $\pi_1, \pi_2$ of $K$, the extensions $K(\sqrt[1/e]{\pi_1}), K(\sqrt[1/e]{\pi_2})$ are $K$-isomorphic if and only if the unit $\pi_1/\pi_2 \in \mathfrak{o}^\times$ is in $\mathfrak{o}^{\times e}$. In other words, the two extensions are isomorphic if and only if the uniformisers $\pi_1$ and $\pi_2$ generate the same ramified line in $K^\times/K^{\times e}$. This completes the proof. \[\square\]

Remark 5.1.2 We are accustomed to the idea that the roots of an irreducible polynomial $\varphi \in F[T]$ ($F$ being a field) are indistinguishable from each other because the group $\text{Gal}(F_\varphi|F)$ ($F_\varphi$ being the splitting field of $\varphi$) permutes them transitively. Somewhat similarly, totally ramified extensions of $K$ of given degree $e$ are indistinguishable from each other because their parameters (by prop. 5.1.1, the ramified lines in $K^\times/K^{\times e}$ or equivalently the sections of $\tilde{w}: K^\times/K^{\times e} \to \mathbb{Z}/e\mathbb{Z}$) are permuted (simply) transitively by the group $H^1(\mathbb{Z}/e\mathbb{Z}, k^\times/k^{\times e})_1$.

Remark 5.1.3 When we fix a uniformiser $\pi$ of $K$, ramified lines in $K^\times/K^{\times e}$ (and hence totally ramified extensions of $K$ of degree $e$) are parametrised by the group $k^\times/k^{\times e}$ of order $g = \gcd(q - 1, e)$. The map $x \mapsto x^{\frac{1}{e\varphi}}$ identifies this group with the kernel $e\mathbb{k}\mathcal{X}$ of $\mathbb{k}\mathcal{X} \to \mathbb{k}\mathcal{X}$. Under this parametrisation (dependant upon the choice of $\pi$), the totally ramified degree-$e$ extension of $K$ corresponding to $\zeta \in e\mathbb{k}\mathcal{X}$ is $K(\sqrt[e]{\xi^e}\pi)$ for any $\xi \in k^\times$ such that $\xi^{\frac{1}{e\varphi}} = \zeta$.

Proposition 5.1.4. — For every $L \in \mathcal{T}_{e,1}(K)$, the group $\text{Aut}_K(L)$ is canonically isomorphic to $e\mathbb{k}\mathcal{X}$ and hence cyclic of order $g = \gcd(q - 1, e)$.

Proof. Indeed, $L = K(\sqrt[1/e]{\pi})$ for some uniformiser $\pi$ of $K$, and the $K$-conjugates of $\sqrt[1/e]{\pi}$ in $L$ are precisely $\xi\sqrt[1/e]{\pi}$, where $\xi$ is an $e$-th root of 1 in $K$. The map $\sigma \mapsto \sigma(\sqrt[1/e]{\pi})/\sqrt[1/e]{\pi}$ is thus an isomorphism $\text{Aut}_K(L) \to e\mathbb{k}\mathcal{X}$.

This isomorphism is independent of the choice of $\pi$. Indeed, every other uniformiser $\pi'$ of $K$ such that $L = K(\sqrt[1/e]{\pi'})$ is of the form $\pi' = \varepsilon\pi$ for some...
$\varepsilon \in k^\times$ (ignoring 1-units of $K$, which we can). We may thus take $\varepsilon \sqrt{\pi}$ for $\sqrt{\pi}$, and we have
\[
\frac{\sigma(\sqrt{\pi})}{\sqrt{\pi'}} = \frac{\sigma(\varepsilon \sqrt{\pi})}{\varepsilon \sqrt{\pi'}} = \frac{\varepsilon \sigma(\sqrt{\pi})}{\varepsilon \sqrt{\pi}} = \frac{\sigma(\sqrt{\pi})}{\sqrt{\pi}}
\]
for every $\sigma \in \text{Aut}_K(L)$, which was to be proved.

**Corollary 5.1.5.** — Some $L \in T_{e,1}(K)$ is galoisian over $K$ if and only if $e \mid q - 1$. If so, then every $L \in T_{e,1}(K)$ is galoisian (and indeed cyclic) over $K$.

**Proof.** A finite separable extension $L$ of $K$ is galoisian over $K$ if and only if $\text{Aut}_K(L)$ has order $[L : K]$. For an $L \in T_{e,1}(K)$, this happens precisely when $\gcd(q - 1, e) = e$ (prop. 5.1.4), or equivalently $e \mid q - 1$. \hfill \qed

### 5.2 Serre’s mass formula in tame degrees

For the next corollary, we need to recall the statement of Serre’s mass formula [12]. Let $n > 0$ be any integer and denote by $T_{n,1}(K)$ the set of $K$-isomorphism classes of finite (separable) totally ramified extensions of $K$ of ramification index $n$. For every $L \in T_{n,1}(K)$, put $c_K(L) = w(\delta_{L|K}) - (n - 1)$, where $\delta_{L|K}$ denotes the discriminant of $L|K$. The mass formula asserts that
\[
(5.2.1) \quad \sum_{L \in T_{n,1}(K)} \frac{1}{|\text{Aut}_K(L)|} q^{-c_K(L)} = n.
\]
where $|\text{Aut}_K(L)|$ is the order of the group of $K$-automorphisms of $L$.

**Corollary 5.2.2.** — Serre’s mass formula (5.2.1) holds over $K$ in every tame degree $e$ (prime to $p$).

**Proof.** Indeed, for every $L \in T_{e,1}(K)$, we have $c_K(L) = 0$, $|\text{Aut}_K(L)| = g$ (5.1.4) and there are $g$ such $L$ (5.1.1), where $g = \gcd(q - 1, e)$. \hfill \qed

In fact we can do slightly better if we use the results of [3] where a new proof of Serre’s mass formula in degree $p$ was given. Let $\bar{K}$ be a separable algebraic closure of $K$, and let $E \subset \bar{K}$ run through totally ramified extensions of degree $n$ over $K$, which we express by $[E] \in T_{n,1}(K)$. Serre [12] shows that (5.2.1) is equivalent to
\[
(5.2.3) \quad \sum_{E \subset \bar{K}, [E] \in T_{n,1}(K)} q^{-c_K(E)} = n.
\]
Proposition 5.2.4. — Serre’s mass formula (5.2.3) holds over \( K \) in degree \( n = ep \) (with \( e \) prime to \( p \)).

Proof. Let \( E \subset \tilde{K} \) be a totally ramified extension of degree \( ep \) over \( K \), and let \( L \) be the maximal tamely ramified extension of \( K \) in \( E \); we have \( [L : K] = e \). By the formula for the transitivity of the discriminant, we have

\[
w(\delta_{E|K}) = (e - 1)p + w_L(\delta_{E|L})
\]

where \( w \) (resp. \( w_L \)) is the normalised valuation of \( K \) (resp. \( L \)). It follows that \( c_K(E) = c_L(E) \). Next, notice that there are precisely \( e \) totally ramified extensions of \( K \) in \( \tilde{K} \) of degree \( e \) over \( K \), since there are \( g = \gcd(q - 1, e) \) isomorphism classes in \( T_{e,1}(K) \) (5.1.1), and each class \([L]\) is represented by \( e/g \) extensions \( L \subset \tilde{K} \), because \( g = |\text{Aut}_K(L)| \) (5.1.4). Now, by decomposing the sum \( \sum_{[E:K]=ep} (5.2.3) \) as \( \sum_{[L:K]=e} \sum_{[E:L]=p} \), we have

\[
\sum_{[E:K]=ep} q^{-c_K(E)} = \sum_{[L:K]=e} \sum_{[E:L]=p} q^{-c_L(E)} = \sum_{[L:K]=e} \sum_{[E:L]=p} q^{-c_L(E)}.
\]

But \( \sum_{[E:L]=p} q^{-c_L(E)} = p \) by [3, th. 35], and hence \( \sum_{[E:K]=ep} q^{-c_K(E)} = ep \), as was to be proved.

Remark 5.2.5 The same dévissage reduces the proof of (5.2.3) for arbitrary \( n \) to the case \( n = p^r \). Note that a proof of (5.2.2) for \( e \) prime (\( \neq p \)) can also be found in [3] (§8).

6 The orthogonality relation

Let us make some remarks about the special case \( e \mid q - 1 \). More precisely, suppose that the (cyclic) group \( \mu_e \subset K^\times \) of \( e \)-th roots of 1 has order \( e \), and let \( M = K(\sqrt[e]{K^\times}) \) be the maximal abelian extension of \( K \) of exponent dividing \( e \). We have the perfect pairing (3.1.1)

\[
\text{Gal}(M|K) \times (K^\times/K^{\times e}) \longrightarrow \mu_e
\]

of free rank-2 \((\mathbb{Z}/e\mathbb{Z})\)-modules, defined by \((\sigma, \bar{x}) = \sigma(y)/y\) for any \( y \in M^\times \) such that \( y^e = x \). It is easy to determine the orthogonal complement of the inertia subgroup \( \Gamma_0 \subset \text{Gal}(M|K) \):

Proposition 6.0.1. — The orthogonal complement of the inertia subgroup \( \Gamma_0 \) of \( \text{Gal}(M|K) \) is the subgroup \( k^\times/k^{\times e} \) of \( K^\times/K^{\times e} \) (and conversely).

Proof. Indeed, the fixed field \( M^{\Gamma_0} \) of the inertia subgroup is the maximal unramified extension \( M_0 \) of \( K \) in \( M \). It is easy to see that, \( \omega \) being a
generator of \(k^\times\), the extension \(K(\sqrt[w]{\omega})\) of \(K\) in \(M\) is unramified and of degree \(e\) over \(K\). At the same time, the ramification index of \(M|K\) is at least \(e\), as it contains \(K(\sqrt[\pi]{\omega})\) for any uniformiser \(\pi\) of \(K\). As \([M:K] = e^2\), we must have \(M_0 = K(\sqrt[k\times]{\omega})\), which was to be proved. 

**Proposition 6.0.2.** — For every subgroup \(D \subset K^\times/K^{\times e}\), the maximal unramified extension of \(K\) in \(K(\sqrt[\sqrt{D}]{}D)\) is \(K(\sqrt[\sqrt{D_0}]{}D_0)\), with \(D_0 = D \cap (k^\times/k^{\times e})\).

**Proof.** Let \(L = K(\sqrt[\sqrt{D}]{}D)\), and let \(L_0\) be the maximal unramified extension of \(K\) in \(L\); it is clear that \(K(\sqrt[\sqrt{D_0}]{}D_0) \subset L_0\). Conversely, if \(C \subset k^\times/k^{\times e}\) is the subgroup such that \(L_0 = K(\sqrt[\sqrt{C}]{}C)\), then \(C \subset D\) and hence \(C \subset D_0\). It follows that \(C = D_0\).

**Remark 6.0.3** As a corollary, \(L = K(\sqrt[\sqrt{D}]{}D)\) is totally ramified over \(K\) if and only if \(D \cap (k^\times/k^{\times e}) = \{1\}\).

**Remark 6.0.4** The analogue of prop. 6.0.1 in degree \(p\) (where \(q = p^{f_0}\)) can be found in [2] (§1) in characteristic 0 and in [2] (§5) in characteristic \(p\).

### 7 The parametrisation of \(T_{e,f}(K)\)

Recall that \(T_{e,f}(K)\) is defined as the set of \(K\)-isomorphism classes of finite separable extensions of \(K\) of ramification index \(e\) and residual degree \(f\). We will see that it can be identified with the set of orbits for the action of \(G_f = \text{Gal}(K_f|K)\) on the set \(R_e(K_f)\) of ramified lines in \(K_f^\times/K_f^{\times e}\).

There is a canonical surjection \(T_{e,1}(K_f) \to T_{e,f}(K_f)\), and a canonical bijection \(T_{e,1}(K_f) \to R_e(K_f)\) (prop. 5.1.1, applied to \(K_f\)), so the question is: When are the extensions defined by two distinct ramified lines in \(K_f^\times/K_f^{\times e}\) isomorphic as extensions of \(K\) (although they are not \(K_f\)-isomorphic)?

#### 7.1 The parametrisation of \(T_{e,f}(K)\)

Recall that the set \(R_e(K_f)\) carries a natural action of the group \(G_f\) (4.2). It is the orbit space for this action of \(G_f\) on \(R_e(K_f)\) which parametrises \(T_{e,f}(K)\):

**Proposition 7.1.1.** — The extensions \(L, L'\) corresponding to two ramified lines \(D, D' \subset K_f^\times/K_f^{\times e}\) are \(K\)-isomorphic if and only if \(D' = \sigma(D)\) for some \(\sigma \in G_f\).

**Proof.** The proof is similar to that of (3.3.1), although there the extensions \(L, L'\) were kummerian whereas here they need not even be galoisian (over \(K_f\)). Suppose first that \(D' = \sigma(D)\), and let \(\varpi\) be a
uniformiser of $K_f$ whose image generates $D$, so that the image of $\sigma(\varpi)$ generates $D'$, and

$$L = K_f[T]/(T^e - \varpi), \quad L' = K_f[T]/(T^e - \sigma(\varpi)).$$

Consider the (unique) $K$-automorphism $\tilde{\sigma}$ of $K_f[T]$ such that $\tilde{\sigma}(a) = \sigma(a)$ for every $a \in K_f$ and $\tilde{\sigma}(T) = T$. Composing it with the projection $K_f[T] \to L'$ induces a $K$-morphism $L \to L'$ which is a $K$-isomorphism. Conversely, if $L = K_f(\sqrt[1]{e}\varpi)$ for some uniformiser $\varpi$ of $K_f$, and if we have a $K$-isomorphism $\tilde{\sigma}: L \to L'$, then its restriction to the maximal unramified extensions of $K$ in $L$ and $L'$ is a $K$-automorphism $\sigma: K_f \to K_f$, and the uniformiser $\sigma(\varpi)$ of $K_f$ has the $e$-th root $\tilde{\sigma}(\sqrt[1]{e}\varpi)$ in $L'$, so $L' = K_f(\sqrt[1]{e}\sigma(\varpi))$. In other words, $D' = \sigma(D)$. □

**Corollary 7.1.2.** — The set $\mathcal{T}_{e,f}(K)$ is in natural bijection with the set of orbits $\mathcal{R}_e(K_f)/G_f$ for the action of $G_f$ on $\mathcal{R}_e(K_f)$. □

**Corollary 7.1.3.** — An extension $L \in \mathcal{T}_{e,1}(K_f)$ is galoisian over $K$ if and only if the corresponding orbit consists of a single ($G_f$-stable) $D \in \mathcal{R}_e(K_f)$ and $e \mid q^f - 1$.

**Proof.** Indeed, for $L$ to be galoisian over $K$ it must be galoisian over $K_f$, which is equivalent to $e \mid q^f - 1$, and further all its $K$-conjugates must coincide, which is equivalent to $D$ being $G_f$-stable (3.2.2). □

### 7.2 The presentation of the group

Suppose that $e \mid q^f - 1$ and let $D \in \mathcal{R}_e(K_f)^{G_f}$, so that the extension $L = K_f(\sqrt[1]{e}D)$ is in $\mathcal{T}_{e,f}(K)$ and galoisian over $K$ (7.1.3). The inertia subgroup $\Gamma_0 = \text{Gal}(L|K_f)$ of $\Gamma = \text{Gal}(L|K)$ is canonically isomorphic to $\text{Hom}(D, \mu_e) = \mu_e$, and the identification $\Gamma_0 = \mu_e$ is $G_f$-equivariant (3.2.2). We thus have an extension

$$(7.2.1) \quad 1 \to \mu_e \to \Gamma \to G_f \to 1$$

and we would like to compute its class in $H^2(G_f, \mu_e)_q$ in terms of the parameter $D$ of $L$. Recall ($\S 4$) that we’ve assigned a class $[D]$ to $D$ in $H^2(G_f, e k_f^\times)_q$, and notice that $\mu_e = e k_f^\times$.

**Proposition 7.2.2.** — The class of the extension (7.2.1) is the same as the class $[D] \in H^2(G_f, e k_f^\times)_q$ of $D$.

**Proof.** We will actually compute a presentation of the group $\Gamma$ (as in [7]) and observe that it is the extension corresponding to the class of $D$ as defined in (4.4).
Let \( \pi \) be a uniformiser of \( K \) and suppose that the \( G_f \)-stable ramified line \( D \) is generated by (the image of) \( \xi \pi \) for some \( \xi \in k_f^\times \) (such that \( \xi^{q-1} = \alpha^e \) for some \( \alpha \in k_f^\times \)), so that \( L = K_f(\sqrt[\varphi](\xi \pi)) \).

Choose a generator \( \tau \) of \( \Gamma_0 \), so that \( \tau(\sqrt[\varphi](\xi \pi)) = \zeta \sqrt[\varphi](\xi \pi) \) for a certain (generator) \( \zeta \in \mu_e \). Notice that \( N_f(\xi)^{q-1} = 1 \), so \( N_f(\alpha)^e = 1 \), and hence \( N_f(\alpha) = \zeta^s \) for some \( s \) (mod. \( e \)). As \( N_f(\alpha) \in k^\times \), we must have \( (q-1)s \equiv 0 \) (mod. \( e \)).

Also choose a lift \( \tilde{\sigma} \in \Gamma \) of the canonical generator \( \sigma \in G_f \) (which acts on \( k_f^\times \) as ( )\( ^{q} \)). Now,

\[
\tilde{\sigma}(\sqrt[\varphi](\xi \pi)^e = \tilde{\sigma}(\xi \pi) = \xi^{q-1} \cdot \xi \pi = (\alpha \sqrt[\varphi](\xi \pi))^e,
\]

so that \( \tilde{\sigma}(\sqrt[\varphi](\xi \pi)) = \zeta^j \alpha \sqrt[\varphi](\xi \pi) \) for some \( j \) (mod. \( e \)). Replacing \( \tilde{\sigma} \) by \( \tau^{-j} \tilde{\sigma} \), we may assume that \( \tilde{\sigma}(\sqrt[\varphi](\xi \pi)) = \alpha \sqrt[\varphi](\xi \pi) \). We then have \( \tilde{\sigma}^2(\sqrt[\varphi](\xi \pi)) = \tilde{\sigma}(\alpha \sqrt[\varphi](\xi \pi)) \) and so on, hence

\[
\tilde{\sigma}^f(\sqrt[\varphi](\xi \pi)) = N_f(\alpha) \sqrt[\varphi](\xi \pi) = \zeta^s \sqrt[\varphi](\xi \pi) = \tau^s(\sqrt[\varphi](\xi \pi)).
\]

It follows that \( \tilde{\sigma}^f = \tau^s \). Finally,

\[
\tau^q \tilde{\sigma}(\sqrt[\varphi](\xi \pi)) = \tau^q(\alpha \sqrt[\varphi](\xi \pi)) = \zeta^q \alpha \sqrt[\varphi](\xi \pi) = \tilde{\sigma}(\alpha \sqrt[\varphi](\xi \pi)) = \tilde{\sigma}(\sqrt[\varphi](\xi \pi)),
\]

and hence \( \tilde{\sigma} \tau \tilde{\sigma}^{-1} = \tau^q \). We have found that the group \( \Gamma \) (of order \( ef \)) is generated by \( \langle \tau, \tilde{\sigma} \rangle \), and the relations

\[
\tau^e = 1, \quad \tilde{\sigma}^f = \tau^s, \quad \tilde{\sigma} \tau \tilde{\sigma}^{-1} = \tau^q
\]

hold. But we have seen that the group (1.5.1) with this presentation has \( ef \) elements, so we have indeed found a presentation for \( \Gamma \). This shows that the class of \( D \) is the same as the class of the extension (7.2.1).

\[\square\]

Remark 7.2.3 Notice that the group \( \Gamma \) is commutative if and only if \( \tau^q = \tau \) or in other words \( q \equiv 1 \) (mod. \( e \)) or still \( e \mid (q - 1) \). Prop. 1.6.4 says that \( \Gamma \) is cyclic if and only if moreover \( s \) is prime to \( \gcd(e, f) \).

Remark 7.2.4 We have seen that the set \( T_{e,f}(K) \) of K-isomorphism classes of finite separable extensions of \( K \) of ramification index \( e \) and residual degree \( f \) has the cardinality \( \sum_{t \mid g_f} \phi(t)/\chi_q(t) \), in the notation of (4.2.1), where \( g_f = \gcd(q^f - 1, e) \). If \( e \mid (q^f - 1) \), precisely \( g = \gcd(q - 1, e) \) of these are galoisian over \( K \). If \( e \mid (q - 1) \), all of them are abelian over \( K \). These are the only galoisian or abelian cases.
Remark 7.2.5 It follows that the maximal abelian tamely ramified extension of $K$ is $K_\infty^{(\sqrt[q-1]{\pi})}$, where $K_\infty$ is the maximal unramified extension of $K$ and $\pi$ is any fixed uniformiser of $K$.

Remark 7.2.6 More generally, the maximal tamely ramified extension of $K$ is $M = K_\infty^{(\sqrt[m]{\pi})}$, where $K_\infty$ is the maximal unramified extension of $K$, $\pi$ is any fixed uniformiser of $K$, and $m$ runs through all integers prime to $p$. The group $\text{Gal}(M|K)$ admits the presentation $\langle \tau, \tilde{\sigma} | \tilde{\sigma}\tau\tilde{\sigma}^{-1} = \tau^{q} \rangle$, and one can explicitly give the action of $\tau$ and $\tilde{\sigma}$ on $M$. See for example [9, p. 463] in characteristic 0 (but the same proof works in characteristic $p$, as we have seen).

7.3 The invariants of an orbit

We have seen (7.1.2) that orbits for the action of $G_f$ on the set $\mathcal{R}_e(K_f)$ of ramified lines in $K_f^x/K_f^{xe}$ correspond bijectively to extensions $L \in \mathcal{T}_{e,f}(K)$ of $K$ of ramification index $e$ and residual degree $f$. We are now going to review a certain number of invariants of the $G_f$-orbit which recover the invariants of $L$ such as the galoisian closure $\hat{L}$ of $L$ over $K$, or the smallest extension $\tilde{L}$ of $\hat{L}$ for which the exact sequence $1 \to \Gamma_0 \to \Gamma \to \Gamma/\Gamma_0 \to 1$ splits, where $\Gamma = \text{Gal}(\hat{L}|K)$ and $\Gamma_0$ is the inertia subgroup. These invariants are going to be attached to the orbit by choosing a representative $D \in \mathcal{R}_e(K_f)$, and sometimes also a uniformiser $\pi$ for $K$. It can be easily seen that these choices are immaterial.

As $\mathcal{T}_{e,f}(K)$ contains no extensions galoisian over $K$ unless $e | q^f - 1$, let us make this hypothesis. Then $L \in \mathcal{T}_{e,f}(K)$ is galoisian over $K$ if and only if the corresponding $G_f$-orbit consists of a single ramified line $D$ (7.1.3). In general, if $D$ is a representative of the $G_f$-orbit corresponding to $L$ (galoisian or not), and if $\xi \in k_f^x$ is such that $D$ is generated by $\xi \pi$ (so that $L = K_f^{(\sqrt[\xi]{\pi})}$), then the order $d$ of $\xi^{q-1}$ in $k_f^x/k_f^{xe}$ depends only on $L$, not on the choices of $D$ and $\pi$, and the galoisian closure of $L$ over $K$ is $\hat{L} = K_{df}^{(\sqrt[\xi]{\pi})}$ (2.4.1).

Indeed, if we replace $\pi$ by $\pi' = u\pi$ for some $u \in k^x$ and $D$ by $\sigma(D)$ for some $\sigma \in G_f$, then $\xi$ gets replaced by $\sigma(\xi u^{-1})$. But then $\xi^{q-1}$ and $\sigma(\xi u^{-1})^{-1}$ have the same order because $\sigma$ is an automorphism of $k_f^x/k_f^{xe}$ and $u^{q^{-1}} = 1$.

Now suppose that $L \in \mathcal{T}_{e,f}(K)$ is galoisian over $K$ (and in particular $e | q^f - 1$). Then the class in $H^2(G_f, \mu_e)_q$ of the extension (7.2.1)

$$1 \to \mu_e \to \text{Gal}(L|K) \to G_f \to 1$$

is the same as the class of the corresponding $G_f$-stable ramified line $D$ (4.5.1), (7.2.2). If $\hat{c}$ is the order of this class, then the compositum $LK_{\hat{c}f}$
is the smallest extension \( \hat{L} \) of \( L \) which is split over \( K \) in the sense that the short exact sequence \( 1 \rightarrow \mu_e \rightarrow \text{Gal}(\hat{L}|K) \rightarrow \hat{G}_f \rightarrow 1 \) splits (2.4.4).

### 7.4 Examples

Recall the notation in force throughout the paper: \( K \) is a local field with finite residue field \( k \) of cardinality \( q \). \( K_f \) is the degree-\( f \) unramified extension of \( K \) with residue field \( k_f \), and \( e > 0 \) is an integer prime to \( q \). The group \( \text{Gal}(K_f|K) = \text{Gal}(k_f|k) \) is denoted \( G_f \). The normalised valuation of \( K \) (resp. \( K_f \)) is \( w \) (resp. \( w_f \)). We denote by \( \pi \) a uniformiser of \( K \), so that \( w_f(\pi) = 1 \) for every \( f \).

**Example 7.4.1** Take \( q = 2 \) so that \( K \) is either a totally ramified (finite) extension of \( \mathbb{Q}_2 \) or \( K = \mathbb{F}_2(\sqrt[3]{\pi}) \). For every odd \( e > 0 \) (and \( f = 1 \)), the valuation \( w \) provides an isomorphism \( \overline{w}: K^\times/K_2^\times \rightarrow \mathbb{Z}/e\mathbb{Z} \), so there is only one ramified line (namely the whole of \( K^\times/K_f^\times \)) and hence \( K \) has a unique totally ramified extension of degree \( e \) (up to \( K \)-isomorphism), namely \( K(\sqrt[3]{\pi}) \). Its galoisian closure is \( K_r(\sqrt[3]{\pi}) \), where \( r \) is the order of 2 in \( (\mathbb{Z}/e\mathbb{Z})^\times \), and the extension \( \text{Gal}(K_r(\sqrt[3]{\pi})|K) \) of \( G_r \) by the inertia subgroup \( \text{Gal}(K_r(\sqrt[3]{\pi})|K_r) = \mu_e \) (7.2.1) splits. For \( e = 3 \), it is the extension \( \mathfrak{S}_3 \) of \( G_2 = \mathbb{Z}^\times \) by \( \mu_3 = \mathfrak{A}_3 \).

**Example 7.4.2** Keep \( q = 2 \) and take \( e = 3 \), \( f = 2 \), so that \( k_f^\times \) is (cyclic) of order \( 2^2 - 1 = 3 \) and so is \( k_f^\times/k_2^\times \). There are therefore three ramified lines in \( k_f^\times/K_2^\times \), only one which (the one generated by any uniformiser \( \pi \) of \( K \)), is \( G_2 \)-stable while the other two ramified lines are in the same \( G_2 \)-orbit. So \( K \) has precisely two extensions (up to \( K \)-isomorphism) of ramification index 3 and residual degree 2, only one of which, namely \( L = K_2(\sqrt[3]{\pi}) \), is galoisian over \( K \); it is also split over \( K \) in the sense that the short exact sequence of groups

\[
1 \rightarrow \text{Gal}(L|K_2) \rightarrow \text{Gal}(L|K) \rightarrow \text{Gal}(K_2|K) \rightarrow 1
\]

admits a section; it is the same as the \( \mathfrak{S}_3 \)-extension of \( K \) of the previous example. The galoisian closure of the other extension of \( K \) of ramification index 3 and residual degree 2, namely \( K_2(\sqrt[3]{\omega\pi}) \), where \( \omega \) is a generator of \( k_2^\times \), is \( K_{2c}(\sqrt[3]{\omega\pi}) \) where \( c = 3 \) is the order of \( \omega \) in \( k_2^\times/k_2^\times \). The extension \( \text{Gal}(K_6(\sqrt[3]{\omega\pi})|K) \) of \( G_6 \) by \( \mu_3 \) (7.2.1) is split, and indeed \( K_6(\sqrt[3]{\omega\pi}) = K_6(\sqrt[3]{\pi}) \) because \( \omega \in k_6^3 \) (and indeed \( k_2^\times \subset k_6^3 \)). The special case \( K = \mathbb{Q}_2, \pi = 2 \) is treated in [6, Beispiel 3.1].

**Example 7.4.3** Take \( q \) to be odd, and take \( e = 2 \). For every \( f > 0 \), the group \( k_f^\times \) is (cyclic) of even order \( q^f - 1 \), so \( k_f^\times/k_f^\times \) has order 2. Therefore there are two ramified lines in \( K_f^\times/K_f^\times \). They are both \( G_f \)-stable, so both
the extensions $K_f(\sqrt[
u]{\pi})$ and $K_f(\sqrt[\pi]{\omega})$, where $\omega$ is a generator of $k_f^\times$, are galoisian over $K$, and these two are the only extensions of $K$ of ramification index 2 and residual degree $f$.

The short exact sequence (7.2.1) corresponding to the first one is clearly split. If $f$ is odd, so is the one corresponding to $K_f(\sqrt[\pi]{\omega})|K$ because the group $H^2(G_f, k_f^\times/k_f^{\times 2})$ is then trivial. The splitting also follows from the fact that the map $k^\times/k^{\times e} \to k_f^\times/k_f^{\times e}$ is an isomorphism when $f$ is odd, or the fact that any extension of finite groups of mutually prime orders splits. If $f$ is even, the order-2 group $H^2(G_f, k_f^\times/k_f^{\times 2})$ is generated by the image of $\omega$, so the extension $K_f(\sqrt[\pi]{\omega})$ does not split over $K$ (and hence it is cyclic over $K$) but $K_{2f}(\sqrt[\pi]{\omega})$ does split. Indeed, $K_{2f}(\sqrt[\pi]{\omega}) = K_{2f}(\sqrt[\pi]{\omega})$, because $k_f^\times \subset k_{2f}^\times$.

Example 7.4.4  Allow $q$ (a prime power) and $f > 0$ to be arbitrary, and take $e = q^f - 1$. There are then $e$ ramified lines in $K_f/K_f^{\times e}$, of which $q - 1$ are $G_f$-stable. When $\pi$ has been chosen, the ramified lines are parametrised by $k_f^\times/k_f^{\times e} = k_f^\times$, and the $G_f$-stable ones correspond to elements of $k^\times$. The corresponding galoisian extensions of $K$ of ramification index $e$ and residual degree $f$ are all split because $H^2(G_f, k_f^\times)$ vanishes (§2). If $f = 1$, then every ramified line is $G_f$-stable, and the corresponding galoisian extensions are all abelian (7.2.4).

Suppose now that $f > 1$, and let $\omega$ be a generator of $k_f^\times$, so that the extension $K_f(\sqrt[\pi]{\omega})$ is not galoisian over $K$. As the order of $\omega^{q^{-1}}$ in $k_f^\times$ is $d = 1 + q + \cdots + q^{f-1}$, the galoisian closure of $K_f(\sqrt[\pi]{\omega})|K$ is $K_{df}(\sqrt[\pi]{\omega})$. Whether this galoisian extension of $K$ is split or not depends on the class $[\bar{\omega}] \in H^2(G_{df}, k_{df}^\times/k_{df}^{\times e})$. We claim that $\bar{\omega} \in q-1(k_{df}^\times/k_{df}^{\times e})$ has order $q-1$. Indeed, $\omega = \omega_d (q^{df-1})/(q^{df-1})$ for some generator $\omega_d$ of $k_{df}^\times$, where the exponent $r = (q^{df-1})/(q^{df-1})$ is $\equiv d \pmod{e}$, so $\bar{\omega} = \bar{\omega}_d$ in $k_{df}^\times/k_{df}^{\times e}$. Now, this group has order $e$ (because $e$ divides the order $q^{df-1}$ of $k_{df}^\times$), it is generated by $\bar{\omega}_d$, and $d$ divides $e$, so the order of $\bar{\omega}_d^e = e/d = q - 1$.

It follows that the order of $[\bar{\omega}]$ must divide $q - 1$, and consequently the galoisian extension $K_{ef}(\sqrt[\pi]{\omega})$ (recall that $e = (q - 1)d$) must be split over $K$, and indeed $K_{ef}(\sqrt[\pi]{\omega}) = K_{ef}(\sqrt[\pi]{\omega})$ because $\omega \in k_{ef}^{\times e}$. As the group $q-1(k_{df}^\times/k_{df}^{\times e})$ has order $q - 1$ and is generated by $\bar{\omega}$, the quotient $H^2(G_{df}, k_{df}^\times/k_{df}^{\times e})|q$ has order dividing $q - 1$ and is generated by $[\bar{\omega}]$. What is the exact order?

**Proposition 7.4.5.** — In the case at hand (7.4.4), the order of the group $H^2(G_{df}, k_{df}^\times/k_{df}^{\times e})|q$ is $\gcd(q - 1, 1 + q^f + q^{2f} + \cdots + q^{(d-1)f})$, which equals $q - 1$ if and only if $f \equiv 0 \pmod{q - 1}$.

28
Proof. The group $H^2$ in question has order $(q - 1) \gcd(e, r)/e$, where

$$r = \frac{q^{df} - 1}{q - 1} = \frac{(q^f - 1)(1 + q^f + q^{2f} + \cdots + q^{(d-1)f})}{q - 1} = d(1 + q^f + q^{2f} + \cdots + q^{(d-1)f}),$$

so $\gcd(e, r) = d \gcd(q - 1, 1 + q^f + q^{2f} + \cdots + q^{(d-1)f})$, and the first claim follows because $e = (q - 1)d$. Next, observe that $q \equiv 1 \pmod{q - 1}$, hence

$$1 + q^f + q^{2f} + \cdots + q^{(d-1)f} \equiv d \equiv f \pmod{q - 1},$$

so the order of $H^2$ is $q - 1$ precisely when $f \equiv 0 \pmod{q - 1}$.

Example 7.4.6 Take $q$ to be odd, and let us look for all extensions $L$ of $K$ (up to $K$-isomorphism) with ramification index 4 and residual degree 2. Notice that there are four of them, namely $L^{(i)} = K_2(\sqrt[4]{\omega^i \pi})$ ($i \in \mathbb{Z}/4\mathbb{Z}$), where $\pi$ is a uniformiser of $K$ and $\omega$ is a generator of $k_2^\times$. Abbreviate $C = k_2^\times/k_2^{\times 4}$.

If $q \equiv 1 \pmod{4}$ (so that $q - 1 \equiv 0$ and $1 + q \equiv 2$), they are all galoisian (indeed abelian) over $K$; two of them, namely $L^{(0)}$ and $L^{(2)}$ are split over $K$ (indeed $L^{(2)} = K_2(\sqrt[4]{\omega^{1+q} \pi})$ and $\omega^{1+q} \in k_2^\times$) whereas the other two, namely $L^{(1)}$ and $L^{(3)}$, are cyclic over $K$ and split by $K_4$ because $[\bar{\omega}] = [\bar{\omega}^3]$ is the order-2 element of the order-2 group $H^2(G_2, C)/C = C/C^2$.

If $q \equiv 3 \pmod{4}$ (so that $q - 1 \equiv 2$ and $1 + q \equiv 0$), only $L^{(0)}$ and $L^{(2)}$ are galoisian over $K$ (because $2C = \{\bar{\omega}^0, \bar{\omega}^2\}$ but they are not abelian (because $q - 1 \not\equiv 0 \pmod{4}$). Of these, $L^{(0)}$ is split over $K$ so $\text{Gal}(L^{(0)}/K)$ is the dihedral group $D_8$ (1.5.3), whereas $L^{(2)}$ is not split over $K$ (because $\bar{\omega}$ has order 2 in $H^2(G_2, C)/C = 2C$), so $\text{Gal}(L^{(2)}/K)$ is the quaternionic group $H_8$ (1.5.3). However, $L^{(2)}$ is split by $K_4$ and indeed $L^{(2)}K_4 = K_4(\sqrt[4]{\pi})$, although $L^{(2)}$ itself is not of the form $K_2(\sqrt[4]{\pi'})$ for any uniformiser $\pi'$ of $K$.

Let us determine the galoisian closures of $\hat{L}^{(1)}$, $\hat{L}^{(3)}$ of $L^{(1)}$ and $L^{(3)}$ over $K$. Since the order of $(\bar{\omega})^2$ (resp. $(\bar{\omega}^3)^2$) in $C$ is 2, we have $\hat{L}^{(1)} = L^{(1)}K_4$ and $\hat{L}^{(3)} = L^{(3)}K_4$. Are these galoisian extensions split over $K$? Now, for a suitable generator $\omega_3$ of $k_2^\times$, we have $\omega = \omega_3^{1+q^2}$, so $\omega$ and $\bar{\omega}$ are both equal to $\omega_3^2$ in $k_2^\times/k_2^{\times 4}$ (and hence $\hat{L}^{(1)} = \hat{L}^{(3)}$), which has order 2 in $H^2(G_4, k_2^\times/k_2^{\times 4})_q$, so the extension $\hat{L}^{(1)} = \hat{L}^{(3)}$ is not split over $K$. However, $\hat{L} = L^{(1)}K_8 = L^{(3)}K_8$ is split, and indeed $\hat{L} = K_8(\sqrt[4]{\pi})$.

To summarise, the set $T_{4,2}(K)$ always consists of four extensions when $q \equiv 1 \pmod{2}$. If $q \equiv 1 \pmod{4}$, then all four are abelian, but only two of them are split; the other two (which are cyclic) split in $T_{4,4}(K)$. If
q \equiv 3 \pmod{4}, then only two of the four extensions are galoisian over K, and only one of them (a \(\mathcal{D}_8\)-extension) is split; the other (an \(\mathcal{H}_8\)-extension) splits in \(T_{4,4}(K)\). The two extensions which are not galoisian become so — and become one — in \(T_{4,4}(K)\), but that extension is not split over K, it splits only in \(T_{4,8}(K)\).

Remark 7.4.7 It follows from Examples (7.4.3) and (7.4.6) that a local field K of odd residual cardinality q has an \(\mathcal{H}_8\)-extension or a \(\mathcal{D}_8\)-extension L if and only if \(q \equiv 3 \pmod{4}\). If so, L is unique; it is a ramified quadratic extensions of \(K(\sqrt[8]{K})\) (which itself is the unique element of \(T_{2,2}(K)\)), and it is cyclic over \(K_2\); cf. Remark (1.5.4). Explicit generation of L when \(K = \mathbb{Q}_p\) can be found in [5] in the case of the \(\mathcal{H}_8\)-extension.

Let us find the analogue of this for odd primes \(l\) such that gcd\((l, q) = 1\).

Recall that there are five groups \(\Gamma\) of order \(l^3\), three of which are commutative (of exponents \(l\), \(l^2\) and \(l^3\) respectively), and two of which are not. The centre \(Z \subset \Gamma\) of both these groups has order \(l\), and the quotient \(\Gamma / Z\) is commutative of exponent \(l\), but one \(\Gamma\) has exponent \(l^2\) and the other has exponent \(l^3\). The latter is sometimes denoted \(\mathcal{H}_{l^3}\).

Remark 7.4.8 Assume that gcd\((l, q) = 1\) (where \(l \neq 2\)), let \(\Gamma\) be a group of order \(l^3\), and suppose that K has a \(\Gamma\)-extension L. As the abelian case can be easily analysed, suppose that \(\Gamma\) is not commutative. As K then has an abelian extension of degree \(l^2\) and exponent \(l\) (of group \(\Gamma / Z\)), we must have \(q \equiv 1 \pmod{l}\) or equivalently \(v_l(q - 1) > 0\).

The pair \((e, f)\) for \(L|K\) cannot be \((1, l^2)\) or \((l^3, 1)\) because \(\Gamma\) is not cyclic (or because L contains \(K(\sqrt[8]{K})\) which has ramification index \(l\) and residual degree \(l\) over K, in view of \(v_l(q - 1) > 0\)); it cannot be \((l, l^2)\) either, because \(\Gamma\) is not commutative. So \((e, f) = (l^2, l)\). For the same reason, \(q \not\equiv 1 \pmod{l^2}\). The conjunction of these two conditions is equivalent to \(v_l(q - 1) = 1\).

Proposition 7.4.9. — Conversely, if \(v_l(q - 1) = 1\), then K has \(l\) galoisian extensions \(L\) of degree \(l^3\) which are not abelian. They all have ramification index \(l^2\) and residual degree \(l\), and the group \(\text{Gal}(L|K)\) is always isomorphic to \(\mathcal{H}_{l^3}\).

Proof. As \(q' \equiv 1 \pmod{l^2}\), there are \(l^2\) ramified lines in \(K_{l^3}^x / K_l^x l^2\). When we choose a uniformiser \(\pi\) of K, the set \(\mathcal{R}_{l^2}(K_\ell)\) of such lines is in bijection with \(C = k_l^x / k_l^x l^2\). As gcd\((l^2, q - 1) = l\), there are \(l\) \(G_l\)-stable ramified lines. We claim that \(H^2(G_l, C)\) is trivial. Indeed, \(q \equiv 1 + cl \pmod{l^2}\) for some \(c \in [1, l]\), so
\[
1 + q + \cdots + q^{l-1} \equiv 1 + (1 + cl) + \cdots + (1 + (l - 1)cl) \equiv l \pmod{l^2}.
\]
Therefore the group $\text{Gal}(L|K)$ for the $l$ galoisian extensions $L$ of $K$ of ramification index $l^2$ and residual degree $l$ admits the presentation (1.5.1)

$$\langle \tau, \tilde{\sigma} | \tau^{l^2} = 1, \tilde{\sigma}^l = 1, \tilde{\sigma} \tau \tilde{\sigma}^{-1} = \tau^q \rangle$$

defining the group $H_{l^3}$ (the unique group of order $l^3$ and exponent $l^2$ which is not commutative). This completes the proof.

Example 7.4.10 As a final example, consider the case $q \equiv 1 \pmod{2^2}$ or equivalently $v_2(q-1) > 1$. We have seen that every galoisian extension in $T_{2^2,2}(K)$ is in fact abelian. But for some $m > 2$, there might be galoisian extensions in $T_{2^m,2}(K)$ which are not abelian. A necessary and sufficient condition for that to happen is that $2^m$ divide $q^2 - 1$ but not $q - 1$. In view of $v_2(q+1) = 1$, this condition is equivalent to $v_2(q-1) = m - 1$.

When $v_2(q-1) = m - 1$, there are $2^{m-1}$ extensions $L \in T_{2^m,2}(K)$ which are galoisian but not abelian; for every such $L$, the resulting short exact sequence (7.2.1)

$$1 \to \mu_{2^m} \to \text{Gal}(L|K) \to G_2 \to 1$$
splits because the group $H^2(G_2, k^x_2/k_2^{x2^m})_q$ vanishes. For some related results, see [11, 1.2].

8 Acknowledgements One of the authors (CSD) wishes to express his heartfelt thanks to Rakesh Yadav, Georg-August-Universität, Göttingen, for supplying [5], and to M. Franck Pierron, Université Paris-Sud, Orsay, for supplying [11].

Bibliography

[1] Albert (A). — On $p$-adic fields and rational division algebras, Ann. of Math. (2) 41, 1940, pp. 674–693.

[2] Dalawat (C). — Further remarks on local discriminants, J. Ramanujan Math. Soc. 25 (2010) 4, 391–417. Cf. arXiv:0909.2541.

[3] Dalawat (C). — Serre’s “formule de masse” in prime degree, Monatshefte Math. 166 (2012), 73–92. Cf. arXiv:1004.2016.

[4] Eilenberg (S). — Topological methods in abstract algebra. Cohomology theory of groups, Bull. Amer. Math. Soc. 55 (1949) 3–37.

[5] Fujisaki (G). — A remark on quaternion extensions of the rational $p$-adic field, Proc. Japan Acad. Ser. A Math. Sci. 66 (1990) 8, 257259.
[6] Greve (C). — Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern, Dissertation, Universität Paderborn, Oktober 2010.

[7] Gross (B) & Reeder (M). — Arithmetic invariants of discrete Langlands parameters, Duke Math. J. 154 (2010) 3, 431–508. ($25.00)

[8] Hasse (H). — Zahlentheorie, Akademie-Verlag, Berlin, 1969, 611 pp.

[9] Iwasawa (K). — On Galois groups of local fields, Trans. Amer. Math. Soc. 80 (1955), 448–469.

[10] Reeder (M). — Notes on Group Theory, 5 October 2011, available at his website https://www2.bc.edu/~reederma/Groups.pdf.

[11] Riou-Perrin (B). — Plongement d’une extension diédrale dans une extension diédrale ou quaternionienne, Thèse de troisième cycle (1979), Publ. math. d’Orsay, n° 79-04.

[12] Serre (J-P). — Une “formule de masse” pour les extensions totalement ramifiées de degré donné d’un corps local, Comptes Rendus 286 (1978), 1031–1036.

[13] Waterhouse (W). — The normal closures of certain Kummer extensions, Canad. Math. Bull. 37 (1994) 1, 133–139.