II. Reciprocity Maps Existence Theorems

The fundamental results given in this chapter do not necessarily form a sequence of logical steps for a proof of class field theory, but are written and commented so as to be used. This is so true that, as we will see several times, a classical proof consists in *deducing* local class field theory from global class field theory, as was initiated by Hasse and Schmidt in 1930 (see [Ha4] and [SchFK], respectively), and in particular to base some local computations on global arguments (a typical example being the global computation of a local Hilbert symbol in 7.5); however here, in the description of the results, we will go from local to global, which seems more natural.

Chapter I contains tools coming directly from elementary considerations on number fields and local fields; on the contrary the present chapter relies on the (nontrivial) existence, for each place of the number field K, of the local reciprocity map (or local norm residue symbol). [1] The existence of the local reciprocity map, and thus of the global one as we will see in 3.2, is in fact of a cohomological nature, even though other approaches are possible, such as the Lubin–Tate theory of formal groups. [2]

§1 The Local Reciprocity Map — Local Class Field Theory

Let K be a number field and let $v \in Pl$ fixed. Since the case $v \in Pl_\infty$ is immediate (see 1.4.6), we will usually assume that we are dealing with a finite place, but everything which is detailed below can also be applied to the local extension $\mathbb{C}/\mathbb{R}$, an unramified abelian extension whose Frobenius is equal to complex conjugation c.

As usual, if v is finite *all* the corresponding local fields are taken in the completion $\mathbb{C}_\ell$ of an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$, where ℓ is the residue characteristic of v. Let K_v be the v-completion of K; let $\overline{K}_v = \overline{\mathbb{Q}}_\ell$ (resp. $\overline{K}_v^{\mathrm{ab}}$) be the algebraic (resp. abelian) closure of K_v in $\mathbb{C}_\ell$, and $\overline{G}_v$ (resp. $\overline{G}_v^{\mathrm{ab}}$) the profi-

[1] Its proof can be found in [d, CF, Ch. VI; Se2, Ch. XI, XIII], [f, Art1; Haz], [c, Neu1, Ch. IV]; the first proof is actually due to Hasse–Chevalley [h, Che1].

[2] [f, Lang2, Ch. 8; Iw1], [d, CF, Ch. VI, § 3], [c, Neu1, Ch. V, § 4].

nite group $\mathrm{Gal}(\overline{K}_v/K_v)$ (resp. $\mathrm{Gal}(\overline{K}_v^{\mathrm{ab}}/K_v) \simeq \overline{G}_v/[\overline{G}_v, \overline{G}_v]$), where $[\overline{G}_v, \overline{G}_v]$ denotes the topological closure of the commutator subgroup of $\overline{G}_v$.

Now let L be a finite extension of K; for each $w \in Pl_{L,v}$, L_w is the w-completion of L. We fix L_w/K_v and the embeddings i_v and i_w for $w|v$, as explained in I.2.4.

Note. Since any finite extension of local fields can be written (in infinitely many ways) as L_w/K_v, we are indeed studying an arbitrary local extension; here, the use of this global point of view will not matter since it will in any case be the natural setting for the definition of the global reciprocity map corresponding to L/K (the only one which interests us here and for which we must consider simultaneously all the completions of L/K and all the corresponding local reciprocity maps).

a) Decomposition of Places: Local and Global Cases

In this subsection, we recall the main classical properties of the places in an arbitrary extension L/K, both in the local and global cases. As explained in the above Note, we work in the setting of a global extension L/K.

1.1 Local Galois Groups, Inertia Groups, Frobenius'. In this paragraph, we will constantly refer to Section 2 of Chapter I.

1.1.1 Galois Case. If L/K is Galois with Galois group G, the decomposition group of $w \in Pl_{L,v}$ in L/K, denoted D_w, can be canonically identified with $G_w := \mathrm{Gal}(L_w/K_v)$, and under this isomorphism the inertia group I_w of w in L/K, which is a normal subgroup of D_w, corresponds to the inertia group G_w^0 of L_w/K_v. We will sometimes use the notation D_w^0 instead of I_w when the higher ramification groups are needed in a global situation, and then more generally $D_w^i \simeq G_w^i$ or $D_{w,i} \simeq G_{w,i}$, $i \geq 0$, with the definitions recalled in 1.3.

Since the field L^{D_w} is the decomposition field of w in L/K, we know that $i_w(L^{D_w})$ is dense in K_v. The inertia field is L^{I_w}; similarly $i_w(L^{I_w})$ is dense in the subfield L_w^{nr} of L_w fixed under G_w^0 (the largest subfield of L_w unramified over K_v). [3]

1.1.2 Non-Galois Case. Even when the extension L/K is not Galois the extension L_w/K_v may still be Galois (see Example I.2.2.3, (ii)), so that G_w (hence G_w^0 which is still a normal subgroup of G_w) can exist even when D_w does not make sense; this explains the independent choice of notations between the local and global cases.

[3] We use the superscript "nr" (as "non ramifié" from the french), thus following most authors.

1.1.3 Abelian Case. If L/K is abelian, the groups $D_w,\ I_w$, do not depend on the choice of $w \in Pl_{L,v}$ and, by abuse of notation, are simply denoted $D_v,\ I_v$; similarly for the fixed subfields $L^{D_v},\ L^{I_v}$. The notations $G_v,\ G_v^0,\ L_v,\ L_v^{\mathrm{nr}}$ are also legitimate since L_w does not depend on the choice of $w|v$, and neither does the isomorphism $G_w \simeq D_w$ which sends $\tau \in G_w$ to $i_w^{-1} \circ \tau \circ i_w$ on L.

In the Galois case the G_w for $w|v$ are equal (since the L_w are equal), but the canonical isomorphism $G_w \to D_w$ depends on the choice of $w|v$, which explains that in this case G_w is not denoted G_v.

1.1.4 Maximal Abelian Subextensions. We now assume that L/K is any finite extension. In the sequel, we will refer to the following diagram, in which $L'_{w'}/K_v$ comes from a subextension L'/K of L/K, w' is the place of L' below w, L_w^{ab} (resp. $L_{w'}'^{\mathrm{ab}} = L_w^{\mathrm{ab}} \cap L'_{w'}$) is the maximal abelian extension of K_v in L_w (resp. in $L'_{w'}$), and where $L_w^{\mathrm{ab}'}$ is the maximal abelian extension of $L'_{w'}$ in L_w ($L_w^{\mathrm{ab}'}$ contains $L'_{w'}L_w^{\mathrm{ab}}$, but is not necessarily equal to it).

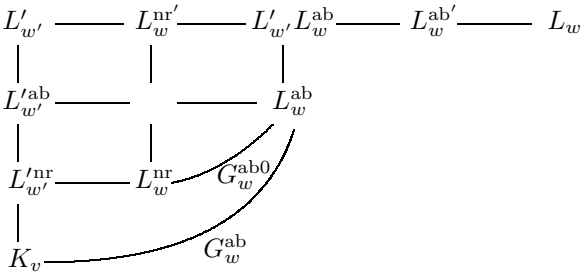


Fig. 1.1

By abuse of notation we set $G_w^{\mathrm{ab}} := \mathrm{Gal}(L_w^{\mathrm{ab}}/K_v)$; if L_w/K_v is Galois then G_w exists and we indeed have $G_w^{\mathrm{ab}} \simeq G_w/[G_w, G_w]$. We denote by $G_w^{\mathrm{ab}\,0}$ the inertia group of L_w^{ab}/K_v. If L_w/K_v is Galois (with Galois group G_w), the inertia group of L_w^{ab}/K_v is equal to $G_w^{\mathrm{ab}\,0} \simeq G_w^0/[G_w, G_w]$ which is not the abelianization of G_w^0 but the image of G_w^0 in G_w^{ab}, in accordance with the general property of higher ramification groups (in upper numbering) which is that for any normal subgroup H of G_w, we have $(G_w/H)^i = G_w^i H/H$ (see [d, Se2, Ch. IV, § 3]).

We proceed in an analogous manner to define the groups D_w^{ab} and I_w^{ab} which lift G_w^{ab} and $G_w^{\mathrm{ab}\,0}$ respectively, when L/K is Galois; we have $D_w^{\mathrm{ab}} = D_w/[D_w, D_w]$ and $I_w^{\mathrm{ab}} = I_w/[D_w, D_w]$.

Note that, even in the Galois case, G_w^{ab} is not necessarily isomorphic to the decomposition group $D_w(L^{\mathrm{ab}}/K)$ of w in L^{ab}/K, the latter corresponding to the quotient of G_w^{ab} which gives $\mathrm{Gal}((L^{\mathrm{ab}})_v/K_v)$ (see I.2.7).

1.1.5 Maximal Unramified Subextensions — Frobenius'. We denote by $\overline{K}_v^{\mathrm{nr}}$ the maximal unramified extension of K_v in $\overline{K}_v$; it will of course be obtained by the local infinite class field theory correspondence 1.7, but its direct construction is classical and elementary: recall that, when v is finite, $\overline{K}_v^{\mathrm{nr}}$ is the lift, via the Hensel Lemma I.3.2, of the algebraic closure $\overline{F}_v$ of the residue field $F_v \simeq \mathbb{F}_{q_v}$ of K_v, since for each degree $n \geq 1$, the unique unramified extension of degree n of K_v is equal to $K_v(\mu_{q_v^n-1})$;[4] it is a cyclic extension. It follows that $\overline{K}_v^{\mathrm{nr}}$ is contained in $\overline{K}_v^{\mathrm{ab}}$, that it is procyclic with Galois group:

$$\mathrm{Gal}(\overline{K}_v^{\mathrm{nr}}/K_v) \simeq \varprojlim_{n\geq 1} \mathbb{Z}/n\mathbb{Z} =: \widehat{\mathbb{Z}} \simeq \prod_{p\,\mathrm{prime}} \mathbb{Z}_p,$$

the profinite completion of $\mathbb{Z}$. For any subextension M/K_v (finite or not) of $\overline{K}_v^{\mathrm{nr}}/K_v$, we denote by:

$$\mathrm{Frob}(M/K_v)$$

the Frobenius automorphism of M/K_v; it is a topological generator of the group $\mathrm{Gal}(M/K_v)$, restriction of $\mathrm{Frob}(\overline{K}_v^{\mathrm{nr}}/K_v)$ to M. The Frobenius action $\mathrm{Frob}(\overline{K}_v^{\mathrm{nr}}/K_v)(x) \equiv x^{q_v} \bmod (\pi_v)$ for integers x is here characterized by:

$$\mathrm{Frob}(\overline{K}_v^{\mathrm{nr}}/K_v)(\zeta) = \zeta^{q_v} \ \text{ for all } \zeta \in \bigcup_{n\geq 1} \mu_{q_v^n-1},$$

otherwise, $\mathrm{Frob}(\overline{K}_v^{\mathrm{nr}}/K_v)(\zeta) - \zeta^{q_v}$ is a local unit (we are reduced to consider $1-\zeta'$ where $\zeta' \neq 1$ is of order prime to the residue characteristic of v) which must be in (π_v), a contradiction.

In the above context 1.1.4, we then have $L_w^{\mathrm{nr}} = L_w \cap \overline{K}_v^{\mathrm{nr}}$; this is the maximal unramified subextension of L_w/K_v. As we have just mentioned, it is cyclic, unique, contained in L_w^{ab}, and L_w/L_w^{nr} is totally ramified;[5] L_w^{nr} exists even when L_w/K_v is not Galois; in the Galois case, it is the subfield fixed under G_w^0 (see 1.1.1).

We immediately check that $\overline{L}_w^{\mathrm{nr}} = L_w\overline{K}_v^{\mathrm{nr}}$ or, more canonically:

$$\overline{k}^{\mathrm{nr}} = k\,\overline{\mathbb{Q}}_\ell^{\mathrm{nr}} = \bigcup_{n\geq 1} k(\mu_{\ell^n-1}),$$

for any algebraic extension k of $\mathbb{Q}_\ell$, where ℓ is the corresponding residue characteristic (for this, we must check that $k(\mu_{\ell^n-1})/k$ is unramified, even if ℓ^n is not a power of q_v, which is immediate).

In (Fig. 1.1) above we have given the various maximal unramified extensions using a principle of notation identical to the one used for maximal abelian extensions (noting that since L_w/L_w^{nr} is totally ramified, we indeed have here that $L_w^{\mathrm{nr}'} = L'_{w'}L_w^{\mathrm{nr}}$). The diagram can be justified by the very nature of $\overline{K}_v^{\mathrm{nr}}$. This gives the following result.

[4] [e, Ko3, Prop. 1.77].
[5] [d, Se2, Ch. III, § 5, Cor. 3 to Th. 3].

1.1.6 Exact Sequence of Inertia Groups. Let L'/K be a subextension of L/K. If L_w/K_v and $L'_{w'}/K_v$ are Galois with respective Galois groups G_w and $G_{w'}$, we have the following exact sequence of inertia groups (which is still valid if these local extensions are infinite as we will see in 1.2.3):

$$1 \longrightarrow G'^0_w \longrightarrow G^0_w \longrightarrow G^0_{w'} \longrightarrow 1,$$

where $G'^0_w := \mathrm{Gal}(L_w/L_w^{\mathrm{nr}'})$, $G^0_{w'} := \mathrm{Gal}(L'_{w'}/L'^{\mathrm{nr}}_{w'})$.

The cyclicity of L^{nr}_w/K_v implies the following property of the Frobenius automorphism.

1.1.6.1 Proposition. *We have (see (Fig. 1.1)):*

$$\mathrm{Frob}(L^{\mathrm{nr}}_w/K_v)^{f'_{w'}} = \mathrm{Frob}(L^{\mathrm{nr}}_w/L'^{\mathrm{nr}}_{w'}) = \mathrm{Frob}(L_w^{\mathrm{nr}'}/L'_{w'})_{|L^{\mathrm{nr}}_w},$$

where $f'_{w'} := [L'^{\mathrm{nr}}_{w'} : K_v]$ is the residue degree of $L'_{w'}/K_v$. □

1.1.6.2 Notations. We denote by $e_w := [L_w : L^{\mathrm{nr}}_w]$ and $e^{\mathrm{ab}}_w := [L^{\mathrm{ab}}_w : L^{\mathrm{nr}}_w]$ the ramification index of L_w/K_v and of L^{ab}_w/K_v, respectively; since the extension L_w/L^{ab}_w is totally ramified, the residue degree $f_w := [L^{\mathrm{nr}}_w : K_v]$ of L_w/K_v is equal to f^{ab}_w, that of L^{ab}_w/K_v. □

1.2 Global Decomposition and Inertia Groups. We still consider a finite extension L/K with a subextension L'/K.

1.2.1 Exact Sequences of Decomposition and Inertia Groups. When L/K and L'/K are Galois, recall how the groups $D_{w'}$ and $I_{w'}$ (in L'/K), $D'_w := D_w(L/L')$ and $I'_w := I_w(L/L')$, are related to the groups D_w and I_w in L/K (with $w \,|\, w' \,|\, v$ in $L \supseteq L' \supseteq K$).

We have the following diagram, where L^{D_w} and $L'^{D_{w'}}$ are respectively the decomposition fields of w and w' in L/K and L'/K, where L^{I_w} and $L'^{I_{w'}}$ are the corresponding inertia fields, and where $L^{D'_w}$ and $L^{I'_w}$ are the decomposition and inertia fields of w in the extension L/L'.

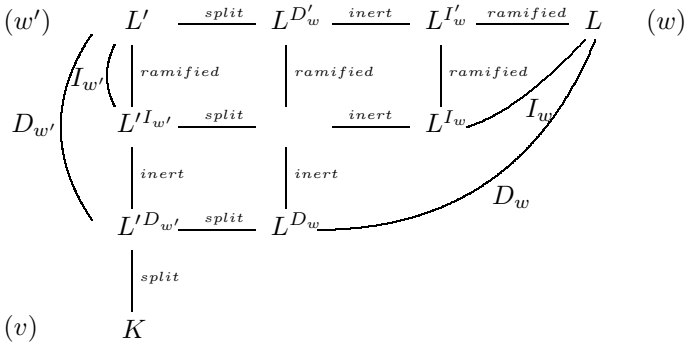


Fig. 1.2

In this diagram, all the field compositums are direct, the linear disjunction (on their intersection) coming from the fact that in each case at least one of the extensions is Galois. In particular, note that the decomposition and inertia properties propagate under ground field extension. For L/K Galois, all of this comes from existence and uniqueness of the fields L_1, L_2, $K \subseteq L_1 \subseteq L_2 \subseteq L$ for which w is totally ramified in L/L_2, totally inert in L_2/L_1 (which is a cyclic extension), and totally split in L_1/K. This means that w is of residue degree and ramification index equal to 1 in L_1/K, of residue degree $[L_2 : L_1]$ in L_2/L_1, and of ramification index $[L : L_2]$ in L/L_2. [6]

We can summarize the above with the following, where $L' \subseteq L$.

1.2.1.1 Proposition. *When L/K and L'/K are Galois, we have the exact sequences:*

$$1 \longrightarrow D'_w = D_w(L/L') \longrightarrow D_w \longrightarrow D_{w'} \longrightarrow 1,$$
$$1 \longrightarrow I'_w = I_w(L/L') \longrightarrow I_w \longrightarrow I_{w'} \longrightarrow 1,$$

which come from the restriction map $\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L'/K)$. □

1.2.1.2 Definition (global Frobenius'). Let L/K be Galois. Let v be a place of K and $w|v$ in L. When w is unramified in L/K, we denote by $\left(\frac{L/K}{w}\right)$ the global Frobenius of w in L/K, i.e., the image of the local Frobenius $\mathrm{Frob}(L_w/K_v)$ in $\mathrm{Gal}(L/K)$ under the canonical isomorphism $G_w \simeq D_w$. □

Then, in an analogous way as for 1.1.6.1:

1.2.1.3 Proposition. *When L/K and L'/K are Galois, and if w is unramified in L/K, we have:*

$$\left(\frac{L/K}{w}\right)^{|D_{w'}(L'/K)|} = \left(\frac{L/L'}{w}\right). \qquad \square$$

1.2.2 Non-Galois Case. In the case where the extensions are not necessarily Galois, see 1.2.5 which again proves these propagation properties using local arguments. In the non-Galois case, we can still define the decomposition and inertia fields L_1 and L_2 of w in L/K if we set:

$$L_1 := \{x \in L,\ i_w(x) \in K_v\}, \quad L_2 := \{x \in L,\ i_w(x) \in L_w^{\mathrm{nr}}\}.$$

These fields depend on the choice of w. We then say that w is totally split (resp. unramified) in L/K if $L_1 = L$ (resp. $L_2 = L$).

Note that now the extensions $i_w(L)/i_v(K)$ and $K_v/i_v(K)$ are not anymore necessarily linearly disjoint over their intersection $i_w(L_1)$: look at the

[6] [a, Sam, Ch. VI, § 2], [d, Lang1, Ch. I].

case $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, where w is the place with residue characteristic equal to $\ell = 5$ for which $i_w(\sqrt[3]{2})$ is not contained in $\mathbb{Q}_5$ (if $\sqrt[3]{2} \in \mathbb{Q}_5$, take $i_w(\sqrt[3]{2}) := j\sqrt[3]{2} \in \mathbb{Q}_5(j)$).

1.2.3 Infinite Galois Case. When L/K is an infinite Galois extension with Galois group G, we also define the decomposition field (resp. the inertia field) of w in L/K as the set of elements of L whose image under i_w is contained in K_v (resp. $\overline{K}_v^{\mathrm{nr}}$); thus, this defines the groups D_w and I_w in a way which is compatible with the finite case. It is also possible to define these groups as in the finite case (see [c, Wa, App., § 2]).

1.2.3.1 Proposition. *We have the following homeomorphisms:*

$$D_w \simeq \varprojlim_{L'} D_{w'}(L'/K), \quad I_w \simeq \varprojlim_{L'} I_{w'}(L'/K),$$

where L' ranges in the set of all finite Galois extensions of K in L ordered by inclusion, and where, for each L', w' is the place of L' below w. [7]

Proof. Since D_w is a closed subgroup of the profinite group $G \simeq \varprojlim_H G/H$, where H ranges in the set of all closed normal subgroups of finite index of G, a general result gives:

$$D_w \simeq \varprojlim_H D_w H/H \ ;$$

if L' denotes the subfield of L fixed under H, by the above we thus have:

$$D_w H/H \simeq \mathrm{Gal}(L'/L' \cap L^{D_w}) = D_{w'}(L'/K),$$

proving the result. The proof is the same for the inertia group. □

1.2.3.2 Exercise. Let Σ be a finite set of places of L. Prove in the same way that $\langle D_w \rangle_{w \in \Sigma} = \varprojlim_{L'} \langle D_{w'}(L'/K) \rangle_{w' \in \Sigma'}$. □

In applications, L/K will usually be abelian (infinite class field theory) and so the groups $D_w =: D_v$ and $I_w =: I_v$ will thus be independent of the choice of $w|v$.

1.2.4 Infinite Non-Galois Case. When L/K is an (arbitrary) infinite algebraic extension, we use the definition given in 1.2.2 to define the decomposition and inertia fields of w; this means that by definition an infinite

[7] The place w is defined by means of a choice of coherent extensions w' of v, and denoted $w = \varinjlim_{L'} w'$.

extension is totally split (resp. unramified) at w if and only if any finite subextension is totally split (resp. unramified) at w.

The following exercise justifies by local arguments the existence and basic properties of the decomposition and inertia fields in the most general situation.

1.2.5 Exercise (propagation of decomposition and nonramification). Let L/K be a fixed extension and let M be another extension of K.

(i) Let $v' \in Pl_M$ be totally split in M/K. Show that every place $w' \in Pl_{LM,v'}$ is totally split in LM/L.

(ii) Let $v' \in Pl_M$ be a finite place unramified in M/K. Show that every place $w' \in Pl_{LM,v'}$ is unramified in LM/L.

Answer. We first show the evident relation (where v is the place of K below v', and w that of L below w', which is thus above v):

$$(LM)_{w'} = L_w M_{v'},$$

by writing that $(LM)_{w'} := i_{w'}(LM)K_v$ is the compositum of $i_w(L)i_{v'}(M)$ with K_v (see I.2.6, I.2.6.1).

(i) By assumption, we have $M_{v'} = K_v$ so that $(LM)_{w'} = L_w$.

(ii) By existence and uniqueness of the maximal unramified subextensions of local extensions (or using the formula $F^{\mathrm{nr}} = F \cap \overline{K}_v^{\mathrm{nr}}$ for any extension F of K_v), we have:

$$L_w \cap (LM)_{w'}^{\mathrm{nr}} = L_w^{\mathrm{nr}},$$

and since by assumption $M_{v'} \subseteq (LM)_{w'}^{\mathrm{nr}}$, we have:

$$(LM)_{w'} = L_w M_{v'} \subseteq L_w (LM)_{w'}^{\mathrm{nr}},$$

so $(LM)_{w'}$ is equal to the direct compositum of L_w with $(LM)_{w'}^{\mathrm{nr}}$ over L_w^{nr}. Since L_w/L_w^{nr} is totally ramified, when these extensions are finite, the multiplicativity property of ramification indices immediately shows that $(LM)_{w'}/L_w$ is unramified. For infinite extensions, simply note that $M_{v'} =: K_v(\mu)$, where μ is of the form $\bigcup_n \mu_{q_v^n - 1}$ for suitable integers n, and that $L_w M_{v'} = L_w(\mu)$ is contained in $\overline{L}_w^{\mathrm{nr}}$.

If M/K is abelian and if $v \in Pl_K$, then in case (i) (resp. (ii)), every place $w \in Pl_{L,v}$ is totally split (resp. unramified) in LM/L. □

1.3 Higher Ramification. It is also useful to keep in mind a number of results on higher ramification (which will of course be in parallel with the fundamental results of class field theory when the extension is abelian), in particular what follows. [8]

[8] After [d, Se2, Ch. IV, §§ 1, 2], [e, Ko3, Ch. 1, § 3.7].

Let v be a finite place of K and denote by ℓ the residue characteristic of v. Assume that L_w/K_v is a finite Galois extension with Galois group G_w.

1.3.1 Higer Ramification Groups. For each $i \geq 0$, we define the higher ramification group (in lower numbering) by:

$$G_{w,i} := \{s \in G_w,\ \mathrm{w}(s(x) - x) \geq i + 1 \ \ \forall x \text{ integer of } L_w\},$$

which is a normal subgroup of G_w. We have $G_{w,0} = G_w^0$, the inertia group.

We also have for all $i \geq 1$:

$$G_{w,i} = \{s \in G_{w,0},\ \mathrm{w}(\pi_w^{s-1} - 1) \geq i\},$$

where π_w is a uniformizer of L_w.

1.3.2 Inertia Group. Recall that the group $G_{w,1}$ is an ℓ-group and the quotient $G_{w,0}/G_{w,1}$ is a cyclic group isomorphic to a subgroup of $F_w^\times$ (hence whose order is prime to ℓ): indeed, the kernel of the map sending $s \in G_{w,0}$ to the residue class $\overline{u_s}$ of $u_s := \pi_w^{s-1}$ is by definition equal to $G_{w,1}$. This result shows that for a global finite p-extension [9] L/K and for a finite place v of K with residue characteristic $\ell \neq p$, the order of $I_w \simeq G_{w,0}$ divides $|F_w^\times| = q_w - 1$.

1.3.3 Inertia Group in the Abelian Case. When L_w/K_v is *abelian*, we can write for $s \in G_{w,0}$ and $u_s := \pi_w^{s-1}$:

$$u_s^{t-1} = (\pi_w^{s-1})^{t-1} = (\pi_w^{t-1})^{s-1} \ \text{ for all } t \in G_w\ ;$$

since $\pi_w^{t-1} =: u(t) \in U_w$, we obtain:

$$\overline{u_s}^{\,t-1} = \overline{u(t)}^{\,s-1} = \overline{1} \ \text{ for all } t \in G_w$$

since F_w (equal to the residue field of L_w^{nr}) is fixed under $G_{w,0}$. It follows that $\overline{u_s} \in F_v^\times$; in this case, we have an injection of the form:

$$G_{w,0}/G_{w,1} \longrightarrow F_v^\times.$$

We have obtained:

1.3.3.1 Proposition. *In any abelian extension L/K (finite or not), the group $D_{v,0}(L/K)/D_{v,1}(L/K)$ (which measures the tame ramification)* [10] *is isomorphic to a subgroup of $F_v^\times$.* □

[9] Recall that "p-extension" or "pro-p-extension" always means Galois extension whose Galois group is a p-group or a pro-p-group.

[10] "Tame ramification" of a finite place in an extension means that the corresponding ramification index of the place is prime to the residue characteristic.
As explained in 1.1.1, for $i \geq 0$, $D_{w,i}(L/K)$ denotes the ramification groups in a global Galois extension L/K; in particular, $D_{w,0}(L/K) = I_w(L/K)$ and $D_{w,i}(L/K) \simeq G_{w,i}$ for all $i \geq 0$.

For example, if $\mathrm{Gal}(L/K) \simeq \mathbb{Z}_p^r$ (i.e., if L/K is $\mathbb{Z}_p$-free of finite type), then L/K is unramified outside places dividing p (same result if $\mathrm{Gal}(L/K)$ is an arbitrary free pro-p-group [Y]).

For the definition of the ramification groups in upper numbering G_w^i, see [d, Se2, Ch. IV, § 3].

We will come back to higher ramification groups in 1.6.2 when we will perform conductor computations.

b) Local Class Field Theory Correspondence

Let L/K be a finite extension of number fields, L'/K a subextension, and let $v \in Pl$, $w \in Pl_{L,v}$, and w' below w (thus, above v) in L'. We denote by U_v, $U'_{w'}$, and U_w the unit groups of the fields K_v, $L'_{w'}$, and L_w. The first fundamental result in the local case is the following (use Fig. 1.1).

1.4 Theorem (local reciprocity map, norm residue symbol). *There exists a canonical homomorphism:*

$$\begin{array}{rccc} (\bullet\,,\, L_w/K_v) : & K_v^\times & \longrightarrow & G_w^{\mathrm{ab}} := \mathrm{Gal}(L_w^{\mathrm{ab}}/K_v) \\ & x & \longmapsto & (x\,,\, L_w/K_v) \end{array}$$

having the following properties:

(i) We have the exact sequence:

$$1 \longrightarrow \mathrm{N}_{L_w/K_v}(L_w^\times) \longrightarrow K_v^\times \xrightarrow{(\bullet\,, L_w/K_v)} G_w^{\mathrm{ab}} \longrightarrow 1\ ;$$

(ii) the composition of $(\bullet\,, L_w/K_v)$ and of the projection $G_w^{\mathrm{ab}} \longrightarrow \mathrm{Gal}(L'^{\mathrm{ab}}_{w'}/K_v)$ is equal to $(\bullet\,, L'_{w'}/K_v)$;

(iii) the image of U_v (resp. of U_v^i, $i \geq 1$) under $(\bullet\,, L_w/K_v)$ is equal to the inertia group $G_w^{\mathrm{ab}\,0}$ (resp. to the ith higher ramification group in upper numbering $G_w^{\mathrm{ab}\,i}$) in L_w^{ab}/K_v, and in particular we have the exact sequence:

$$1 \longrightarrow \mathrm{N}_{L_w/K_v}(U_w) \longrightarrow U_v \longrightarrow G_w^{\mathrm{ab}\,0} \longrightarrow 1\ ;$$

(iv) for all $x' \in L'^\times_{w'}$, the image of $(x'\,, L_w/L'_{w'})$ in G_w^{ab} is equal to $(\mathrm{N}_{L'_{w'}/K_v}(x')\,, L_w/K_v)$; in particular, we have:

$$\mathrm{Gal}(L_w^{\mathrm{ab}}/L'^{\mathrm{ab}}_{w'}) = (\mathrm{N}_{L'_{w'}/K_v}(L'^\times_{w'})\,, L_w/K_v),$$

and the inertia group of $L_w^{\mathrm{ab}}/L'^{\mathrm{ab}}_{w'}$ is equal to $(\mathrm{N}_{L'_{w'}/K_v}(U'_{w'})\,, L_w/K_v)$;

(v) for all $x \in K_v^\times$, the image of $(x\,, L_w/K_v)$ under the transfer map[11] *(from G_w^{ab} to $\mathrm{Gal}(L_w^{\mathrm{ab}'}/L'_{w'})$), is equal to $(x\,, L_w/L'_{w'})$;*

(vi) for any isomorphism τ of L_w and all $x \in K_v^\times$, we have:

$$(\tau x\,, \tau L_w/\tau K_v) = \tau \circ (x\,, L_w/K_v) \circ \tau^{-1} \text{ on } \tau L_w^{\mathrm{ab}}\ ;$$

[11] See Remark 1.4.1.

(vii) if L_w^{ab}/K_v is unramified, then for all $x \in K_v^\times$ we have: [12]

$$(x\,,\, L_w/K_v) = \mathrm{Frob}(L_w^{\mathrm{ab}}/K_v)^{\mathrm{v}(x)}\ ;$$

in other words:

$$(\pi_v\,,\, L_w/K_v) = \mathrm{Frob}(L_w^{\mathrm{ab}}/K_v),$$

for any uniformizer π_v of K_v. □

The symbol $(\bullet\,,\, L_w/K_v)$ is called the local norm residue symbol or the local reciprocity map.

1.4.1 Remark (transfer map). For the cohomological definition and the properties of the transfer map, see [d, Se2, Ch. VII, § 8] or [f, Neu2, Th. 8.8]. Here we do not assume that L_w/K_v is Galois, and the result is obtained (by restriction) from the analogous computation in the Galois closure of L_w over K_v. Recall how to compute $\mathrm{Ver} : G/[G,G] \longrightarrow H/[H,H]$ for any subgroup H of finite index of a group G: let $(s_i)_{i=1,\dots,(G:H)}$ be a system of representatives of the elements of G/H; for any fixed $s \in G$ and for each i put $s\,s_i =: s_j\,t_i$, $t_i \in H$, then we have:

$$\mathrm{Ver}(s \bmod [G,G]) = \prod_{i=1}^{(G:H)} t_i \bmod [H,H].$$ □

1.4.2 Remark (local Frobenius' for finite places). Recall that if L_w^{ab}/K_v is unramified (i.e., $L_w^{\mathrm{ab}} = L_w^{\mathrm{nr}}$), it is cyclic and its Frobenius $\mathrm{Frob}(L_w^{\mathrm{ab}}/K_v)$ is the unique generator σ of G_w^{ab} such that $\sigma(x) \equiv x^{q_v} \bmod (\pi_v)$ for all integers x of L_w^{ab}, where $q_v := |F_v|$, or such that $\sigma(\zeta) = \zeta^{q_v}$ for a root of unity ζ of order $q_v^{f_w^{\mathrm{ab}}} - 1$ generating L_w^{ab} over K_v. □

Note. If we denote respectively by N' and j' the norm map in $L'_{w'}/K_v$ and the canonical injection $K_v \longrightarrow L'_{w'}$, we have:

$$\mathrm{N}' \circ j' = [L'_{w'} : K_v] \text{ on } K_v^\times,\quad j' \circ \mathrm{N}' = \sum_i \sigma'_i \text{ on } L'^\times_{w'},$$

where the σ'_i are the $[L'_{w'} : K_v]$ K_v-isomorphisms of $L'_{w'}$ in $\mathbb{C}_\ell$ (in the Galois case, $\sum_i \sigma'_i =: \nu'$ is the algebraic norm in $L'_{w'}/K_v$). This applies to (iv) and (v).

1.4.3 Corollary. *We have (with Notations 1.1.6.2):*

(i) $K_v^\times/\mathrm{N}_{L_w/K_v}(L_w^\times) \simeq G_w^{\mathrm{ab}}$ has order equal to $e_w^{\mathrm{ab}}\, f_w^{\mathrm{ab}}$;

(ii) $U_v/\mathrm{N}_{L_w/K_v}(U_w) \simeq G_w^{\mathrm{ab}\,0}$ has order equal to e_w^{ab}. Thus, if L_w^{ab}/K_v is unramified we have:

$$U_v = \mathrm{N}_{L_w/K_v}(U_w)$$

[12] See Remark 1.4.2 in the case of finite places; see Remark 1.4.6 in the case of infinite places.

(i.e., $\mathrm{N}_{L_w/K_v}(L_w^\times) = \pi_v^{f_w^{\mathrm{ab}}\mathbb{Z}} \oplus U_v$*), and* $x \in K_v^\times$ *is a norm in* L_w/K_v *if and only if:*

$$\mathrm{v}(x) \equiv 0 \bmod (f_w^{\mathrm{ab}}). \qquad \square$$

By 1.4, (iii), and the fact that for a finite place v with residue characteristic equal to ℓ the group U_v^1 is the ℓ-Sylow subgroup of U_v, we deduce that $G_w^{\mathrm{ab}\,1} = G_{w,1}^{\mathrm{ab}}$ (the ℓ-Sylow subgroup of $G_{w,0}^{\mathrm{ab}}$) (see 1.3.2).

1.4.4 Proposition. *The map* $\mathrm{N}_{L_w/K_v} : L_w^\times \longrightarrow K_v^\times$ *is an open map.*

Proof. It is enough to show that for all $j \geq 0$ there exists $i \geq 0$ such that $U_v^i \subseteq \mathrm{N}_{L_w/K_v}(U_w^j)$. The properties of the logarithm and exponential in K_v (see [c, Wa, Ch. 5, § 1]) imply that, for i sufficiently large we have:

$$\log(U_v^i) = (\pi_v^i) =: [L_w : K_v](\pi_v^{i-h}),$$

where $h := \mathrm{v}([L_w : K_v])$, and for $i \geq j + h$ sufficiently large:

$$U_v^i = (U_v^{i-h})^{[L_w:K_v]} = \mathrm{N}_{L_w/K_v}(U_v^{i-h}) \subseteq \mathrm{N}_{L_w/K_v}(U_w^j). \qquad \square$$

It is clear that 1.4.3, (ii) is a deep result which is not simply elementary v-adic analysis, but it implies that $\mathrm{N}_{L/K}$ is an open map as a map from J_L to J_K (this will be clear in Section 2). A direct proof may be found in [d, Lang1, Ch. IX, § 3] and in [f, Art1, Ch. VII, § 2]; see also 1.6.4.

1.4.5 Remark. By its very nature, in a certain sense the norm residue symbol:

$$(\bullet,\, L_w/K_v),$$

does not depend on the extension L_w/K_v, but only on its maximal abelian subextension; for instance, this allows us to write:

$$(\bullet,\, L_w/K_v) = (\bullet,\, L_w^{\mathrm{ab}}/K_v) \quad \text{and} \quad \mathrm{N}_{L_w/K_v}(L_w^\times) = \mathrm{N}_{L_w^{\mathrm{ab}}/K_v}(L_w^{\mathrm{ab}\times}),$$

showing that the definition of this symbol for an arbitrary extension is useful in practice and gives more precise information. This proves for example that any element of $\mathbb{Q}_2^\times$ is the norm of an element of $\mathbb{Q}_2(\sqrt[3]{2}\,)$.

In particular, we deduce the following equality:

$$L_w^{\mathrm{ab}\times} = \mathrm{N}_{L_w/L_w^{\mathrm{ab}}}(L_w^\times) \cdot {}_{\mathrm{N}}L_w^{\mathrm{ab}\times},$$

where ${}_{\mathrm{N}}L_w^{\mathrm{ab}\times}$ is the kernel of $\mathrm{N}_{L_w^{\mathrm{ab}}/K_v}$. $\square$

1.4.6 Remark. Let us explicitly describe the case $v \in Pl_\infty^{\mathrm{r}}$ (the reciprocity map is the trivial map when v is complex). In this case $K_v = \mathbb{R}$ hence, since

the only nontrivial algebraic extension of $\mathbb{R}$ is $\mathbb{C}$ (which is in addition abelian and unramified over $\mathbb{R}$), the reciprocity map $(\bullet, \mathbb{C}/\mathbb{R})$ is given by:

$$(x\,, \mathbb{C}/\mathbb{R}) := c^{\mathrm{v}(x)} \text{ for all } x \in \mathbb{R}^\times,$$

where c is complex conjugation, and where $\mathrm{v}(x) = 0$ (resp. 1) if $x > 0$ (resp. $x < 0$). This is the only way to have the exact sequence in 1.4, (i). It is also the formula of statement (vii) since $c = \mathrm{Frob}(\mathbb{C}/\mathbb{R})$ (the local Frobenius at v).

In this case, when $L_w = \mathbb{C}$ (i.e., $i_w(L)$ is a nonreal extension of $i_v(K) \subset \mathbb{R}$), we have $G_w = G_w^{\mathrm{ab}} = \langle\, c\,\rangle$, $G_w^0 = 1$, $f_w = 2$, $e_w = 1$. If L/K is Galois, the decomposition group D_w is generated by the global Frobenius $c_w := i_w^{-1} \circ c \circ i_w$; c_w is called "a" complex conjugation of L/K. □

Let K_v be the v-completion of the number field K.

1.5 Theorem (local existence). *For any subgroup of finite index N of $K_v^\times$ there exists*[13] *a unique finite abelian extension M of K_v such that $\mathrm{N}_{M/K_v}(M^\times) = N$; the norm residue symbol in M/K_v yields the exact sequence:*

$$1 \longrightarrow N \longrightarrow K_v^\times \longrightarrow \mathrm{Gal}(M/K_v) \longrightarrow 1.$$

In addition, the bijection from the set of subgroups of finite index of $K_v^\times$ to the set of finite abelian extensions of K_v is a Galois correspondence; in other words we have the following properties (where M_1 and M_2 are abelian over K_v and correspond respectively to N_1 and $N_2 \subseteq K_v^\times$):

(i) we have $M_1 \subseteq M_2$ if and only if $N_2 \subseteq N_1$;

(ii) $M_1 M_2$ corresponds to $N_1 \cap N_2$;

(iii) $M_1 \cap M_2$ corresponds to $N_1 N_2$;

(iv) if $M_1 \subseteq M_2$, we have $\mathrm{Gal}(M_2/M_1) \simeq N_1/N_2$, where the isomorphism is obtained from the restriction of $(\bullet, M_2/K_v)$ to N_1. □

Note. The subgroups of finite index of $K_v^\times$ are open, but the converse is false (look for example at the case of U_v). However, when we take limits to describe $\mathrm{Gal}(\overline{K}_v^{\mathrm{ab}}/K_v)$, it is not $K_v^\times$ and its topology which occur (see 1.7).

1.5.1 Remarks. (i) Properties (i) to (iv) logically follow from the existence of this bijection, because of 1.4, (i), (ii) (the equality $\mathrm{Gal}(M_2/M_1) = (N_1, M_2/K_v)$ is a particular case of 1.4, (iv)).

(ii) By 1.4, (ii), (iii), the subgroup of $K_v^\times$ corresponding to the inertia subfield M^{nr} of M is $U_v\, N$, where N corresponds to M, since the kernel of $K_v^\times \longrightarrow \mathrm{Gal}(M/K_v)/\mathrm{Im}(U_v) = \mathrm{Gal}(M^{\mathrm{nr}}/K_v)$ is $U_v N$; similarly, its maximal tamely ramified subextension corresponds to $U_v^1\, N$. It is clear that $U_v N = \pi_v^{f\mathbb{Z}} \oplus U_v$, where f is the residue degree of M/K_v. We recover the

[13] in some fixed algebraic closure of K_v; here it is convenient to use $\overline{K}_v = \overline{\mathbb{Q}}_\ell \subset \mathbb{C}_\ell$, where ℓ is the residue characteristic or ∞ (see the introduction to Section 1).

existence and the uniqueness of the unramified extension of degree n of K_v: it corresponds to $\pi_v^{n\mathbb{Z}} \oplus U_v$.

(iii) The group N corresponding to M/K_v is called the norm group of the extension M/K_v. □

1.5.2 Exercise. Prove the above Remark (i).

Answer. Suppose $M_1 \subseteq M_2$; since $(N_2,\, M_2/K_v) = 1$ by definition, one gets $(N_2,\, M_1/K_v) = 1$, proving that $N_2 \subseteq N_1$. We now put:

$$H := (N_1,\, M_2/K_v) \subseteq \mathrm{Gal}(M_2/M_1)\ ;$$

then $|H| = (N_1 : N_2) = (K_v^\times : N_2)(K_v^\times : N_1)^{-1} = [M_2 : M_1]$, proving (iv):

$$(N_1,\, M_2/K_v) = \mathrm{Gal}(M_2/M_1),$$

which we will now use systematically.

Let M_1, M_2 be arbitrary, and let N and N' be the norm groups of $M := M_1M_2$ and $M' := M_1 \cap M_2$; we put:

$$H_i := \mathrm{Gal}(M/M_i) = (N_i,\, M/K_v),\ i = 1,\, 2\ ;$$

we have the inclusions:

$$N \subseteq N_1 \cap N_2 \subseteq N_1N_2 \subseteq N'.$$

We have $H_1H_2 = \mathrm{Gal}(M/M')$, hence, since $H_i = (N_i,\, M/K_v)$, we have $(N_1N_2,\, M/K_v) = (N',\, M/K_v)$, and finally $N' = N_1N_2$ since these groups contain the kernel N of $(\bullet,\, M/K_v)$. In the same way, $H_1 \cap H_2 = 1$ yields:

$$(N_1,\, M/K_v) \cap (N_2,\, M/K_v) = (N_1 \cap N_2,\, M/K_v) = 1,$$

thus $N_1 \cap N_2 = N$.

If $N_2 \subseteq N_1$ then $N_1N_2 = N_1$ yields (by uniqueness) $M_1 \cap M_2 = M_1$ (or $N_1 \cap N_2 = N_2$ and $M_1M_2 = M_2$), which finishes the proof. □

To illustrate the local class field theory correspondence, let us look at the following situation which will be considered again in the Paragraph 2.6.

1.5.3 Example (local extensions coming from non-Galois extensions). Let L/K be a finite extension of number fields and, for $v \in Pl$, let L_w for $w \in Pl_{L,v}$ be the completions of L above v; recall that the L_w are defined only up to K_v-conjugation. Let L_v^{ab} be the maximal abelian subextension of $L_v := \bigcap_{w|v} L_w$; it is independent of the choice of the K_v-conjugates of the L_w since we have $L_v^{\mathrm{ab}} = \bigcap_{w|v} L_w^{\mathrm{ab}}$, while L_v does depend on them, but we will see that L_v will not really be used as such. We set:

$$G_v^{\mathrm{ab}} := \mathrm{Gal}(L_v^{\mathrm{ab}}/K_v).$$

Then the subgroup of $K_v^\times$ corresponding to L_v^{ab} is the subgroup generated by the $\mathrm{N}_{L_w/K_v}(L_w^\times)$ for $w|v$; in particular we have the equality:

$$\mathrm{N}_{L_v/K_v}(L_v^\times) = \langle\, \mathrm{N}_{L_w/K_v}(L_w^\times) \,\rangle_{w|v}$$

and the exact sequence:

$$1 \longrightarrow \mathrm{N}_{L_v/K_v}(L_v^\times) \longrightarrow K_v^\times \longrightarrow G_v^{\mathrm{ab}} \longrightarrow 1,$$

which can also be written using the corresponding abelianizations:

$$\mathrm{N}_{L_v^{\mathrm{ab}}/K_v}(L_v^{\mathrm{ab}\times}) = \langle\, \mathrm{N}_{L_w^{\mathrm{ab}}/K_v}(L_w^{\mathrm{ab}\times}) \,\rangle_{w|v},$$

$$1 \longrightarrow \mathrm{N}_{L_v^{\mathrm{ab}}/K_v}(L_v^{\mathrm{ab}\times}) \longrightarrow K_v^\times \longrightarrow G_v^{\mathrm{ab}} \longrightarrow 1.$$

We will also encounter the field compositum $\hat{L}_v^{\mathrm{ab}} := \langle\, L_w^{\mathrm{ab}} \,\rangle_{w|v}$; by local class field theory, the field $\hat{L}_v^{\mathrm{ab}}$ corresponds to the subgroup:

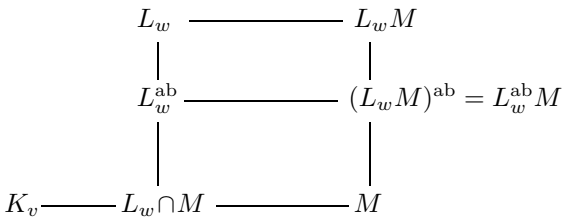
$$\bigcap_{w|v} \mathrm{N}_{L_w/K_v}(L_w^\times) = \bigcap_{w|v} \mathrm{N}_{L_w^{\mathrm{ab}}/K_v}(L_w^{\mathrm{ab}\times}). \qquad \square$$

Let us return to the general situation; we then have the following additional property which can easily be deduced from 1.4 and which we state in a slightly different setting.

1.5.4 Corollary (norm lifting theorem). *Let L/K be a number field extension and for $v \in Pl$, let M/K_v be a finite abelian extension.*
If N is the subgroup of $K_v^\times$ corresponding to M over K_v, then for $w|v$ the subgroup N' of $L_w^\times$ corresponding to L_wM over L_w is:

$$\{y \in L_w^\times,\ \mathrm{N}_{L_w/K_v}(y) \in N\} =: \mathrm{N}^{-1}_{L_w/K_v}(N).$$

Proof. We give the proof using the following diagram:



We have $N' = \mathrm{Ker}((\,\bullet\,, L_wM/L_w))$. Since $(L_wM)^{\mathrm{ab}} = L_w^{\mathrm{ab}}M$, we have the isomorphisms:

$$\mathrm{Gal}(L_w M/L_w) \simeq \mathrm{Gal}(L_w^{\mathrm{ab}} M/L_w^{\mathrm{ab}}) \simeq \mathrm{Gal}(M/L_w \cap M)\ ;$$

it follows that $y \in N'$ if and only if the image of $(y\,,\, L_w M/L_w)$ in $\mathrm{Gal}(M/L_w \cap M)$ is trivial. Using 1.4, (iv) applied to $L_w M/K_v$, the image of $(y\,,\, L_w M/L_w)$ in $\mathrm{Gal}(L_w^{\mathrm{ab}} M/K_v)$, which is an element of $\mathrm{Gal}(L_w^{\mathrm{ab}} M/L_w^{\mathrm{ab}})$, is equal to $(\mathrm{N}_{L_w/K_v}(y)\,,\, L_w^{\mathrm{ab}} M/K_v)$ whose image in $\mathrm{Gal}(M/L_w \cap M)$ is obtained by restriction to M, giving $(\mathrm{N}_{L_w/K_v}(y)\,,\, M/K_v)$ by 1.4, (ii). Since by definition $\mathrm{Ker}((\bullet\,,\, M/K_v)) = N$, we obtain the given formula for N'. □

c) Local Conductors and Norm Groups

Let L/K be an extension of number fields, and let $v \in Pl_0$ and $w \in Pl_{L,v}$. Using 1.4.4, the following definition makes sense.

1.6 Definitions (local conductors). (i) The smallest power $\mathfrak{p}_v^{m_w}$, $m_w \geq 0$, such that:

$$U_v^{m_w} \subseteq \mathrm{N}_{L_w/K_v}(L_w^{\times})$$

(or, equivalently, $U_v^{m_w} \subseteq \mathrm{N}_{L_w/K_v}(U_w)$) is called the norm conductor or conductor of L_w/K_v and is denoted:

$$\mathfrak{f}_{L_w/K_v}.$$

(ii) The conductor of $(L^{\mathrm{ab}})_v/K_v$, the completion of L^{ab}/K at v, is called the norm v-conductor or v-conductor of L/K and denoted:

$$\mathfrak{f}_v := \mathfrak{f}_v(L/K). \qquad \square$$

1.6.1 Remarks. (i) By 1.4, (iii), m_w is the smallest integer m for which we have (using upper numbering):

$$G_w^{\mathrm{ab}\,m} = 1.$$

Since $\mathrm{N}_{L_w/K_v}(L_w^{\times}) = \mathrm{N}_{L_w^{\mathrm{ab}}/K_v}(L_w^{\mathrm{ab}\times})$, we have equality of the conductors of the extensions L_w/K_v and L_w^{ab}/K_v (so that in practice we always are reduced to compute $\mathfrak{f}_{L_w^{\mathrm{ab}}/K_v}$ by using the formula that we will give in 1.6.2).

(ii) By definition, we have $\mathfrak{f}_v(L/K) = \mathfrak{f}_v(L^{\mathrm{ab}}/K)$; in addition $\mathfrak{f}_v(L^{\mathrm{ab}}/K)$ divides the $\mathfrak{f}_{L_w^{\mathrm{ab}}/K_v}$ for $w|v$.

(iii) Local class field theory implies the local conductor theorem which says that v is ramified in L_w^{ab}/K_v if and only if $\mathfrak{f}_{L_w^{\mathrm{ab}}/K_v} \neq 1$ (use 1.4.3, (ii)). Note however that L_w/L_w^{ab} is totally ramified; the conductor is thus equal to 1 if and only if $L_w^{\mathrm{ab}} = L_w^{\mathrm{nr}}$. □

It seems that it would be useful to define a generalized v-conductor $\mathfrak{f}_v[L/K]$ when L/K is any extension; it should be the conductor of L_v^{ab} because of the normic properties that we will see in 2.6 and of Definition 3.1.4 of the generalized norm residue symbol.

In the Galois case, $L_v^{\mathrm{ab}} = L_{w_0}^{\mathrm{ab}}$ for any place $w_0|v$, and $\mathfrak{f}_v[L/K]$ is given by $\mathfrak{f}_{L_{w_0}/K_v}$ (which is then independent of the choice of w_0).

Concerning $\hat{L}_v^{\mathrm{ab}} := \langle\, L_w^{\mathrm{ab}} \,\rangle_{w|v}$ in the general case, we easily check that its conductor is equal to the l.c.m. of the $\mathfrak{f}_{L_w/K_v}$, $w|v$.

We can summarize the above by the following diagram where the corresponding conductors divide each other in the given order:

$$\underset{(1)}{K_v} \text{ ——— } \underset{\mathfrak{f}_v(L/K)}{(L^{\mathrm{ab}})_v} \text{ ——— } \underset{\mathfrak{f}_v[L/K]}{L_v^{\mathrm{ab}}} \text{ ——— } \underset{\mathfrak{f}_{L_w/K_v}}{L_w^{\mathrm{ab}}} \text{ ——— } \underset{\text{l.c.m.}(\mathfrak{f}_{L_w/K_v})}{\hat{L}_v^{\mathrm{ab}}}$$

However, we will not have any use for the generalized v-conductor and in global class field theory, only the $\mathfrak{f}_v$ (the v-conductors for L^{ab}/K) will enter, whose product will define a global conductor.

1.6.2 Remark (conductor computation). For the explicit computation of the conductor $\mathfrak{f}_{L_w/K_v}$, we refer to [d, Se2, Ch. XV, § 2, Cor. 2 to Th. 1, Ch. IV, § 3] from which we deduce the following formula:

$$\mathfrak{f}_{L_w/K_v} = \mathfrak{f}_{L_w^{\mathrm{ab}}/K_v} =: \mathfrak{p}_v^{m_w}, \text{ with } m_w := \frac{1}{g_0^{\mathrm{ab}}} \sum_{\substack{i\geq 0 \\ g_i^{\mathrm{ab}}>1}} g_i^{\mathrm{ab}},$$

where g_i^{ab} is the order of the higher ramification group $G_{w,i}^{\mathrm{ab}}$ (in lower numbering) in L_w^{ab}/K_v; for each $i \geq 1$, $G_{w,i}^{\mathrm{ab}}$ is defined from $G_{w,0}^{\mathrm{ab}}$ (of order $g_0^{\mathrm{ab}} = e_w^{\mathrm{ab}}$) by:

$$G_{w,i}^{\mathrm{ab}} = \{s \in G_{w,0}^{\mathrm{ab}},\ \mathrm{w}((\pi_w^{\mathrm{ab}})^{s-1} - 1) \geq i\},$$

where π_w^{ab} is a uniformizer of L_w^{ab} (see 1.3.1).

If v is tamely ramified in L_w^{ab}/K_v (i.e., if the residue characteristic ℓ of v does not divide e_w^{ab}), we have $G_{w,1}^{\mathrm{ab}} = 1$, hence $m_w = 1$. □

We will assume known this conductor formula since it can be obtained by a direct study of the norm on the groups U_v, as is done in [d, Se2, Ch. V and XV] following Hasse, study which reduces to proving the property of the local reciprocity map assumed in 1.4, (iii). It is nothing but the translation of the lower numbering to the upper numbering for ramification groups when we look for the first trivial $G_w^{\mathrm{ab}\,m}$ (see 1.6, (i)). This is a great advantage since the computation of the higher ramification groups *in lower numbering* is always effective and easy in practice (see the example given below).

We use the same method to compute the v-conductor $\mathfrak{f}_v$ from the groups $(G^{\mathrm{ab}})_{v,i}$, where $(G^{\mathrm{ab}})_v := \mathrm{Gal}((L^{\mathrm{ab}})_v/K_v)$.

As an application, we give the following result for the Kummer case, which illustrates the computation of local conductors from the classical results on higher ramification groups mentioned above.

1.6.3 Proposition (*v*-conductors of a Kummer extension of prime degree p). *Let K be a number field containing the group μ_p of pth roots of unity and let $L = K(\sqrt[p]{\alpha})$, $\alpha \in K^\times \backslash K^{\times p}$. Let v be a finite place of K ramified in L/K. The norm v-conductor of L/K is equal to $\mathfrak{p}_v$ if $v \nmid p$, and to $\mathfrak{p}_v^{pe_v+1-r}$ if $v|p$, where e_v is the ramification index of v in $K/\mathbb{Q}(\mu_p)$ and r is the largest integer for which the congruence:*

$$\frac{\alpha}{x^p} \equiv 1 \bmod \mathfrak{p}_v^r,\ x \in K^\times,$$

has a solution (the case $\mathrm{v}(\alpha) \not\equiv 0 \bmod (p)$ meaning $r = 0$).

Proof. Let $\alpha_v := i_v(\alpha) \in K_v^\times$; then $L_v := K_v(\sqrt[p]{\alpha_v})$ is the completion L_w of L at some place $w|v$, and by definition the conductor of L_v/K_v is equal to $\mathfrak{f}_v$. We set $G_v := \mathrm{Gal}(L_v/K_v)$.

If $v \nmid p$ is ramified (i.e., $\mathrm{v}(\alpha) \not\equiv 0 \bmod (p)$), we have $\mathfrak{f}_v = \mathfrak{p}_v$ (tame ramification). This case follows in fact trivially, directly from Definition 1.6.

Assume now that $v|p$. In this case the formula of 1.6.2 yields $\mathfrak{f}_v = \mathfrak{p}_v^{t+1}$, where t is the largest integer such that $g_t \neq 1$, and we have:

$$t = \mathrm{w}(\pi_w^{\sigma-1} - 1),$$

where π_w is a uniformizer of L_v and σ a generator of G_v.

(i) If $\mathrm{v}(\alpha) \not\equiv 0 \bmod (p)$, we can always assume that $\mathrm{v}(\alpha) = 1$, hence that $\pi_w = \sqrt[p]{\alpha_v}$. We then have $\pi_w^{\sigma-1} - 1 =: \zeta - 1$, where ζ is a generator of μ_p, giving $t = pe_v$. But in this case $r = 0$, proving the result.

(ii) If $\mathrm{v}(\alpha) \equiv 0 \bmod (p)$, we can reduce to the case where $\alpha_v \in U_v$. By I.6.3, (ii), the integer r satisfies:

$$1 \leq r \leq pe_v - 1\ ;$$

changing $\alpha_v \bmod (U_v)^p$ if necessary, we can assume that $\alpha_v \in U_v^r$; then, by definition of r, $\alpha_v(U_v^1)^p$ is disjoint from U_v^{r+1}. Let us write:

$$\sqrt[p]{\alpha_v} := 1 + \pi_w^\rho\, u_w,\ \rho \geq 1,\ u_w \in U_w\ ;$$

this yields:

$$\alpha_v = 1 + \pi_w^{pe_v(p-1)+\rho}\, u'_w + \pi_w^{p\rho}\, u_w^p,\ u'_w \in U_w$$

since $\mathrm{v}(p) = e_v(p-1)$ and v is ramified in L_v/K_v. We must have $\rho < pe_v$, otherwise we would get $r \geq pe_v$, a contradiction. Thus we must have $p\rho < pe_v(p-1) + \rho$, hence $\rho = r$. Writing that $\sigma(\sqrt[p]{\alpha_v}) = \zeta \sqrt[p]{\alpha_v}$ and that $\pi_w^{\sigma-1} = \xi \in U_w^t \backslash U_w^{t+1}$, we obtain:

$$1 + \pi_w^r\, \xi^r\, u_w^\sigma = \zeta(1 + \pi_w^r\, u_w),$$

hence, since $\mathrm{w}(1-\zeta) = pe_v > r$:

$$\mathrm{w}(\xi^r\, u_w^{\sigma-1} - 1) = pe_v - r.$$

Lemma. *We have* $r \not\equiv 0 \bmod (p)$.

Proof. Assume that $r = \lambda p$ and set $\alpha_v =: 1 + \pi_v^{\lambda p}\,\eta_v,\ \eta_v \in U_v$; since $r = \lambda p < pe_v$ we have $\lambda < e_v$. Since F_v is a finite field, there exists $\eta'_v \in U_v$ such that $\eta_v \equiv \eta_v'^p \bmod (\pi_v)$; it is then immediately checked that:

$$\frac{\alpha_v}{(1+\pi_v^{\lambda}\,\eta'_v)^p} \in U_v^{r+1},$$

a contradiction. □

It follows that $\xi^r \in U_w^t \setminus U_w^{t+1}$. But it is clear that $u_w^{\sigma-1} \in U_w^{t+1}$, which yields:

$$\mathrm{w}(\xi^r - 1) = pe_v - r.$$

It follows that $\mathrm{w}(\xi^r - 1) = \mathrm{w}(\xi - 1) = t = pe_v - r$, finishing the computation of the v-conductor in the wild case. □

Note. If $v|p$ and if $\mathrm{v}(\alpha) \not\equiv 0 \bmod (p)$, then $r = 0$ and the v-conductor is maximal; if $\mathrm{v}(\alpha) \equiv 0 \bmod (p)$, we have $1 \le r \le pe_v - 1$, so that $2 \le pe_v + 1 - r \le pe_v$, where the lower bound is in agreement with statement III.1.3.2.

The following result on norm actions can be useful in practice.

1.6.4 Proposition. *Let L_w/K_v be a completion of an arbitrary finite extension L/K of number fields.*
There exists a function ψ_w from $\mathbb{N}$ to $\mathbb{N}$ such that $\mathrm{N}_{L_w/K_v}(U_w^{\psi_w(n)}) = U_v^n$ for all sufficiently large n.
*If in addition L_w/K_v is Galois with Galois group G_w, the above relation holds as soon as $G_{w,\psi_w(n)}$ (the $\psi_w(n)$*th *higher ramification group) is trivial.*

Proof. Referring to [d, Se2], we can sketch the following proof: we use [IV, 3, Rem., 2] which allows us to define ψ_w in complete generality from the Galois case, and using [V, 6, Cor. 3] for norm aspects. It is then clear that if L_w/K_v is unramified, $\mathrm{N}_{L_w/K_v}(U_w^n) = U_v^n$ for all $n \ge 0$ ([V, 2, Prop. 3] or 1.4.3, (ii)); if L_w/K_v is tamely ramified, the above equality holds for all $n \ge 1$ ([XV, 2, Cor. 1 to Th. 1] or once again 1.4.3, (ii)). □

1.6.5 Exercise (norm groups and conductors of quadratic extensions of $\mathbb{Q}_\ell$). Let ℓ be a prime number. If $\ell \neq 2$, since:

$$\mathbb{Q}_\ell^\times = \langle\, \ell \,\rangle \oplus \langle\, \zeta \,\rangle \oplus \langle\, 1+\ell \,\rangle_{\mathbb{Z}_\ell},\ \text{where } \langle\, \zeta \,\rangle = \mu_{\ell-1},$$

Kummer theory shows, through the study of $\mathbb{Q}_\ell^\times/\mathbb{Q}_\ell^{\times\,2}$, that quadratic extensions of $\mathbb{Q}_\ell$ are:

$$\mathbb{Q}_\ell(\sqrt{\zeta}),\ \mathbb{Q}_\ell(\sqrt{\ell}),\ \mathbb{Q}_\ell(\sqrt{\ell\zeta}).$$

If $\ell = 2$, knowing that in this case:

$$\mathbb{Q}_2^\times = \langle\, 2 \,\rangle \oplus \langle\, -1 \,\rangle \oplus \langle\, 5 \,\rangle_{\mathbb{Z}_2},$$

we obtain the following list of quadratic extensions of $\mathbb{Q}_2$:

$$\mathbb{Q}_2(\sqrt{5}\,),\ \mathbb{Q}_2(\sqrt{-1}\,),\ \mathbb{Q}_2(\sqrt{-5}\,),\ \mathbb{Q}_2(\sqrt{2}\,),\ \mathbb{Q}_2(\sqrt{-2}\,),\ \mathbb{Q}_2(\sqrt{10}\,),\ \mathbb{Q}_2(\sqrt{-10}\,).$$

Compute all the norm groups and conductors.

Answer. For $\ell \neq 2$, the subgroups of index 2 of $\mathbb{Q}_\ell^\times$ are the following:

$$\begin{aligned} N_1 &:= \langle\, \ell^2 \,\rangle \oplus \langle\, \zeta \,\rangle \oplus \langle\, 1+\ell \,\rangle_{\mathbb{Z}_\ell}, \\ N_2 &:= \langle\, \ell \,\rangle \oplus \langle\, \zeta^2 \,\rangle \oplus \langle\, 1+\ell \,\rangle_{\mathbb{Z}_\ell}, \\ N_3 &:= \langle\, \ell\zeta \,\rangle \oplus \langle\, \zeta^2 \,\rangle \oplus \langle\, 1+\ell \,\rangle_{\mathbb{Z}_\ell}. \end{aligned}$$

The unique unramified extension $\mathbb{Q}_\ell(\sqrt{\zeta}\,)$ corresponds to N_1 since the residue degree is 2 or the ramification index is 1 using 1.4.3; then, if we denote by N the norm in these quadratic extensions, we have:

$$\mathrm{N}(\sqrt{-\ell}\,) = \ell,\ \mathrm{N}(\sqrt{-\ell\zeta}\,) = \ell\zeta.$$

Thus, it is more natural to write the three quadratic extensions of $\mathbb{Q}_\ell$ in the form:

$$\mathbb{Q}_\ell(\sqrt{\zeta}\,),\ \mathbb{Q}_\ell(\sqrt{-\ell}\,),\ \mathbb{Q}_\ell(\sqrt{-\ell\zeta}\,),$$

in which case they correspond respectively to N_1, N_2, N_3 (conductors (1), (ℓ), and (ℓ) using 1.6). We then have:

$$\mathbb{Q}_\ell(\sqrt{-\ell}\,) = \mathbb{Q}_\ell(\sqrt{\ell}\,) \ \text{ and } \ \mathbb{Q}_\ell(\sqrt{-\ell\zeta}\,) = \mathbb{Q}_\ell(\sqrt{\ell\zeta}\,),$$

if and only if $\ell \equiv 1 \bmod (4)$ (otherwise the extensions on the right hand sides are permuted).

For $\ell = 2$, the norm groups are the following:

$$\begin{aligned} N_1 &:= \langle\, 4 \,\rangle \oplus \langle\, -1 \,\rangle \oplus \langle\, 5 \,\rangle_{\mathbb{Z}_2}, \\ N_2 &:= \langle\, 2 \,\rangle \oplus \langle\, 5 \,\rangle_{\mathbb{Z}_2}, \\ N_3 &:= \langle\, -2 \,\rangle \oplus \langle\, 5 \,\rangle_{\mathbb{Z}_2}, \\ N_4 &:= \langle\, 2 \,\rangle \oplus \langle\, -1 \,\rangle \oplus \langle\, 5^2 \,\rangle_{\mathbb{Z}_2}, \\ N_5 &:= \langle\, 2 \,\rangle \oplus \langle\, -5 \,\rangle_{\mathbb{Z}_2}, \\ N_6 &:= \langle\, 2 \times 5 \,\rangle \oplus \langle\, -1 \,\rangle \oplus \langle\, 5^2 \,\rangle_{\mathbb{Z}_2}, \\ N_7 &:= \langle\, -2 \,\rangle \oplus \langle\, -5 \,\rangle_{\mathbb{Z}_2}. \end{aligned}$$

The unramified extension is $\mathbb{Q}_2(\sqrt{5}\,)$ and corresponds to N_1 (we can also note that $\mathrm{N}(2+\sqrt{5}\,) = -1$ and $\mathrm{N}(5+2\sqrt{5}\,) = 5$). We then have the following computations:

$$\begin{array}{ll}
\mathrm{N}(1+\sqrt{-1}\,)=2, & \mathrm{N}(2+\sqrt{-1}\,)=5,\\
\mathrm{N}(\sqrt{-5}\,)=5, & \mathrm{N}(3+\sqrt{-5}\,)\in -2\mathbb{Q}_2^{\times\,2},\\
\mathrm{N}(\sqrt{2}\,)=-2, & \mathrm{N}(1+\sqrt{2}\,)=-1,\\
\mathrm{N}(\sqrt{-2}\,)=2, & \mathrm{N}(1+\sqrt{-2}\,)\in -5\mathbb{Q}_2^{\times\,2},\\
\mathrm{N}(\sqrt{10}\,)=-10, & \mathrm{N}(3+\sqrt{10}\,)=-1,\\
\mathrm{N}(\sqrt{-10}\,)=10, & \mathrm{N}(2+\sqrt{-10}\,)\in -2\mathbb{Q}_2^{\times\,2};
\end{array}$$

they show that the (ramified) extensions $\mathbb{Q}_2(\sqrt{-1}\,)$, $\mathbb{Q}_2(\sqrt{-5}\,)$, $\mathbb{Q}_2(\sqrt{2}\,)$, $\mathbb{Q}_2(\sqrt{-2}\,)$, $\mathbb{Q}_2(\sqrt{10}\,)$, and $\mathbb{Q}_2(\sqrt{-10}\,)$ correspond respectively to N_2, N_3, N_4, N_5, N_6, N_7 and have as conductors (4), (4), (8), (8), (8), (8). □

1.6.6 Exercise. Let v be a finite place of K and let n be a nonzero integer. Show that $K_v^\times/K_v^{\times n}$ is finite.

Assume that K_v contains the group μ_n of nth roots of unity; compute the norm group N corresponding to $M := K_v\big(\sqrt[n]{K_v^\times}\,\big)$.

Answer. Let p be a prime number and let p^e be the largest power of p dividing n; it is sufficient to show that the p-torsion group $K_v^\times/K_v^{\times p^e}$ is finite. By I.3.1.1, we have $K_v^\times \simeq \mathbb{Z}\oplus\mu_{q_v-1}\oplus\mu_\ell(K_v)\oplus\mathbb{Z}_\ell^{[K_v:\mathbb{Q}_\ell]}$, where ℓ is the residue characteristic of v, and the result follows.

Classical Kummer theory says that M is the maximal abelian extension of exponent n of K_v; but the quotient $K_v^\times/N$ is maximal of exponent n if and only if $N = K_v^{\times n}$.

When $\mu_n \subset K_v^\times$, for each p dividing n we have more precisely:

$$K_v^\times/K_v^{\times p^e} \simeq (\mathbb{Z}/p^e\mathbb{Z})^2 \ \ (\text{resp. } (\mathbb{Z}/p^e\mathbb{Z})^{[K_v:\mathbb{Q}_\ell]+2})$$

if $\ell \neq p$ (resp. $\ell = p$). Without the Kummer hypothesis the norm group $K_v^{\times n}$ still corresponds to the maximal abelian extension of exponent n of K_v (which is not a Kummer extension and cannot be generated by radicals) and the structure of its Galois group is modified (in an explicit way). □

1.6.7 Remark (local Hilbert symbols). One might think that in the Kummer case ($\mu_n \subset K_v$, $M := K_v\big(\sqrt[n]{K_v^\times}\,\big)$) the symbol $(\bullet,\, M/K_v)$ is "easy"; as the long search for explicit formulas shows, this is not the case. If we set for all $x,\ y \in K_v^\times$:

$$(y\,,\, M/K_v)\big(\sqrt[n]{x}\,\big) = (y\,,\, K_v\big(\sqrt[n]{x}\,\big)/K_v)\big(\sqrt[n]{x}\,\big) =: \ (x\,,\, y)_v\,\sqrt[n]{x},$$

we thus define the local Hilbert symbol of order n:[14]

$$(\bullet,\ \bullet)_v : K_v^\times \times K_v^\times \longrightarrow \mu_n$$

whose knowledge is equivalent to that of the norm residue symbol (we will study it in Section 7). In most books, the definition is the *inverse* of the more canonical present one. □

[14] [a, Se1; D, Ch. IV], [d, AT, Ch. 12; Se2, Ch. XIV], [e, Ko3, Ch. 2, § 1].

Note. Since the 1928 original papers of Artin–Hasse, a very large number of contributions (Mills, Hasse, Kneser, Šafarevič, Shiratani, Brückner, Iwasawa, Vostokov, Wiles, Henniart, Sen, Kolyvagin, Coleman, de Shalit, Miki, Jaulent, ...) have given explicit formulas for the local Hilbert symbol and reciprocity laws; these techniques, closely related to the theory of formal groups that we have already mentioned (Lubin–Tate (1965)) (see [f, Lang2, Ch. 9]) are outside the setting studied here. In fact, from a theoretical point of view, all these laws can be expressed in the unified setting of p-adic Galois representations, developed in particular by Fontaine, Messing, ... In this setting, one can say that all the known results on the local Hilbert symbol are contained in the reciprocity law of Bloch and Kato, conjecturally generalized by Perrin-Riou, and independently proved by Benois, Colmez, Kato–Kurihara–Tsuji, ...

1.6.8 Remarks. (i) However, in the regular case, also called by abuse of language the tame case (i.e., when the residue characteristic ℓ of v does not divide n), n is then a divisor of $q_v - 1$, and we have the following simple formula (proved in 7.1.5) for the Hilbert symbol of order n:

$$(x\,,\,y)_v \equiv \left((-1)^{\mathrm{v}(x)\mathrm{v}(y)}\ \frac{x^{\mathrm{v}(y)}}{y^{\mathrm{v}(x)}}\right)^{\frac{q_v-1}{n}} \bmod (\pi_v)\ ;$$

this indeed pinpoints $(x\,,\,y)_v \in \mu_n(K_v)$ since the residue map:

$$\mu_n(K_v) \longrightarrow \mu_n(F_v) = (F_v^\times)^{\frac{q_v-1}{n}}$$

is an isomorphism. When v is a real place at infinity ($K_v = \mathbb{R}$ and $n = 2$), $(x\,,\,y)_v$ is given by the sign of the analogous expression:

$$(x\,,\,y)_v = \mathrm{sgn}((-1)^{\mathrm{v}(x)\mathrm{v}(y)} x^{\mathrm{v}(y)} y^{-\mathrm{v}(x)}) = (-1)^{\mathrm{v}(x)\mathrm{v}(y)}.$$

(ii) In the absolute quadratic case, Exercise 1.6.5 gives the answer in complete generality.

(iii) Finally, we will see, perhaps surprisingly, that to compute explicitly a local Hilbert symbol in the irregular (or wild) case, we can always proceed globally, without knowing any explicit formula; this will be explained together with the statements of global class field theory (see 7.5). □

We will devote Section 7 of this chapter to the more general notion of symbols and their properties; we will see that Hilbert symbols play an important role.

d) Infinite Local Class Field Theory

We will conclude by showing that finite local class field theory contains all information concerning the structure of the abelian closure $\overline{K}_v^{\mathrm{ab}}$ of K_v, for $v \in Pl_0$, and the class field theory correspondence.

1.7 Limiting Procedure. By infinite Galois theory and the local class field theory correspondence, we can relate the topological groups:

$$\mathrm{Gal}(\overline{K}_v^{\mathrm{ab}}/K_v) \simeq \varprojlim_M \mathrm{Gal}(M/K_v),$$

for the set of finite abelian extensions M of K_v, to:

$$\varprojlim_N (K_v^\times/N),$$

where N ranges in the set of subgroups of finite index of $K_v^\times$, and by definition we obtain the profinite completion $\widehat{K_v^\times} := \varprojlim_N (K_v^\times/N)$ of $K_v^\times$. It is easily checked (see 1.6.6) that the subgroups $K_v^{\times n}$ for $n > 0$ form a cofinal subset of the set of subgroups N of finite index, hence that:

$$\widehat{K_v^\times} = \varprojlim_{n\geq 1} (K_v^\times/K_v^{\times n})\ ;$$

since U_v is a profinite group, we immediately obtain (choosing a uniformizer π_v):

$$\widehat{K_v^\times} = \pi_v^{\widehat{\mathbb{Z}}} \bigoplus U_v,$$

where by abuse of notation we have set:

$$\pi_v^{\widehat{\mathbb{Z}}} := \varprojlim_{n\geq 1} (\langle\, \pi_v \,\rangle/\langle\, \pi_v \,\rangle^n) \simeq \varprojlim_{n\geq 1} (\mathbb{Z}/n\mathbb{Z}) = \widehat{\mathbb{Z}},$$

which is legitimate since $\langle\, \pi_v \,\rangle$ has no $\mathbb{Z}$-torsion. Recall that if ℓ is the residue characteristic and q_v the order of the residue field of v, we have:

$$U_v \simeq \mu_{q_v-1} \bigoplus \mu_\ell(K_v) \bigoplus \mathbb{Z}_\ell^{[K_v\,:\,\mathbb{Q}_\ell]}.$$

A fundamental system of neighbourhoods of 1 in the profinite group $\widehat{K_v^\times}$ is given by the $(\widehat{K_v^\times})^n$ for $n > 0$, or by the $\pi_v^{n\widehat{\mathbb{Z}}} \oplus U_v^i$, $n > 0,\ i \geq 0$.

More precisely, properties 1.4, (i), (ii) of the norm residue symbol imply the existence of an isomorphism of inverse systems giving the homeomorphism $\rho_v : \widehat{K_v^\times} \longrightarrow \overline{G}_v^{\mathrm{ab}}$ and showing that there exists an analog to Theorem 1.5 on the correspondence of infinite local class field theory, replacing $K_v^\times$ by $\widehat{K_v^\times}$ and the notion of subgroup of finite index (of $K_v^\times$) by that of *closed* subgroup of $\widehat{K_v^\times}$ because of the infinite Galois theory.

Let us describe this correspondence in a little more detail. Let M be a finite abelian extension of K_v with norm group $N := \mathrm{N}_{M/K_v}(M^\times)$, and consider the local reciprocity exact sequence:

$$1 \longrightarrow N \longrightarrow K_v^\times \xrightarrow{(\bullet, M/K_v)} \mathrm{Gal}(M/K_v) \longrightarrow 1.$$

The norm residue symbol $(\bullet, M/K_v)$ is still continuous for the topology of $K_v^\times$, diagonally embedded in $\widehat{K_v^\times}$, induced by that of $\widehat{K_v^\times}$ as a profinite group (neighbourhoods in $K_v^\times$: the $K_v^{\times n}$, $n > 0$); thus extending by continuity we obtain the exact sequence:

$$1 \longrightarrow \mathrm{adh}(N) \longrightarrow \widehat{K_v^\times} \xrightarrow{(\bullet, M/K_v)} \mathrm{Gal}(M/K_v) \longrightarrow 1,$$

where adh denotes closure in $\widehat{K_v^\times}$ for its topology, and the norm group which now corresponds to M is:

$$\mathrm{adh}(N) := \bigcap_{n>0} \big(N \,.\, (\widehat{K_v^\times})^n\big).$$

This defines in an evident way the local reciprocity map (or norm residue symbol):

$$(\bullet, M/K_v) : \widehat{K_v^\times} \longrightarrow \mathrm{Gal}(M/K_v),$$

for any abelian extension M (finite or not); it is also the composition of ρ_v and of the projection $\overline{G}_v^{\mathrm{ab}} \longrightarrow \mathrm{Gal}(M/K_v)$.

One checks, from the finite case, that the image of U_v (compact) under $(\bullet, M/K_v)$ is the inertia group. To summarize:

1.7.1 Theorem. *There exists a homeomorphism of profinite groups (the infinite local reciprocity map):*

$$\rho_v =: (\bullet, \overline{K}_v/K_v) \ : \ \widehat{K_v^\times} \longrightarrow \overline{G}_v^{\mathrm{ab}} := \mathrm{Gal}(\overline{K}_v^{\mathrm{ab}}/K_v),$$

whose composition with the projection $\overline{G}_v^{\mathrm{ab}} \longrightarrow \mathrm{Gal}(M/K_v)$ *is equal to* $(\bullet, M/K_v)$ *for any abelian extension* M/K_v.

The inertia group $\mathrm{Gal}(\overline{K}_v^{\mathrm{ab}}/\overline{K}_v^{\mathrm{nr}})$ *is the image of* U_v *under* ρ_v, *and the higher ramification groups (in upper numbering) correspond to the* U_v^i, $i \geq 1$.

The image of a uniformizer π_v *under* ρ_v *is a (noncanonical) extension of* $\mathrm{Frob}(\overline{K}_v^{\mathrm{nr}}/K_v)$.

Finally, there exists a bijective correspondence, between the set of abelian extensions of K_v *and the set of closed subgroups of* $\widehat{K_v^\times}$, *which satisfies the Galois properties (i) to (iv) of 1.5.* □

1.8 Norm Groups in Infinite Local Class Field Theory. Note that if M/K_v is infinite, the notation $\mathrm{N}_{M/K_v}(M^\times)$ does not make any sense directly, but since:

$$\mathrm{Gal}(M/K_v) = \varprojlim_{M'} \mathrm{Gal}(M'/K_v),$$

for $K_v \subseteq M' \subseteq M$, M'/K_v finite with norm group N', we have:

$$\mathrm{Gal}(M/K_v) = \varprojlim_{M'} \widehat{K_v^\times}/\mathrm{adh}(N') \simeq \widehat{K_v^\times} \Big/ \bigcap_{M'} \mathrm{adh}(N')$$

(by I.5.5, applied to $A = \widehat{K_v^\times}$ compact and $B = 1$), so that the norm group corresponding to M in $\widehat{K_v^\times}$ can be written:

$$\bigcap_{\substack{M' \subseteq M \\ M'/K_v \text{ finite}}} \mathrm{adh}(\mathrm{N}_{M'/K_v}(M'^\times)).$$

Note also that the usual (locally compact) topology of $K_v^\times$ is absolutely not used here, and is not induced by that of $\widehat{K_v^\times}$ (which is compact); in particular, U_v is not open in $\widehat{K_v^\times}$ since it is not of finite index.

If M (finite or not) corresponds to the norm group N, then M^{nr} still corresponds to the group $U_v\, N$, and its maximal tamely ramified subextension corresponds to $U_v^1\, N$.

We thus easily obtain the structure of the group $\overline{G}_v^{\mathrm{ab}}$ since that of $\widehat{K_v^\times} \simeq \widehat{\mathbb{Z}} \oplus U_v$ is known; we deduce a number of consequences, such as the following result.

1.8.1 Proposition. *Let $v \in Pl_0$. The extension $\overline{K}_v^{\mathrm{ab}}$ is the direct compositum over K_v of $\overline{K}_v^{\mathrm{nr}}$ and of a (nonunique) maximal totally ramified abelian extension of K_v, the extension $\overline{K}_v^{\mathrm{nr}}$ being fixed by the image of U_v under the local reciprocity map, while the maximal totally ramified extension is fixed by that of the subgroup $\pi_v^{\widehat{\mathbb{Z}}}$, where π_v is a uniformizer.* □

1.8.2 Remark. If we want to limit ourselves to the maximal pro-p-subextension $\overline{K}_{v\,(p)}^{\mathrm{ab}}$ of $\overline{K}_v^{\mathrm{ab}}$, p prime, $v \in Pl_0$ of residue characteristic equal to ℓ, we simply note that in terms of p-Sylow subgroups we have:

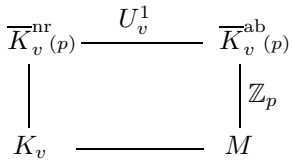
(i) for $p \neq \ell$, $\left(\widehat{K_v^\times}\right)_p \simeq \mathbb{Z}_p \oplus (\mu_{q_v-1})_p$, where $(\mu_{q_v-1})_p \simeq (F_v^\times)_p$ corresponds to the inertia group, giving the following diagram:

$$\begin{array}{ccc} \overline{K}_{v\,(p)}^{\mathrm{nr}} & \overset{(\mu_{q_v-1})_p}{\longrightarrow} & \overline{K}_{v\,(p)}^{\mathrm{ab}} \\ \Big| & & \Big| \mathbb{Z}_p \\ K_v & \longrightarrow & M \end{array}$$

(ii) for $p = \ell$, $\left(\widehat{K_v^\times}\right)_p \simeq \mathbb{Z}_p \oplus U_v^1$, with an inertia group which is, here, isomorphic to:

$$U_v^1 \simeq \mu_p(K_v) \oplus \mathbb{Z}_p^{[K_v\,:\,\mathbb{Q}_p]},$$

which corresponds to the following analogous diagram:



In these two diagrams, the (nonunique) field M defines a maximal totally ramified abelian pro-p-extension of K_v, finite in the case $p \neq \ell$, containing $[K_v : \mathbb{Q}_p]$ independent totally ramified $\mathbb{Z}_p$-extensions in the case $p = \ell$.

In case (i), if p^h is the p-part of $q_v - 1$, K_v contains the group μ_{p^h}, in which case Kummer theory shows that we can choose $M = K_v(\sqrt[p^h]{-\pi_v})$. □

After treating the global case (Ch. III, § 4, (c), (d)), it will be useful to compare the structures of $\overline{K}_v^{\mathrm{ab}}/K_v$ and of $\overline{K}^{\mathrm{ab}}/K$, for instance by checking that for each place v, the decomposition group of v in $\overline{K}^{\mathrm{ab}}/K$ does give a quotient of the Galois group of the abelian closure of K_v. In fact we will obtain the much stronger result that the trivial inclusion $(\overline{K}^{\mathrm{ab}})_v \subseteq \overline{K}_v^{\mathrm{ab}}$ is an equality (Theorem III.4.5, in the direction of the Grunwald–Wang theorem).

1.8.3 Exercise (the case of $\overline{\mathbb{Q}}_\ell^{\mathrm{ab}}$). Assume that $K = \mathbb{Q}$ and that v is finite; we have $K_v = \mathbb{Q}_\ell$, where ℓ is the corresponding residue characteristic. We thus have $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell^{\mathrm{ab}}/\mathbb{Q}_\ell) \simeq \ell^{\widehat{\mathbb{Z}}} \oplus \mathbb{Z}_\ell^\times$.

(i) Show that $\overline{\mathbb{Q}}_\ell^{\mathrm{nr}} = \mathbb{Q}_\ell(\mu')$, where μ' is the group of roots of unity of order prime to ℓ, and that the field M fixed under the image of $\ell^{\widehat{\mathbb{Z}}}$ is equal to $\mathbb{Q}_\ell(\mu_{\ell^\infty})$.

(ii) Assume that $\ell \neq 2$. Since $\mathbb{Q}_\ell$ contains a primitive $(\ell-1)$th root of unity, it is clear that the extension $\mathbb{Q}_\ell(\sqrt[\ell-1]{-\ell})$ of $\mathbb{Q}_\ell$ is abelian. Show that it is equal to $\mathbb{Q}_\ell(\mu_\ell)$, and deduce that there exists in $\mathbb{Q}_\ell(\mu_\ell)$ a uniformizer π (called Dwork's uniformizer) such that $\pi^{\ell-1} = -\ell$.

Answer. (i) The elementary theory of cyclotomic fields over $\mathbb{Q}$ shows that $\mathbb{Q}_\ell(\mu')/\mathbb{Q}_\ell$ is unramified and that $\mathbb{Q}_\ell(\mu_{\ell^\infty})/\mathbb{Q}_\ell$ is totally ramified. Hence we already have that $\mathbb{Q}_\ell(\mu') \subseteq \overline{\mathbb{Q}}_\ell^{\mathrm{nr}}$. If $n \geq 1$ is some integer, we know that the field $\mathbb{Q}_\ell(\mu_{\ell^n-1})$ has degree n (the Frobenius is of order n), which defines the unique unramified extension of degree n of $\mathbb{Q}_\ell$, proving the first result of (i).

The norm group of the field M is $\ell^{\widehat{\mathbb{Z}}}$ and we have $\mathrm{Gal}(M/\mathbb{Q}_\ell) \simeq U_v = \mathbb{Z}_\ell^\times$. Using the cyclotomic polynomials Φ_m, we see that for all $t \geq 1$, $\ell = \Phi_{\ell^t}(1)$ is the norm of $1-\zeta_t$ in $\mathbb{Q}_\ell(\mu_{\ell^t})/\mathbb{Q}_\ell$, where ζ_t generates μ_{ℓ^t}. Thus $\mathbb{Q}_\ell(\mu_{\ell^t}) \subset M$. Let N_t be the norm group of $\mathbb{Q}_\ell(\mu_{\ell^t})$. Since $\mathbb{Q}_\ell(\mu_{\ell^t})/\mathbb{Q}_\ell$ is totally ramified of degree $\ell^{t-1}(\ell-1)$, we have $N_t = \ell^{\mathbb{Z}} \oplus V$ with V of index $\ell^{t-1}(\ell-1)$ in U_ℓ. If $\ell \neq 2$, the only possibility is $V = 1 + \ell^t\mathbb{Z}_\ell$; if $\ell = 2$ and $t \geq 2$, we have $\mathrm{Gal}(L_\ell/\mathbb{Q}_\ell) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{t-2}\mathbb{Z}$ and the only possibility is $V = 1 + 4.2^{t-2}\mathbb{Z}_2$

since V must be contained in the norm group of $\mathbb{Q}(\mu_4)$ which is equal to $2^{\mathbb{Z}} \oplus (1+4\mathbb{Z}_2)$ (using 1.6.5). Thus in all cases we have $N_t = \ell^{\mathbb{Z}} \oplus U_v^t$ and, by 1.8, the norm group of $\mathbb{Q}_\ell(\mu_{\ell^\infty})$ is equal to $\bigcap_t \mathrm{adh}(\ell^{\mathbb{Z}} \oplus U_v^t) = \ell^{\widehat{\mathbb{Z}}}$ proving that $M = \mathbb{Q}_\ell(\mu_{\ell^\infty})$.

Thus, here we have $\overline{\mathbb{Q}}_\ell^{\mathrm{ab}} = \mathbb{Q}_\ell(\mu)$, the field generated by all the roots of unity.

(ii) The norm of $\sqrt[\ell-1]{-\ell}$ in $\mathbb{Q}_\ell(\sqrt[\ell-1]{-\ell})/\mathbb{Q}_\ell$ is equal to ℓ since:

$$\mathrm{Irr}(\sqrt[\ell-1]{-\ell}, \mathbb{Q}_\ell) = X^{\ell-1} + \ell \ ;$$

the norm group of $\mathbb{Q}_\ell(\sqrt[\ell-1]{-\ell})$ thus contains that of M, hence $\mathbb{Q}_\ell(\sqrt[\ell-1]{-\ell}) \subset M$, whence the equality $\mathbb{Q}_\ell(\sqrt[\ell-1]{-\ell}) = \mathbb{Q}_\ell(\mu_\ell)$ (note that $\mathbb{Q}_\ell(\sqrt[\ell-1]{\ell})$ is also totally ramified and abelian over $\mathbb{Q}_\ell$, but is not contained in M). The conclusion is clear.

Note that $1-\zeta_1$ is also a uniformizer, hence $\dfrac{(1-\zeta_1)^{\ell-1}}{-\ell}$ is the $(\ell-1)$th power of a unit of $\mathbb{Q}_\ell(\mu_\ell)$. □

In the case where $K = \mathbb{Q}$, we will be able to compute by global means the local norm residue symbol for abelian extensions of the completions of $\mathbb{Q}$ (see Exercise 3.4.3).

1.9 Exercise (Abhyankar's lemma). Let M_1 and M_2 be finite extensions of a nonarchimedean local field k. Assume that M_2/k is tamely ramified (i.e., $e(M_2/k)$ is not divisible by the residue characteristic of k) and that $e(M_2/k)$ divides $e(M_1/k)$. Show that $M_1 M_2/M_1$ is unramified.

Answer. See [Cor1, Th. 3] for the use of this result, and more generally [d, Lang1, Ch. II, § 5] for the study of not necessarily Galois tamely ramified extensions. □

§2 Idèle Groups in an Extension L/K

Let L/K be a finite extension of number fields. We use the local notations of Section 1 (in particular of 1.1); if L/K (resp. L_w/K_v for $w \in Pl_{L,v}$) is Galois, we set $G := \mathrm{Gal}(L/K)$ (resp. $G_w := \mathrm{Gal}(L_w/K_v)$) and we introduce the decomposition group D_w of w in L/K.

a) Canonical Injection of C_K in C_L

Let J_K and J_L be the respective idèle groups of K and L. For $v \in Pl_K$, recall the relations between the different embeddings of K and L in the corresponding components $K_v^\times$ and $\bigoplus_{w|v} L_w^\times$ of J_K and J_L. The embedding:

$$i_v \ : \ K \longrightarrow K_v$$

comes from the choice of a conjugate K_v of the v-completion of K; for all $w \,|\, v$, L_w is defined in a similar way as an extension of K_v; the embedding:

$$i_w \ : \ L \longrightarrow L_w$$

is then an extension of i_v, such that the family $(i_w)_{w|v}$ is a complete set of representatives of the classes of $\mathbb{Q}$-embeddings of L in $\overline{K}_v$ extending i_v.

It is convenient to consider J_K as a subgroup of J_L using the diagonal embedding $j_{L/K} : J_K \longrightarrow J_L$ for which the image of $\boldsymbol{x} =: (x_v)_v \in J_K$ is given by $(x_w)_w$, with $x_w = x_v$ for all $w \,|\, v$. This map is injective. Similarly:

2.1 Proposition. *The canonical map $j_{L/K} : C_K \longrightarrow C_L$, induced by $J_K \longrightarrow J_L$, is injective.*

Proof. Let $\boldsymbol{x} =: (x_v)_v \in J_K$ be an idèle such that $j_{L/K}(\boldsymbol{x}) = i_L(y)$ for $y \in L^\times$, and let v be a fixed place of K; we thus have:

$$i_w(y) = x_v \ \text{ for all } w|v.$$

This implies that all the K-conjugates of y are equal (seen in $\overline{K} \subset \overline{K}_v$, these conjugates are the $\tau_w \circ i_w(y) = \tau_w(x_v) = x_v$ for the $w|v$ and the K_v-isomorphisms τ_w of L_w); thus there is only one, so $y \in K^\times$, proving the result. □

Note. If we only have, for a single place v of K, $(x_v)_{w|v} = (i_w(y))_{w|v}$ for an $x_v \in K_v$ and an $y \in L^\times$, this yields $y \in K^\times$.

2.1.1 Remarks. (i) This property leads to a simple definition of the idèle class group of an infinite algebraic extension L/K by taking the direct limit of the $C_{L'}$ for $L' \subset L$, L'/K finite.

(ii) We will see later that the corresponding map $C_K/D_K \longrightarrow C_L/D_L$, which class field theory identifies with the transfer map $\overline{G}_K^{\mathrm{ab}} \longrightarrow \overline{G}_L^{\mathrm{ab}}$ (for L/K finite), has a kernel isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{r_1^{\mathrm{c}}}$, where r_1^{c} is the number of real places of K totally complexified in L/K. □

b) Relations Between Local and Global Norms

Let L/K be an arbitrary finite extension, $\mathrm{N}_{L/K}$ the norm in L/K, and fix a place v of K. For $y \in L^\times$, we have, giving in detail the computations:

$$i_v(\mathrm{N}_{L/K}(y)) = \prod_\sigma \sigma(y)$$

(where σ ranges in the set of $\mathbb{Q}$-embeddings of L which extend i_v)

$$= \prod_{w|v} \prod_{\tau_w} \tau_w \circ i_w(y)$$

(where τ_w ranges in the set of K_v-isomorphisms of L_w)

$$= \prod_{w|v} \mathrm{N}_{L_w/K_v}(i_w(y)),$$

which can be summarized as follows.

2.2 Proposition. *For any place v of K we have:*

$$i_v(\mathrm{N}_{L/K}(y)) = \prod_{w|v} \mathrm{N}_{L_w/K_v}(i_w(y)) \quad \text{for all } y \in L^\times. \qquad \square$$

By abuse of notation, this formula is in general written:

$$\mathrm{N}_{L/K}(y) = \prod_{w|v} \mathrm{N}_{L_w/K_v}(y),$$

by saying that, for each place v of K, "the global norm of y is equal to the product of its local norms above v".

This can be reinterpreted as the commutativity of the following diagram.

$$\begin{array}{ccc} L^\times & \xhookrightarrow{\bigoplus_{w|v} i_w} & \bigoplus_{w|v} L_w^\times \\ \Big\downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \Big\downarrow{\scriptstyle \prod_{w|v} \mathrm{N}_{L_w/K_v}} \\ K^\times & \xhookrightarrow{i_v} & K_v^\times \end{array}$$

Fig. 2.1

From this we obtain a canonical definition of the norm in L/K of an idèle $\boldsymbol{y} \in J_L$.

2.2.1 Definition. Let $\boldsymbol{y} =: (y_w)_w \in J_L$, we set:

$$\mathrm{N}_{L/K}(\boldsymbol{y}) := \Big(\prod_{w|v} \mathrm{N}_{L_w/K_v}(y_w) \Big)_v. \qquad \square$$

This norm map indeed extends that defined on $L^\times$ thanks to the above commutative diagram. Taking quotients, we also define:

$$\mathrm{N}_{L/K} \ : \ C_L = J_L/L^\times \longrightarrow C_K = J_K/K^\times.$$

c) Galois Structure of J_L: Semi-Local Theory

When L/K is Galois with Galois group G, it is necessary to put on J_L a G-module structure compatible (algebraically and topologically) with that of the diagonal embedding of $L^\times$ in J_L. For this, it is sufficient to define explicitly the operation of G on the semi-local factor (seen as a K_v-algebra):

$$\bigoplus_{w|v} L_w, \quad v \in Pl_K,$$

operation which we will then restrict to $\bigoplus_{w|v} L_w^\times$. Thus, it must be such that the diagonal embedding:

$$(i_w)_{w|v} : L \longrightarrow \bigoplus_{w|v} L_w$$

is a G-module homomorphism, is continuous for the v-topology of a K-algebra on L, i.e., $L \simeq K^{[L:K]}$ with the product of the topologies induced by $|\bullet|_v$ on K. Thus, by density of $((i_w)_{w|v})(L)$ in $\bigoplus_{w|v} L_w$ (chinese remainder Theorem I.4.3), this defines it uniquely. From this remark we can give the following more precise algorithmic proof. For another direct proof, see 2.3.4, (i).

2.3 Existence and Definition of the Galois Action. Let $w_0 \in Pl_{L,v}$ fixed. Sometimes, by abuse of notation, we consider L_{w_0} as a subspace of $\bigoplus_{w|v} L_w$.[15] Therefore, it will be sufficient to know the action of G on such a subspace L_{w_0}. Let V_{w_0} be a neighbourhood of 0 in L for w_0; for each $s \in G$, sV_{w_0} is an analogous neighbourhood for sw_0, which we can denote V_{sw_0}; this defines V_w for each $w|v$ since G acts transitively on $Pl_{L,v}$. The approximation theorem means that $i_{w_0}\Big(\bigcap_{w\neq w_0} V_w\Big)$ is dense in the field L_{w_0} for every V_{w_0}, and that the closure of $((i_w)_{w|v})\Big(\bigcap_{w\neq w_0} V_w\Big)$ in $\bigoplus_{w|v} L_w$ is of the form $L_{w_0} \oplus V$, where V is a neighbourhood of 0 in $\bigoplus_{w\neq w_0} L_w$.

Note. When v is finite we can for instance take $\bigcap_{w\neq w_0} V_w = \prod_{w\neq w_0} \mathfrak{p}_w^m$ for m as large as we like, hence $V = \bigoplus_{w\neq w_0} (\pi_w)^m$ since $i_w(\mathfrak{p}_w) = (\pi_w)$, where $\pi_w = \pi$ is a suitable element (independent of $w|v$) of the maximal ideal of $\mathbb{C}_\ell$.

Furthermore, if $s \in G$ we have $s\Big(\bigcap_{w\neq w_0} V_w\Big) = \bigcap_{w\neq w_0} (sV_w) = \bigcap_{w\neq sw_0} V_w$, which, by going to the limit, easily gives the definition of the action of G which in particular is such that (in terms of subspaces of $\bigoplus_{w|v} L_w$):

[15] It is important to distinguish between the two sets since an approximation of $y \in L_{w_0}$ by an element of $L^\times$ may be very different from an approximation of $(y, 0, \ldots, 0)$, but the context will be clear.

$$s.L_{w_0} = L_{sw_0} \text{ for all } s \in G.$$

Hence, for all $s \in G$ we obtain a continuous K_v-isomorphism s_{w_0} depending on w_0, still denoted s by abuse of notation:

$$s : L_{w_0} \longrightarrow L_{sw_0},$$

which defines an element of $G_{w_0} = \mathrm{Gal}(L_{w_0}/K_v)$ if and only if $s \in D_{w_0}$ (in this case, we recover the canonical isomorphism $D_{w_0} \simeq G_{w_0}$ of I.2.5).

2.3.1 Exercise. (i) Check that for all $y_0 \in L_{w_0}$:

$$s\,(y_0, 0, \ldots, 0) = (0, \ldots, \tau(y_0), \ldots, 0)$$

(as element of the subspace L_{sw_0}), where $\tau \in \mathrm{Gal}(L_{sw_0}/K_v)$ is the extension by continuity of:

$$i_{sw_0} \circ s \circ i_{w_0}^{-1} \text{ on } i_{w_0}(L)$$

(i.e., if $z \in L$ is such that $i_{w_0}(z)$ is an approximation of y_0 in the field L_{w_0}, then $\tau(i_{w_0}(z)) = i_{sw_0}(s(z))$ is an approximation of $s(y_0)$ in L_{sw_0}).

(ii) Apply this (for $K = \mathbb{Q}$) to the fields $L = \mathbb{Q}(\sqrt{2}, \sqrt{5}\,)$ and $L = \mathbb{Q}(\sqrt{2+\sqrt{2}}\,)$ for the residue characteristic $\ell = 7$, and compute the action of G on $(\sqrt{3}, 0)$ and $(\sqrt{2}, 0)$ in each case.

(iii) Check the formula $s_{s'w_0} \circ s'_{w_0} = (ss')_{w_0}$, for any $s,\ s' \in G$.

Answer. Let $y \in L^\times$ such that:

$$\begin{aligned} y &\equiv z \bmod \mathfrak{p}_{w_0}^n, \\ y &\equiv 0 \bmod \mathfrak{p}_w^n \ \ \forall w \neq w_0, \end{aligned}$$

where $i_{w_0}(z) \equiv y_0 \bmod \pi_{w_0}^n$ in L_{w_0}; thus we have:

$$\begin{aligned} s(y) &\equiv s(z) \bmod \mathfrak{p}_{sw_0}^n, \\ s(y) &\equiv 0 \bmod \mathfrak{p}_{w'}^n \ \ \forall w' \neq sw_0. \end{aligned}$$

Since the embedding of y is an approximation of $(y_0, 0, \ldots, 0)$, an approximation of $s(y_0, 0, \ldots, 0)$ is given by the embedding of $s(y)$, which clearly is close to $(0, \ldots, i_{sw_0}(s(z)), \ldots, 0)$. The case of infinite places is similar.

Points (ii) and (iii) are left to the reader. □

We deduce from all the above the following explicit result (semi-local theory) stated in terms of representations.

2.3.2 Theorem. *Let L/K be Galois with Galois group G.*
For any place v of K, the K_v-representation $\bigoplus_{w|v} L_w$ of G is induced by the representation of the decomposition group D_{w_0} of $w_0|v$ defined by L_{w_0}.

Thus it is the regular representation of G.

Proof. Since G acts transitively on $Pl_{L,v}$, we have $\bigoplus_{w|v} L_w = \sum_{s\in G} L_{sw_0} = \bigoplus_{\overline{s}\in G/D_{w_0}} L_{\overline{s}w_0} = \bigoplus_{\overline{s}\in G/D_{w_0}} \overline{s}.L_{w_0}$, giving $\bigoplus_{w|v} L_w$ as induced representation. The representation L_{w_0}, of $D_{w_0} \simeq G_{w_0}$, is the regular one (normal basis theorem for L_{w_0}/K_v); the uniqueness of the induced representation yields the result by [Se4, § 3.3 or § 7.1]. □

2.3.3 Corollary. *The action of $s \in G$ on an $\boldsymbol{y} =: (y_w)_{w|v} \in \bigoplus_{w|v} L_w$, is such that $(s.\boldsymbol{y})_{sw} = s(y_w)$ for all $w|v$, where by abuse in the second member $s := s_w : L_w \longrightarrow L_{sw}$ is also the K_v-isomorphism defined above.* □

2.3.4 Remarks. (i) Since we also have $\bigoplus_{w|v} L_w \simeq L \otimes_K K_v$, in this context the G-module action is defined by $s\,.\,(x \otimes a) = (s\,.\,x) \otimes a$ for all $s \in G$, $x \in L$, and $a \in K_v$, giving again 2.3.2 (normal basis theorem for L/K); writing this explicitly as in (Ch. I, § 2), we would recover the above results.

(ii) Finally, if we introduce the algebraic norm $\nu_{L/K} := \sum_{s\in G} s$, we have on J_L the relation $j_{L/K} \circ \mathrm{N}_{L/K} = \nu_{L/K}$. □

Note. In the non-Galois case, we would have, on J_L, $j_{L/K} \circ \mathrm{N}_{L/K} = \sum_i \tau_i$, where the τ_i are the isomorphisms $J_L \longrightarrow J_{\sigma_i L}$ corresponding to the $[L : K]$ K-isomorphisms σ_i of L in $\mathbb{C}_\ell$ by density. In other words, on the local factor L_w, τ_i is the extension by continuity of $i_{\sigma_i w} \circ \sigma_i \circ i_w^{-1}$ on $i_w(L)$.

2.4 Proposition. *Let L/K be a finite Galois extension, and put $G = \mathrm{Gal}(L/K)$. Then $J_L^G = j_{L/K}(J_K)$, $H^1(G, J_L) = 1$, and $C_L^G = j_{L/K}(C_K)$.*

Proof. Consider the following more general situation. Let G be a *finite* group and H a subgroup of G. Let A be a G-module and B a sub-H-module of A (considered as a H-module). For $\overline{s} \in G/H$, $B_{\overline{s}} := \overline{s}.B := s.B$ does not depend on the choice of the representative $s \in \overline{s}$. Suppose that $A = \bigoplus_{\overline{s}\in G/H} B_{\overline{s}}$ (in other words, the G-module A is induced by the H-module B); then, for the usual cohomology H^r, $r \geq 0$, as well as for Tate's modified cohomology $\widehat{H}^r$, $r \in \mathbb{Z}$, we have (Shapiro's lemma):

$$H^r(G, A) \overset{\text{can}}{\simeq} H^r(H, B). \ [16]$$

[16] See [d, CF, Ch. VII, § 7, Prop. 7.2]; for the most general situation of Shapiro's lemma concerning the links between cohomology and representation theory, see [g, NSW, Ch. I, § 6, Prop. 1.6.3 and Rem.].

For example, this is the case for the regular representation $A = \bigoplus_{w|v} L_w$ of $G = \mathrm{Gal}(L/K)$, with $B = L_{w_0} \times \{0\} \times \cdots \times \{0\}$, $H = D_{w_0}$ for any $w_0|v$, hence for the modules $A = \bigoplus_{w|v} L_w^\times$ or $\bigoplus_{w|v} U_w$, with $B = L_{w_0}^\times \times \{1\} \times \cdots \times \{1\}$ or $U_{w_0} \times \{1\} \times \cdots \times \{1\}$ (review the definitions to see that the action of D_{w_0} on B becomes the natural one of G_{w_0} on L_{w_0} under the isomorphism $D_{w_0} \simeq G_{w_0}$).

We thus have $J_L^G = j_{L/K}(J_K)$ because of 2.3.2.

Using the fact that $J_L = \varinjlim_{\Sigma} U_L^{\Sigma'}$, $\Sigma \subset Pl^{\mathrm{nc}}$ finite containing the ramified places (where Σ' is the set of places of L above those of Σ), and the fact that the cohomology of finite groups commutes with direct limits, the proof of $H^1(G, J_L) = 1$ follows from the identity $H^r\Big(G, \prod_{i\in I} A_i\Big) \simeq \prod_{i\in I} H^r(G, A_i)$ for all $r \geq 0$ (here with "A_i" $= \bigoplus_{w|v} L_w^\times$ or $\bigoplus_{w|v} U_w$, and $r = 1$), from Shapiro's lemma, then from the Theorem 90;[17] see also [d, CF, Ch. VII, Prop. 7.3].

The proof of $C_L^G = j_{L/K}(C_K)$ then uses the cohomology exact sequence $1 \to L^{\times G} \xrightarrow{i} J_L^G \longrightarrow C_L^G \longrightarrow H^1(G, L^\times) = 1$ and 2.1. □

2.4.1 Remarks. Let G be a finite group, and A a G-module.

(i) We recall that $\widehat{H}^{-r-1} := \widehat{H}_r$, for $r \geq 0$, in the context of Tate's modified cohomology, and that we have:

$$H^0(G, A) = A^G, \qquad \widehat{H}^0(G, A) = A^G/\nu A,$$
$$H_0(G, A) = A/I_G A, \quad \widehat{H}_0(G, A) = {}_\nu A/I_G A,$$

where $\nu := \nu_G := \sum_{s\in G} s$, and where I_G is the augmentation ideal of G.

(ii) Recall also that we have the canonical isomorphisms:

$$\widehat{H}^r(G, A)^* \simeq \widehat{H}^{-r-1}(G, A^*), \quad r \in \mathbb{Z},$$
$$H_0(G, A)^* \simeq H^0(G, A^*),$$
$$\widehat{H}^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}\,(G, \mathbb{Q}/\mathbb{Z}) =: G^{\mathrm{ab}\,*},$$
$$\widehat{H}_1(G, \mathbb{Z}) \simeq I_G/I_G^2,$$

where * (see I.5.7) is the usual duality for abelian groups X (i.e., $X^* := \mathrm{Hom}(X, \mathbb{Q}/\mathbb{Z})$),[18] and where $G^{\mathrm{ab}} := G/[G, G]$.

(iii) For instance, the case $r = -2$, $A = \mathbb{Z}$ (with $\mathbb{Z}^* = \mathbb{Q}/\mathbb{Z}$), gives the canonical isomorphism $I_G/I_G^2 \simeq G^{\mathrm{ab}}$. □

[17] We have $H^1(D_{w_0}, U_{w_0}) = 1$ in the unramified case, because π_v is a uniformizer of L_{w_0}, which yields ${}_\nu U_{w_0} \subseteq {}_\nu L_{w_0}^\times = (L_{w_0}^\times)^{1-\sigma} = U_{w_0}^{1-\sigma}$ for a generator σ of D_{w_0}.

[18] [g, NSW, Ch. III, § 1, Prop. 3.1.1].

We would thus have all the necessary tools to start the computation of the cohomology of idèle groups and of idèle class groups, as developed by Hochschild, Nakayama, and Weil, then by Tate [19], which leads to the cohomological statement of class field theory, which is probably its most intrinsic form (hence the most generalizable), but which does not allow the explicit description of the arithmetic invariants which are involved (see 3.2 for some insights about these cohomological aspects).

d) Local Norm Groups — The Non-Galois Case

We come back to the situation of an arbitrary finite extension L/K, and we will lay the groundwork for a fundamental local to global principle, that which corresponds to the norm in L/K.

2.5 Local Norm Groups — General Definitions. (i) We say that $x \in K^\times$ is a local norm at $v \in Pl$ for L/K if:

$$i_v(x) \in \mathrm{N}_{L/K}\Big(\bigoplus_{w|v} L_w^\times\Big),$$

which is equivalent to the existence of elements $y_w \in L_w^\times$ such that:

$$i_v(x) = \prod_{w|v} \mathrm{N}_{L_w/K_v}(y_w).$$ [20]

(ii) We say that $x \in K^\times$ is a local norm everywhere for L/K if x is a local norm at v for L/K for every place v.

2.5.1 Remark. It follows from 1.5.3 that x is a local norm at v for L/K if and only if:

$$i_v(x) \in \mathrm{N}_{L_v^{\mathrm{ab}}/K_v}(L_v^{\mathrm{ab}\times}),$$

with $L_v^{\mathrm{ab}} = \bigcap_{w|v} L_w^{\mathrm{ab}}$. In practice the field L_v^{ab} has in general a small degree and we can search directly whether or not $i_v(x) \in \mathrm{N}_{L_v^{\mathrm{ab}}/K_v}(L_v^{\mathrm{ab}\times})$. Of course a sufficient condition is that $i_v(x)$ must be a norm in a local extension L_{w_0}/K_v for some $w_0|v$ (which is the case if for example $L_{w_0}^{\mathrm{ab}} = K_v$).

As for the notion of v-conductor, we will also have to distinguish between the local norm group at v for L/K and the local norm group at v for L^{ab}/K, the former being the group $i_v^{-1}(\mathrm{N}_{L_v^{\mathrm{ab}}/K_v}(L_v^{\mathrm{ab}\times}))$, contained in the latter $i_v^{-1}(\mathrm{N}_{(L^{\mathrm{ab}})_v/K_v}((L^{\mathrm{ab}})_v^\times))$. □

[19] See [h, HN; We2; Che3], [d, CF, Ch. VII; Iy1, Ch. IV; Se2, Ch. XI], [e, Ko3, Ch. 2], [g, NSW, Ch. VIII, § 1]; see also the formalism developed in [f, Neu2].

[20] This formula shows, by approximation in L and the use of 1.4.4, that x is a local norm at v if and only if it is arbitrary close, at v, to a global norm.

2.5.2 Proposition. *The subgroup of elements of $K^\times$ which are local norms everywhere for L/K is equal to:*

$$\{x \in K^\times,\ i(x) \in \mathrm{N}_{L/K}(J_L)\}.$$

Proof. One inclusion is trivial and the other comes from the fact that, apart from the places v which are ramified in all the extensions L_w/K_v for $w|v$, and those for which $\mathrm{v}(x) \neq 0$, we have $i_v(x) \in \mathrm{N}_{L_{w_0}/K_v}(U_{w_0})$, where $w_0|v$ is unramified (see 1.4.3, (ii)), hence $i_v(x) = \mathrm{N}_{L_{w_0}/K_v}(u_0) \in \mathrm{N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big)$, completing $u_0 \in U_{w_0}$ outside w_0 by components equal to 1. We can thus obtain $i(x)$ as the norm of an idèle of L. □

Because of this fact it is not necessary to give specific notations for the local norm groups and in particular the subgroups of elements of $K^\times$ which are local norms everywhere for L/K is denoted *by abuse of notation*:

$$K^\times \cap \mathrm{N}_{L/K}(J_L)$$

(instead of $i^{-1}(i(K^\times) \cap \mathrm{N}_{L/K}(J_L))$). In the same way:

$$K^\times \cap \mathrm{N}_{L/K}\Big(\bigoplus_{w|v} L_w^\times\Big),$$

denotes the local norm group at v for L/K.

2.5.3 Remarks. (i) It is clear that any $x \in K^\times$ is a local norm almost everywhere for L/K.

(ii) More generally, we could say that x is a local norm at $w|v$ for L/K when $i_v(x) \in \mathrm{N}_{L_w/K_v}(L_w^\times)$, but in the non-Galois case this depends on the choice of w and does not have the desired meaning (it is the same problem as that of local conductors defined in 1.6 since we want to define local notions attached only to the places v of the base field K). For instance, if $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$, -1 is a local norm at the real place w above $v = \infty$ (trivial since $L_w = K_v = \mathbb{R}$) but not at the complex place w' ($L_{w'} = \mathbb{C}$, $K_v = \mathbb{R}$); however -1 is a local norm at v, and *must be* since -1 is here a global norm:

$$-1 = \mathrm{N}_{L/\mathbb{Q}}(-1) = \mathrm{N}_{L/\mathbb{Q}}(1 - \sqrt[3]{2}) = \cdots$$

Still in $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, we have a similar example with $5 = \mathrm{N}_{L/\mathbb{Q}}\Big(\dfrac{5}{3 - \sqrt[3]{2}}\Big)$ which is a local norm at $w|5$ such that $L_w = \mathbb{Q}_5$ but not at the place w' such that $L_{w'} = \mathbb{Q}_5(j)$. In these two examples we have $L_v^{\mathrm{ab}} = K_v$.

In other words, the idea of a local norm is attached to the formula of Subsection (b):

$$\text{“}\, i_v(\mathrm{N}_{L/K}(y)) = \prod_{w|v} \mathrm{N}_{L_w/K_v}(i_w(y))\,\text{”},$$

which suggests a necessary condition to have $x = \mathrm{N}_{L/K}(y)$. Indeed, the local-global principle attached to the norm for the extension L/K is the fact (true or not) that $x \in K^\times$ is a norm for L/K (i.e., $x =: \mathrm{N}_{L/K}(y)$ for $y \in L^\times$) if and only if x is a local norm everywhere for L/K; the least one can ask is that the trivial direction be true. □

2.5.4 Corollary (Galois case). *Assume that L/K is Galois and, for $v \in Pl$, consider the semi-local factor $\bigoplus_{w|v} L_w^\times$. Since the L_w for $w|v$ are equal, we have $L_v^{\mathrm{ab}} = L_{w_0}^{\mathrm{ab}}$ for $w_0|v$ arbitrarily fixed, and we obtain:*

$$\mathrm{N}_{L/K}\Big(\bigoplus_{w|v} L_w^\times\Big) = \mathrm{N}_{L_{w_0}/K_v}(L_{w_0}^\times) = \mathrm{N}_{L_{w_0}^{\mathrm{ab}}/K_v}(L_{w_0}^{\mathrm{ab}\times}),$$

$$\mathrm{N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big) = \mathrm{N}_{L_{w_0}/K_v}(U_{w_0}) = \mathrm{N}_{L_{w_0}^{\mathrm{ab}}/K_v}(U_{L_{w_0}^{\mathrm{ab}}}).$$

Hence, $x \in K^\times$ is a local norm at v for L/K if and only if, for some arbitrary $w_0|v$, there exists $y_{w_0} \in L_{w_0}^{\mathrm{ab}\times}$ such that:

$$i_v(x) = \mathrm{N}_{L_{w_0}^{\mathrm{ab}}/K_v}(y_{w_0}).$$

If $\mathrm{v}(x) = 0$, then x is a local norm at v if and only if $i_v(x)$ is a local norm of local units, in other words:

$$i_v(x) \in \mathrm{N}_{L_{w_0}^{\mathrm{ab}}/K_v}(U_{L_{w_0}^{\mathrm{ab}}}).$$ □

Once again, $L_{w_0}^{\mathrm{ab}}$ can strictly contain the completion $(L^{\mathrm{ab}})_v$ of L^{ab}.

For questions concerning local norms of local units in the *non-Galois* case, the intersection and the compositum of the fields L_w^{ab} (for $w|v$) play a fundamental role, and the above discussion is not valid; hence it is necessary to study the following subsection whose results (apparently not in the literature) will be used later in genus theory (Ch. IV, § 4).

2.6 Local Norm Invariants for Non-Galois Extensions. Let L/K be an arbitrary finite extension. For $v \in Pl$, let L_w be the completions of L for $w|v$; denote by L_v^{ab} (resp. by $\hat{L}_v^{\mathrm{ab}}$) the intersection (resp. the compositum) of the L_w^{ab} for $w|v$. To ease notations, we set:

$$N_w := \mathrm{N}_{L_w/K_v}(L_w^\times),\ V_w := \mathrm{N}_{L_w/K_v}(U_w)\ ;$$

then we get:

$$\mathrm{N}_{L/K}\Big(\bigoplus_{w|v} L_w^\times\Big) = \langle\, N_w \,\rangle_{w|v},\ \mathrm{N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big) = \langle\, V_w \,\rangle_{w|v}.$$

2.6.1 Lemma 1. *We have $(K_v^\times : \langle\, N_w \,\rangle_{w|v}) = [L_v^{\mathrm{ab}} : K_v] = e_v^{\mathrm{ab}} f_v^{\mathrm{ab}}$, where e_v^{ab} and f_v^{ab} are the ramification index and the residue degree of the extension L_v^{ab}/K_v, repectively, and we have $(U_v : U_v \cap \langle\, N_w \,\rangle_{w|v}) = e_v^{\mathrm{ab}}$.* □

Denote by $G^0(M/M') := (\mathrm{Gal}(M/M'))^0$ the inertia group of v in M/M', where M and M' are abelian extensions of K_v such that $M' \subseteq M$.

2.6.2 Lemma 2. *We have the following canonical isomorphisms:*

$$G^0(L_{w_0}^{\mathrm{ab}}/K_v) \simeq U_v/V_{w_0} \text{ for any } w_0|v,$$
$$G^0(\hat{L}_v^{\mathrm{ab}}/K_v) \simeq U_v \Big/ \bigcap_{w|v} V_w,$$
$$G^0(\hat{L}_v^{\mathrm{ab}}/L_{w_0}^{\mathrm{ab}}) \simeq V_{w_0} \Big/ \bigcap_{w|v} V_w \text{ for any } w_0|v. \qquad \square$$

2.6.3 Proposition. *Let $\check{L}_v^{\mathrm{ab}}$ be the subfield of $\hat{L}_v^{\mathrm{ab}}$ fixed under the subgroup of $\mathrm{Gal}(\hat{L}_v^{\mathrm{ab}}/K_v)$ generated by the $G^0(\hat{L}_v^{\mathrm{ab}}/L_w^{\mathrm{ab}})$ for $w|v$, and let $\check{e}_v^{\mathrm{ab}}$ be the ramification index of $\check{L}_v^{\mathrm{ab}}/K_v$.*
We have the canonical isomorphism:

$$G^0(\check{L}_v^{\mathrm{ab}}/K_v) \simeq U_v \Big/ \mathrm{N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big),$$

and therefore the formula $\Big(U_v : \mathrm{N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big)\Big) = \check{e}_v^{\mathrm{ab}}$. In other words:

$$(U_K^{\mathrm{res}} : \mathrm{N}_{L/K}(U_L^{\mathrm{res}})) = \prod_{v \in Pl_0} \check{e}_v^{\mathrm{ab}}. \qquad \square$$

2.6.4 Proposition. *The number $\check{e}_v^{\mathrm{ab}}$ is a multiple of e_v^{ab} and these indices are equal when the L_w^{ab} for $w|v$ are all equal (for instance in the Galois case).* $\square$

Proof of the statements. The results 2.6.1 and 2.6.2 are proved by giving systematically the norm groups corresponding to the abelian extensions under study and their inertia subfields, and by using properties 1.5 of the correspondence of local class field theory (if N is the norm group corresponding to the abelian extension M of K_v, by 1.4, (iii), the group corresponding to the inertia field of M is equal to $U_v N$). If, to simplify notations we set:

$$N_v := \langle\, N_w \,\rangle_{w|v},\ \hat{N}_v := \bigcap_{w|v} N_w,\ V_v := \langle\, V_w \,\rangle_{w|v},\ \hat{V}_v := \bigcap_{w|v} V_w,$$

we obtain more precisely the following list:

FIELDS	CORRESPONDING NORM GROUPS	
K_v	$K_v^\times$	$K_v^\times$
L_w^{ab}	N_w	$U_v N_w$
L_v^{ab}	N_v	$U_v N_v$
$\hat{L}_v^{\mathrm{ab}}$	$\hat{N}_v$	$U_v \hat{N}_v$

Hence:

$$\mathrm{Gal}(L_v^{\mathrm{ab}}/K_v) \simeq K_v^\times/N_v, \text{ of order } e_v^{\mathrm{ab}} f_v^{\mathrm{ab}},$$

and the inertia group of L_v^{ab}/K_v is given by:

$$U_v N_v/N_v \simeq U_v/U_v \cap N_v, \text{ of order } e_v^{\mathrm{ab}},$$

proving Lemma 1.

Furthermore:

$$G^0(L_{w_0}^{\mathrm{ab}}/K_v) \simeq U_v N_{w_0}/N_{w_0} \simeq U_v/U_v \cap N_{w_0} \simeq U_v/V_{w_0},$$
$$G^0(\hat{L}_v^{\mathrm{ab}}/K_v) \simeq U_v \hat{N}_v/\hat{N}_v \simeq U_v/U_v \cap \hat{N}_v \simeq U_v \Big/ \bigcap_{w|v} (U_v \cap N_w) = U_v/\hat{V}_v.$$

From the exact sequence of inertia groups 1.1.6:

$$1 \longrightarrow G^0(\hat{L}_v^{\mathrm{ab}}/L_{w_0}^{\mathrm{ab}}) \longrightarrow G^0(\hat{L}_v^{\mathrm{ab}}/K_v) \longrightarrow G^0(L_{w_0}^{\mathrm{ab}}/K_v) \longrightarrow 1,$$

we deduce that the kernel of the map $U_v\hat{N}_v/\hat{N}_v \longrightarrow U_v N_{w_0}/N_{w_0}$ is:

$$G^0(\hat{L}_v^{\mathrm{ab}}/L_{w_0}^{\mathrm{ab}}) \simeq N_{w_0} \cap (U_v\hat{N}_v)/\hat{N}_v = V_{w_0}\hat{N}_v/\hat{N}_v \simeq V_{w_0}/\hat{V}_v,$$

finishing the proof of Lemma 2.

The subgroup of $\mathrm{Gal}(\hat{L}_v^{\mathrm{ab}}/K_v)$ generated by the $G^0(\hat{L}_v^{\mathrm{ab}}/L_w^{\mathrm{ab}})$ is thus:

$$\mathrm{Gal}(\hat{L}_v^{\mathrm{ab}}/\check{L}_v^{\mathrm{ab}}) \simeq V_v\hat{N}_v/\hat{N}_v \simeq V_v/\hat{V}_v,$$

showing that the field $\check{L}_v^{\mathrm{ab}}$ and its inertia subfield have respective norm groups equal to:

$$V_v\hat{N}_v \text{ and } U_vV_v\hat{N}_v = U_v\hat{N}_v,$$

so that:

$$G^0(\check{L}_v^{\mathrm{ab}}/K_v) \simeq U_v\hat{N}_v/V_v\hat{N}_v \simeq U_v/V_v,$$

since $U_v \cap (V_v\hat{N}_v) = V_v(U_v \cap \hat{N}_v) = V_v\hat{V}_v = V_v$, proving 2.6.3.

Since L_v^{ab} is a subfield of $\check{L}_v^{\mathrm{ab}}$, we have $e_v^{\mathrm{ab}} | \check{e}_v^{\mathrm{ab}}$. Since $e_v^{\mathrm{ab}} = (U_v : U_v \cap N_v)$ and $V_v \subseteq U_v \cap N_v$, we have more precisely:

$$\frac{\check{e}_v^{\mathrm{ab}}}{e_v^{\mathrm{ab}}} = (U_v \cap N_v : V_v) \ ;$$

if the L_w^{ab} are all equal, $L_v^{\mathrm{ab}} = \hat{L}_v^{\mathrm{ab}} = \check{L}_v^{\mathrm{ab}}$, hence $e_v^{\mathrm{ab}} = \check{e}_v^{\mathrm{ab}}$, proving 2.6.4. □

2.6.5 Remark. In the Galois case, we thus have the formula:

$$(U_K^{\mathrm{res}} : \mathrm{N}_{L/K}(U_L^{\mathrm{res}})) = \prod_{v \in Pl_0} e_v^{\mathrm{ab}},$$

which must not be mistaken for the corresponding formula for the maximal abelian subextension of L/K:

$$(U_K^{\rm res} : {\rm N}_{L^{\rm ab}/K}(U_{L^{\rm ab}}^{\rm res})) = \prod_{v \in Pl_0} e_v(L^{\rm ab}/K). \qquad \square$$

2.6.6 Exercise. Consider the following irreducible polynomial in $\mathbb{Q}[X]$:

$$P := X^4 + 14X^2 - 19,$$

and take $K = \mathbb{Q}$, $L = K(\theta)$ with ${\rm Irr}(\theta, \mathbb{Q}) = P$, and $v = 2$.

(i) Show that $Pl_{L,v} = \{w_1, w_2\}$ with:

$$L_{w_1} = \mathbb{Q}_2(\sqrt{-1}\,),\ L_{w_2} = \mathbb{Q}_2(\sqrt{3}\,).$$

Compute the indices in U_v of ${\rm N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big)$ and of $U_v \cap {\rm N}_{L/K}\Big(\bigoplus_{w|v} L_w^\times\Big)$.

(ii) Give also a direct numerical check by showing that the norm groups N_{w_1} and N_{w_2} are respectively equal to:

$$\langle\, 2\,\rangle \oplus (1 + 4\mathbb{Z}_2) \ \text{ and } \ \langle\, -2\,\rangle \oplus (1 + 4\mathbb{Z}_2).$$

Answer. We can check (by computing the roots) that we have the following factorization into irreducibles of $\mathbb{Q}_2[X]$:

$$P = (X^2 + a^2)(X^2 - 3b^2),\ a,\ b \in \mathbb{Q}_2^\times,$$

giving the two completions $\mathbb{Q}_2(\sqrt{-1}\,)$ and $\mathbb{Q}_2(\sqrt{3}\,)$. We easily obtain:

$$\hat{L}_v^{\rm ab} = \mathbb{Q}_2(\sqrt{-1}, \sqrt{3}\,),$$

hence $\check{L}_v^{\rm ab} = \hat{L}_v^{\rm ab}$ and $\check{e}_v^{\rm ab} = 2$ since $\hat{L}_v^{\rm ab}/\mathbb{Q}_2(\sqrt{-1}\,)$ and $\hat{L}_v^{\rm ab}/\mathbb{Q}_2(\sqrt{3}\,)$ are unramified. Since $L_v^{\rm ab} = \mathbb{Q}_2$, we have $e_v^{\rm ab} = 1$, which gives an example for which:

$$\Big(U_v : {\rm N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big)\Big) \neq \Big(U_v : U_v \cap {\rm N}_{L/K}\Big(\bigoplus_{w|v} L_w^\times\Big)\Big).$$

For (ii), Exercise 1.6.5 then yields the norm groups. It follows that $V_{w_1} = V_{w_2} = 1 + 4\mathbb{Z}_2$, hence finally ${\rm N}_{L/K}\Big(\bigoplus_{w|v} U_w\Big) = 1 + 4\mathbb{Z}_2$, which is of index 2 in $U_v = \langle\, -1\,\rangle \oplus (1 + 4\mathbb{Z}_2)$.

One checks that -1 can be written:

$${\rm N}_{\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2}(1 + \sqrt{3}\,) \,.\, {\rm N}_{\mathbb{Q}_2(\sqrt{-1})/\mathbb{Q}_2}(1 + \sqrt{-1}\,)^{-1},$$

but is not the norm of local units. $\square$

2.6.7 Conclusion. (i) We can keep in mind for later use (in particular for genus theory) that when L/K is not Galois, local norm problems involve the following diagrams of local fields (for a finite number of finite places v):

$$K_v \text{ ——— } L_v^{\rm ab} := \bigcap_{w|v} L_w^{\rm ab} \text{ ——— } \check{L}_v^{\rm ab} \text{ ——— } \hat{L}_v^{\rm ab} := \langle\, L_w^{\rm ab}\,\rangle_{w|v}$$

and the inertia groups of $\check{L}_v^{\mathrm{ab}}/K_v$, where $\mathrm{Gal}(\hat{L}_v^{\mathrm{ab}}/\check{L}_v^{\mathrm{ab}})$ is generated by the inertia groups of the $\hat{L}_v^{\mathrm{ab}}/L_w^{\mathrm{ab}}$ for $w|v$.

(ii) The norm group of L_v^{ab}/K_v is equal to:

$$\langle \mathrm{N}_{L_w/K_v}(L_w^{\times}) \rangle_{w|v},$$

and we have seen that the norm group of $\check{L}_v^{\mathrm{ab}}/K_v$ is equal to:

$$\langle \mathrm{N}_{L_w/K_v}(U_w) \rangle_{w|v} \cdot \bigcap_{w|v} \mathrm{N}_{L_w/K_v}(L_w^{\times}) \ ;$$

we note that:

$$\begin{aligned} U_v \cap \bigcap_{w|v} \mathrm{N}_{L_w/K_v}(L_w^{\times}) &= \bigcap_{w|v} \left(U_v \cap \mathrm{N}_{L_w/K_v}(L_w^{\times})\right) \\ &= \bigcap_{w|v} \mathrm{N}_{L_w/K_v}(U_w) \subseteq \langle \mathrm{N}_{L_w/K_v}(U_w) \rangle_{w|v}. \end{aligned}$$

In particular $u \in U_v$ is a *norm of local elements* (i.e., u is an element of $\langle \mathrm{N}_{L_w/K_v}(L_w^{\times}) \rangle_{w|v}$) if and only if:

$$u \in \mathrm{N}_{L_v^{\mathrm{ab}}/K_v}(L_v^{\mathrm{ab}\,\times}),$$

and u is a *norm of local units* (i.e., u is an element of $\langle \mathrm{N}_{L_w/K_v}(U_w) \rangle_{w|v}$, which is more difficult to characterize), if and only if:

$$u \in \mathrm{N}_{\check{L}_v^{\mathrm{ab}}/K_v}(\check{L}_v^{\mathrm{ab}\,\times}),$$

which can be expressed in terms of the corresponding norm residue symbol *without referring to units*.

(iii) The case of the places at infinity is trivial for unit groups; we can simply note that for $v \in Pl_\infty$ the field $L_v^{\mathrm{ab}} = L_v$, equal to $\mathbb{R}$ or to $\mathbb{C}$, is different from K_v if and only if v is real and *all* the places $w|v$ are complex (i.e., $f_v^{\mathrm{ab}} = 2$).

§3 Global Class Field Theory: Idelic Version

We now start the study of the fundamental step in global class field theory; it consists in giving the properties of the global reciprocity map (whose existence, from the point of view that we have adopted, only relies on the existence of the local reciprocity maps which has been assumed). We will state in parallel the existence theorem (understood to mean of abelian extensions corresponding to norm groups) whose proof uses independent direct techniques of Kummer extensions and which, because of this, is generally proved at the end of the exposition.

a) Global Reciprocity Map — The Product Formula — Global Class Field Theory Correspondence

Let L/K be a finite extension of number fields and let L^{ab}/K be its maximal abelian subextension whose Galois group will be denoted G^{ab} by abuse of notation (we have $G^{\mathrm{ab}} \simeq G/[G,G]$ when the extension L/K is Galois with Galois group G). We give here the crucial definition of the book.

3.1 Global Reciprocity Map. Let $J := J_K$ be the idèle group of K. We define the global reciprocity map as being:

$$\rho_{L/K} \ : \ J \longrightarrow G^{\mathrm{ab}}$$

sending $\boldsymbol{x} =: (x_v)_v \in J$ to:

$$\rho_{L/K}(\boldsymbol{x}) := \prod_{v \in Pl} \left(\frac{x_v \, , \, L^{\mathrm{ab}}/K}{v} \right),$$

where $\left(\frac{x_v, \, L^{\mathrm{ab}}/K}{v} \right) \in G^{\mathrm{ab}}$ is the image of $(x_v, \, (L^{\mathrm{ab}})_v/K_v) \in \mathrm{Gal}((L^{\mathrm{ab}})_v/K_v)$ under the canonical isomorphism:

$$\mathrm{Gal}((L^{\mathrm{ab}})_v/K_v) \simeq D_v(L^{\mathrm{ab}}/K) \subseteq G^{\mathrm{ab}},$$

where $D_v(L^{\mathrm{ab}}/K)$ is the decomposition group of v in the extension L^{ab}/K (see I.2.7, Fig. 2.3).

3.1.1 Remarks. (i) Since the x_v are almost all units, property 1.4, (vii) of the local norm residue symbol shows that the $\left(\frac{x_v \, , \, L^{\mathrm{ab}}/K}{v} \right)$ are almost all equal to 1, so the product makes sense.

(ii) The definition of $\rho_{L/K}(\boldsymbol{x})$ shows that $\rho_{L/K} = \rho_{L^{\mathrm{ab}}/K}$ but, as in the local case, we must also define $\rho_{L/K}$ for an arbitrary extension. In keeping with the notations that we have used, we can also by definition denote by $\left(\frac{\bullet \, , \, L/K}{v} \right)$ the symbol $\left(\frac{\bullet \, , \, L^{\mathrm{ab}}/K}{v} \right)$, all the more so that a little later we will introduce a generalized symbol denoted $\left[\frac{\bullet \, , \, L/K}{v} \right]$ to avoid any confusion.

(iii) The definition of $\rho_{L/K}$ does not use all the local information relative to L/K: indeed, the local symbols $(\bullet, \, (L^{\mathrm{ab}})_v/K_v)$ are the restrictions of the $(\bullet, \, L_v^{\mathrm{ab}}/K_v)$, themselves restrictions of the symbols $(\bullet, \, L_w^{\mathrm{ab}}/K_v)$ of local class field theory. This can be explained by the fact that we globalize and that, for each v, $(L^{\mathrm{ab}})_v/K_v$ is the largest local extension whose Galois group can be interpreted as a subgroup of G^{ab}. □

3.1.2 Definition (Hasse symbols). Restricting the symbols $\left(\frac{\bullet \, , \, L^{\mathrm{ab}}/K}{v} \right)$ to $i_v(K^\times) \subset K_v^\times$, by composition with i_v we define symbols on $K^\times$, called Hasse symbols, and denoted in an analogous manner:

$$\left(\frac{\bullet\,,\,L/K}{v}\right) := \left(\frac{\bullet\,,\,L^{\mathrm{ab}}/K}{v}\right) \;:\; K^\times \longrightarrow \quad G^{\mathrm{ab}}$$
$$x \quad \longmapsto \quad \left(\frac{i_v(x)\,,\,L^{\mathrm{ab}}/K}{v}\right). \qquad \square$$

They are not essentially different from the preceding ones since the image of $K^\times$ is dense in each $K_v^\times$, but the point is that we will see that on $K^\times$ these symbols are not anymore independent. More precisely, for $x \in K^\times$ the notation $\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right)$, allows us to distinguish between the Hasse symbol (defined on $K^\times$) and its analog $\left(\frac{x_v\,,\,L^{\mathrm{ab}}/K}{v}\right)$ (defined on $K_v^\times$) used to define $\rho_{L/K}$.

Let L/K be a finite extension of number fields, L'/K a subextension of L/K, and let $v \in Pl$. The Hasse symbols only depend on L^{ab}/K. Their properties follow of course from those of the symbols $(\,\bullet\,,\,(L^{\mathrm{ab}})_v/K_v)$, except that the global context modifies certain statements (compare with 1.4 whose notations we again use), such as 3.1.3, (iv) below which uses the fact that the global norm in L'/K is the product of the local norms, and (v) which means that v splits into several places w' in L'/K, which is less precise.

3.1.3 Theorem (properties of the Hasse symbol). *(i) We have the exact sequence:*

$$1 \longrightarrow K^\times \cap \mathrm{N}_{(L^{\mathrm{ab}})_v/K_v}((L^{\mathrm{ab}})_v^\times) \longrightarrow K^\times \xrightarrow{\left(\frac{\bullet\,,L^{\mathrm{ab}}/K}{v}\right)} D_v(L^{\mathrm{ab}}/K) \longrightarrow 1,$$

where the kernel is the local norm group at v for L^{ab}/K (see 2.5.1);

(ii) the composition of $\left(\frac{\bullet\,,\,L^{\mathrm{ab}}/K}{v}\right)$ and of the projection $G^{\mathrm{ab}} \longrightarrow \mathrm{Gal}(L'^{\mathrm{ab}}/K)$, is equal to $\left(\frac{\bullet\,,\,L'^{\mathrm{ab}}/K}{v}\right)$;

(iii) the image of $K^\times_{\{v\}}$ (the subgroup of $K^\times$ of elements prime to v) under $\left(\frac{\bullet\,,\,L^{\mathrm{ab}}/K}{v}\right)$ is the group $I_v(L^{\mathrm{ab}}/K)$;

(iv) for all $x' \in L'^\times$, the image of $\prod\limits_{w'|v}\left(\frac{x'\,,\,L^{\mathrm{ab}'}/L'}{w'}\right)$ in G^{ab} is equal to $\left(\frac{\mathrm{N}_{L'/K}(x')\,,\,L^{\mathrm{ab}}/K}{v}\right)$;

(v) for all $x \in K^\times$, the image of $\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right)$ under the transfer map (from G^{ab} to $\mathrm{Gal}(L^{\mathrm{ab}'}/L')$), is equal to $\prod\limits_{w'|v}\left(\frac{x\,,\,L^{\mathrm{ab}'}/L'}{w'}\right)$;

(vi) for any $\mathbb{Q}$-isomorphism τ of L^{ab} in $\overline{\mathbb{Q}}$ and all $x \in K^\times$, we have:

$$\left(\frac{\tau x\,,\,\tau L^{\mathrm{ab}}/\tau K}{\tau v}\right) = \tau \circ \left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right) \circ \tau^{-1} \text{ on } \tau L^{\mathrm{ab}}\,;$$

(vii) if v is unramified in L^{ab}/K then we have, for all $x \in K^\times$:

$$\left(\frac{x\,,\, L^{\mathrm{ab}}/K}{v}\right) = \left(\frac{L^{\mathrm{ab}}/K}{v}\right)^{\mathrm{v}(x)},$$

where $\left(\frac{L^{\mathrm{ab}}/K}{v}\right)$ denotes the Frobenius of v for L^{ab}/K. □

3.1.3.1 Remark (global Frobenius'). Recall that for a place v of K, unramified in L^{ab}/K, the global Frobenius of v for L^{ab}/K is the canonical image in G^{ab} of the local Frobenius $\mathrm{Frob}((L^{\mathrm{ab}})_v/K_v)$ (i.e., we have $\left(\frac{L^{\mathrm{ab}}/K}{v}\right) = i_{w_0}^{-1} \circ \mathrm{Frob}((L^{\mathrm{ab}})_v/K_v) \circ i_{w_0}$ for any $w_0|v$ in L^{ab}). In particular, if $v \in P_\infty^{\mathrm{r}}$, then $\left(\frac{L^{\mathrm{ab}}/K}{v}\right) = i_{w_0}^{-1} \circ c \circ i_{w_0}$, is the image of the restriction to $(L^{\mathrm{ab}})_v$ of complex conjugation c.

If v is finite, the Frobenius of v in L^{ab}/K is thus the unique generator σ of the decomposition group of $\mathfrak{p}_v$ such that:

$$\sigma(x) \equiv x^{q_v} \bmod \mathfrak{p}_v \text{ for all integers } x \text{ of } L^{\mathrm{ab}},$$

where $q_v := |F_v| = \mathrm{N}\mathfrak{p}_v$. □

3.1.3.2 Examples. (i) For $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[6]{2}\,)$, $v = (7)$, $x = 7$, we have:

$$\left(\frac{x,\, L/K}{v}\right) = \left(\frac{7,\, \mathbb{Q}(\sqrt{2}\,)/\mathbb{Q}}{(7)}\right) = 1$$

since $L^{\mathrm{ab}} = \mathbb{Q}(\sqrt{2}\,)$ and 2 is a square in $\mathbb{Q}_7^\times$, but:

$$(x,\, L_v/K_v) = (7,\, \mathbb{Q}_7(\sqrt[6]{2}\,)/\mathbb{Q}_7) = \mathrm{Frob}(\mathbb{Q}_7(\sqrt[6]{2}\,)/\mathbb{Q}_7),$$

(of order 3) since $\mathbb{Q}_7(\sqrt[6]{2}\,) = L_v^{\mathrm{ab}}$ is the unramified extension of degree 3 of $\mathbb{Q}_7$ (see 1.4, (vii)). This means that 7 is a local norm at (7) in L^{ab}/K but not in L/K.

(ii) For $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[6]{2}\,)$, $v = (43)$, $L' = \mathbb{Q}(\sqrt[3]{2}\,)$ (for which $L^{\mathrm{ab}'} = L$), $x' = -1 + 15\sqrt[3]{2} - 10\sqrt[3]{4}$ (for which $\mathrm{N}_{L'/K}(x') = 43^2$), we have:

$$\left(\frac{\mathrm{N}_{L'/K}(x'),\, L^{\mathrm{ab}}/K}{v}\right) = \left(\frac{43^2,\, \mathbb{Q}(\sqrt{2}\,)/\mathbb{Q}}{(43)}\right) = \left(\frac{\mathbb{Q}(\sqrt{2}\,)/\mathbb{Q}}{(43)}\right)^2 = 1,$$

the square of the Frobenius (of order 2) since 43 is inert in $\mathbb{Q}(\sqrt{2}\,)/\mathbb{Q}$ (see 3.1.3, (vii)). Since $v = (43)$ is totally split in L'/K, we check that:

$$\prod_{w'|v} \left(\frac{x',\, L/L'}{w'}\right) = \left(\frac{L/L'}{w_1'}\right)\left(\frac{L/L'}{w_2'}\right),$$

the product of two of the three (nontrivial) relative Frobenius', giving the result by restriction in L^{ab}/K and illustrating 3.1.3, (iv). □

3.1.4 Remark (generalized norm residue symbol for L/K). As already noted, we have $\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right) = 1$ if and only if x is a local norm at v for L^{ab}/K. If we want to characterize the subgroup of elements of $K^\times$ which are local norms at v for L/K, we need to define a generalized norm residue symbol which must thus be intermediate between the symbol $(\bullet\,,\,L_w/K_v)$, which characterizes the elements which are local norms in L_w/K_v, which is not suitable (see 2.5.3, (ii)), and the Hasse symbol which does not deal with L/K but with L^{ab}/K. Since this subgroup is $\{x \in K^\times,\ i_v(x) \in \mathrm{N}_{L_v^{\mathrm{ab}}/K_v}(L_v^{\mathrm{ab}\times})\}$, where $L_v^{\mathrm{ab}} := \bigcap_{w|v} L_w^{\mathrm{ab}}$, local class field theory tells us that we must use $(\bullet\,,\,L_v^{\mathrm{ab}}/K_v)$ restricted to $i_v(K^\times)$; by composition with i_v, this defines the symbol:

$$\left[\frac{\bullet\,,\,L/K}{v}\right] \,:\, K^\times \longrightarrow G_v^{\mathrm{ab}} := \mathrm{Gal}(L_v^{\mathrm{ab}}/K_v)$$

called the generalized norm residue symbol for L/K. This symbol cannot be interpreted in G^{ab} since G_v^{ab} can be strictly larger than $\mathrm{Gal}((L^{\mathrm{ab}})_v/K_v) \simeq D_v(L^{\mathrm{ab}}/K)$ but, for all $x \in K^\times$,

$$\left[\frac{x\,,\,L/K}{v}\right]_{|(L^{\mathrm{ab}})_v} \text{ can be identified with } \left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right). \qquad \square$$

Note that if L/K is Galois, the generalized norm residue symbol at v can be identified, for any $w_0|v$, with the local norm residue symbol $(\bullet\,,\,L_{w_0}^{\mathrm{ab}}/K_v)$ restricted to $i_v(K^\times)$.

3.2 Cohomological Statement of Class Field Theory (1951/1952). Let L be a finite Galois extension of the number field K, and let $G := \mathrm{Gal}(L/K)$. Assuming that the cohomological version of class field theory can be (in part) summarized by the magical formulas:

$$\begin{aligned} \widehat{H}^r(G,\mathbb{Z}) &\overset{\mathrm{can}}{\simeq} \widehat{H}^{r+2}(G,C_L), \quad \text{for the global case,} \\ \widehat{H}^r(G_w,\mathbb{Z}) &\overset{\mathrm{can}}{\simeq} \widehat{H}^{r+2}(G_w,L_w^\times),\ w \in Pl_L, \quad \text{for the local case,} \end{aligned}$$

where the $\widehat{H}^r$ for $r \in \mathbb{Z}$ are Tate's modified cohomology groups, we deduce once again the existence of "a" global reciprocity map in the following way.

3.2.1 Global Reciprocity Map. Take $r = -2$, which in the global case yields:

$$\widehat{H}^{-2}(G,\mathbb{Z}) \overset{\mathrm{can}}{\simeq} \widehat{H}^0(G,C_L)\ ;$$

but classically, we have:

$$\widehat{H}^0(G, C_L) = C_L^G/\nu_{L/K}(C_L) \simeq C_K/\mathrm{N}_{L/K}(C_L) \simeq J_K/K^\times \mathrm{N}_{L/K}(J_L),$$

the fact that:

$$C_L^G = j_{L/K}(C_K) \simeq C_K \quad \text{and} \quad \nu_{L/K}(C_L) = j_{L/K} \circ \mathrm{N}_{L/K}(C_L) \simeq \mathrm{N}_{L/K}(C_L),$$

with the usual definitions of ν, j, N, being elementary (see (§ 2, (a), (b), (c))).

On the other hand, we have:

$$\widehat{H}^{-2}(G, \mathbb{Z}) := \widehat{H}_1(G, \mathbb{Z}) \overset{\text{can}}{\simeq} G^{\text{ab}}$$

(see 2.4.1, (ii), (iii), or [d, CF, Ch. IV, § 3, Prop. 1]), giving the result, except that we must identify the map $J_K/K^\times \mathrm{N}_{L/K}(J_L) \longrightarrow G^{\text{ab}}$. But the surjection:

$$J_K/\mathrm{N}_{L/K}(J_L) \longrightarrow\!\!\!\!\!\rightarrow G^{\text{ab}},$$

which we obtain from it, and the fact (which is immediate by 1.4.3, (ii)) that:

$$J_K/\mathrm{N}_{L/K}(J_L) \simeq \bigoplus_v \left(K_v^\times/\mathrm{N}_{L_{w_0}/K_v}(L_{w_0}^\times)\right),$$

indeed suggests that it is the map defined in 3.1 from the local reciprocity maps:

$$\widehat{H}^0(G_{w_0}, L_{w_0}^\times) \simeq K_v^\times/\mathrm{N}_{L_{w_0}/K_v}(L_{w_0}^\times) \longrightarrow\!\!\!\!\!\rightarrow \widehat{H}^{-2}(G_{w_0}, \mathbb{Z}) \simeq G_{w_0}^{\text{ab}},$$

where for each place v of K we have chosen a place w_0 of L above v.

This does not make it any easier to obtain the kernel of this surjection, which is the very heart of global class field theory.

3.2.2 Fundamental Class. Note that for $r = 0$ we obtain:

$$\widehat{H}^2(G, C_L) \overset{\text{can}}{\simeq} \widehat{H}^0(G, \mathbb{Z}) = \mathbb{Z}/[L : K]\mathbb{Z} \simeq [L : K]^{-1}\mathbb{Z}/\mathbb{Z},$$

since $\nu_{L/K}$ acts on $\mathbb{Z}$ as multiplication by $[L : K]$. The element $u_{L/K} \in \widehat{H}^2(G, C_L)$, which is the inverse image of the class $[L : K]^{-1} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, is called the fundamental class of L/K.

Hence, the isomorphisms of global class field theory:

$$\widehat{H}^r(G, \mathbb{Z}) \overset{\text{can}}{\simeq} \widehat{H}^{r+2}(G, C_L), \quad r \in \mathbb{Z},$$

are given by the cup product $x \mapsto x \smile u_{L/K}$ for all $x \in \widehat{H}^r(G, \mathbb{Z})$.

For a general view of the cohomological approach, we refer the reader to [d, CF, Ch. VII; Iy1, Ch. IV; Se2, Ch. XI] or to [e, Ko3, Ch. 2], [g, NSW, Ch. III, § 1], as well as to the concrete explanations of [i, Gar], and to Koch's lecture in [i, Miy0] for the history of the concept of class formation for which the fundamental class plays a basic role.

We will now introduce a finite set S of places, which will be a parameter allowing us to specify the decomposition (i.e., splitting) of the elements of S in the correspondence of class field theory.

Notations. (i) Let $S = S_0 \cup S_\infty$ be a finite set of noncomplex places of K. For any finite extension L/K, we denote by $L^{\mathrm{ab}\,S}/K$ the maximal S-split subextension of L^{ab}/K (i.e., in which every place of S is totally split).

(ii) We denote by $\rho^S_{L/K}$ the composite:

$$J \xrightarrow{\rho_{L/K}} G^{\mathrm{ab}} := \mathrm{Gal}(L^{\mathrm{ab}}/K) \longrightarrow G^{\mathrm{ab}\,S} := \mathrm{Gal}(L^{\mathrm{ab}\,S}/K).\ ^{21}$$

(iii) We set $\langle S \rangle := \prod_{v\in S} K_v^\times \prod_{v\in Pl\setminus S} \{1\} =: \bigoplus_{v\in S} K_v^\times$, considered as a subgroup of J (see I.4.1.2, (ii)). □

The fundamental Theorem 1.4 (for the local reciprocity maps) has a global analog in which the multiplicative group $K_v^\times$ is replaced by the multiplicative group J. Let L/K be a finite extension of number fields and L'/K a subextension of L/K. We denote by S' the set of places of L' above those of S.

3.3 Theorem (properties of the global reciprocity map). *The global reciprocity map $\rho^S_{L/K}$ has the following properties:*

(i) We have the exact sequence:

$$1 \longrightarrow K^\times \langle S \rangle \mathrm{N}_{L/K}(J_L) \longrightarrow J_K \xrightarrow{\rho^S_{L/K}} G^{\mathrm{ab}\,S} \longrightarrow 1\ ;$$

(ii) the composition of $\rho^S_{L/K}$ and of the projection $G^{\mathrm{ab}\,S} \longrightarrow \mathrm{Gal}(L'^{\mathrm{ab}\,S}/K)$ is equal to $\rho^S_{L'/K}$;

(iii) for any $v \in Pl$, the image of $K_v^\times$ (resp. of U_v, resp. of U_v^i for $i \geq 1$) [22] *under $\rho^S_{L/K}$ is the decomposition group (resp. the inertia group, resp. the ith higher ramification group in upper numbering) of v for $L^{\mathrm{ab}\,S}/K$;*

(iv) for all $\boldsymbol{x'} \in J_{L'}$, the image of $\rho^{S'}_{L/L'}(\boldsymbol{x'})$ in $G^{\mathrm{ab}\,S}$ is equal to $\rho^S_{L/K}(\mathrm{N}_{L'/K}(\boldsymbol{x'}))$; in particular, we have:

$$\mathrm{Gal}(L^{\mathrm{ab}\,S}/L'^{\mathrm{ab}\,S}) = \rho^S_{L/K}(\mathrm{N}_{L'/K}(J_{L'}))\ ;$$

(v) for all $\boldsymbol{x} \in J_K$, the image of $\rho^S_{L/K}(\boldsymbol{x})$ under the transfer map, from $G^{\mathrm{ab}\,S}$ to $\mathrm{Gal}(L^{\mathrm{ab}'\,S'}/L')$, is equal to $\rho^{S'}_{L/L'}(\boldsymbol{x'})$, where $\boldsymbol{x'}$ is the image of $\boldsymbol{x}$ under the canonical injection $J_K \longrightarrow J_{L'}$;

[21] where $\rho_{L/K}$ will also be denoted $\rho^{\mathrm{res}}_{L/K}$, in accordance with the principles of notation given in Sections 3 and 4 of Chapter I.

[22] where $K_v^\times$, U_v, and U_v^i are considered as subgroups of J_K.

(vi) for any $\mathbb{Q}$-isomorphism τ of L in $\overline{\mathbb{Q}}$ and all $\boldsymbol{x} \in J_K$, we have:

$$\rho^{\tau S}_{\tau L/\tau K}(\tau \boldsymbol{x}) = \tau \circ \rho^{S}_{L/K}(\boldsymbol{x}) \circ \tau^{-1} \text{ on } \tau L^{\mathrm{ab}\, S},$$

noting that $\tau L^{\mathrm{ab}\, S} = (\tau L^{\mathrm{ab}})^{\tau S} = (\tau L)^{\mathrm{ab}\, \tau S}$ (abelianized over τK);

(vii) if the support of $\boldsymbol{x} =: (x_v)_v \in J_K$ is prime to the ramification of $L^{\mathrm{ab}\, S}/K$ (i.e., $x_v = 1$ if v is ramified), we have:

$$\rho^{S}_{L/K}(\boldsymbol{x}) = \prod_{v \in Pl} \left(\frac{L^{\mathrm{ab}\, S}/K}{v} \right)^{\mathrm{v}(x_v)},$$

where $\left(\frac{L^{\mathrm{ab}\, S}/K}{v} \right)$ denotes the Frobenius of v for $L^{\mathrm{ab}\, S}/K$. If π_v is a uniformizer of K_v (seen as an idèle of support $\{v\}$) and if $L^{\mathrm{ab}\, S}/K$ is unramified at v, then $\rho^{S}_{L/K}(\pi_v) = \left(\frac{L^{\mathrm{ab}\, S}/K}{v} \right)$. □

Note. In (i) we have by definition $K^{\times} \langle S \rangle \mathrm{N}_{L/K}(J_L) = K^{\times} \mathrm{N}_{L^S/K}(J_{L^S})$ since $L^{S\,\mathrm{ab}} = L^{\mathrm{ab}\, S}$. In (vii), we can replace the assumption on ramification by the weaker condition: x_v sufficiently close to 1 if v is ramified.

At this point we can note that the norm group N_v corresponding to $(L^{\mathrm{ab}})_v/K_v$ is $N \cap K_v^{\times}$, where $N := K^{\times} \mathrm{N}_{L/K}(J_L)$: indeed, by 3.1, the restriction to $K_v^{\times} \subset J_K$ of $\rho_{L^{\mathrm{ab}}/K}$ can be identified with the norm residue symbol $(\,\bullet\,, (L^{\mathrm{ab}})_v/K_v)$, proving our claim (considering N_v as canonically embedded in J_K).

This proves the following important relationship between local and global class field theories for L^{ab}/K.

3.3.1 Corollary. *For any place v of K, we have the identity:*

$$(K^{\times} \mathrm{N}_{L/K}(J_L)) \cap K_v^{\times} = \mathrm{N}_{(L^{\mathrm{ab}})_v/K_v}((L^{\mathrm{ab}})_v^{\times}).$$ □

3.3.2 Remarks. (i) There exists an infinity of finite sets Σ of places of K such that, by restricting $\rho_{L/K}$ to $\bigoplus_{v \in \Sigma} K_v^{\times}$, we obtain the exact sequence:

$$1 \longrightarrow N \cap \left(\bigoplus_{v \in \Sigma} K_v^{\times} \right) \longrightarrow \bigoplus_{v \in \Sigma} K_v^{\times} \xrightarrow{\rho_{L/K}} G^{\mathrm{ab}} \longrightarrow 1,$$

where $N := K^{\times} \mathrm{N}_{L/K}(J_L)$ (for this, by 3.3, (iii), it suffices that the decomposition groups of the places $v \in \Sigma$ for L^{ab}/K generate G^{ab}, which uses the density theorem which we will recall in 4.6).

(ii) In terms of reduced idèles, since $U_{\infty} \subset \mathrm{N}_{L/K}(J_L)$, we systematically replace the exact sequence of 3.3, (i) by:

$$1 \longrightarrow K^\times \,.\, \bigoplus_{v\in S_0} K_v^\times \bigoplus_{v\in S_\infty} \{\pm 1\}\,.\,\mathrm{N}_{L/K}(J_{L,0}) \longrightarrow J_{K,0} \xrightarrow{\rho^S_{L/K}} G^{\mathrm{ab}\,S} \longrightarrow 1.$$

We will do this only if it is technically necessary. □

3.3.3 Corollary. *For any finite extension L/K of number fields, we have:*

$$K^\times \mathrm{N}_{L/K}(J_L) = K^\times \mathrm{N}_{L^{\mathrm{ab}}/K}(J_{L^{\mathrm{ab}}}).$$ □

By giving a numerical example, it is easy to show that the equality:

$$\mathrm{N}_{L/K}(J_L) = \mathrm{N}_{L^{\mathrm{ab}}/K}(J_{L^{\mathrm{ab}}})$$

is in general false.

3.3.4 Corollary. *We obtain the exact sequences:*

$$1 \longrightarrow K^\times \mathrm{N}_{L/K}(J_L) \longrightarrow J_K \xrightarrow{\rho_{L/K}} G^{\mathrm{ab}} \longrightarrow 1,$$
$$1 \longrightarrow K^\times \langle\, Pl^{\mathrm{r}}_\infty \,\rangle \mathrm{N}_{L/K}(J_L) \longrightarrow J_K \xrightarrow{\rho^{\mathrm{ord}}_{L/K}} \mathrm{Gal}(L^{\mathrm{ab\,nc}}/K) \longrightarrow 1,$$

where $L^{\mathrm{ab\,nc}}$ is the maximal noncomplexified (i.e., Pl^{r}_∞-split) abelian subextension of L or, equivalently, the maximal abelian subextension of L which stays real under all the real embeddings of K. □

Let L/K be a finite extension, and let $N := K^\times \mathrm{N}_{L/K}(J_L)$, so that we have the exact sequence:

$$1 \longrightarrow N \longrightarrow J_K \xrightarrow{\rho_{L/K}} G^{\mathrm{ab}} \longrightarrow 1.$$

Theorem 3.3 gives then the important result:

3.3.5 Corollary (decomposition law of places in L^{ab}/K). *For each place $v \in Pl$, we have the isomorphisms:*

$$K_v^\times N/N \simeq D_v(L^{\mathrm{ab}}/K), \quad U_v N/N \simeq I_v(L^{\mathrm{ab}}/K),$$

where $K_v^\times$ and U_v are considered as subgroups of J_K.
In particular, v is unramified in L^{ab}/K if and only if $U_v \subset N$. Hence, if v is unramified in L^{ab}/K, we have $K_v^\times N/N = \langle\, \pi_v \,\rangle N/N$ since $U_v \subset N$, and the residue degree f_v of v for L^{ab}/K is equal to the order in J_K/N of any uniformizer π_v (seen as an idèle with support $\{v\}$).
The place v is totally split in L^{ab}/K if and only if $K_v^\times \subset N$. □

Recall that for $v \in Pl^{\mathrm{r}}_\infty$, $K_v^\times = \mathbb{R}^\times$, $\pi_v = -1$, and $U_v = \mathbb{R}^{\times +}$, so that in this case we always have $U_v \subseteq N$ (i.e., nonramification of the infinite places).

Indeed, $v \in Pl_\infty^{\mathrm{r}}$ does not become complex in L^{ab}/K if and only if -1 (seen as an idèle with support $\{v\}$ and not diagonally embedded!) belongs to N.

3.4 Product Formula — Classical Applications. The fact that the subgroup $\mathrm{N}_{L/K}(J_L)$ is in the kernel of $\rho_{L/K}$ is clear since for each v, $\langle \mathrm{N}_{L_w/K_v}(L_w^\times)\rangle_{w|v}$ which corresponds to $L_v^{\mathrm{ab}} := \bigcap_{w|v} L_w^{\mathrm{ab}}$ by local class field theory (see 1.5.3), is in the kernel of $(\bullet, L_v^{\mathrm{ab}}/K_v)$, hence a fortiori in that of $(\bullet, (L^{\mathrm{ab}})_v/K_v)$, hence of $\left(\frac{\bullet, L^{\mathrm{ab}}/K}{v}\right)$ since L_v^{ab} contains $(L^{\mathrm{ab}})_v$.

On the contrary, the fact that the kernel of $\rho_{L/K}$ contains the diagonal embedding of $K^\times$ is the *most remarkable* fact (and the least trivial) of global class field theory. We can consider this fact as the idelic version of Artin's reciprocity law (1924/1927), that we will give in 4.3.2 and 4.4; it is also called the product formula since it can be stated in the following way in terms of Hasse symbols (see 3.1.2).

3.4.1 Theorem (product formula). *Let L/K be a finite extension of number fields. For all $x \in K^\times$ we have:*

$$\prod_{v \in Pl} \left(\frac{x\,,\, L^{\mathrm{ab}}/K}{v}\right) = 1. \qquad \square$$

This property allows us to define the reciprocity map on the idèle class group:

$$\rho_{L/K} \;:\; C_K \longrightarrow G^{\mathrm{ab}}.$$

This product formula, which says that the Hasse symbols are not independent on $K^\times$, can also be considered as the general reciprocity law, since it generalizes (among other results) the quadratic reciprocity law of Gauss. To illustrate this, we are going to show that we can deduce the quadratic reciprocity law without using any additional deep arguments (we will give in 7.4 the nth power reciprocity law analogous to the quadratic reciprocity law when K contains μ_n; see also [f, Lem1] and [Wy] for further examples and the history of the subject).

3.4.2 Example (quadratic reciprocity law). Take $K = \mathbb{Q}$ and consider $L = \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}}p}\right)$ for a positive odd prime p; thus the extension $L/\mathbb{Q}$ is only ramified at p. For convenience, we identify $\mathrm{Gal}(L/\mathbb{Q})$ with the multiplicative group $\{\pm 1\}$. The places of $\mathbb{Q}$ will be denoted either v, or else ℓ and ∞.

The computation of the Hasse symbols $\left(\frac{x\,,\, L/\mathbb{Q}}{v}\right)$, $x \in \mathbb{Q}^\times$, can be reduced successively, by multiplicativity, to that of the:

$$\left(\frac{-1\,,\, L/\mathbb{Q}}{v}\right), \quad \text{and of the} \quad \left(\frac{q\,,\, L/\mathbb{Q}}{v}\right)$$

for any positive prime q. Recall that, by 3.1.3, (vii), $\left(\frac{x\,,\,L/\mathbb{Q}}{v}\right) = 1$ except perhaps for (finite or infinite) places v such that $\mathrm{v}(x) \neq 0$ and the ramified places v (hence here p).

(i) $\left(\frac{-1\,,\,L/\mathbb{Q}}{v}\right)$ is equal to 1 except perhaps for $v \in \{\infty, p\}$; but we have:

$$\left(\frac{-1\,,\,L/\mathbb{Q}}{\infty}\right) = \big(-1\big)^{\frac{p-1}{2}}$$

(indeed, $L_\infty/\mathbb{Q}_\infty = \mathbb{C}/\mathbb{R}$ or $\mathbb{R}/\mathbb{R}$ if $\big(-1\big)^{\frac{p-1}{2}} = -1$ or 1 respectively, and -1 is a local norm only in the second case, or (by 3.1.3, (vii)) $\left(\frac{-1\,,\,L/\mathbb{Q}}{\infty}\right)$ is the Frobenius of ∞ for $L/\mathbb{Q}$); using the product formula, we obtain:

$$\left(\frac{-1\,,\,L/\mathbb{Q}}{p}\right) = \big(-1\big)^{\frac{p-1}{2}}$$

(even though a direct computation is easy).

(ii) $\left(\frac{q\,,\,L/\mathbb{Q}}{v}\right)$ is equal to 1 except perhaps for $v \in \{p, q\}$:
If $q = p$, the product formula (reduced to a single term) yields:

$$\left(\frac{p\,,\,L/\mathbb{Q}}{p}\right) = 1.$$

Assume now that $q \neq p$:

- If $v = p$, then $\left(\frac{q\,,\,L/\mathbb{Q}}{p}\right) = 1$ if and only if q (which belongs to U_p) is a norm for the extension $L_p/\mathbb{Q}_p$ (since this extension is ramified, we have $(U_p : U_p \cap \mathrm{N}_{L_p/\mathbb{Q}_p}(L_p^\times)) = 2$ by local theory); but the only subgroup of index 2 of $U_p = \mathbb{Z}_p^\times = \mu_{p-1} \oplus (1 + p\mathbb{Z}_p)$ is $\mu_{p-1}^2 \oplus (1 + p\mathbb{Z}_p) = (U_p)^2$, hence q is a norm for $L_p/\mathbb{Q}_p$ if and only if $q \in (U_p)^2$, hence if and only if $\overline{q} \in \mathbb{F}_p^{\times 2}$, so that:

$$\left(\frac{q\,,\,L/\mathbb{Q}}{p}\right) = \left(\frac{q}{p}\right)$$

(the usual quadratic residue symbol). We can of course use 1.6.5.

- If $v = q$, to compute $\left(\frac{q\,,\,L/\mathbb{Q}}{q}\right)$ we see that $L_q/\mathbb{Q}_q$ is unramified and we have, by 3.1.3, (vii), $\left(\frac{q\,,\,L/\mathbb{Q}}{q}\right) = \left(\frac{L/\mathbb{Q}}{q}\right)$ which is equal to 1 if and only if q is split in $L/\mathbb{Q}$, hence if and only if $L_q = \mathbb{Q}_q\Big(\sqrt{(-1)^{\frac{p-1}{2}}p}\Big) = \mathbb{Q}_q$, hence:

$$\left(\frac{q\,,\,L/\mathbb{Q}}{q}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right),$$

where we use here the Kronecker symbol, equal to the quadratic residue symbol if $q \neq 2$, and otherwise defined by $\left(\frac{a}{2}\right) = 1$ or -1 according as $a \equiv 1 \bmod (8)$ or not. [23]

Hence, using the product formula we have $\left(\frac{q\,,\,L/\mathbb{Q}}{p}\right)\left(\frac{q\,,\,L/\mathbb{Q}}{q}\right) = 1$, which can be interpreted as follows.

- For $q \notin \{2, p\}$ we get $\left(\frac{q}{p}\right)\left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = 1$, hence (using (i)):

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = \Big(-1\Big)^{\frac{p-1}{2}\frac{q-1}{2}}\ ;$$

- for $q = 2$ this yields $\left(\frac{2}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{2}\right)$; we check, by choosing $p \equiv 1, 3, 5, 7 \bmod (8)$, that this can be written:

$$\left(\frac{2}{p}\right) = \Big(-1\Big)^{\frac{p^2-1}{8}}.$$

Note that the above computations never went any further than the use of the Hensel lemma in the $\mathbb{Q}_\ell$ (to characterize the elements of $\mathbb{Q}_\ell^{\times 2}$) and ramification theory in a quadratic field. □

The product formula enables us to make convenient explicit computations, even for the local case, as is shown in the following exercise which gives the local reciprocity map for abelian extensions of the completions of $\mathbb{Q}$ (by Exercise 1.8.3 any abelian extension of $\mathbb{Q}_\ell$ is contained in the maximal cyclotomic extension $\mathbb{Q}_\ell(\mu)$). This procedure will be systematized in 4.4.3 and illustrated in 7.5 for the computation of local Hilbert symbols.

3.4.3 Exercise (local reciprocity map in $\overline{\mathbb{Q}}_\ell^{\mathrm{ab}}/\mathbb{Q}_\ell$). Assume that $K = \mathbb{Q}$ and consider for a fixed prime ℓ the abelian extension $L = \mathbb{Q}(\mu_{\ell^n})$ with $n \geq 1$; we will denote by $L_q/\mathbb{Q}_q = \mathbb{Q}_q(\mu_{\ell^n})/\mathbb{Q}_q$ the completion of $L/\mathbb{Q}$ at $v = q$ finite, and we will consider the embedding $i : \mathbb{Q}^\times \longrightarrow J_\mathbb{Q}$ as being the identity.

(i) Find the norm group N corresponding to L_ℓ.

(ii) Check that for all prime q, $q > 0$, and $q \neq \ell$, the local norm residue symbol $(q\,,\,L_q/\mathbb{Q}_q)$ is the Frobenius automorphism σ_q defined by $\zeta \to \zeta^q$ for all $\zeta \in \mu_{\ell^n}$.

(iii) Show that $(q\,,\,L_\ell/\mathbb{Q}_\ell) = \sigma_q^{-1}$.

(iv) Let $x \in \mathbb{Q}_\ell^\times$, and write $x =: \ell^{v_\ell(x)}u$. Deduce from the above that:

$$(x\,,\,L_\ell/\mathbb{Q}_\ell) = \sigma_u^{-1} = \sigma_{u^{-1}},$$

[23] This symbol at 2 is not multiplicative: $\left(\frac{3}{2}\right) = \left(\frac{5}{2}\right) = \left(\frac{15}{2}\right) = -1$; it is multiplicative however on $1 + 4\mathbb{Z}_2$, which is the present context.

defined by $\zeta \to \zeta^{u^{-1}}$ for all $\zeta \in \mu_{\ell^n}$.

Show that for $L = \mathbb{Q}(\mu_{\ell^\infty})$, the local reciprocity map:

$$\widehat{\mathbb{Q}_\ell^\times} = \ell^{\widehat{\mathbb{Z}}} \oplus U_\ell \longrightarrow \mathrm{Gal}(L_\ell/\mathbb{Q}_\ell)$$

induces the isomorphism $U_\ell \simeq \mathrm{Gal}(L_\ell/\mathbb{Q}_\ell)$ which sends $u \in U_\ell$ to $\sigma_u^{-1} = \sigma_{u^{-1}}$ defined by $\zeta \to \zeta^{u^{-1}}$ for all $\zeta \in \mu_{\ell^\infty}$.

Answer. (i) We have $\mathbb{Q}_\ell^\times = \ell^{\mathbb{Z}} \oplus U_\ell$ with $U_\ell = \mu_{\ell-1} \oplus (1 + \ell\mathbb{Z}_\ell)$ if $\ell \neq 2$, and $U_2 = \{\pm 1\} \oplus (1 + 4\mathbb{Z}_2)$. We know that if ζ_n is a generator of μ_{ℓ^n} we have $\mathrm{N}_{L/\mathbb{Q}}(1 - \zeta_n) = \Phi_{\ell^n}(1) = \ell \in N$; since in addition $L_\ell/\mathbb{Q}_\ell$ is totally ramified of degree $\ell^{n-1}(\ell-1)$, we have $N = \ell^{\mathbb{Z}} \oplus V$ with V of index $\ell^{n-1}(\ell-1)$ in U_ℓ.

If $\ell \neq 2$, the only possibility is $V = 1 + \ell^n\mathbb{Z}_\ell$; if $\ell = 2$ and $n \geq 2$, we have $\mathrm{Gal}(L_\ell/\mathbb{Q}_\ell) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$ and the only possibility is $V = 1 + 4.2^{n-2}\mathbb{Z}_2$ since V must be contained in the norm group of $\mathbb{Q}(\mu_4)$ which is equal to $2^{\mathbb{Z}} \oplus (1 + 4\mathbb{Z}_2)$ (using 1.6.5).

Thus in all cases we have:

$$N = \ell^{\mathbb{Z}} \oplus (1 + \ell^n\mathbb{Z}_\ell).$$

(ii) By 1.4, (vii), we have $(q\,,\, L_q/\mathbb{Q}_q) = \mathrm{Frob}(L_q/\mathbb{Q}_q)$, equal to σ_q for a cyclotomic field: indeed, for all $\zeta \in \mu_{\ell^n}$ the congruence $\mathrm{Frob}(L_q/\mathbb{Q}_q)(\zeta) \equiv \zeta^q \mod (q)$ is equivalent to the equality (use 1.1.5 with the characteristic q!).

(iii) We have the product formula $\prod_v \left(\frac{q\,,\, L/\mathbb{Q}}{v}\right) = 1$, where $\left(\frac{q\,,\, L/\mathbb{Q}}{v}\right)$ is the canonical image of $(q\,,\, L_v/\mathbb{Q}_v)$ in $\mathrm{Gal}(L/\mathbb{Q})$, and we know that $(q\,,\, L_v/\mathbb{Q}_v) = 1$ except perhaps if $L_v/\mathbb{Q}_v$ is ramified (which occurs only for $v = \ell$) or if q is not a unit at v (hence only for $v = q$ since we chose $q > 0$); this yields $\left(\frac{q\,,\, L/\mathbb{Q}}{\ell}\right) = \left(\frac{q\,,\, L/\mathbb{Q}}{q}\right)^{-1} =: \sigma_q^{-1}$ by abuse of notation (we have also $\left(\frac{q\,,\, L/\mathbb{Q}}{q}\right)(\zeta) = \left(\frac{L/\mathbb{Q}}{q}\right)(\zeta) = \zeta^q$ in $L/\mathbb{Q}$ since $L/\mathbb{Q}$ is a cyclotomic field); interpreted in $\mathrm{Gal}(L_\ell/\mathbb{Q}_\ell)$, we get $(q\,,\, L_\ell/\mathbb{Q}_\ell) = \sigma_q^{-1}$.

(iv) We deduce that, for any rational number $a > 0$ prime to ℓ, we have $(a\,,\, L_\ell/\mathbb{Q}_\ell) = \sigma_a^{-1}$ hence, by density, that $(a\,,\, L_\ell/\mathbb{Q}_\ell) = \sigma_a^{-1}$ for all $a \in U_\ell$; in particular it follows that $(x\,,\, L_\ell/\mathbb{Q}_\ell) = \sigma_u^{-1}$ since $(\ell\,,\, L_\ell/\mathbb{Q}_\ell) = 1$. It is then immediate to obtain the local reciprocity map for $\mathbb{Q}_\ell(\mu_{\ell^\infty})/\mathbb{Q}_\ell$ by taking inverse limits.

Note that if μ' is the group of roots of unity of order prime to ℓ, then $\mathbb{Q}_\ell(\mu')$ is the maximal unramified extension of $\mathbb{Q}_\ell$ and its norm group is equal to U_ℓ (see 1.8.3); the isomorphism $\ell^{\widehat{\mathbb{Z}}} \longrightarrow \mathrm{Gal}(\mathbb{Q}_\ell(\mu')/\mathbb{Q}_\ell)$ is given by $\ell \to \sigma_\ell := \mathrm{Frob}(\mathbb{Q}_\ell(\mu')/\mathbb{Q}_\ell))$. Since $\overline{\mathbb{Q}}_\ell^{\mathrm{ab}}$ is the direct compositum of $\mathbb{Q}_\ell(\mu')$ with $\mathbb{Q}_\ell(\mu_{\ell^\infty})$ over $\mathbb{Q}_\ell$, the case of abelian extensions of $\mathbb{Q}_\ell$ is completely explicit. □

See in 4.4.3.3 a slightly more global version of this exercise.

The product formula has the following converse which gives more precise information on the dependence of the Hasse symbols. Let L/K be a finite extension of number fields.

3.4.4 Theorem (converse of the product formula). *Let $(s_v)_{v\in Pl}$ be a family of elements $s_v \in \mathrm{Gal}(L^{\mathrm{ab}}/K)$ satisfying the following conditions:*

(i) $s_v \in D_v(L^{\mathrm{ab}}/K)$ for all v,

(ii) $s_v = 1$ for almost all v, and $\prod_v s_v = 1$.

Then there exists $x \in K^\times$ such that $\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right) = s_v$ for all $v \in Pl$.

Proof. Let Σ be the (finite) support of $(s_v)_v$. Since the image of $K^\times$ under the Hasse symbol $\left(\frac{\bullet\,,\,L^{\mathrm{ab}}/K}{v}\right)$ is equal to $D_v(L^{\mathrm{ab}}/K)$, for each $v \in \Sigma$ there exists $x(v) \in K^\times$ such that $\left(\frac{x(v)\,,\,L^{\mathrm{ab}}/K}{v}\right) = s_v$; consider the idèle $\boldsymbol{x} := (x_v)_v$, whose components outside Σ are equal to 1, and where we have chosen $x_v := i_v(x(v))$ for $v \in \Sigma$. We then have:

$$\rho_{L/K}(\boldsymbol{x}) = \prod_v \left(\frac{x_v\,,\,L^{\mathrm{ab}}/K}{v}\right) = \prod_v s_v = 1,$$

so that there exist $x \in K^\times$ and $\boldsymbol{y} =: (y_w)_w \in J_L$ such that:

$$\boldsymbol{x} = i(x)\mathrm{N}_{L/K}(\boldsymbol{y})\ ;$$

but $\left(\prod_{w|v} \mathrm{N}_{L_w/K_v}(y_w)\,,\,(L^{\mathrm{ab}})_v/K_v\right) = 1$ for all v since by definition we already have $(\mathrm{N}_{L_w/K_v}(y_w)\,,\,L_w^{\mathrm{ab}}/K_v) = 1$ for all $w|v$. Hence x is a solution to our problem. □

This result can in fact be expressed in terms of generalized norm residue symbols (see 3.1.4). For all $v \in Pl$, let $L_v^{\mathrm{ab}} := \bigcap_{w|v} L_w^{\mathrm{ab}}$, $G_v^{\mathrm{ab}} := \mathrm{Gal}(L_v^{\mathrm{ab}}/K_v)$ (see 1.5.3).

3.4.4′ Theorem. *For any family $(\sigma_v)_{v\in Pl} \in \bigoplus_{v\in Pl} G_v^{\mathrm{ab}}$ such that the product of the images of the $\sigma_v|_{(L^{\mathrm{ab}})_v}$ in G^{ab} is equal to the identity, there exists $x \in K^\times$ such that $(i_v(x), L_v^{\mathrm{ab}}/K_v) =: \left[\frac{x\,,\,L/K}{v}\right] = \sigma_v$ for all $v \in Pl$.*

Proof. We use here the fact that the local symbol:

$$(\bullet\,, L_v^{\mathrm{ab}}/K_v) : K_v^\times \longrightarrow G_v^{\mathrm{ab}}$$

is surjective to construct an idèle $\boldsymbol{x} := (x_v)_v$ such that $(x_v, L_v^{\mathrm{ab}}/K_v) = \sigma_v$ for each $v \in \Sigma$, $x_v = 1$ outside Σ (where Σ is the support of $(\sigma_v)_v$).

Since $\left(\frac{x_v\,,\,L^{\rm ab}/K}{v}\right)$ is the canonical image in $G^{\rm ab}$ of $\sigma_v|_{(L^{\rm ab})_v}$ (see 3.1.4), we still have $\rho_{L/K}(\boldsymbol{x}) = 1$, $\boldsymbol{x} = i(x)\mathrm{N}_{L/K}(\boldsymbol{y})$, and x is still a solution, but note that we now use the (more precise) fact that for all v, $\left(\prod_{w|v}\mathrm{N}_{L_w/K_v}(y_w)\,,\,L_v^{\rm ab}/K_v\right) = 1$ for the same reasons as in the preceding case, or note that by 1.5.3 we have directly:

$$\langle\,\mathrm{N}_{L_w/K_v}(L_w^\times)\,\rangle_{w|v} = \mathrm{N}_{L_v^{\rm ab}/K_v}(L_v^{\rm ab\times}).$$ □

We will see in IV.4.5.5 that genus theory gives some additional information on this converse aspect of the product formula and shows that x can be chosen in a suitable S-unit group.

This finishes the first applications of the product formula.

We now come to the global existence theorem (i.e., the existence of abelian extensions of the global field K). By opposition to the local case, all the abelian extensions of K will be taken in a fixed algebraic closure $\overline{K}$ of K which may be independent of our various complex fields $\mathbb{C}_\ell$ or $\mathbb{C}_\infty$.

The analog of the local existence theorem can be obtained from the idèle class group C_K of K in the following way (coming back to J_K for convenience).

3.5 Theorem (global existence). *For any closed subgroup N of finite index of J_K containing $K^\times$, there exists a unique abelian extension M of K such that $K^\times\mathrm{N}_{M/K}(J_M) = N$; the reciprocity map yields the exact sequence:*

$$1 \longrightarrow N \longrightarrow J_K \xrightarrow{\rho_{M/K}} \mathrm{Gal}(M/K) \longrightarrow 1.$$

In addition, the bijection between the closed subgroups of finite index of J_K containing $K^\times$ and the finite abelian extensions of K is a Galois correspondence which has the following properties (where M_1 and M_2 are abelian over K and correspond respectively to N_1 and N_2):

(i) we have $M_1 \subseteq M_2$ if and only if $N_2 \subseteq N_1$;
(ii) M_1M_2 corresponds to $N_1 \cap N_2$;
(iii) $M_1 \cap M_2$ corresponds to N_1N_2;
(iv) if $M_1 \subseteq M_2$, we have $\mathrm{Gal}(M_2/M_1) \simeq N_1/N_2$. □

3.5.1 Remarks. (i) As in the local case, the above Galois properties come from the existence of the correspondence and from 3.3, (i), (ii) on the global reciprocity map.

(ii) Similarly, if M corresponds to N, the decomposition subfield (resp. the inertia subfield) of a place v in M/K corresponds to $K_v^\times N$ (resp. to U_vN), i.e., is fixed under $\rho_{M/K}(K_v^\times)$ (resp. $\rho_{M/K}(U_v)$).

For instance, the field corresponding to the closed subgroup of finite index $N := K^\times U^{\rm res}$ (resp. $K^\times U^{\rm ord}$) is the maximal abelian unramified (resp. unramified and Pl_∞-split) extension of K. This field $H^{\rm res}$ (resp. $H^{\rm ord}$) is called

the Hilbert class field of K in the restricted (resp. ordinary) sense. From I.5.1 or I.5.1.1 we deduce that $\mathrm{Gal}(H^{\mathrm{res}}/K) \simeq \mathcal{C}\ell^{\mathrm{res}}$ (resp. $\mathrm{Gal}(H^{\mathrm{ord}}/K) \simeq \mathcal{C}\ell^{\mathrm{ord}}$). We will find again these fields in the Paragraph 5 as particular cases of the ray class fields corresponding to the open subgroups $K^\times U_{\mathfrak{m}}^{\mathrm{res}}$.

The subfield of M fixed under $\rho_{M/K}(U_v^1) =: D_v^1(M/K) = D_{v,1}(M/K)$ is the maximal v-tamely ramified subextension of K in M. Hence the maximal tamely ramified extension of K in M corresponds to the idèle group:

$$\prod_v U_v^1 \,.\, N.$$

Warning: $K^\times \prod_v U_v^1$ is not of finite index in J_K.

In the statements it is not necessary to refer to a set S; if we want that the places in such a set split completely, it is necessary and sufficient to include $\langle\, S \,\rangle$ in the subgroup N under consideration (see 3.3.5).

(iii) By abuse of notation, we will say that N is the norm group corresponding to the extension M/K.

(iv) Finally, recall that an open subgroup of J_K containing $K^\times$ is of finite index and necessarily contains a subgroup of the form $U_{\mathfrak{m}}^{\mathrm{res}}$ (see I.4.2.3). Thus there is an *equivalence* between a closed subgroup of finite index of J_K containing $K^\times$ and an open subgroup of J_K containing $K^\times$ (which corresponds to an open subgroup of C_K). Hence this contains the assertion about the existence of a conductor which will be studied in Section 4.

(v) The situation is the same if we express the correspondence in terms of subgroups of $J_{K,0}$ containing the diagonal embedding of $K^\times$ since we can go from one point of view to the other thanks to the identity $N = N_0 \oplus U_\infty$, which is self-explanatory. □

Note that in the correspondence of class field theory, the group $\mathrm{N}_{L/K}(J_L)$ does not characterize the extension L^{ab} (in other words, although the equality $\mathrm{N}_{L'/K}(J_{L'}) = \mathrm{N}_{L''/K}(J_{L''})$ clearly implies $L'^{\mathrm{ab}} = L''^{\mathrm{ab}}$, the converse is false). More precisely, Stern has given the following result (for the proof and the study of some consequences for norms, see [St]).

3.5.2 Proposition. *Let L' and L'' be two finite extensions of K, and let L be a Galois extension of K containing L' and L''. Set:*

$$G := \mathrm{Gal}(L/K), \quad H' := \mathrm{Gal}(L/L'), \quad H'' := \mathrm{Gal}(L/L'').$$

Denote by $H_{[*]}$ the set of primary elements (i.e., of order a prime power) of a group H. Then the following conditions are equivalent:

(i) $\mathrm{N}_{L'/K}(J_{L'}) \subseteq \mathrm{N}_{L''/K}(J_{L''})$,

(ii) $K^\times \cap \mathrm{N}_{L'/K}(J_{L'}) \subseteq K^\times \cap \mathrm{N}_{L''/K}(J_{L''})$,

(iii) $\mathrm{N}_{L'/K}(L'^\times) \cap \mathrm{N}_{L''/K}(L''^\times)$ *is of finite index in* $\mathrm{N}_{L''/K}(L''^\times)$,

(iv) $\bigcup_{s\in G} s\, H'_{[*]}\, s^{-1} \subseteq \bigcup_{s\in G} s\, H''_{[*]}\, s^{-1}$. □

Finally, as in the local case (same proof), we have the following consequence of 3.3.

3.5.3 Corollary (norm lifting theorem). *Let L/K be a finite extension of number fields and let M/K be an abelian extension.*
If N is the subgroup of J_K corresponding to M, then the subgroup N' of J_L corresponding to LM over L is given by:

$$\{\boldsymbol{y} \in J_L, \ \ \mathrm{N}_{L/K}(\boldsymbol{y}) \in N\} =: \mathrm{N}_{L/K}^{-1}(N). \qquad \square$$

3.5.4 Proposition (relative decomposition and inertia groups). *Let L/K be a finite extension and let L'/K be a subextension. Denote by N and N' the subgroups of J corresponding to L^{ab} and L'^{ab} (so that $N \subseteq N'$).*
Under the isomorphisms $D_v(L^{\mathrm{ab}}/K) \simeq K_v^\times N/N$ and $I_v(L^{\mathrm{ab}}/K) \simeq U_v N/N$ (see 3.3.5), we then have:

$$D_v(L^{\mathrm{ab}}/L'^{\mathrm{ab}}) \simeq N' \cap K_v^\times / N \cap K_v^\times,$$
$$I_v(L^{\mathrm{ab}}/L'^{\mathrm{ab}}) \simeq N' \cap U_v / N \cap U_v.$$

Proof. Indeed, we have the general exact sequence (see 1.2):

$$1 \longrightarrow D_v(L^{\mathrm{ab}}/L'^{\mathrm{ab}}) \longrightarrow D_v(L^{\mathrm{ab}}/K) \longrightarrow D_v(L'^{\mathrm{ab}}/K) \longrightarrow 1,$$

which can be written:

$$1 \longrightarrow N' \cap (K_v^\times N)/N \longrightarrow K_v^\times N/N \longrightarrow K_v^\times N'/N' \longrightarrow 1 \ ;$$

it is then immediate to check that $N' \cap (K_v^\times N)/N \simeq N' \cap K_v^\times / N \cap K_v^\times$. The case of inertia groups is completely similar. $\square$

3.6 Theorem (Galois action). *Let M/K be a finite abelian extension of number fields and let g be an automorphism group of K with fixed subfield k.*
Let $N := K^\times \mathrm{N}_{M/K}(J_M)$ be the norm group corresponding to M/K.
We have the following facts:

(i) M/k is Galois if and only if g acts on N;

(ii) M/k is abelian if and only if g is commutative and there exists a subgroup n of J_k, containing the diagonal embedding of $k^\times$, such that $N = \mathrm{N}_{K/k}^{-1}(n)$, in which case M is the compositum of K with the abelian extension of k corresponding to n.

Proof. (i) Let τ be a k-isomorphism of M extending $t \in g$. By 3.3, (vi), the group corresponding to τM over $\tau K = K$ is equal to $\tau N = tN$ (since $\rho_{\tau M/K}(\tau \boldsymbol{x}) = 1$ is equivalent to $\rho_{M/K}(\boldsymbol{x}) = 1$); thus the uniqueness theorem indeed implies that $\tau M = M$ if and only if $tN = N$ (i.e., g acts on N).

(ii) If M/k is abelian, g is commutative and there exists n in J_k containing $k^\times$, corresponding to M/k. By 3.5.3, we have $N = \mathrm{N}_{K/k}^{-1}(n)$.

Conversely, assume that g is commutative and that N is of the form $\mathrm{N}_{K/k}^{-1}(n)$. Since by 1.4.3 and 1.4.4, for all $\mathfrak{m}$ (built on the ramified places in K/k), $\mathrm{N}_{K/k}(U_{K,\mathfrak{m}}^{\mathrm{res}})$ contains $U_{k,\mathfrak{n}}^{\mathrm{res}}$ for a suitable $\mathfrak{n}$ in k, it follows that $\mathrm{N}_{K/k} : J_K \longrightarrow J_k$ is an open map and so n, which contains $\mathrm{N}_{K/k}(N)$ with N open, is an open subgroup of J_k, hence of finite index since it contains $k^\times$.

Let k' be the abelian extension corresponding to n over k; since g is commutative, the field Kk' is the compositum of two abelian extensions of k and corresponds, over K, to $\mathrm{N}_{K/k}^{-1}(n) = N$. Hence, by uniqueness we have $Kk' = M$. □

This theorem is the starting point for a more general Galois study; for instance, if M/k is Galois and $[M : K]$ is prime to $|g|$, the action of g on J_K/N or, equivalently, that of g on $\mathrm{Gal}(M/K)$, characterizes the semidirect product $\mathrm{Gal}(M/k) = \mathrm{Gal}(M/K) \rtimes g$.

3.6.1 Example. Let $K/\mathbb{Q}$ be Galois with Galois group $G =: g$, and let H (resp. $\mathcal{C}\ell$) be the restricted or the ordinary Hilbert class field (resp. class group) of K (see 3.5.1, (ii)). If $|G|$ and $|\mathcal{C}\ell|$ are coprime, $\mathrm{Gal}(H/\mathbb{Q}) \simeq \mathcal{C}\ell \rtimes G$ is characterized by the relations:

$$s' \circ \rho_{H/K}(\mathit{cl}(\boldsymbol{x})) \circ s'^{-1} = \rho_{H/K}(\mathit{cl}(s\boldsymbol{x})),$$

for any s' extending $s \in G$ and any idèle $\boldsymbol{x}$ (with $\mathit{cl}(\bullet) \in J/K^\times U \simeq \mathcal{C}\ell$), which become, in terms of Artin symbols that we will introduce in Subsection (b):

$$s' \circ \left(\frac{H/K}{\mathit{cl}(\mathfrak{a})}\right) \circ s'^{-1} = \left(\frac{H/K}{\mathit{cl}(s\,\mathfrak{a})}\right),$$

for any s' extending $s \in G$ and any ideal $\mathfrak{a}$ (with $\mathit{cl}(\bullet) \in \mathcal{C}\ell$). Thus the Galois structure of $\mathcal{C}\ell$ gives that of $\mathrm{Gal}(H/\mathbb{Q})$. Note that if $\mathcal{C}\ell \neq 1$, $\mathcal{C}\ell \rtimes G$ is never a direct product since this is equivalent to $\mathcal{C}\ell = \mathcal{C}\ell^G$, therefore to $\mathcal{C}\ell = 1$ because of the assumption on the orders (hint: if the class $\mathbf{c}$ is fixed under G, then, since $\mathbb{Q}$ is principal, $1 = \nu_{L/K}(\mathbf{c}) := \prod_{s\in G} \mathbf{c}^s = \mathbf{c}^{|G|}$; or use the fact that one can write $H = KM$ with $M/\mathbb{Q}$ abelian and unramified). □

The most complete achievement of Theorem 3.6 is then the Šafarevič–Weil theorem,[24] which characterizes the group extension:

$$1 \longrightarrow \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(M/k) \longrightarrow g \longrightarrow 1,$$

which is of a cohomological nature, in terms of the fundamental class briefly mentioned in 3.2.2. More precisely, the element of $H^2(g, \mathrm{Gal}(M/K))$ associated to this group extension is the image of the fundamental class under the

[24] See [e, Ko3, Ch. 2, § 7.1] and [i, Miy0, Koch] for the history of this result whose name would aptly be "Šafarevič–Hochschild–Nakayama–Jehne theorem", as explained by Koch.

composite of canonical maps:

$$H^2(g, C_K) \longrightarrow H^2(g, C_K/\mathscr{C}_K(N)) \xrightarrow{\rho_{M/K}} H^2(g, \mathrm{Gal}(M/K)),$$

where $N \subset J_K$ is the norm group corresponding to M/K.

b) Global Class Field Theory in $\overline{K}^{\mathbf{ab}}/K$

To conclude, we want to show how the global reciprocity map behaves when we take the inverse limit of the J/N (from the correspondence of 3.5), hoping that this will not create some new and dreadful object; we will see that this is not the case.

3.7 Reciprocity Map in $\overline{K}^{\mathrm{ab}}/K$. By the general principles, we can go to the limit as in the local case by writing that:

$$\overline{G}^{\mathrm{ab}} := \mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K) \simeq \varprojlim_N J/N,$$

where N ranges in the set of open (or closed of finite index) subgroups of J containing $K^\times$. As already explained, these subgroups N must necessarily contain a subgroup of the form $U_{\mathfrak{m}}^{\mathrm{res}} = U_{0,\mathfrak{m}}^{\mathrm{res}} \oplus U_\infty$, where (see I.5.2):

$$U_{0,\mathfrak{m}}^{\mathrm{res}} := \prod_{v \in Pl_0 \setminus T} U_v \prod_{v \in T} U_v^{m_v}$$

if $\mathfrak{m} = \prod_{v \in T} \mathfrak{p}_v^{m_v}$, and where $U_\infty := \bigoplus_{v|\infty} U_v \simeq (\mathbb{R}^{\times +})^{r_1} \times (\mathbb{C}^\times)^{r_2}$ is the connected component of the unit element of J. Thus the group $\overline{G}^{\mathrm{ab}}$ is also of the form (using reduced idèles):

$$\varprojlim_{N_0} J_0/N_0,$$

where N_0 ranges in the set of open subgroups of J_0 containing $K^\times$, of which a cofinal subset is formed by the $K^\times U_{0,\mathfrak{m}}^{\mathrm{res}}$.

We are going to see however that these inverse limits can easily be written in terms of quotients of J or J_0, which in practice avoids working in C or C_0.

3.7.1 Definition. Let ρ be the limit reciprocity map: $\rho : J \longrightarrow \overline{G}^{\mathrm{ab}}$, defined for all $\boldsymbol{x} \in J$ by:

$$\rho(\boldsymbol{x}) := (\rho_{M/K}(\boldsymbol{x}))_M \in \varprojlim_M \mathrm{Gal}(M/K) \simeq \varprojlim_N J/N,$$

for the finite abelian extensions M/K, N denoting the norm group of M (i.e., the kernel of the reciprocity map $\rho_{M/K}$ defined in 3.1). □

The fundamental canonical exact sequence I.5.2.2 (in terms of reduced idèles):

$$1 \longrightarrow K^\times U_0^{\mathrm{ord}} \longrightarrow J_0 \longrightarrow \mathcal{C}\ell^{\mathrm{ord}} \longrightarrow 1,$$

shows that there exists a finite number of representative idèles $\boldsymbol{x}_0^i \in J_0$, $1 \le i \le h := |\mathcal{C}\ell^{\mathrm{ord}}|$, such that $J_0 = \{\boldsymbol{x}_0^i,\ 1 \le i \le h\}\, K^\times\, U_0^{\mathrm{ord}}$.

We have:

$$J/K^\times U_\infty \simeq J_0/K^\times = \{\boldsymbol{x}_0^i,\ 1 \le i \le h\}\, K^\times\, U_0^{\mathrm{ord}}/K^\times,$$

which is represented by the set $\{\boldsymbol{x}_0^i,\ 1 \le i \le h\}\, U_0^{\mathrm{ord}}$; we can then apply I.5.5 to $A = J$, the subgroups $N \subset J$ corresponding to the finite abelian extensions M/K, $B = K^\times U_\infty$, and the compact set $\{\boldsymbol{x}_0^i,\ 1 \le i \le h\}\, U_0^{\mathrm{ord}}$, and so we deduce that ρ is *surjective* (its kernel being trivially equal to $\bigcap\limits_N N$).

We have of course the analogous surjective map $\rho : J_0 \longrightarrow \overline{G}^{\mathrm{ab}}$, defined by $\rho(\boldsymbol{x}_0) := (\rho_{M/K}(\boldsymbol{x}_0))_M$, whose kernel is $\bigcap\limits_{N_0} N_0$.

We thus have the following homeomorphisms:

$$\begin{aligned}\overline{G}^{\mathrm{ab}} &\simeq \varprojlim_N\ J/N \simeq J\Big/\bigcap_N N \simeq J\Big/\bigcap_{\mathfrak{m}} (K^\times U_{\mathfrak{m}}^{\mathrm{res}}) \simeq C/D\\ &\simeq \varprojlim_{N_0}\ J_0/N_0 \simeq J_0\Big/\bigcap_{N_0} N_0 \simeq J_0\Big/\bigcap_{\mathfrak{m}} (K^\times U_{0,\mathfrak{m}}^{\mathrm{res}}) \simeq C_0/D_0,\end{aligned}$$

where $D := \mathcal{C}\ell\Big(\bigcap\limits_{\mathfrak{m}} (K^\times U_{\mathfrak{m}}^{\mathrm{res}})\Big)$, $D_0 := \mathcal{C}\ell_0\Big(\bigcap\limits_{\mathfrak{m}} (K^\times U_{0,\mathfrak{m}}^{\mathrm{res}})\Big)$, are the connected components of the unit element of C and C_0 respectively, and where we recall that (see I.4.2.5, I.4.2.8, (ii)):

$$D = \mathcal{C}\ell\Big(\bigcap_{\mathfrak{m}} (E^{\mathrm{ord}} U_{\mathfrak{m}}^{\mathrm{res}})\Big),\quad D_0 = \mathcal{C}\ell_0\Big(\bigcap_{\mathfrak{m}} (E^{\mathrm{ord}} U_{0,\mathfrak{m}}^{\mathrm{res}})\Big).$$

3.7.2 Remark. Note that in general the $U_{0,\mathfrak{m}}^{\mathrm{ord}}$ do not form a fundamental system of neighbourhoods of 1 in J_0; in a similar way, although the $U_{0,\mathfrak{m}}^{\mathrm{res}}$ form such a fundamental system, this is not the case for the $U_{\mathfrak{m}}^{\mathrm{res}}$ in J (because of the archimedean factors), and only $\bigcap\limits_{\mathfrak{m}} (K^\times U_{0,\mathfrak{m}}^{\mathrm{res}})$ represents the closure of the image of $K^\times$ in J_0, so that we have:

$$D_0 = \mathrm{adh}_0(K^\times)/K^\times = \mathrm{adh}_0(E^{\mathrm{ord}})/E^{\mathrm{ord}}.$$

However, we can write $D = \mathrm{adh}(K^\times U_\infty)/K^\times$. □

Summarizing these results, we obtain the following description of $\overline{G}^{\mathrm{ab}} := \mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K)$ by means of the usual reciprocity maps $\rho_{M/K}$ for finite abelian extensions M/K.

3.7.3 Theorem. *The infinite reciprocity map* $\rho : J \longrightarrow \overline{G}^{\mathrm{ab}}$ *(resp.* $\rho : J_0 \longrightarrow \overline{G}^{\mathrm{ab}}$*), which associates with* $\boldsymbol{x} \in J$ *(resp.* $\boldsymbol{x}_0 \in J_0$*),* $(\rho_{M/K}(\boldsymbol{x}))_M$ *(resp.* $(\rho_{M/K}(\boldsymbol{x}_0))_M$*, is surjective.*
Thus ρ *induces the canonical homeomorphisms:*

$$\overline{G}^{\mathrm{ab}} \simeq J/\mathrm{adh}(K^\times U_\infty) \simeq J_0/\mathrm{adh}_0(K^\times). \qquad \square$$

Of course, the composition of ρ and the restriction $\overline{G}^{\mathrm{ab}} \longrightarrow \mathrm{Gal}(M/K)$ yields the reciprocity map $\rho_{M/K}$ for any abelian extension M/K (finite or not).

3.7.4 Corollary. *Taking quotients by the diagonal embeddings of* $K^\times$*, we can write:*

$$\overline{G}^{\mathrm{ab}} \simeq C/D \simeq C_0/D_0,$$

where $D = \mathscr{A}\Big(\bigcap_{\mathfrak{m}} (K^\times U_{\mathfrak{m}}^{\mathrm{res}})\Big) = \mathrm{adh}(K^\times U_\infty)/K^\times$, $D_0 = \mathscr{A}_0\Big(\bigcap_{\mathfrak{m}} (K^\times U_{0,\mathfrak{m}}^{\mathrm{res}})\Big) = \mathrm{adh}_0(K^\times)/K^\times$. $\square$

3.8 Infinite Global Class Field Theory Correspondence. The correspondence for *infinite* idelic class field theory can be expressed in terms of either:

- closed subgroups of J containing $K^\times U_\infty$,
- closed subgroups of C containing D,
- closed subgroups of J_0 containing $K^\times$,
- closed subgroups of C_0 containing D_0.

In addition, the bijection between the set of abelian extensions of K and the set of closed subgroups of J_0 containing $K^\times$ (for instance) is a Galois correspondence having the properties (i) to (iv) of 3.5.

3.8.1 Remarks. (i) Under this correspondence, the decomposition and inertia groups are still related to the images under ρ of the groups $K_v^\times$ and U_v but this is not enough to identify them; in other words the computation of $K_v^\times \mathrm{adh}_0(K^\times)/\mathrm{adh}_0(K^\times)$ or of $K_v^\times/K_v^\times \cap \mathrm{adh}_0(K^\times)$ is neither sufficient nor a priori easy. It is however easy to see that we have $\rho(U_v) = I_v(\overline{K}^{\mathrm{ab}}/K)$ and that $\rho(K_v^\times)$ is dense in $D_v(\overline{K}^{\mathrm{ab}}/K)$. In addition there is a topological problem since J induces on $K_v^\times$ its usual topology (with neighbourhoods U_v^m), while it is that induced by $\widehat{K_v^\times}$ (with neighbourhoods $\pi_v^{n\mathbb{Z}} \oplus U_v^m$) which is suitable since $D_v(\overline{K}^{\mathrm{ab}}/K)$ is obtained by an inverse limiting process (which we will give in III.4.12.5 following III.4.5); recall also the problem that we have met in I.4.2.8, (iv). All this needs Theorem III.4.3 of Schmidt–Chevalley, which uses the local-global principle 6.3.3 on powers. It is thus natural to delay the study of all questions dealing with the global structure of $\overline{K}^{\mathrm{ab}}/K$ which are

logically equivalent to the study of the properties of D and D_0, and will be the object of the next chapter.

(ii) The group D is also called the universal norm group simply because it corresponds to $\overline{K}^{\mathrm{ab}}$ by infinite class field theory, and because it is contained in the images in C of all the norm groups $K^{\times}\mathrm{N}_{L/K}J_L$ of finite extensions L of K. As we have already mentioned, D is the connected component of the unit element of C and also its maximal divisible subgroup. We will show this last point in III.4.15.1. Exactly the same things can be said about D_0 in C_0. □

In terms of classes of reduced idèles, the above yields:

$$C_0 = \{\mathscr{A}_0(\boldsymbol{x}_0^i),\ 1 \le i \le h\}\,.\,\mathscr{A}_0(U_0^{\mathrm{ord}}),$$

and the exact sequence:

$$1 \longrightarrow \mathscr{A}_0(U_0^{\mathrm{ord}})D_0/D_0 \longrightarrow C_0/D_0 \longrightarrow \mathscr{C}\ell^{\mathrm{ord}} \longrightarrow 1,$$

shows that the study of C_0/D_0 can be reduced to that of:

$$\mathscr{A}_0(U_0^{\mathrm{ord}})D_0/D_0 \simeq K^{\times}U_0^{\mathrm{ord}}\Big/\bigcap_{\mathfrak{m}}(K^{\times}U_{0,\mathfrak{m}}^{\mathrm{res}}) \simeq U_0^{\mathrm{ord}}\Big/\bigcap_{\mathfrak{m}}(E^{\mathrm{ord}}U_{0,\mathfrak{m}}^{\mathrm{res}}),$$

which is $U_0^{\mathrm{ord}}/\mathrm{adh}_0(E^{\mathrm{ord}})$ or, equivalently, the quotient of $U_0^{\mathrm{ord}}/E^{\mathrm{ord}}$ by the connected component D_0.

We obtain the following result.

3.8.2 Theorem (global exact sequence of class field theory). *We have the exact sequence:*

$$1 \longrightarrow U_0^{\mathrm{ord}}/\mathrm{adh}_0(E^{\mathrm{ord}}) \xrightarrow{\ \rho\ } \overline{G}^{\mathrm{ab}} \longrightarrow \mathscr{C}\ell^{\mathrm{ord}} \longrightarrow 1,$$

in which $U_0^{\mathrm{ord}}/\mathrm{adh}_0(E^{\mathrm{ord}}) \simeq \mathrm{Gal}(\overline{K}^{\mathrm{ab}}/H^{\mathrm{ord}})$ *and* $\mathscr{C}\ell^{\mathrm{ord}} \simeq \mathrm{Gal}(H^{\mathrm{ord}}/K)$. □

For instance, if K is equal to $\mathbb{Q}$ or to a *principal* imaginary quadratic field, this yields $\overline{G}^{\mathrm{ab}} \simeq U_0^{\mathrm{ord}}/i_0(\mu(K))$.

The determination of the structures of $\mathrm{adh}_0(E^{\mathrm{ord}})$ and D_0 is the object of Theorem III.4.4.6.

The point of view of the notes of Artin–Tate [d, AT, Ch. 9, § 1], and before of the book of Weil [h, We2, III], is to give explicitly the structure of D (in particular for the computation of the cohomology of C and of C/D). Our point of view consists also in looking at the formulas:

$$\overline{G}^{\mathrm{ab}} \simeq \varprojlim_{N}\ J/N \simeq \varprojlim_{N_0}\ J_0/N_0 \simeq \varprojlim_{\mathfrak{m}}\ \mathscr{C}\ell_{\mathfrak{m}}^{\mathrm{res}},$$

which show how the finite case, which is amenable to numerical computations, regularizes when one takes the limit, but there is no difficulty in expressing and in proving certain results thanks to the properties of C/D or of C_0/D_0, and we will do so when needed (for instance in Chapter III, Section 4, and in the Appendix).

The structure of the inverse limit $\varprojlim_{\mathfrak{m}} \mathcal{C}_{\mathfrak{m}}^{\mathrm{res}}$ and especially those of its p-Sylow subgroups are quite complex, and their arithmetic computation will be the object of Chapter III.

3.8.3 Remark. It is interesting to note a difference between the local and global cases. In the global case, the map:

$$\rho : J \longrightarrow \mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K)$$

is surjective, while in the local case, the analogous map:

$$\rho_v := (\,\bullet\,, \overline{K}_v^{\mathrm{ab}}/K_v) : K_v^{\times} \longrightarrow \mathrm{Gal}(\overline{K}_v^{\mathrm{ab}}/K_v)$$

only has a dense image. This comes from the fact that in the local case $\overline{K}_v^{\mathrm{nr}}/K_v$ is infinite, contrary to the global case where H^{ord}/K is finite: indeed, the relative Galois groups $\mathrm{Gal}(\overline{K}_v^{\mathrm{ab}}/\overline{K}_v^{\mathrm{nr}})$ and $\mathrm{Gal}(\overline{K}^{\mathrm{ab}}/H^{\mathrm{ord}})$ are the images under the continuous maps ρ_v and ρ of the compact groups U_v and U_0^{ord}, but $K_v^{\times}/U_v \simeq \mathbb{Z}$ is not compact, contrary to $J_0/K^{\times}U_0^{\mathrm{ord}}$ which is finite. Note also that for any $x_v \in K_v^{\times}$ (seen as an idèle), $\rho(x_v)$ corresponds to $\rho_v(x_v)_{|_{(\overline{K}^{\mathrm{ab}})_v}}$ under the identification of $D_v(\overline{K}^{\mathrm{ab}}/K)$ with $\mathrm{Gal}((\overline{K}^{\mathrm{ab}})_v/K_v)$. But we will prove in III.4.5 that $(\overline{K}^{\mathrm{ab}})_v = \overline{K}_v^{\mathrm{ab}}$; thus we indeed have that $\rho_{|_{K_v^{\times}}}$ corresponds to ρ_v, which confirms the topological problems we have mentionned at several occasions. □

§4 Global Class Field Theory: Class Group Version

a) Global Norm Conductor — Properties

Let L/K be a finite extension of number fields; the use of generalized ideal class groups implies that we must introduce the fundamental notion of a global norm conductor. To begin with, recall that from our point of view, the existence of a modulus $\mathfrak{m}$ satisfying the condition:

$$U_{\mathfrak{m}}^{\mathrm{res}} \subseteq \mathrm{N}_{L/K}(J_L),$$

which says that the group $\mathrm{N}_{L/K}(J_L)$ is open, hence that the group:

$$K^{\times}\mathrm{N}_{L/K}(J_L),$$

is open with finite index in J_K, comes essentially from local class field theory since, for every place v unramified in L/K we have, for the places w of L above v:

$$U_v = \mathrm{N}_{L_w/K_v}(U_w)$$

(see 1.4.3, (ii)), and that for every place v ramified in L/K, there exists a sufficiently large i such that for all $w|v$ we have (see 1.4.4):

$$U_v^i \subseteq (U_v)^{[L_w:K_v]} \subseteq \mathrm{N}_{L_w/K_v}(U_w).$$

The existence of $\mathfrak{m}$ (also called an admissible modulus) trivially implies that of a *smallest* admissible modulus since we have $U_v^{m_1} U_v^{m_2} = U_v^{\min(m_1, m_2)}$, for any $v \in Pl$. The support of this modulus is contained in the set of places ramified in L/K.[25] We can thus state the following.

4.1 Theorem and Definition (global norm conductor). *Let L/K be a finite extension of number fields.*
There exists a smallest modulus $\mathfrak{f}_{L/K} =: \mathfrak{f}$ of K, such that:

$$U_{\mathfrak{f}}^{\mathrm{res}} \subseteq K^{\times}\mathrm{N}_{L/K}(J_L).$$

This modulus is called the global norm conductor or the conductor of L/K. It only depends on the maximal abelian subextension L^{ab}/K of L/K and hence is also equal to $\mathfrak{f}_{L^{\mathrm{ab}}/K}$, the global norm conductor of L^{ab}/K (see 3.3.3). □

Note. According to our point of view, $\mathfrak{f}$ is a nonzero integral ideal of K and in particular does not involve any infinite places. Moreover, its support is contained in the set of places ramified in L/K (even with the meaning of the above footnote) since it is an admissible module for $K^{\times}\mathrm{N}_{L/K}(J_L)$ which contains $\mathrm{N}_{L/K}(J_L)$. See the more precise result 4.2.

4.1.1 Proposition (conductor of a compositum of fields). *If L^{ab} is the compositum, over K, of the extensions $M_1, \ldots, M_n$, then its conductor is equal to the l.c.m. of the conductors of the M_i for $1 \leq i \leq n$.*

Proof. Immediate from Definition 4.1 and the fact that we have:

$$K^{\times}\mathrm{N}_{L/K}(J_L) = \bigcap_{i=1}^{n} (K^{\times}\mathrm{N}_{M_i/K}(J_{M_i})),$$

by 3.5, (ii). □

For example, if L/K is a p-elementary extension (i.e., $\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/p\mathbb{Z})^r$, p prime), its norm group and its conductor can be computed from

[25] More precisely, in the non-Galois case we have $U_v \subset \mathrm{N}_{L/K}(J_L)$ if and only if L_v^{ab}/K_v is unramified, so that this support is contained in the set of places v such that *all* $w|v$ ramify in L/K. For the sequel (abelian case), this information is useless.

the case of a cyclic extension of degree p; if $\mu_p \subset K$, the result immediately follows from 1.6.3, otherwise we can be reduced to the Kummer case because of norm lifting Theorem 3.5.3.

4.1.2 Remark. If M is the intersection of the M_i, we can only say that the conductor of M divides the g.c.d. of the conductors of the M_i; for example, for $K = \mathbb{Q}$, $M_1 = \mathbb{Q}(\sqrt{-1})$, $M_2 = \mathbb{Q}(\sqrt{2})$, we have $\mathfrak{f}_1 = (4)$, $\mathfrak{f}_2 = (8)$ (see 1.6.5), g.c.d.$(\mathfrak{f}_1, \mathfrak{f}_2) = (4)$, but $M_1 \cap M_2 = \mathbb{Q}$. □

The global norm conductor has the following property (which comes from the local case, as is shown by the proof of Lemma 4.2.1).

4.2 Theorem (of the conductor). *Let L/K be a finite extension of number fields and let $\mathfrak{f}$ be its global norm conductor. Let v be a finite place of K. Then v is ramified in L^{ab}/K if and only if $\mathfrak{p}_v$ divides $\mathfrak{f}$ (i.e., the support of $\mathfrak{f}$ is equal to the set R of places which are ramified in L^{ab}/K).*

4.2.1 Lemma (computation of a global norm conductor). *Let L/K be a finite extension. Then $\mathfrak{f} := \mathfrak{f}_{L/K}$ is equal to the product of the local v-conductors of L^{ab}/K, in other words $\mathfrak{f} = \prod_{v \in Pl_0} \mathfrak{f}_v(L^{\mathrm{ab}}/K)$ (see 1.6, (ii)).*

Proof of the statements. In the fundamental Corollary 3.3.1 we have observed that the norm groups N_v (corresponding to $(L^{\mathrm{ab}})_v/K_v$) are the $N \cap K_v^{\times}$, where $N := K^{\times}\mathrm{N}_{L/K}(J_L)$; thus, using 1.4.3, (ii), it is clear that $U_v^{m_v} \subseteq N_v$ for all v (taking $m_v = 0$ if $v \notin R$), is equivalent to $U_{\mathfrak{m}}^{\mathrm{res}} \subseteq N$, for $\mathfrak{m} = \prod_{v \in R} \mathfrak{p}_v^{m_v}$. This proves the result as well as the theorem of the conductor. □

The above lemma gives a result which is essential for the practical computation of a global conductor: indeed, in general we know a multiple of the discriminant of L^{ab}/K, so that we are reduced to a finite (explicit) number of computations of local v-conductors of cyclic extensions by 4.1.1 (for this, we use Formula 1.6.2).

We illustrate the above on an example showing that the local information coming from the L_v^{ab}/K_v should not be mistaken for that coming from the subextension L^{ab}/K, even when L/K is Galois.

Example. Consider the extension $L = \mathbb{Q}(\sqrt[3]{7}, j)$ of $K = \mathbb{Q}$, in which the ramified places are 3 and 7. For the place $v = 7$ of K, we obtain $L_v^{\mathrm{ab}} = \mathbb{Q}_7(\sqrt[3]{7})$ which is a cyclic extension of degree 3 of $\mathbb{Q}_7$; it follows that we have $\mathfrak{f}_{L_v^{\mathrm{ab}}/K_v} = (7)$ (7 is tamely ramified in L_v^{ab}/K_v) while the global conductor $\mathfrak{f} = \prod_v \mathfrak{f}_v(L^{\mathrm{ab}}/K)$, which is the conductor of $L^{\mathrm{ab}}/K = \mathbb{Q}(j)/\mathbb{Q}$, is equal to (3) (i.e., for $v = 7$ the local v-conductor of L^{ab}/K is equal to 1, or equivalently, we have $L_v^{\mathrm{ab}} = \mathbb{Q}_7(\sqrt[3]{7})$, but $(L^{\mathrm{ab}})_v = \mathbb{Q}_7$). □

4.2.2 Exercise. Deduce from the proof of Lemma 4.2.1 the equivalence of the following conditions:

$$U_{\mathfrak{m}}^{\rm res} \subseteq N := K^{\times}{\rm N}_{L/K}(J_L) \ \text{ and } \ U_{\mathfrak{m}}^{\rm res} \subseteq {\rm N}_{L^{\rm ab}/K}(U_{L^{\rm ab}}^{\rm res}).$$

Answer. One direction is clear since $N = K^{\times}{\rm N}_{L^{\rm ab}/K}(J_{L^{\rm ab}})$; for the other, it suffices to check that $N \cap U_v = N_v \cap U_v = {\rm N}_{(L^{\rm ab})_v/K_v}(U_{(L^{\rm ab})_v})$, where $U_{(L^{\rm ab})_v}$ is the unit group of $(L^{\rm ab})_v$.

Beware that the results of 2.6 show that $U_{\mathfrak{m}}^{\rm res} \subseteq K^{\times}{\rm N}_{L/K}(J_L)$ is in general not equivalent to $U_{\mathfrak{m}}^{\rm res} \subseteq {\rm N}_{L/K}(U_L^{\rm res}) = \prod\limits_v {\rm N}_{\check{L}_v^{\rm ab}/K_v}(U_{\check{L}_v^{\rm ab}})$ since we have:

$$\Big({\rm N}_{L^{\rm ab}/K}(U_{L^{\rm ab}}^{\rm res}) : \prod_v {\rm N}_{\check{L}_v^{\rm ab}/K_v}(U_{\check{L}_v^{\rm ab}})\Big) = \prod_v \frac{\check{e}_v^{\rm ab}}{e_v(L^{\rm ab}/K)} \ ;$$

neither is it equivalent to $U_{\mathfrak{m}}^{\rm res} \subset {\rm N}_{L/K}(J_L)$, which means that for all v, $U_v^{m_v} \subseteq {\rm N}_{L_v^{\rm ab}/K_v}(U_{L_v^{\rm ab}})$, since the index:

$$\Big({\rm N}_{L^{\rm ab}/K}(U_{L^{\rm ab}}^{\rm res}) : \prod_v {\rm N}_{L_v^{\rm ab}/K_v}(U_{L_v^{\rm ab}})\Big) = \prod_v \frac{e_v^{\rm ab}}{e_v(L^{\rm ab}/K)},$$

can also be different from 1 (recall that $\check{e}_v^{\rm ab} := e(\check{L}_v^{\rm ab}/K_v)$ and $e_v^{\rm ab} := e(L_v^{\rm ab}/K_v)$). This remark remains in the case where L/K is only Galois (use the example given above). □

We also give the following classical property which is summarized under the name "Führerdiskriminantenproduktformel".

4.2.3 Proposition. *Let L/K be a finite extension of number fields. Then the relative discriminant of the subextension $L^{\rm ab}/K$ is:*

$$\mathfrak{d}_{L^{\rm ab}/K} = \prod_{\chi} \mathfrak{f}_{\chi},$$

where χ ranges in the dual of $G^{\rm ab}$ and where $\mathfrak{f}_{\chi}$ is the global norm conductor of the subfield of $L^{\rm ab}$ fixed under the kernel of χ. □

4.2.4 Nonabelian Artin Conductors. Recall, without any justification, that these (abelian) conductors have the following Galois generalization which comes from higher ramification theory. [26]

Denote by $\Psi(\Gamma)$ the set of absolutely irreducible characters of a finite group Γ. Let L/K be a finite Galois extension with Galois group G, and let L_{w_0}/K_v, with Galois group G_{w_0}, be a completion of L/K at $v \in Pl_0$ and a fixed $w_0|v$; for any $\psi \in \Psi(G_{w_0})$ we set:

$$\mathfrak{f}_v^{\rm art}(\psi) := \mathfrak{p}_v^{m_{v,\psi}},$$

[26] [d, Se2, Ch. VI, § 2; CF, Ch. VI, § 4], [c, Neu1, Ch. VII, § 11].

with:

$$m_{v,\psi} := \frac{1}{g_0} \sum_{i \geq 0} g_i \left(\psi(1) - \frac{1}{g_i} \sum_{s \in G_{w_0,i}} \psi(s) \right),$$

where $G_{w_0,i}$ is the ith higher ramification group of L_{w_0}/K_v (in lower numbering) and $g_i := |G_{w_0,i}|$. For an arbitrary character χ we define $\mathfrak{f}_v^{\mathrm{art}}(\chi)$ by linearity, and this modulus is called the local v-conductor of the character χ. If ψ is of degree 1, the factor:

$$\psi(1) - \frac{1}{g_i} \sum_{s \in G_{w_0,i}} \psi(s),$$

is equal to 0 or 1 depending on whether or not the restriction of ψ to $G_{w_0,i}$ is the unit character, and we recover the norm conductor of the cyclic extension fixed under the kernel of ψ (see [d, Se2, Ch. VI, § 2, Prop. 5, Cor.]).

This gives the local Artin v-conductors for the extension L/K. We then define the global Artin conductors, for any $\psi \in \Psi(G)$, by:

$$\mathfrak{f}^{\mathrm{art}}(\psi) := \prod_{v \in Pl_0} \mathfrak{f}_v^{\mathrm{art}}(\mathrm{Res}_v(\psi)),$$

where $\mathrm{Res}_v(\psi)$ is the restriction of ψ to $D_{w_0}(L/K) \simeq G_{w_0}$ (it does not depend on the choice of w_0). We thus have the corresponding formula for the relative discriminant of L/K (Artin–Hasse):

$$\mathfrak{d}_{L/K} = \prod_{\psi \in \Psi(G)} (\mathfrak{f}^{\mathrm{art}}(\psi))^{\psi(1)}.$$

An important property of the Artin conductor is that it *characterizes* the ramification for the extension L/K (and not only for the extension L^{ab}/K), but this is not anymore part of class field theory.

The reader can refer to [e, Ko3, Ch. 5, § 1] to have an overview on questions dealing with Artin L-functions, whose study at $s = 0$ is the object of Stark's conjectures.

b) Artin's Reciprocity Map — Reciprocity Law — Global Computation of Hasse Symbols — Decomposition Law

To go from the idelic to the generalized class group point of view, we have at our disposal the fundamental exact sequence of Theorem I.5.1, relative to the usual data T, $\mathfrak{m}$, and S prime to T:

$$1 \longrightarrow K^{\times} U_{\mathfrak{m}}^S / K^{\times} \simeq U_{\mathfrak{m}}^S / E_{\mathfrak{m}}^S \longrightarrow C \xrightarrow{\gamma_{\mathfrak{m}}^S} \mathcal{C}\ell_{\mathfrak{m}}^S \longrightarrow 1.$$

Furthermore, the above fundamental results (in idelic terms) for a finite extension L/K and a finite set S of noncomplex places of K unramified in L^{ab}/K, are:

(α) the exact sequence:

$$1 \longrightarrow K^\times \langle S \rangle \mathrm{N}_{L/K}(J_L)/K^\times \longrightarrow C \xrightarrow{\rho^S_{L/K}} G^{\mathrm{ab}\,S} \longrightarrow 1,$$

with $\langle S \rangle := \bigoplus_{v \in S} K_v^\times$, where $K^\times \mathrm{N}_{L/K}(J_L)$ is an open subgroup of J, and $G^{\mathrm{ab}\,S} := \mathrm{Gal}(L^{\mathrm{ab}\,S}/K)$;

(β) the existence theorem which says that, conversely, for any open subgroup N of J containing the image of $K^\times$, there exists L/K such that we indeed have:

$$1 \longrightarrow N \langle S \rangle / K^\times \longrightarrow C \xrightarrow{\rho^S_{L/K}} G^{\mathrm{ab}\,S} \longrightarrow 1.$$

We then see that we may successively:

(α') factor $\rho^S_{L/K}$ as a map from $\mathcal{C}\ell^S_{\mathfrak{m}}$ to $G^{\mathrm{ab}\,S}$, for $\mathfrak{m}$ multiple of the norm conductor of L/K;

(β') express the existence theorem in terms of subgroups of $\mathcal{C}\ell^S_{\mathfrak{m}}$, which will be equivalent to classifying abelian extensions of K by their conductor.

4.3 The Fundamental Diagram for Artin and Reciprocity Maps. The translation in terms of generalized class groups of the properties of the global reciprocity map relies on the following commutative diagram, in which L/K is a finite extension of number fields, $\mathfrak{m}$ is any multiple of the norm conductor $\mathfrak{f}$ of L/K, and S is a finite set of noncomplex places of K, disjoint from the set T containing the support of $\mathfrak{m}$. Recall that $U^S_{\mathfrak{m}} = U^{\mathrm{res}}_{\mathfrak{m}} \langle S \rangle$ and, by our assumption on $\mathfrak{m}$, that we have:

$$U^{\mathrm{res}}_{\mathfrak{m}} \subseteq K^\times \mathrm{N}_{L/K}(J_L)\ ;$$

we also recall that the map $\gamma^S_{\mathfrak{m}}$ defines the fundamental exact sequence of I.5.1 and that $\alpha^S_{\mathfrak{m}}$ is the canonical map:

$$I_T \longrightarrow \mathcal{C}\ell^S_{\mathfrak{m}}.$$

This commutative diagram has the following form (where N denotes $\mathrm{N}_{L/K}$):

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
 & & K^\times U^S_{\mathfrak{m}}/K^\times & = & K^\times U^S_{\mathfrak{m}}/K^\times & & & & \\
 & & \downarrow & & \downarrow & & & & \\
1 & \longrightarrow & K^\times \langle S \rangle \mathrm{N}(J_L)/K^\times & \longrightarrow & C & \xrightarrow{\rho^S_{L/K}} & \mathrm{Gal}(L^{\mathrm{ab}\,S}/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow \gamma^S_{\mathfrak{m}} & & \| & & \\
1 & \longrightarrow & \alpha^S_{\mathfrak{m}}(\mathrm{N}(I_{L,T})) & \longrightarrow & \mathcal{C}\ell^S_{\mathfrak{m}} & \xrightarrow{\alpha^S_{L/K}} & \mathrm{Gal}(L^{\mathrm{ab}\,S}/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & & & \\
 & & 1 & & 1 & & & &
\end{array}$$

To show its validity, it is sufficient to define $\alpha_{L/K}$ since, as for $\rho^S_{L/K}$, $\alpha^S_{L/K}$ will be the composition of $\alpha_{L/K}$ with the canonical projection $G^{\rm ab} \longrightarrow G^{{\rm ab}\,S}$.[27] The map $\alpha_{L/K}$ must thus be such that $\alpha_{L/K} \circ \gamma_{\mathfrak{m}} = \rho_{L/K}$.

Recall that if $\boldsymbol{x} =: (x_v)_v \in J$, $\rho_{L/K}(\boldsymbol{x}) = \prod\limits_v \left(\dfrac{x_v\,,\, L^{\rm ab}/K}{v}\right)$, and that $K^\times \subseteq {\rm Ker}(\rho_{L/K})$; it follows that we can replace $\boldsymbol{x}$ modulo $K^\times$ by $\boldsymbol{x}_{\mathfrak{m},{\rm pos}} =: (x'_v)_v \in J_{T,\mathfrak{m},{\rm pos}}$ (see I.4.3.3) so that we now have:

$$\rho_{L/K}(\boldsymbol{x}) = \rho_{L/K}(\boldsymbol{x}_{\mathfrak{m},{\rm pos}}) = \prod_v \left(\frac{x'_v\,,\, L^{\rm ab}/K}{v}\right) = \prod_{v \in Pl_0 \setminus T} \left(\frac{x'_v\,,\, L^{\rm ab}/K}{v}\right),$$

the symbols on $T \cup Pl_\infty$ being trivial since $U^{\rm res}_{\mathfrak{m}} \subseteq {\rm N}_{L^{\rm ab}/K}(U^{\rm res}_{L^{\rm ab}})$ (see 4.2.2); furthermore $\gamma_{\mathfrak{m}}(\boldsymbol{x}_{\mathfrak{m},{\rm pos}})$ is of the form $\mathscr{A}^{\rm res}_{\mathfrak{m}}(\mathfrak{a})$, where $\mathfrak{a} := \prod\limits_{v \in Pl_0} \mathfrak{p}_v^{{\rm v}(x'_v)}$ is prime to T, and defined modulo $P_{T,\mathfrak{m},{\rm pos}}$ (because of the choice of $\boldsymbol{x}_{\mathfrak{m},{\rm pos}}$). For $v \in Pl_0 \setminus T$, v is unramified in $L^{\rm ab}/K$ and we have $\left(\dfrac{x'_v\,,\, L^{\rm ab}/K}{v}\right) = \left(\dfrac{L^{\rm ab}/K}{v}\right)^{{\rm v}(x'_v)}$ (see 1.4, (vii), or 3.1.3, (vii) by density), so that we must set:

$$\alpha_{L/K}(\mathscr{A}^{\rm res}_{\mathfrak{m}}(\mathfrak{a})) := \prod_{v \in Pl_0} \left(\frac{L^{\rm ab}/K}{v}\right)^{{\rm v}(\mathfrak{a})}.$$

The diagram for $S = \emptyset$ follows by computing $\gamma_{\mathfrak{m}}(K^\times {\rm N}(J_L))$. The general case is immediate by taking quotients with $\langle\, S \,\rangle$.

It is classical to lift $\alpha_{L/K}$ to I_T, denoting also the Frobenius $\left(\dfrac{L^{\rm ab}/K}{v}\right)$ by $\left(\dfrac{L^{\rm ab}/K}{\mathfrak{p}_v}\right)$ for any finite place v unramified in $L^{\rm ab}/K$.

4.3.1 Definitions (Artin map and Artin group). (i) Let L/K be a finite extension of number fields and let T be a finite set of finite places containing the set R of places ramified in $L^{\rm ab}/K$. The Artin map (or Artin symbol) on I_T is the map:

$$\alpha_{L/K} \;:\; I_T \longrightarrow G^{\rm ab} := {\rm Gal}(L^{\rm ab}/K)$$

which sends $\mathfrak{a} \in I_T$ to:

$$\left(\frac{L^{\rm ab}/K}{\mathfrak{a}}\right) := \prod_{\mathfrak{p}} \left(\frac{L^{\rm ab}/K}{\mathfrak{p}}\right)^{{\rm v}_{\mathfrak{p}}(\mathfrak{a})}.$$

(ii) Its kernel $A_{L/K,T}$ is called the Artin group of $L^{\rm ab}/K$ in $I_T \subseteq I_R$. □

[27] In accordance with our general principles, we have $\alpha_{L/K} =: \alpha^{\rm res}_{L/K}$, and similarly for $\gamma_{\mathfrak{m}}$ and for $\rho_{L/K}$.

The diagram shows, by lifting $\alpha_{\mathfrak{m}}^{\mathrm{res}}(\mathrm{N}(I_{L,T}))$ to I_T, the following.

4.3.2 Theorem. *The kernel of the Artin map $\alpha_{L/K}$ on I_T, $T \supseteq R$, is equal to the subgroup:*

$$P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T}),$$

for any $\mathfrak{m}$ which is a multiple of the norm conductor $\mathfrak{f}$ of L^{ab}/K. □

This shows that $P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T})$ is independent of $\mathfrak{m}$, as long as this modulus is a multiple of $\mathfrak{f}$, a result which is not a priori clear.

4.3.3 Remark. As for the composite map $\alpha_{L/K}^{S} \ : \ I_T \longrightarrow G^{\mathrm{ab}\,S}$, its kernel is equal to:

$$A_{L/K,T}^{S} := P_{T,\mathfrak{m},\mathrm{pos}}\langle\, S\,\rangle\mathrm{N}_{L/K}(I_{L,T}) := P_{T,\mathfrak{m},\Delta_\infty}\,.\,\langle\, S_0\,\rangle\mathrm{N}_{L/K}(I_{L,T}),$$

for any $\mathfrak{m}$ multiple of $\mathfrak{f}$, where $\Delta_\infty := Pl_\infty^{\mathrm{r}} \setminus S_\infty$ (see I.4.4).

By definition, since $A_{L/K,T}^{S}$ corresponds to $L^{\mathrm{ab}\,S}/K$, we have:

$$P_{T,\mathfrak{m},\mathrm{pos}}\langle\, S\,\rangle\mathrm{N}_{L/K}(I_{L,T}) = P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L^{\mathrm{ab}\,S}/K}(I_{L^{\mathrm{ab}\,S},T}),$$

for any $\mathfrak{m}$ multiple of the conductor of $L^{\mathrm{ab}\,S}$. □

4.4 Artin's Reciprocity Law. The canonical isomorphism:

$$I_T/P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T}) \xrightarrow{\alpha_{L/K}} G^{\mathrm{ab}}$$

defines the Artin reciprocity law. It is the ideal version of the idelic version of the global reciprocity law asserting that $K^\times$ is in the kernel of $\rho_{L/K}$.

4.4.1 Takagi Groups — Artin and Norm Conductors. The groups:

$$T_{L/K,T,\mathfrak{m}} := P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T}),$$

which were introduced by Takagi to make explicit the congruence groups of Weber (see Subsection (d)), are thus independent of the choice of $\mathfrak{m}$ (multiple of the norm conductor $\mathfrak{f}$ of L/K); hence the canonical choice is that of:

$$T_{L/K,R,\mathfrak{f}} := P_{R,\mathfrak{f},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,R}),$$

where R is the support of $\mathfrak{f}$. This group is called simply the Takagi group of L/K and "the groups" $T_{L/K,T,\mathfrak{m}}$, the Takagi groups modulo $\mathfrak{m}$; they only depend on L^{ab}/K, but the possibility of choosing $\mathfrak{m}$ (multiple of $\mathfrak{f}$) may have some practical importance. In particular, we have the equality (for any $\mathfrak{m}$ multiple of $\mathfrak{f}$):

$$P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T}) = P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L^{\mathrm{ab}}/K}(I_{L^{\mathrm{ab}},T}).$$

The identity $A_{L/K,T} = T_{L/K,T,\mathfrak{m}} = P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T})$ is classically stated by saying that:

"The Artin group is equal to the Takagi group".

If we say that the (abelian!) Artin conductor of L/K is by definition the smallest modulus $\mathfrak{f}_A$ of K, with support equal to R, such that $P_{R,\mathfrak{f}_A,\mathrm{pos}}$ is in the kernel of the Artin map $\alpha_{L/K}$, the above results show that $\mathfrak{f} = \mathfrak{f}_A$. We can thus speak of the conductor of L/K (or of L^{ab}/K) without being specific. The fact that $P_{T,\mathfrak{m}_1,\mathrm{pos}}\,P_{T,\mathfrak{m}_2,\mathrm{pos}} = P_{T,\mathrm{g.c.d.}(\mathfrak{m}_1,\mathfrak{m}_2),\mathrm{pos}}$, where $\mathfrak{m}_1$ and $\mathfrak{m}_2$ have supports contained in T, can easily be checked directly thanks to the chinese remainder theorem, but the idelic formulation in the introduction to Subsection (a) is much more immediate; we thus obtain the existence of the abelian Artin conductor (by choosing $T = R$).

4.4.2 History. These statements in terms of ideal groups (the equality of the Artin and Takagi groups, and the isomorphism $I_T/T_{L/K,T,\mathfrak{m}} \simeq G^{\mathrm{ab}}$) form the historical approach to the fundamental results of class field theory. In particular, the only proof of the equality, valid for any number field:

$$(I_T : P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T})) = [L^{\mathrm{ab}} : K],$$

was split in the difficult proofs of the first inequality of class field theory ("$\geq$", Takagi) and of the second inequality or universal equality ("$\leq$", Weber (1897) using analytic methods, and Hasse–Scholz (1929) in the general case). It is only later (1920/1924) that Artin introduced the map $\alpha_{L/K}$, constructed with the Frobenius symbols, and showed (1927), using ideas of Čebotarev (the crossing with a cyclic cyclotomic field), that $\alpha_{L/K}$ gave the exact sequence:

$$1 \longrightarrow P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T}) \longrightarrow I_T \longrightarrow G^{\mathrm{ab}} \longrightarrow 1,$$

thus giving for the first time the general notion of a global reciprocity map; the idelic version of Section 3 (Chevalley (1936/1940)) representing only the translation in the other direction, showing that it is possible (although apparently illogical but very useful) to go from a global approach of class field theory to a local approach (after Hasse–Schmidt (1930)).

The direct proof of the existence of an Artin conductor for an abelian extenion L/K, i.e., the existence of $\mathfrak{m}$ such that $\alpha_{L/K}$ is trivial on $P_{T,\mathfrak{m},\mathrm{pos}}$ (or such that $K^{\times}U_{\mathfrak{m}}^{\mathrm{res}} \subseteq \mathrm{Ker}(\rho_{L/K})$ in idelic terms) uses very strongly the properties of cyclotomic fields (in other words, essentially class field theory for $\mathbb{Q}$ with which we must begin); although it is only a series of elementary exercises (see [d, Lang1, Ch. X, § 2]), this proof is still considered as deep since it involves the construction of abelian extensions of K satisfying certain local conditions and giving already enough information on $\mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K)$. For

instance, one of the key arguments is Lemma 1 of [d, Lang1, Ch. X, § 2] which originates in Birkhoff–Vandiver (1907), of which several proofs have been given by Chevalley in [h, Che1], Iyanaga in [h, Iy2], van der Waerden (1934), Takagi (1948); this lemma states that if $a > 1$ and $e \geq 1$ are integers and p a prime number, there exists a prime number q such that a modulo (q) is of order equal to p^e.

At this step, we should mention, among other interesting studies of Kubota (like [Kub2, Kub3]), the paper [KO] of Kubota–Oka (2000) proving that Artin's reciprocity law can be deduced from the case of cyclotomic extensions and Kummer extensions. This paper is based on the Schmidt–Chevalley theorem.

The necessity of performing such constructions shows that it seems impossible to give a naïve proof of the fact that (to give a minimal example in the case of conductor 1):

$$\text{“}\mathfrak{p} \text{ is a principal prime ideal of } K = \mathbb{Q}(\sqrt{10}\,),$$

if and only if:

$$\text{the Frobenius of } \mathfrak{p} \text{ in } K(\sqrt{5}\,)/K \text{ is trivial”}$$

(since $K(\sqrt{5}\,)$ is the Hilbert class field of K). This example may not be completely convincing since it can be solved using genus theory (here Gauss's genus theory of quadratic forms, see IV.4.2.10), which can be considered as intermediate between naïve and highly nontrivial. On the contrary, the analogous result:

$$\text{“}\mathfrak{p} \text{ is a principal prime ideal of } K = \mathbb{Q}(\sqrt{-23}\,),$$

if and only if:

$$\text{the Frobenius of } \mathfrak{p} \text{ in } K(\theta)/K \text{ is trivial”}$$

(where $\mathrm{Irr}(\theta, \mathbb{Q}) := X^3 - X - 1$), seems faultless (see 5.2.1 for more details), except that $\mathbb{Q}(\sqrt{-23}\,)$ has no nontrivial units, and to stress even more the origin of the difficulties for an arbitrary base field, we can cite Tate (from [d, CF, Ch. VII, § 6]) who asserts: “It may well be that it is the connected component that prevents a simple proof of the reciprocity law in the general case”. Indeed, we will see that $D_0 = 1$ if and only if the $\mathbb{Z}$-rank of E^{ord} is equal to zero (i.e., K is equal to $\mathbb{Q}$ or to an imaginary quadratic field, fields for which questions having to do with reciprocity laws are indeed simpler).

Finally, we can replace $\mathbb{Q}(\sqrt{-23}\,)$ by $\mathbb{Q}(\sqrt{79}\,)$, whose Hilbert class field is also of degree 3, and obtain the same conclusion.

The advantage of Artin's formulation above is that in general we know how to compute the Frobenius' (in particular numerically). Thus, we are going to give a global method for the computation of the symbols:

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right),\ x\in K^{\times},\ v\in Pl.$$

4.4.3 Computation of Hasse Symbols by Global Means. Call R the set of (finite) places ramified in L^{ab}/K, and let $\mathfrak{m}$ be a multiple of the conductor $\mathfrak{f}$ (it does not matter if the support T of $\mathfrak{m}$ strictly contains R, which will be the case if the conductor and its support are not precisely known). Finally, set $\mathfrak{m} =: \prod_{v\in T}\mathfrak{p}_v^{m_v}$ with $m_v\geq 0$.

Let $x\in K^{\times}$; fix a place v of K, and let us consider several cases:

(α) $v\in Pl_{\infty}^{\mathrm{r}}$. By 3.1.3, (vii), we have:

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right)=\left(\frac{L^{\mathrm{ab}}/K}{v}\right)^{\mathrm{v}(x)},$$

where $\mathrm{v}(x)=0$ (resp. 1) if $i_v(x)>0$ (resp. $i_v(x)<0$).

(β) $v\in Pl_0\backslash T$. Similarly, since v is unramified, we have:

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right)=\left(\frac{L^{\mathrm{ab}}/K}{v}\right)^{\mathrm{v}(x)}.$$

(γ) $v\in T$. Let $x'\in K^{\times}$ be such that (chinese remainder theorem):

(i) $i_v(x'x^{-1})\in U_v^{m_v}$,

(ii) $i_{v'}(x')\in U_{v'}^{m_{v'}}$, for each place $v'\in T,\ v'\neq v$,

(iii) $i_{v'}(x')>0$ for each place $v'\in Pl_{\infty}^{\mathrm{rc}}$ (i.e., each real place v' complexified in L^{ab}/K).

Then, by the product formula we have:

$$\left(\frac{x'\,,\,L^{\mathrm{ab}}/K}{v}\right)=\prod_{v'\in Pl,v'\neq v}\left(\frac{x'\,,\,L^{\mathrm{ab}}/K}{v'}\right)^{-1},$$

and since $\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right)=\left(\frac{x'\,,\,L^{\mathrm{ab}}/K}{v}\right)$, by (i) and the definition of the local v-conductor of L^{ab}/K, we have:

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right)=\prod_{v'\in Pl,v'\neq v}\left(\frac{x'\,,\,L^{\mathrm{ab}}/K}{v'}\right)^{-1};$$

let us compute the symbols occurring in the right hand side:

- if $v'\in T\backslash\{v\},\ i_{v'}(x')\in U_{v'}^{m_{v'}}$ (by (ii)) and we have $\left(\frac{x'\,,\,L^{\mathrm{ab}}/K}{v'}\right)=1$,
- if $v'\in Pl_{\infty}$, $\left(\frac{x'\,,\,L^{\mathrm{ab}}/K}{v'}\right)=1$ since either $\left(\frac{L^{\mathrm{ab}}/K}{v'}\right)=1$ if v' is complex or noncomplexified real, or $\mathrm{v}'(x')=0$ for v' complexified real (by (iii)),

- if $v' \in Pl_0\backslash T$, v' is unramified and we can write (by 3.1.3, (vii)):

$$\left(\frac{x'\,,\,L^{\mathrm{ab}}/K}{v'}\right)^{-1} = \left(\frac{L^{\mathrm{ab}}/K}{v'}\right)^{-\mathrm{v}'(x')}\;;$$

finally, we have obtained:

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right) = \prod_{v'\in Pl_0\backslash T}\left(\frac{L^{\mathrm{ab}}/K}{v'}\right)^{-\mathrm{v}'(x')}.$$

It follows that if we write:

$$(x') =: \mathfrak{p}_v^{\mathrm{v}(x')}\mathfrak{a} = \mathfrak{p}_v^{\mathrm{v}(x)}\mathfrak{a}$$

(we have $\mathrm{v}(x') = \mathrm{v}(x)$ by (i) even when $m_v = 0$), then $\mathfrak{a}$ is prime to T by (ii) and we obtain, since $Pl_0\backslash T$ does not contain v:

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right) = \left(\frac{L^{\mathrm{ab}}/K}{\mathfrak{a}}\right)^{-1} = \alpha_{L/K}(\mathfrak{a})^{-1},$$

which finishes the hand computation of the Hasse symbol of an $x \in K^\times$ which is not necessarily prime to the place v under consideration.

We will come back to this procedure in 7.5 for the practical computation of Hilbert symbols.

4.4.3.1 Remarks. (i) The auxiliary element x' is called a v-associate (or a $\mathfrak{p}_v$-associate) of x.

(ii) In the case where $v \in T$ is unramified (i.e., $v \notin R$), the above computation still yields $(x') = \mathfrak{p}_v^{\mathrm{v}(x)}\mathfrak{a}$, $\mathfrak{a}$ prime to T, but the v-associate x' is then such that $\alpha_{L/K}((x')) = 1$ (the Artin map is defined since here (x') is prime to R; moreover $\mathfrak{f}\,|\,\mathfrak{m}' := \mathfrak{m}\,\mathfrak{p}_v^{-m_v}$ and $(x') \in P_{T,\mathfrak{m}'}$ with $i_{v'}(x') > 0$ on Pl_∞^{rc}; since by definition $L^{\mathrm{ab}\,S} = L^{\mathrm{ab}}$ for $S = Pl_\infty^{\mathrm{r}}\backslash Pl_\infty^{\mathrm{rc}}$, the formula given in 4.3.3 yields $P_{T,\mathfrak{m}',Pl_\infty^{\mathrm{rc}}} \subseteq P_{T,\mathfrak{m}',\mathrm{pos}}\mathrm{N}_{L^{\mathrm{ab}}/K}(I_{L^{\mathrm{ab}},T})$, giving the result), and we find once again that by 3.1.3, (vii):

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right) = \alpha_{L/K}(\mathfrak{a})^{-1} = \left(\frac{L^{\mathrm{ab}}/K}{\mathfrak{p}_v}\right)^{\mathrm{v}(x)}.$$

(iii) If $\mathfrak{f}$ is primary (i.e., a power of $\mathfrak{p}_v$), then any $x \in K^\times$ (positive at the complexified real places) is equal to its own v-associate, and we have:

$$\left(\frac{x\,,\,L^{\mathrm{ab}}/K}{v}\right) = \alpha_{L/K}\Big((x)\mathfrak{p}_v^{-\mathrm{v}(x)}\Big)^{-1}. \qquad \square$$

4.4.3.2 Example. Let $K = \mathbb{Q}$ and let $L = L^{\mathrm{ab}} = \mathbb{Q}(\sqrt{5}, \sqrt{-3}\,)$. Let us compute the Hasse symbol $\left(\frac{15\,,\,L/\mathbb{Q}}{(3)}\right)$. The conductor of L is equal to (15); we must find $x' \in \mathbb{Q}^\times$ such that:

$$\begin{aligned} \frac{x'}{15} &\equiv 1 \bmod (3), \\ x' &\equiv 1 \bmod (5), \\ x' &> 0\ ; \end{aligned}$$

$x' = 6$ is suitable, so that $\mathfrak{a} = (2)$ and:

$$\left(\frac{15\,,\,L/\mathbb{Q}}{(3)}\right) = \left(\frac{L/\mathbb{Q}}{(2)}\right)^{-1}.$$

But it is easy to see that (2) is inert in $\mathbb{Q}(\sqrt{5}\,)$ and in $\mathbb{Q}(\sqrt{-3}\,)$; the Frobenius of (2) is thus a generator of $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{-15}\,))$. It follows that 15 is not a local norm at (3).

Since the product formula is reduced here to:

$$\left(\frac{15\,,\,L/\mathbb{Q}}{(3)}\right)\left(\frac{15\,,\,L/\mathbb{Q}}{(5)}\right) = 1,$$

the symbol at (5) is the same, but the (3)-associate x' is not suitable anymore for the direct computation of $\left(\frac{15\,,\,L/\mathbb{Q}}{(5)}\right)$; a (5)-associate is for example 40 which indeed gives the expected result.

Finally, if we omit the condition $x' > 0$, for instance for a (3)-associate we can try:

$$x'' = -39,$$

which yields $\mathfrak{a} = (13)$; but the Frobenius of (13) being the generator of $\mathrm{Gal}(L/\mathbb{Q}(\sqrt{-3}\,))$, the result is false! □

4.4.3.3 Exercise (the case of cyclotomic fields). Let $K = \mathbb{Q}$ and let $L = \mathbb{Q}(\mu_m)$; we assume that m is odd or divisible by 4. Describe the method for the computation of $\left(\frac{x\,,\,L/\mathbb{Q}}{(\ell)}\right)$, $x \in \mathbb{Q}^\times$, for a prime divisor ℓ of m.

Deduce the values of $\left(\frac{\ell\,,\,L/\mathbb{Q}}{(\ell)}\right)$ and of $\left(\frac{y\,,\,L/\mathbb{Q}}{(\ell)}\right)$ for y prime to ℓ.

Characterize the x which are local norms at (ℓ) for $L/\mathbb{Q}$.

Answer. The conductor of $L/\mathbb{Q}$ is equal to $m\mathbb{Z}$ (see 5.5); set $m =: \ell^a n$ and $x =: \ell^b y$ with n and y prime to ℓ. We must find $x' = \ell^b y'$, with $y' \in \mathbb{Q}^\times$ such that:

$$\begin{aligned} y' &\equiv y \bmod (\ell^a), \\ \ell^b y' &\equiv 1 \bmod (n), \\ y' &> 0, \end{aligned}$$

which can be achieved thanks to suitable extended Euclid relations. The result is the Artin symbol:

$$\left(\frac{L/\mathbb{Q}}{(y')}\right)^{-1}$$

corresponding to the inverse of $\overline{y'} \in (\mathbb{Z}/m\mathbb{Z})^\times$ under the usual canonical isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$ (see 5.5.2).

It follows that $\left(\frac{\ell,\, L/\mathbb{Q}}{(\ell)}\right)$ (take $b=1$, $y=1$) is the lift of $\left(\frac{\mathbb{Q}(\mu_n)/\mathbb{Q}}{(\ell)}\right)$ to $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_{\ell^a}))$, and that for all $y>0$ prime to ℓ (take $b=0$), $\left(\frac{y\,,\, L/\mathbb{Q}}{(\ell)}\right)$ is the lift of $\left(\frac{\mathbb{Q}(\mu_{\ell^a})/\mathbb{Q}}{(y)}\right)^{-1}$ to $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_n))$. This should be compared with the results of Exercise 3.4.3.

The rational number $x = \ell^b y$ is a local norm at ℓ in $L/\mathbb{Q}$ if and only if $y' \equiv 1 \bmod (m)$; but this is equivalent to:

$$y \equiv 1 \bmod (\ell^a),$$
$$\ell^b \equiv 1 \bmod (n).$$

We see that $N_1 := \ell^{\mathbb{Z}} \oplus (1+\ell^a\mathbb{Z}_\ell)$ and $N_2 := \ell^{f\mathbb{Z}} \oplus \mathbb{Z}_\ell^\times$ are the norm groups of $\mathbb{Q}_\ell(\mu_{\ell^a})$ and $\mathbb{Q}_\ell(\mu_n)$, where $f \,|\, b$ is the residue degree of ℓ in $\mathbb{Q}(\mu_n)/\mathbb{Q}$ (smallest integer such that $\ell^f \equiv 1 \bmod (n)$): use respectively 3.4.3, (i), and the fact that $\mathbb{Q}_\ell(\mu_n)/\mathbb{Q}_\ell$ is unramified; the norm group of $\mathbb{Q}_\ell(\mu_m)$ is then $N_1 \cap N_2 = \ell^{f\mathbb{Z}} \oplus (1+\ell^a\mathbb{Z}_\ell)$ giving again the result. □

Let L/K be a finite extension of number fields and L'/K a subextension of L/K. Let S be a set of noncomplex places of K, disjoint from $T \supseteq R$; we denote by S' the set of places of L' above those of S, and put $G^{\mathrm{ab}\,S} := \mathrm{Gal}(L^{\mathrm{ab}\,S}/K)$. Let us state the functorial properties of the Artin map on:

$$\mathcal{C}\ell^S_{\mathfrak{m}} := I_T/P_{T,\mathfrak{m},\mathrm{pos}}\langle\, S\,\rangle := I_T/P_{T,\mathfrak{m},\Delta_\infty}\cdot\langle\, S_0\,\rangle,$$

with $\Delta_\infty := P^{\mathrm{r}}_\infty \setminus S_\infty$, which follow from those of $\rho^S_{L/K}$ (this is a simple transcription of Theorem 3.3).

4.5 Theorem (properties of the Artin map). *Let $\mathfrak{m}$ with support contained in T be a multiple of the norm conductor of L/K (i.e., of L^{ab}/K).*
We have the following properties:

(i) We have the exact sequence:

$$1 \longrightarrow \mathcal{A}\ell^S_{\mathfrak{m}}(\mathrm{N}_{L/K}(I_{L,T})) \longrightarrow \mathcal{C}\ell^S_{\mathfrak{m}} \xrightarrow{\alpha^S_{L/K}} G^{\mathrm{ab}\,S} \longrightarrow 1,$$

where $\mathcal{A}\ell^S_{\mathfrak{m}}$ is the map $I_T \longrightarrow \mathcal{C}\ell^S_{\mathfrak{m}}$;

(ii) the composition of $\alpha^S_{L/K}$ and of the projection $G^{\mathrm{ab}\,S} \longrightarrow \mathrm{Gal}(L'^{\mathrm{ab}\,S}/K)$ is equal to $\alpha^S_{L'/K}$;

(iii) for each place $v \in T$, set $\mathfrak{m}_v := \mathfrak{p}_v^{\mathrm{v}(\mathfrak{m})}$; then the decomposition group (resp. the inertia group, resp. the higher ramification group with

upper index $i \geq 1$) of $v \in T$ in $L^{\mathrm{ab}\,S}/K$ is the image under $\alpha^S_{L/K}$ of $(P_{T\setminus\{v\},\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}} \cdot \langle\, \mathfrak{p}_v \,\rangle) \cap I_T$ [28] *(resp. of $P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}}$, resp. of $P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v}\mathfrak{p}_v^i,\mathrm{pos}}$); if $v \notin T$ is finite, the decomposition group of v is the image of $\langle\, \mathfrak{p}_v \,\rangle$; if $v \in Pl^{\mathrm{r}}_\infty$, the decomposition group of v for $L^{\mathrm{ab}\,S}/K$ is the image under $\alpha^S_{L/K}$ of $P_{T,\mathfrak{m},Pl^{\mathrm{r}}_\infty\setminus\{v\}}$;*

(iv) for all $\mathfrak{a}' \in I_{L',T}$, prime to the norm conductor of L/L', the image of $\left(\frac{L^{\mathrm{ab}'\,S'}/L'}{\mathfrak{a}'}\right)$ in $G^{\mathrm{ab}\,S}$ is $\left(\frac{L^{\mathrm{ab}\,S}/K}{\mathrm{N}_{L'/K}(\mathfrak{a}')}\right)$; in particular, we have:

$$\mathrm{Gal}(L^{\mathrm{ab}\,S}/L'^{\mathrm{ab}\,S}) \;= \alpha^S_{L/K}(\mathrm{N}_{L'/K}(I_{L',T}))\;;$$

(v) for all $\mathfrak{a} \in I_T$, prime to the norm conductor of L/L', the image of $\left(\frac{L^{\mathrm{ab}\,S}/K}{\mathfrak{a}}\right)$ under the transfer map (from $G^{\mathrm{ab}\,S}$ to $\mathrm{Gal}(L^{\mathrm{ab}'\,S'}/L')$) is $\left(\frac{L^{\mathrm{ab}'\,S'}/L'}{\mathfrak{a}'}\right)$, where $\mathfrak{a}'$ is obtained by extending $\mathfrak{a}$ to L';

(vi) for any $\mathbb{Q}$-isomorphism τ of L in $\overline{\mathbb{Q}}$, we have for all $\mathfrak{a} \in I_T$:

$$\left(\frac{\tau\, L^{\mathrm{ab}\,S}/\tau K}{\tau\mathfrak{a}}\right) = \tau \circ \left(\frac{L^{\mathrm{ab}\,S}/K}{\mathfrak{a}}\right) \circ \tau^{-1} \text{ on } \tau L^{\mathrm{ab}\,S} = (\tau L)^{\mathrm{ab}\,\tau S}. \qquad \square$$

Note. In (iv) and (v), the set T (which contains the set of places of L ramified in L^{ab}/K) may be inadequate. Indeed, consider the following example (with $K = \mathbb{Q}$): $L = \mathbb{Q}(\mu_4, \sqrt[4]{18})$, $L' = \mathbb{Q}(\mu_4)$, $T = \{2\}$, for which $L^{\mathrm{ab}'} = L$, $L^{\mathrm{ab}} = L'\mathbb{Q}(\sqrt{18}) = \mathbb{Q}(\mu_8)$, $L'^{\mathrm{ab}} = L'$; the ideal $\mathfrak{a}' = (3)$ is prime to T but its Artin Symbol in L/L' does not exist; the Artin Symbol of $\mathfrak{a} = (3)$ exists in L^{ab}/K but not its transfer. However, this is not annoying since any element (of the above abelian Galois groups) is the Artin Symbol of a suitable ideal.

4.5.1 Corollary. *We have:*

$$\mathscr{A}^{\mathrm{res}}_{\mathfrak{m}}(\mathrm{N}_{L/K}(I_{L,T})) = \mathscr{A}^{\mathrm{res}}_{\mathfrak{m}}(\mathrm{N}_{L^{\mathrm{ab}}/K}(I_{L^{\mathrm{ab}},T})). \qquad \square$$

4.5.2 Corollary. *We have the exact sequences:*

$$1 \longrightarrow \mathscr{A}^{\mathrm{res}}_{\mathfrak{m}}(\mathrm{N}_{L/K}(I_{L,T})) \longrightarrow \mathscr{C}^{\mathrm{res}}_{\mathfrak{m}} \xrightarrow{\alpha^{\mathrm{res}}_{L/K}} \mathrm{Gal}(L^{\mathrm{ab}}/K) \longrightarrow 1,$$

$$1 \longrightarrow \mathscr{A}^{\mathrm{ord}}_{\mathfrak{m}}(\mathrm{N}_{L/K}(I_{L,T})) \longrightarrow \mathscr{C}^{\mathrm{ord}}_{\mathfrak{m}} \xrightarrow{\alpha^{\mathrm{ord}}_{L/K}} \mathrm{Gal}(L^{\mathrm{ab\,nc}}/K) \longrightarrow 1,$$

where $L^{\mathrm{ab\,nc}}/K$ is the maximal Pl^{r}_∞-split (i.e., noncomplexified) abelian subextension of L/K. $\square$

4.5.3 Example. In the particular case where the extension L^{ab}/K has conductor $\mathfrak{f} = 1$ (i.e., L^{ab}/K is unramified but may be complexified; in other words $L^{\mathrm{ab}} \subseteq H^{\mathrm{res}}$), we obtain, by taking $T = \emptyset$, the exact sequences:

[28] Note that $\left(P_{T\setminus\{v\},\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}} \cdot \langle\, \mathfrak{p}_v \,\rangle\right) \cap I_T = \left\{(x)\,\mathfrak{p}_v^{-\mathrm{v}(x)},\ x \in K^\times_{T\setminus\{v\},\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}}\right\}$.

$$1 \longrightarrow \mathscr{A}^{\mathrm{res}}(\mathrm{N}_{L/K}(I_L)) \longrightarrow \mathscr{C}^{\mathrm{res}} \xrightarrow{\alpha^{\mathrm{res}}_{L/K}} \mathrm{Gal}(L^{\mathrm{ab}}/K) \longrightarrow 1,$$

$$1 \longrightarrow \mathscr{A}^{\mathrm{ord}}(\mathrm{N}_{L/K}(I_L)) \longrightarrow \mathscr{C}^{\mathrm{ord}} \xrightarrow{\alpha^{\mathrm{ord}}_{L/K}} \mathrm{Gal}(L^{\mathrm{ab\,nc}}/K) \longrightarrow 1,$$

which give a description of $\mathrm{Gal}(L^{\mathrm{ab}}/K)$ (resp. of $\mathrm{Gal}(L^{\mathrm{ab\,nc}}/K)$) in terms of usual ideal classes; this occurs only if the base field is not principal in the restricted sense (resp. in the ordinary sense). □

We return to the general setting of Theorem 4.5. For this, let $\mathfrak{m}$ with support contained in T be a multiple of the conductor $\mathfrak{f}$ of L/K, and let A_T be the Artin group of L/K in I_T which we can take to be equal to $T_{T,\mathfrak{m}} = P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T})$. For each $v \in T$ we set $\mathfrak{m}_v := \mathfrak{p}_v^{\mathrm{v}(\mathfrak{m})}$.

4.5.4 Corollary (decomposition law of places in L^{ab}/K). *We have:*

(i) (ramification groups). From the Artin isomorphism $I_T/A_T \simeq G^{\mathrm{ab}}$, we obtain, for each place $v \in T$ and all $i \geq 1$, the isomorphisms:[29]

$$P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v}\mathfrak{p}_v^i,\mathrm{pos}}A_T/A_T \simeq D_v^i(L^{\mathrm{ab}}/K)\ ;$$

in particular, $v \in T$ is unramified in L^{ab}/K if and only if we have:

$$P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}} \subseteq A_T.$$ [30]

Similarly, v is tamely ramified in L^{ab}/K if and only if:

$$P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v}\mathfrak{p}_v,\mathrm{pos}} \subseteq A_T.$$

(ii) (decomposition groups). For $v \in T$, let $\mathfrak{a}_v$ be prime to T and such that $\mathfrak{a}_v = \mathfrak{p}_v\big(u_{\frac{\mathfrak{m}}{\mathfrak{m}_v}}\big)$, $u_{\frac{\mathfrak{m}}{\mathfrak{m}_v}} \in K^{\times}_{T\setminus\{v\},\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}}$ (see I.5.1.2); we then have the isomorphism:

$$\langle\,\mathfrak{a}_v\,\rangle P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}}A_T/A_T \simeq D_v(L^{\mathrm{ab}}/K)\ ;$$

if $v \in Pl_0\backslash T$ (v is thus unramified), we have:

$$\langle\,\mathfrak{p}_v\,\rangle A_T/A_T \simeq D_v(L^{\mathrm{ab}}/K),$$

and the residue degree $f_v(L^{\mathrm{ab}}/K)$ of v in L^{ab}/K is equal to the order of the class of $\mathfrak{p}_v$ in I_T/A_T.

(iii) If $v \in Pl_\infty^{\mathrm{r}}$, then v is noncomplexified in L^{ab}/K if and only if:

$$P_{T,\mathfrak{m},\mathrm{pos}}\langle\,v\,\rangle := P_{T,\mathfrak{m},Pl_\infty^{\mathrm{r}}\setminus\{v\}} \subseteq A_T.$$ □

[29] See 1.1.1 for some notations about higher ramification.
[30] Relate this with the characterization of the conductor given in 4.4.1.

4.5.5 Remark. For the noncomplexification of a real place v, a necessary and sufficient condition is that for an arbitrary element $u_{\mathfrak{m},v} \in K^{\times}_{T,\mathfrak{m},Pl^{\mathrm{r}}_{\infty}\setminus\{v\}}$ such that $i_v(u_{\mathfrak{m},v}) < 0$ then $(u_{\mathfrak{m},v}) \in A_T$.

The case of an infinite place $v \in Pl^{\mathrm{r}}_{\infty}$ can be treated directly if L^{ab} is known (but it is not anymore a class field theoretic proof): we have $f_v = 1$ (resp. 2) if the extension $i_{w_0}(L^{\mathrm{ab}})$ is real (resp. complex) for an arbitrary $w_0|v$ in L^{ab} (we have $i_v(K) \subset \mathbb{R}$ since v is real). □

4.6 Density Theorem (1926). The surjectivity of $\alpha_{L/K}$ can be shown without using analytic arguments, and one can even prove a little more (see [e, Ko3, Ch. 2, § 4.4, Th. 2.70]); however, in practice it is better to consider it through the density theorem which asserts that every class $\mathfrak{a}P_{R,\mathfrak{f},\mathrm{pos}}$, $\mathfrak{a}$ prime to $\mathfrak{f}$, contains an infinity of prime ideals, with density:

$$\frac{1}{|\mathcal{C}^{\mathrm{res}}_{\mathfrak{f}}|}.$$

Thus, for any $\sigma \in G^{\mathrm{ab}}$, we can have the equality $\left(\frac{L^{\mathrm{ab}}/K}{\mathfrak{p}}\right) = \sigma$, for an infinite number of prime ideals $\mathfrak{p}$ of K, unramified in L^{ab}/K, with density equal to:

$$\frac{1}{[L^{\mathrm{ab}} : K]}.$$

Note. One can find in [d, Lang1, Ch. VIII, § 4] the general Galois statement (the Čebotarev theorem) which is in fact deduced, after an argument of Deuring (1934), from the above abelian density theorem; see also [c, Nar1, Ch. 7] and [e, Ko3, Ch. 1, § 6.7]. More precisely, this theorem was conjectured by Frobenius (1896), proved by Čebotarev (1926), with a simplified proof by Schreier (1927); these proofs (using cyclotomic fields) originate, as we have mentioned in 4.4.2, the fundamental proof by Artin of his reciprocity law. The Čebotarev theorem is the following. Let L/K be Galois with Galois group G, and let $t \in G$; then the set of unramified primes $\mathfrak{p}$ of K such that $t = \left(\frac{L/K}{\mathfrak{P}}\right)$, for a $\mathfrak{P}|\mathfrak{p}$ in L, has a density equal to $\frac{1}{[L:K]}\,|\{sts^{-1},\ s \in G\}|$ (note that $s \circ \left(\frac{L/K}{\mathfrak{P}}\right) \circ s^{-1} = \left(\frac{L/K}{s\mathfrak{P}}\right)$ as usual).

In terms of generalized class groups, the existence theorem takes the following form (we do not state once more the four usual properties which characterize this correspondence; see 3.5, (i) to (iv)).

4.7 Theorem (global existence). *Let $\mathfrak{m}$ be a modulus of K built from $T \subset Pl_0$. Then there exists a bijective Galois correspondence between the set of subgroups $\mathcal{C}_{\mathfrak{m}}$ of $\mathcal{C}^{\mathrm{res}}_{\mathfrak{m}}$ (or of subgroups $N_{\mathfrak{m}}$ of I_T containing $P_{T,\mathfrak{m},\mathrm{pos}}$) and the set of abelian extensions M of K, of conductor $\mathfrak{f}$ dividing $\mathfrak{m}$.*
The Artin map yields the equivalent two exact sequences:

$$1 \longrightarrow \mathcal{C}_{\mathfrak{m}} \longrightarrow \mathscr{C}_{\mathfrak{m}}^{\mathrm{res}} \xrightarrow{\alpha_{M/K}^{\mathrm{res}}} \mathrm{Gal}(M/K) \longrightarrow 1,$$
$$1 \longrightarrow N_{\mathfrak{m}} \longrightarrow I_T \xrightarrow{\alpha_{M/K}^{\mathrm{res}}} \mathrm{Gal}(M/K) \longrightarrow 1,$$

with $\mathcal{C}_{\mathfrak{m}} := \alpha_{\mathfrak{m}}^{\mathrm{res}}(\mathrm{N}_{M/K}(I_{M,T}))$ *and* $N_{\mathfrak{m}} := P_{T,\mathfrak{m},\mathrm{pos}}\,\mathrm{N}_{M/K}(I_{M,T})$. □

The group $\mathcal{C}_{\mathfrak{m}}$ (resp. $N_{\mathfrak{m}}$) is called the class group (resp. the congruence group) corresponding to M/K (but it is also a norm group in terms of ideal classes).

4.7.1 Remarks. (i) The Artin group of the decomposition subfield of v in M (with Artin group A_T) is given by:

$$\langle\, \mathfrak{a}_v \,\rangle P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}} A_T, \quad \langle\, \mathfrak{p}_v \,\rangle A_T, \quad \langle\, (u_{\mathfrak{m},v}) \,\rangle A_T,$$

depending on the situation (by 4.5.4, (ii), (iii), and 4.5.5); that of the inertia subfield is given by:

$$P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}} A_T.$$

(ii) The Artin group of the maximal v-tamely ramified subextension is:

$$P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v}\mathfrak{p}_v,\mathrm{pos}} A_T.$$

(iii) If we want S-decomposition, we replace $N_{\mathfrak{m}} := P_{T,\mathfrak{m},\mathrm{pos}}\,\mathrm{N}_{M/K}(I_{M,T})$ by:

$$P_{T,\mathfrak{m},\mathrm{pos}}\langle\, S \,\rangle\, \mathrm{N}_{M/K}(I_{M,T}) := P_{T,\mathfrak{m},\Delta_\infty} \,.\, \langle\, S_0 \,\rangle\, \mathrm{N}_{M/K}(I_{M,T}),$$

where $\Delta_\infty := Pl_\infty^{\mathrm{r}} \setminus S_\infty$. □

4.7.2 Corollary (norm lifting theorem). *Let L/K be a finite extension of number fields, let M/K be an abelian extension, and let $\mathfrak{m}$ with support contained in T be a modulus of K multiple of the conductor of M/K.*
Then any modulus $\mathfrak{m}'$ of L, with support contained in the set of places of L above those of T and such that:

$$\mathrm{N}_{L/K}(P_{L,T,\mathfrak{m}',\mathrm{pos}}) \subseteq P_{T,\mathfrak{m},\mathrm{pos}},$$

is a multiple of the conductor of LM/L.
If $\mathcal{C}$ is the subgroup of $\mathscr{C}_{\mathfrak{m}}^{\mathrm{res}}$ corresponding to M, then the subgroup $\mathcal{C}'$ of $\mathscr{C}_{L,\mathfrak{m}'}^{\mathrm{res}}$ corresponding to LM over L is given by:

$$\left\{\alpha_{L,\mathfrak{m}'}^{\mathrm{res}}(\mathfrak{a}'),\ \mathfrak{a}' \in I_{L,T},\ \alpha_{\mathfrak{m}}^{\mathrm{res}}(\mathrm{N}_{L/K}(\mathfrak{a}')) \in \mathcal{C}\right\} =: \mathrm{N}_{L/K}^{-1}(\mathcal{C}).$$

Proof. We check that the given condition is equivalent to:

$$\mathrm{N}_{L/K}(L^\times U_{L,\mathfrak{m}'}^{\mathrm{res}}) \subseteq K^\times U_{\mathfrak{m}}^{\mathrm{res}}.$$

It follows by 3.3, (iv), that the image of $\rho_{LM/L}(U_{L,\mathfrak{m}'}^{\mathrm{res}})$ in $\mathrm{Gal}(M/K)$ is:

$$\rho_{M/K}(\mathrm{N}_{L/K}(U^{\mathrm{res}}_{L,\mathfrak{m}'})) \subseteq \rho_{M/K}(K^{\times}U^{\mathrm{res}}_{\mathfrak{m}}) = 1 \ ;$$

so that $U^{\mathrm{res}}_{L,\mathfrak{m}'} \subseteq \mathrm{Ker}(\rho_{LM/L})$, which indeed shows that $\mathfrak{m}'$ is a multiple of $\mathfrak{f}_{LM/L}$. The rest is then only a translation of global norm lifting Theorem 3.5.3 in terms of class groups. □

We will return in 5.7 to the action of the norm in this context of generalized class groups.

It is clear that the fields corresponding to $\mathcal{C}_{\mathfrak{m}} = 1$ (i.e., $N_{\mathfrak{m}} = P_{T,\mathfrak{m},\mathrm{pos}}$ in terms of ideal groups, $N_{\mathfrak{m}} = K^{\times}U^{\mathrm{res}}_{\mathfrak{m}}$ in terms of idèle groups) play a crucial role in the correspondence of class field theory; hence we are going to look in more detail at these ray class fields.

§5 Ray Class Fields — Hilbert Class Fields

Let K be a number field and let $\mathfrak{m}$ be a modulus of K built on $T \subset Pl_0$. The unique abelian extension of K corresponding to $K^{\times}U^{\mathrm{res}}_{\mathfrak{m}}$ in the idelic version, in other words to $P_{T,\mathfrak{m},\mathrm{pos}}$ in the ideal group version, is called the restricted (or narrow) ray class field modulo $\mathfrak{m}$, and is denoted:

$$K_{(\mathfrak{m})} =: K_{(\mathfrak{m})^{\mathrm{res}}} \ ;$$

thus, for this field we have $\mathrm{Gal}(K_{(\mathfrak{m})^{\mathrm{res}}}/K) \simeq \mathcal{C}\ell^{\mathrm{res}}_{\mathfrak{m}}$ and:

$$\mathrm{N}_{K_{(\mathfrak{m})^{\mathrm{res}}}/K}(J_{K_{(\mathfrak{m})^{\mathrm{res}}}}) \subset K^{\times}U^{\mathrm{res}}_{\mathfrak{m}} \ \text{ and } \ \mathrm{N}_{K_{(\mathfrak{m})^{\mathrm{res}}}/K}(I_{K_{(\mathfrak{m})^{\mathrm{res}}},T}) \subset P_{T,\mathfrak{m},\mathrm{pos}}.$$

For $\mathfrak{m} = 1$, we obtain $K_{(1)^{\mathrm{res}}}$, denoted H^{res}, and called the restricted Hilbert class field. Hilbert had very early conjectured the existence of the absolute (or wide) class field H^{ord} (for us the maximal Pl^{r}_{∞}-split subextension of H^{res}, called the ordinary class field), and in this context, in which most of the proofs are due to Furtwängler, had predicted the main principles of class field theory.

The extension H^{res}/K (resp. H^{ord}/K) is thus the maximal unramified (resp. unramified and noncomplexified) abelian extension of K, and we have:

$$\mathrm{Gal}(H^{\mathrm{res}}/K) \simeq \mathcal{C}\ell^{\mathrm{res}}, \ \ \mathrm{Gal}(H^{\mathrm{ord}}/K) \simeq \mathcal{C}\ell^{\mathrm{ord}}.$$

a) Elementary Properties — Decomposition Law

We start by giving a number of elementary remarks which we divide in five statements 5.1.1 to 5.1.5.

5.1 Properties of Ray Class Fields. In the sequel we fix a modulus $\mathfrak{m}$ of K, with support T.

5.1.1 Conductor of a Ray Class Field. The existence of a (norm or Artin) conductor for any abelian extension of K implies that the conductor $\mathfrak{f}$ of $K_{(\mathfrak{m})^{\mathrm{res}}}$ divides $\mathfrak{m}$ (and is possibly not equal to it); we thus have $U_{\mathfrak{f}}^{\mathrm{res}} \subseteq K^{\times}U_{\mathfrak{m}}^{\mathrm{res}}$, hence $K^{\times}U_{\mathfrak{f}}^{\mathrm{res}} = K^{\times}U_{\mathfrak{m}}^{\mathrm{res}}$, which means (by uniqueness in the correspondence of class field theory) that $K_{(\mathfrak{m})^{\mathrm{res}}} = K_{(\mathfrak{f})^{\mathrm{res}}}$, and is also equivalent to the condition $P_{T,\mathfrak{m},\mathrm{pos}} = P_{T,\mathfrak{f},\mathrm{pos}}$. In fact, it is simpler to say that $\mathfrak{m}$ is the conductor of $K_{(\mathfrak{m})^{\mathrm{res}}}$ if and only if, for all $v \in T$, we have $\mathcal{C}_{\frac{\mathfrak{m}}{\mathfrak{p}_v}}^{\mathrm{res}} \neq \mathcal{C}_{\mathfrak{m}}^{\mathrm{res}}$, which yields:

$$\left(E_{\frac{\mathfrak{m}}{\mathfrak{p}_v}}^{\mathrm{res}} : E_{\mathfrak{m}}^{\mathrm{res}}\right) < \varphi(\mathfrak{m})\varphi\left(\frac{\mathfrak{m}}{\mathfrak{p}_v}\right)^{-1} \text{for all } v \in T,$$

using formula I.4.5.1 (recall that $\varphi(\mathfrak{m})\varphi\left(\frac{\mathfrak{m}}{\mathfrak{p}_v}\right)^{-1} = q_v$ or $q_v - 1$ depending on whether $\mathrm{v}(\mathfrak{m}) > 1$ or $\mathrm{v}(\mathfrak{m}) = 1$, where $q_v = |F_v|$).

5.1.1.1 Example. For $K = \mathbb{Q}(\sqrt{3})$ and $\mathfrak{m} = \mathfrak{l}_{11}$ (a prime ideal above 11), we find that $[K_{(\mathfrak{m})^{\mathrm{res}}} : K_{(1)^{\mathrm{res}}}] = 1$: this is immediate from the fact that $E^{\mathrm{res}} = \langle\, \varepsilon \,\rangle$ with $\varepsilon := 2 + \sqrt{3}$, that $E_{\mathfrak{l}_{11}}^{\mathrm{res}} = \langle\, \varepsilon^{10} \,\rangle$, and $\varphi(\mathfrak{l}_{11}) = 10$ (see I.4.5.6, (i)). Here, we have $\mathfrak{f} = 1$, in other words $K_{(\mathfrak{l}_{11})^{\mathrm{res}}}$ is equal to the restricted Hilbert class field which is of degree 2 over K. □

5.1.1.2 Exercise. Assume that K is such that E^{res} is finite (so that K is equal to $\mathbb{Q}$ or to an imaginary quadratic field). Characterize the moduli $\mathfrak{m}$ which are not conductors of any abelian extension of K.

Answer. We first note that $\mathfrak{m}$ is a conductor if and only if $K_{(\mathfrak{m})^{\mathrm{res}}}$ has conductor $\mathfrak{m}$; hence the following general case (valid without any assumption on K):

(0) If $\mathfrak{p}_2|2$ has residue degree equal to 1 in $K/\mathbb{Q}$ and if $\mathfrak{n}$ is any modulus not divisible by $\mathfrak{p}_2$, then $\mathfrak{m} := \mathfrak{p}_2\,\mathfrak{n}$ is not a conductor.

Indeed, we have $[K_{(\mathfrak{m})^{\mathrm{res}}} : K_{(\mathfrak{n})^{\mathrm{res}}}] = 1$ since $q_v - 1 = 1$.

The criterion giving the nonconductors $\mathfrak{m}$ can be written: there exists $\mathfrak{p}_v|\mathfrak{m}$ such that:

(1) $\mathrm{v}(\mathfrak{m}) = 1$ and $q_v - 1 \leq u_v$,

or:

(2) $\mathrm{v}(\mathfrak{m}) > 1$ and $q_v \leq u_v$,

with $u_v := \left(E_{\frac{\mathfrak{m}}{\mathfrak{p}_v}}^{\mathrm{res}} : E_{\mathfrak{m}}^{\mathrm{res}}\right)$.

For $u_v = 1$, the only possible solution corresponds to (1) and is relative to case (0); this is the case for the field $\mathbb{Q}$ for which the nonconductors are the $2n\mathbb{Z}$ with n odd. Thus, we only need to consider the case $u_v > 1$.

Assume now that K is an imaginary quadratic field different from $\mathbb{Q}(\mu_4)$ and $\mathbb{Q}(\mu_3)$. Since $u_v = 2$, this is equivalent to $E_{\frac{\mathfrak{m}}{\mathfrak{p}_v}} = \langle\, -1 \,\rangle$, $E_{\mathfrak{m}} = 1$, or to

$\frac{\mathfrak{m}}{\mathfrak{p}_v}|2$, $\mathfrak{m} \nmid 2$. Case (1) yields the following moduli, in addition to those given in case (0):

$$\mathfrak{p}_3,\ \mathfrak{p}_3',\ 2\mathfrak{p}_3,\ 2\mathfrak{p}_3', \quad \text{if 3 is split and 2 is not split,}$$
$$\mathfrak{p}_3,\ 2\mathfrak{p}_3, \quad \text{if 3 is ramified and 2 is not split.}$$

Similarly, case (2) yields the additional moduli:

$$\mathfrak{p}_2^2,\ \mathfrak{p}_2'^2, \text{ if 2 is split,}$$
$$\mathfrak{p}_2^3, \text{ if 2 is ramified.}$$

For $K = \mathbb{Q}(\mu_4)$ or $\mathbb{Q}(\mu_3)$, we proceed in the same way and we obtain the following conductors (in addition to those coming from case (0) for $\mathbb{Q}(\mu_4)$):

$$\mathfrak{p}_2^2,\ \mathfrak{p}_2^3,\ \mathfrak{p}_5,\ \mathfrak{p}_5', \quad \text{for } K = \mathbb{Q}(\mu_4),$$
$$(2),\ \mathfrak{p}_3,\ \mathfrak{p}_3^2,\ 2\mathfrak{p}_3,\ \mathfrak{p}_7,\ \mathfrak{p}_7', \quad \text{for } K = \mathbb{Q}(\mu_3).$$

□

See also in [j, Coh2, Ch. 3, § 5.2] an original algorithmic expression for conductors, discriminants and signatures of abelian extensions of a number field K.

5.1.2 Artin Conductor of an Abelian Field. More generally, by uniqueness in the correspondence of class field theory and by definition of the norm conductor for an abelian extension M of K, the smallest modulus $\mathfrak{n}$ such that:

$$M \subseteq K_{(\mathfrak{n})^{\mathrm{res}}}$$

is again the conductor of M/K, which gives a third definition of the conductor widely used in the case of abelian extensions of $\mathbb{Q}$ (see 5.5, 5.5.1), and which can be expressed as follows. Let $\mathfrak{m}$ be a modulus with support T such that $M \subseteq K_{(\mathfrak{m})^{\mathrm{res}}}$ (which in terms of Artin groups is equivalent to $P_{T,\mathfrak{m},\mathrm{pos}} \subseteq A_T := A_{M/K,T}$); then $\mathfrak{m}$ is the conductor of M if and only if for each $v \in T$, A_T does not contain $P_{T,\frac{\mathfrak{m}}{\mathfrak{p}_v},\mathrm{pos}}$.

5.1.3 S-Decomposition. For any finite set S of noncomplex places of K which is disjoint from T, the maximal S-split subextension $K_{(\mathfrak{m})^S}$ of $K_{(\mathfrak{m})^{\mathrm{res}}}$ corresponds to $K^\times \langle S \rangle U_{\mathfrak{m}}^{\mathrm{res}} = K^\times U_{\mathfrak{m}}^S$ (in the idelic version), to $P_{T,\mathfrak{m},\mathrm{pos}}\langle S \rangle := P_{T,\mathfrak{m},Pl_\infty^{\mathrm{r}} \setminus S_\infty} \cdot \langle S_0 \rangle$ (in the ideal group version), and hence we have:

$$\mathrm{Gal}(K_{(\mathfrak{m})^S}/K) \simeq \mathcal{C}\ell_{\mathfrak{m}}^S \quad \text{and} \quad \mathrm{Gal}(K_{(\mathfrak{m})^{\mathrm{res}}}/K_{(\mathfrak{m})^S}) \simeq \langle\, cl_{\mathfrak{m}}^{\mathrm{res}}(S) \,\rangle,$$

in the same sense as in I.4.4.1, (ii).

When $S = Pl_\infty^{\mathrm{r}}$, we obtain the field $K_{(\mathfrak{m})^{Pl_\infty^{\mathrm{r}}}} =: K_{(\mathfrak{m})^{\mathrm{ord}}}$ which is the ray class field modulo $\mathfrak{m}$ in the ordinary sense, in other words the maximal noncomplexified subextension of $K_{(\mathfrak{m})^{\mathrm{res}}}$; it corresponds respectively to $K^\times U_{\mathfrak{m}}^{\mathrm{ord}}$ or to $P_{T,\mathfrak{m}}$, and we have:

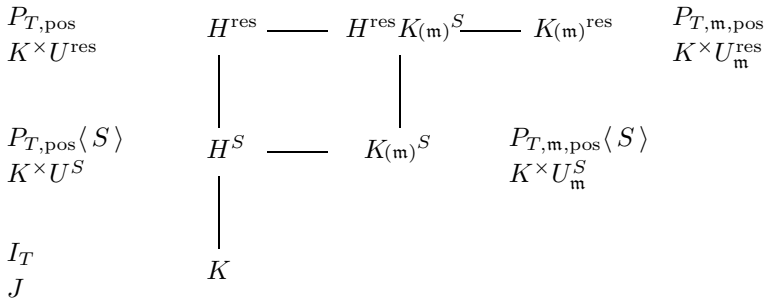
$$\mathrm{Gal}(K_{(\mathfrak{m})}{}^{\mathrm{ord}}/K) \simeq \mathscr{C}\ell_{\mathfrak{m}}^{\mathrm{ord}} \ ;$$

in certain contexts, we can also denote it by $K_{(\mathfrak{m})}{}^{\mathrm{nc}}$.

As in 5.1.1, the conductor $\mathfrak{f}$ of $K_{(\mathfrak{m})}{}^{S}$ is a divisor of $\mathfrak{m}$ which can be characterized in an analogous manner; we simply replace $E^{\mathrm{res}}_{\frac{\mathfrak{m}}{\mathfrak{p}_v}}$ and $E^{\mathrm{res}}_{\mathfrak{m}}$ by $E^{S}_{\frac{\mathfrak{m}}{\mathfrak{p}_v}}$ and $E^{S}_{\mathfrak{m}}$.

When $\mathfrak{m} = 1$, we denote by H^S the field $K_{(1)}{}^{S}$; it is the maximal S-split subextension of the restricted Hilbert class field H^{res}. We will call it the S-split Hilbert class field.

5.1.4 Norm Groups. We have the following general diagram in which, besides each field M, we have indicated the ideal group corresponding to it by class field theory, then the idèle group, and for which the Artin (or reciprocity) map induces the isomorphism $\mathrm{Gal}(M/K) \simeq I_T/N$ (or J/N):



Recall that $P_{T,\mathfrak{m},\mathrm{pos}}\langle\, S\,\rangle := P_{T,\mathfrak{m},Pl^{\mathrm{r}}_{\infty}\setminus S_{\infty}} \cdot \langle\, S_0\,\rangle$. Recall also the four exact sequences induced by the reciprocity or Artin map, in the particular case of ray class fields:

$$\begin{aligned}
1 \longrightarrow K^{\times}U^{\mathrm{res}}_{\mathfrak{m}} \longrightarrow\ & J \xrightarrow{\rho^{\mathrm{res}}} \mathrm{Gal}(K_{(\mathfrak{m})}{}^{\mathrm{res}}/K) \longrightarrow 1,\\
1 \longrightarrow K^{\times}U^{S}_{\mathfrak{m}} \longrightarrow\ & J \xrightarrow{\rho^{S}} \mathrm{Gal}(K_{(\mathfrak{m})}{}^{S}/K) \longrightarrow 1,\\
1 \longrightarrow P_{T,\mathfrak{m},\mathrm{pos}} \longrightarrow\ & I_T \xrightarrow{\alpha^{\mathrm{res}}} \mathrm{Gal}(K_{(\mathfrak{m})}{}^{\mathrm{res}}/K) \longrightarrow 1,\\
1 \longrightarrow P_{T,\mathfrak{m},\mathrm{pos}}\langle\, S\,\rangle \longrightarrow\ & I_T \xrightarrow{\alpha^{S}} \mathrm{Gal}(K_{(\mathfrak{m})}{}^{S}/K) \longrightarrow 1.
\end{aligned}$$

5.1.5 Intersection and Compositum of Ray Class Fields. As already remarked, for $\mathfrak{m}_1,\ \mathfrak{m}_2$ with supports contained in T, we have:

$$P_{T,\mathfrak{m}_1,\mathrm{pos}}\, P_{T,\mathfrak{m}_2,\mathrm{pos}} = P_{T,\mathrm{g.c.d.}(\mathfrak{m}_1,\mathfrak{m}_2),\mathrm{pos}},$$

or in (clearer) idelic terms:

$$K^{\times}U^{\mathrm{res}}_{\mathfrak{m}_1}K^{\times}U^{\mathrm{res}}_{\mathfrak{m}_2}=K^{\times}U^{\mathrm{res}}_{\mathrm{g.c.d.}(\mathfrak{m}_1,\mathfrak{m}_2)},$$

showing, by the usual Galois correspondence, that we always have:

$$K_{(\mathfrak{m}_1)^{\mathrm{res}}}\cap K_{(\mathfrak{m}_2)^{\mathrm{res}}}=K_{(\mathrm{g.c.d.}(\mathfrak{m}_1,\mathfrak{m}_2))^{\mathrm{res}}},$$

which is still true with S-splitting. On the contrary, the trivial inclusion:

$$K_{(\mathfrak{m}_1)^{\mathrm{res}}}K_{(\mathfrak{m}_2)^{\mathrm{res}}}\subseteq K_{(\mathrm{l.c.m.}(\mathfrak{m}_1,\mathfrak{m}_2))^{\mathrm{res}}}$$

may not be an equality, as is shown by the following example.

5.1.5.1 Example. Let $K=\mathbb{Q}(\sqrt{2}\,)$, $\mathfrak{m}_1=(4)$, $\mathfrak{m}_2=(3)$. Then we have $\mathcal{C}\ell^{\mathrm{res}}=\mathcal{C}\ell^{\mathrm{ord}}=1$, $E=:E^{\mathrm{res}}=\langle\,\varepsilon\,\rangle$ with $\varepsilon=3+2\sqrt{2}$, and in particular $\varepsilon^2=1+16+12\sqrt{2}$, which implies:

$$E_{\mathfrak{m}_1}=E^2\ ,\ E_{\mathfrak{m}_2}=E^4\ ,\ E_{\mathfrak{m}_1\mathfrak{m}_2}=E^4,$$

and yields (see I.4.5.6, (i)):

$$[K_{(\mathfrak{m}_1)^{\mathrm{res}}}:K]=4,\ [K_{(\mathfrak{m}_2)^{\mathrm{res}}}:K]=2,\ [K_{(\mathfrak{m}_1\mathfrak{m}_2)^{\mathrm{res}}}:K]=16,$$

thus showing that $[K_{(\mathfrak{m}_1\mathfrak{m}_2)^{\mathrm{res}}}:K_{(\mathfrak{m}_1)^{\mathrm{res}}}K_{(\mathfrak{m}_2)^{\mathrm{res}}}]=2$. □

5.1.5.2 Exercise. Check that for arbitrary moduli $\mathfrak{m}_1$ and $\mathfrak{m}_2$, the general formula is (denoting to simplify notations by $\wedge$ and $\vee$ the g.c.d. and l.c.m. operators):

$$[K_{(\mathfrak{m}_1\vee\mathfrak{m}_2)^{\mathrm{res}}}:K_{(\mathfrak{m}_1)^{\mathrm{res}}}K_{(\mathfrak{m}_2)^{\mathrm{res}}}]=\frac{(E^{\mathrm{res}}_{\mathfrak{m}_1\wedge\mathfrak{m}_2}:E^{\mathrm{res}}_{\mathfrak{m}_1})}{(E^{\mathrm{res}}_{\mathfrak{m}_2}:E^{\mathrm{res}}_{\mathfrak{m}_1\vee\mathfrak{m}_2})}=\frac{(E^{\mathrm{res}}_{\mathfrak{m}_1\wedge\mathfrak{m}_2}:E^{\mathrm{res}}_{\mathfrak{m}_2})}{(E^{\mathrm{res}}_{\mathfrak{m}_1}:E^{\mathrm{res}}_{\mathfrak{m}_1\vee\mathfrak{m}_2})}.$$

It is clear that there exists an identical formula in terms of S-split ray class fields and S-units. □

It is useful to relate the above fact 5.1.5.2 with Proposition 4.1.1. In particular, we see that if $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are the conductors of $K_{(\mathfrak{m}_1)^{\mathrm{res}}}$ and $K_{(\mathfrak{m}_2)^{\mathrm{res}}}$, then $\mathfrak{m}_1\vee\mathfrak{m}_2$ is the conductor of their compositum.

5.2 Decomposition Law of Places in a Ray Class Field. The decomposition law of places in $K_{(\mathfrak{m})^{\mathrm{res}}}/K$ is especially simple and typical of class field theory since it relates this information to questions about ideal classes (see 4.5.4, and compare also with the idelic formulation in 3.3.5); recall that here T is the support of $\mathfrak{m}$:

- If v is a finite place not belonging to T (hence unramified), then its residue degree in $K_{(\mathfrak{m})^{\mathrm{res}}}/K$ is equal to the order of the class of $\mathfrak{p}_v$ in $\mathcal{C}\ell^{\mathrm{res}}_{\mathfrak{m}}=I_T/P_{T,\mathfrak{m},\mathrm{pos}}$; it is totally split if and only if $\mathfrak{p}_v\in P_{T,\mathfrak{m},\mathrm{pos}}$.

• If $v \in T$ is unramified, this means that $K_{(\mathfrak{m})}^{\rm res} = K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})}^{\rm res}$, where $\mathfrak{m}_v := \mathfrak{p}_v^{{\rm v}(\mathfrak{m})}$, and the preceding statement is still valid if we perform the computations in $\mathcal{C}\ell_{\frac{\mathfrak{m}}{\mathfrak{m}_v}}^{\rm res} = I_{T\setminus\{v\}}/P_{T\setminus\{v\},\frac{\mathfrak{m}}{\mathfrak{m}_v},{\rm pos}} \simeq \mathcal{C}\ell_{\mathfrak{m}}^{\rm res}$, the place v being totally split if and only if $\mathfrak{p}_v \in P_{T\setminus\{v\},\frac{\mathfrak{m}}{\mathfrak{m}_v},{\rm pos}}$.

In particular (case $\mathfrak{m} = 1$) the residue degree of a finite place v in $H^{\rm res}/K$ is equal to the order of the restricted class (i.e., in $\mathcal{C}\ell^{\rm res}$) of $\mathfrak{p}_v$; its residue degree in $H^{\rm ord}/K$ is equal to the order of the ordinary class (i.e., in $\mathcal{C}\ell^{\rm ord}$) of $\mathfrak{p}_v$. Hence, the prime ideals which are totally split in $H^{\rm res}/K$ (resp. $H^{\rm ord}/K$) are those which are principal in the restricted (resp. ordinary) sense (see below the example concerning $\mathbb{Q}(\sqrt{-23}\,)$).

• If v is a real place at infinity, then v is totally split in $K_{(\mathfrak{m})}^{\rm res}/K$ if and only if $P_{T,\mathfrak{m},Pl_\infty^{\rm r}\setminus\{v\}} \subseteq P_{T,\mathfrak{m},{\rm pos}}$. Thus this occurs if and only if there exists $\varepsilon_{\mathfrak{m}} \in E_{\mathfrak{m}}^{\rm ord}$ such that:

$$\begin{aligned} &i_u(\varepsilon_{\mathfrak{m}}) > 0, \text{ for each real infinite place } u \neq v,\\ &i_v(\varepsilon_{\mathfrak{m}}) < 0 \end{aligned}$$

(see I.4.5.8, second part of (i) for $S = \emptyset$ and $\delta_\infty = \{v\}$).

• If v is a ramified finite place (i.e., dividing the conductor), we simply perform the computations in the inertia field of v which is given explicitly in Exercise 5.2.2; since this field is the ray class field $K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})}^{\rm res}$, this reduces the computation of the residue degree of v to the preceding situation.

5.2.1 Example. Let $K = \mathbb{Q}(\sqrt{-23}\,)$ and $H = K(\theta_0)$, where ${\rm Irr}(\theta_0, K) = X^3 - X - 1$. The K-conjugates of θ_0 are:

$$\begin{aligned} \theta_0, \quad \theta_1 &:= \frac{1}{\sqrt{-23}}\Big(3\,\theta_0^2 - \frac{9+\sqrt{-23}}{2}\,\theta_0 - 2\Big),\\ \theta_2 &:= \frac{1}{\sqrt{-23}}\Big(-3\,\theta_0^2 + \frac{9-\sqrt{-23}}{2}\,\theta_0 + 2\Big). \end{aligned}$$

We know from I.6.3.3 that H is the Hilbert class field of K and, by 3.6.1, that ${\rm Gal}(H/\mathbb{Q})$ is the dihedral group of order 6. We will illustrate the fact that the Frobenius $\left(\frac{H/K}{\mathfrak{p}}\right)$ of a prime ideal $\mathfrak{p}$ depends only on its class in the class group of K (of order 3). For this, we select the generator σ of ${\rm Gal}(H/K)$ such that $\sigma(\theta_0) = \theta_1$.

It is easily checked that, for $\mathfrak{p} \neq (\sqrt{-23}\,)$, $\left(\frac{H/K}{\mathfrak{p}}\right)$ is characterized by the congruence:

$$\left(\frac{H/K}{\mathfrak{p}}\right)\theta_0 \equiv \theta_0^{{\rm N}\mathfrak{p}} \bmod \mathfrak{p},$$

so that $\left(\frac{H/K}{\mathfrak{p}}\right) = 1,\ \sigma,\ \sigma^2$, according as $\theta_0^{{\rm N}\mathfrak{p}} \equiv \theta_0,\ \theta_1,\ \theta_2 \bmod \mathfrak{p}$. If $\mathfrak{p}$ is inert in $K/\mathbb{Q}$, it is trivial that $\left(\frac{H/K}{\mathfrak{p}}\right) = 1$ since $H/\mathbb{Q}$ is not cyclic, and we always have $\theta_0^{{\rm N}\mathfrak{p}} \equiv \theta_0 \bmod \mathfrak{p}$; but such an ideal is principal for trivial reasons.

Suppose now that $\mathfrak{p}$ is split in $K/\mathbb{Q}$. If $\mathfrak{p}'$ is the conjugate of $\mathfrak{p}$, the Galois operation 3.6.1 gives $\left(\frac{H/K}{\mathfrak{p}'}\right) = \left(\frac{H/K}{\mathfrak{p}}\right)^{-1}$ (which is in accordance with the principality of $\mathfrak{p}\mathfrak{p}'$).

For $\mathfrak{p}_2 = \left(2, \frac{1+\sqrt{-23}}{2}\right)$ we find $\theta_0^2 \equiv \theta_1 \bmod \mathfrak{p}_2$ since $\frac{9+\sqrt{-23}}{2} \in \mathfrak{p}_2$, and for $\mathfrak{p}_3 = \left(3, \frac{1+\sqrt{-23}}{2}\right)$ we find $\theta_0^3 \equiv \theta_2 \bmod \mathfrak{p}_3$ using the congruence $\sqrt{-23} \equiv -1 \bmod \mathfrak{p}_3$ and the relation $\theta_0^3 = \theta_0 + 1$. Thus $\left(\frac{H/K}{\mathfrak{p}_2}\right) = \sigma$ and $\left(\frac{H/K}{\mathfrak{p}_3}\right) = \sigma^2$. In other words, the Artin symbol $\left(\frac{H/K}{\mathfrak{p}_2\mathfrak{p}_3}\right)$ is trivial, and indeed, we have $\mathfrak{p}_2\mathfrak{p}_3 = \left(\frac{1+\sqrt{-23}}{2}\right)$, a principal ideal.

With $\mathfrak{p}_{13} = (13, 4+\sqrt{-23})$ we find $\theta_0^{13} \equiv \theta_1 \bmod \mathfrak{p}_{13}$, so that $\left(\frac{H/K}{\mathfrak{p}_{13}}\right) = \sigma$. We must verify that $\mathfrak{p}_2\mathfrak{p}'_{13}$ is principal, which is indeed the case since $\left(\frac{9+\sqrt{-23}}{2}\right) = \mathfrak{p}_2\mathfrak{p}'_{13}$ (and not $\mathfrak{p}_2\mathfrak{p}_{13}$ since $\sqrt{-23} \equiv -4 \bmod \mathfrak{p}_{13}$ or, equivalently, $\sqrt{-23} \equiv 4 \bmod \mathfrak{p}'_{13}$).

For all the split prime ideals $\mathfrak{p}$ with $\mathrm{N}\mathfrak{p} < 59$ we find $\left(\frac{H/K}{\mathfrak{p}}\right) \in \{\sigma, \sigma^2\}$ and we verify that $\mathfrak{p}$ is always in the "good" nontrivial class.

For the prime number 59, we find $\theta_0^{59} \equiv \theta_0 \bmod \mathfrak{p}_{59}$. This means that $\left(\frac{H/K}{\mathfrak{p}_{59}}\right) = \left(\frac{H/K}{\mathfrak{p}'_{59}}\right) = 1$ and that the prime ideals above 59 are principal (we have $\mathrm{N}(6+\sqrt{-23}) = 59$ which proves the claim). Note that 59 is the least example giving nontrivial principal ideals.

This gives a good idea of a reciprocity law since the splitting of the polynomial $f = X^3 - X - 1$ (into one (f_3), two $(f_1 f'_2)$, or three $(f_1 f'_1 f''_1)$ irreducible factors in $\mathbb{Q}_p[X]$) has been characterized by means of ray classes (i.e., multiplicative congruences). More precisely:

- $\left(\frac{p}{23}\right) = -1$ implies $f = f_1 f'_2$ (indeed, this is equivalent to $\left(\frac{-23}{p}\right) = -1$ (first reciprocity!), and therefore $\mathfrak{p} = (p)$ is inert in $K/\mathbb{Q}$ and split in H/K);
- $\left(\frac{p}{23}\right) = +1$ and $\mathfrak{p}|p$ principal imply $f = f_1 f'_1 f''_1$ ($\mathfrak{p}$ is split in $K/\mathbb{Q}$ and in H/K);
- $\left(\frac{p}{23}\right) = +1$ and $\mathfrak{p}|p$ nonprincipal imply $f = f_3$ ($\mathfrak{p}$ is split in $K/\mathbb{Q}$ and inert in H/K).

One verifies that the first case is equivalent to:

$$\mathfrak{p} \in j_{K/\mathbb{Q}}((a_i)\, P_{\mathbb{Q},(23),\mathrm{pos}}), \quad a_i \in \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\},$$

and that the last one is equivalent to:

$$\mathfrak{p} \in \mathfrak{p}_2 P_K \cup \mathfrak{p}_2^2 P_K.$$

The problem has been "linearized" in an obvious way.

In terms of quadratic forms, we check that the norm form $x^2 + xy + 6y^2 = \mathrm{N}_{K/\mathbb{Q}}\left(x + y\frac{1+\sqrt{-23}}{2}\right)$, $x, y \in \mathbb{Z}$, represents $p \neq 23$ if and only if $X^3 - X - 1$ has three roots in $\mathbb{Q}_p$ (indeed, this is equivalent to $\mathfrak{p}$ split and principal).

The power of class field theory comes from the fact that it is impossible to deduce the above rules from elementary properties of number fields and/or polynomials. See [Wy] for other examples and comments. □

5.2.2 Exercise (study of ramification in a ray class field). Let K be a number field together with sets of places T and S.

(i) Let $\mathfrak{m}$ be a modulus of K with support T, and let $v \in T$. Show that if we set $\mathfrak{m}_v := \mathfrak{p}_v^{\mathrm{v}(\mathfrak{m})}$, then $K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})^S}$ is the inertia field of v in the extension $K_{(\mathfrak{m})^S}/K$.

Deduce a formula for the ramification index of v in $K_{(\mathfrak{m})^S}/K$.

Generalize by giving a description of $\mathrm{Gal}(K_{(\mathfrak{m})^S}/K_{(\mathfrak{n})^{S\cup\delta_\infty}})$, where $\delta_\infty \subseteq Pl_\infty^{\mathrm{r}} \setminus S_\infty$, and where $\mathfrak{n} = \prod_{v\in t} \mathfrak{m}_v$ for $t \subseteq T$.

Compute also the residue degree of v in $K_{(\mathfrak{m})^S}/K$.

(ii) Show that the maximal T-tamely ramified abelian extension (i.e., T-ramified and such that for every place $v \in T$, the ramification index of v in this extension is prime to the residue characteristic of v) is equal to $K_{(\mathfrak{m}_{\mathrm{ta}})^{\mathrm{res}}}$ for $\mathfrak{m}_{\mathrm{ta}} := \prod_{v\in T} \mathfrak{p}_v$.

Answer. (i) We start with the case $S = \emptyset$, and give several approaches.

By the conductor theorem, v is unramified in $K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})^{\mathrm{res}}}$, hence the inertia field M of v in $K_{(\mathfrak{m})^{\mathrm{res}}}/K$ contains $K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})^{\mathrm{res}}}$; since M/K is unramified at v, its conductor $\mathfrak{f}$ is not divisible by $\mathfrak{p}_v$, and since $M \subseteq K_{(\mathfrak{m})^{\mathrm{res}}}$, we have $\mathfrak{f} \,|\, \mathfrak{m}$ (see 5.1.2) hence $\mathfrak{f} \,|\, \frac{\mathfrak{m}}{\mathfrak{m}_v}$, and we have $M \subseteq K_{(\mathfrak{f})^{\mathrm{res}}} \subseteq K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})^{\mathrm{res}}}$.

We can base a proof on the characterization of $I_v(K_{(\mathfrak{m})^{\mathrm{res}}}/K)$ given in 4.5.4, (i), or 4.7.1, so that in this case the inertia field corresponds to the group $P_{T,\frac{\mathfrak{m}}{\mathfrak{m}_v},\mathrm{pos}}$.

The inertia group of v in $K_{(\mathfrak{m})^S}/K$ is $\mathrm{Gal}(K_{(\mathfrak{m})^S}/K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})^S})$; indeed, use 1.2.1 and the fact that:

$$\mathrm{Gal}(K_{(\mathfrak{m})^{\mathrm{res}}}/K_{(\mathfrak{m})^S}) \quad \text{and} \quad \mathrm{Gal}(K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})^{\mathrm{res}}}/K_{(\frac{\mathfrak{m}}{\mathfrak{m}_v})^S})$$

are generated by the decomposition groups of the $v \in S$ in the corresponding extensions.

In idelic terms, the inertia field of v in $K_{(\mathfrak{m})^S}/K$ corresponds to $K^\times U_{\mathfrak{m}}^S U_v$ by 3.3, (iii), or 3.5.1, (ii); but clearly we have $U_{\mathfrak{m}}^S U_v = U_{\frac{\mathfrak{m}}{\mathfrak{m}_v}}^S$.

Formula I.4.5.1, for $\mathfrak{n} = \frac{\mathfrak{m}}{\mathfrak{m}_v}$ (in which case $\varphi(\mathfrak{m}) = \varphi(\mathfrak{n})\varphi(\mathfrak{m}_v)$ since $\mathfrak{n}$ and $\mathfrak{m}_v$ are coprime) and $\delta_\infty = \emptyset$, immediately yields:

$$e_v(K_{(\mathfrak{m})^S}/K) = \frac{\varphi(\mathfrak{m}_v)}{\left(E_{\frac{\mathfrak{m}}{\mathfrak{m}_v}}^S : E_{\mathfrak{m}}^S\right)},$$

for any $v \in T$, which, for $S = \emptyset$ yields:

$$e_v(K_{(\mathfrak{m})^{\mathrm{res}}}/K) = \frac{\varphi(\mathfrak{m}_v)}{\left(E_{\frac{\mathfrak{m}}{\mathfrak{m}_v}}^{\mathrm{res}} : E_{\mathfrak{m}}^{\mathrm{res}}\right)}.$$

The same arguments show that for $t \subseteq T$, $\mathfrak{n} = \prod_{v \in t} \mathfrak{m}_v$, and $\delta_\infty \subseteq Pl_\infty^{\rm r} \backslash S_\infty$, the ray class field $K_{(\mathfrak{n})}{}^{S \cup \delta_\infty}$ is the subfield of $K_{(\mathfrak{m})}{}^S$ fixed under the subgroup generated by the inertia groups of the places of $T \backslash t$ and the decomposition groups of the places of δ_∞.

If $v \in Pl_\infty^{\rm r}$, by I.4.5.1 for $\mathfrak{n} = \mathfrak{m}$ and $\delta_\infty = \{v\}$, we also obtain:

$$f_v(K_{(\mathfrak{m})}{}^S/K) = \frac{2}{\big(E_\mathfrak{m}^{S \cup \{v\}} : E_\mathfrak{m}^S\big)} = \frac{2}{\big|{\rm sgn}_v\big(E_\mathfrak{m}^{S \cup \{v\}}\big)\big|}.$$

To obtain a formula for the residue degree of a finite place v not belonging to $T \cup S$, we use directly 3.3.5 by computing the image of $K_v^\times$ in $J/K^\times U_\mathfrak{m}^S$, so that we obtain:

$$f_v(K_{(\mathfrak{m})}{}^S/K) = \big(K_v^\times : i_v\big(E_\mathfrak{m}^{S \cup \{v\}}\big) U_v\big),$$

but it is still possible to perform a direct computation using I.4.5.1, from which we recover (see 5.2):

$$f_v(K_{(\mathfrak{m})}{}^S/K) = \frac{|\mathcal{C}\ell_\mathfrak{m}^S|}{\big|\mathcal{C}\ell_\mathfrak{m}^{S \cup \{v\}}\big|} = |\langle\, \mathcal{C}\ell_\mathfrak{m}^S(\mathfrak{p}_v)\,\rangle|.$$

The idelic formulation is more convenient if the $S \cup \{v\}$-units are known, the other one relies on a computation of generalized ideal classes (here the class of $\mathfrak{p}_v$); as always, the correspondence is justified by I.5.1.

See also III.1.1.6, (ii) for a slightly more general context.

(ii) The formula for e_v immediately shows that $K_{(\mathfrak{m}_{\rm ta})}{}^{\rm res}$ is T-tamely ramified. Let $L \supseteq K_{(\mathfrak{m}_{\rm ta})}{}^{\rm res}$ be the maximal T-tamely ramified abelian extension of K. Let M be a finite extension of $K_{(\mathfrak{m}_{\rm ta})}{}^{\rm res}$ in L and let $\mathfrak{m} \in \langle\, T \,\rangle_\mathbb{N}$ be a multiple of its conductor, with support T ($\mathfrak{m}_{\rm ta}$ is always the tame part of $\mathfrak{m}$); if N corresponds to M, we have $K^\times U_\mathfrak{m}^{\rm res} \subseteq N$. Since by 3.5.1, (ii) the idèle group corresponding to M is also equal to

$$\prod_v U_v^1 \,.\, N,$$

we have $\prod_v U_v^1 \,.\, K^\times U_\mathfrak{m}^{\rm res} \subseteq \prod_v U_v^1 \,.\, N = N$, giving $K^\times U_{\mathfrak{m}_{\rm ta}}^{\rm res} \subseteq N$, and showing that we have $M \subseteq K_{(\mathfrak{m}_{\rm ta})}{}^{\rm res}$, which does not depend on the choice of $\mathfrak{m}$. This shows that $L = \bigcup_M M$ is finite and equal to the ray class field $K_{(\mathfrak{m}_{\rm ta})}{}^{\rm res}$ (the finiteness of L/K comes from 1.3.3.1 and of the finiteness of $H^{\rm res}/K$, which also implies that of ray class fields). In the same way, $K_{(\mathfrak{m}_{\rm ta})}{}^S$ is the maximal T-tamely ramified S-split abelian extension of K. □

b) Rank Formulas — The Reflection Theorem

When we take limits on $\mathfrak{m}$, we must use slightly different notations. Let K be a number field together with sets of places T and S, and let $\langle\, T \,\rangle_\mathbb{N}$ be the

monoid generated by the $\mathfrak{p}_v$ for $v \in T$. By reference to the notion of Hilbert class field when we use sets T and S which are not necessarily empty, we put the following.

5.3 Notations. (i) From 5.1.2, we set:

$$H_T^S := \bigcup_{\mathfrak{m} \in \langle\, T \,\rangle_{\mathbb{N}}} K_{(\mathfrak{m})}{}^S,$$

which is the maximal T-ramified S-split abelian extension of K. We also use the notation $H_T^{S_0\,\mathrm{res}}$ (resp. $H_T^{S_0\,\mathrm{ord}}$) when $S_\infty = \emptyset$ (resp. $S_\infty = Pl_\infty^{\mathrm{r}}$). [31]

(ii) From 5.2.2, (ii), we define:

$$H_{\mathrm{ta}}^S := \bigcup_{\mathfrak{m}_{\mathrm{ta}}} K_{(\mathfrak{m}_{\mathrm{ta}})}{}^S,$$

which is the maximal tamely ramified S-split abelian extension of K (the tame moduli $\mathfrak{m}_{\mathrm{ta}}$ have an arbitrary support, are prime to the fixed set S, but are squarefree). □

For a fixed finite T, the groups:

$$\mathrm{Gal}(H_T^S/K) \simeq \varprojlim_{\mathfrak{m} \in \langle\, T \,\rangle_{\mathbb{N}}} \mathcal{C}l_{\mathfrak{m}}^S =: \mathcal{C}l_T^S,$$

will be studied in great detail in Chapter III. Meanwhile, we can prove a number of properties on the p-ranks of these groups which had been mentioned at the end of Section 4 of Chapter I.

5.4 Rank Formulas. We start, in the following exercise, with the simplest situation (i.e., without any Galois structure) which is an essential prelude to the reflection theorem.

5.4.1 Exercise (Šafarevič's formula (1964), reflection formula (1998)). The notations are those of I.4.5, I.4.6. For finite and disjoint sets T, $S = S_0 \cup S_\infty$, and for $\mathfrak{m} \in \langle\, T \,\rangle_{\mathbb{N}}$, $\Delta_\infty := Pl_\infty^{\mathrm{r}} \setminus S_\infty$, we set:

$$\begin{aligned} Y_{T,\mathfrak{m}}^S &:= \{\alpha \in K_T^{\times p} K_{T,\mathfrak{m},\Delta_\infty}^{\times},\ (\alpha) = \mathfrak{a}^p \mathfrak{a}_{S_0},\ \mathfrak{a} \in I_T,\ \mathfrak{a}_{S_0} \in \langle\, S_0 \,\rangle\}, \\ V_T^S &:= \{\alpha \in K_T^{\times p} K_{T,\Delta_\infty}^{\times},\ (\alpha) = \mathfrak{a}^p \mathfrak{a}_{S_0}, \\ &\qquad \mathfrak{a} \in I_T,\ \mathfrak{a}_{S_0} \in \langle\, S_0 \,\rangle,\ \ i_v(\alpha) \in K_v^{\times p}\ \ \forall v \in T\}, \end{aligned}$$

$\delta_v := 1$ or 0 according as K_v contains μ_p or not, $\delta := 1$ or 0 according as K contains μ_p or not.

(i) Prove the formula:

[31] In these definitions, T is not assumed finite. When $T = \emptyset$, we recover the S-split Hilbert class field H^S.

$$\mathrm{rk}_p(Y_T^{S_0\,\mathrm{ord}}/K_T^{\times p}) = \mathrm{rk}_p(\mathcal{C}\ell^{S_0\,\mathrm{ord}}) + \delta + |S_0| + r_1 + r_2 - 1.$$

(ii) Show that for any sufficiently large modulus $\mathfrak{m} \in \langle T \rangle_{\mathbb{N}}$, we have $Y_{T,\mathfrak{m}}^S = V_T^S$, and deduce Šafarevič's rank formula:

$$\mathrm{rk}_p(\mathcal{C}\ell_T^S) = \mathrm{rk}_p(V_T^S/K_T^{\times p}) + \sum_{v\in T_p}[K_v:\mathbb{Q}_p] + \sum_{v\in T}\delta_v - \delta - |S_0| + 1 - r_1 - r_2 + \delta_{2,p}|\Delta_\infty|,$$

where $\delta_{2,p}$ is the Kronecker symbol equal to 1 if $p = 2$ and to 0 otherwise.

(iii) We now assume that $\mu_p \subset K$ and $T_p \cup S_p = Pl_p$. Show that $V_T^S/K_T^{\times p}$ is the radical of the maximal elementary S_0-ramified $T \cup \Delta_\infty$-split abelian p-extension denoted $H_{S_0}^{T\cup\Delta_\infty\,[p]}$, and deduce the reflection formula:

$$\mathrm{rk}_p(\mathcal{C}\ell_T^{S_0\cup S_\infty}) - \mathrm{rk}_p(\mathcal{C}\ell_{S_0}^{T\cup\Delta_\infty}) = |T| - |S_0| + \sum_{v\in T_p}[K_v:\mathbb{Q}_p] - r_1 - r_2 + \delta_{2,p}|\Delta_\infty|.$$

Find the corresponding formula when one removes the assumption $T_p \cup S_p = Pl_p$.

(iv) (asked in [j, Coh2, Ch. 3, § 6, Exer. 16]). Let K be a number field such that $(\mathcal{C}\ell_{(4)}^{\mathrm{ord}})_2 = 1$; show that K is totally real.

Answer. (i) If $\alpha \in Y_T^{S_0\,\mathrm{ord}}$ ($\mathfrak{m} = 1$, $\Delta_\infty = \emptyset$), we have $\alpha \in K_T^\times$ and $(\alpha) =: \mathfrak{a}^p\mathfrak{a}_{S_0}$; if we send α to the class of $\mathfrak{a}$ in $\mathcal{C}\ell^{S_0\,\mathrm{ord}}$, we obtain the exact sequence:

$$1 \longrightarrow E^{S_0\,\mathrm{ord}}/(E^{S_0\,\mathrm{ord}})^p \longrightarrow Y_T^{S_0\,\mathrm{ord}}/K_T^{\times p} \longrightarrow {}_p\mathcal{C}\ell^{S_0\,\mathrm{ord}} \longrightarrow 1,$$

where ${}_p\mathcal{C}\ell^{S_0\,\mathrm{ord}}$ is the subgroup of $\mathcal{C}\ell^{S_0\,\mathrm{ord}}$ formed by classes killed by p. By the Dirichlet Theorem I.3.7.1, the rank formula follows.

(ii) Let $\alpha \in K_T^\times$; it is clear, by using the chinese remainder theorem, that if $i_v(\alpha) \in K_v^{\times p}$ for each $v \in T$, we have $\alpha \in K_T^{\times p}K_{T,\mathfrak{m}}^\times$ for all $\mathfrak{m}$ with support T; to have equivalence, it is enough to choose $\mathfrak{m}$ such that $i_T(K_{T,\mathfrak{m}}^\times) \subset \bigoplus_{v\in T}(U_v)^p$ and we then have $Y_{T,\mathfrak{m}}^S = V_T^S$.

Note. If $\mu_p \subset K$, by I.6.3.4, (iii), we can choose $\mathfrak{m} = \prod_{v\in T\setminus T_p}\mathfrak{p}_v \prod_{v\in T_p}\mathfrak{p}_v^{pe_v+1}$.

Let $H_{T\,[p]}^S$ be the maximal elementary p-subextension of H_T^S (i.e., fixed under $(\mathcal{C}\ell_T^S)^p$); by I.4.5.1, $H_{T\,[p]}^S/K$ is finite. Assume that $\mathfrak{m} \in \langle T \rangle_{\mathbb{N}}$ is such that $Y_{T,\mathfrak{m}}^S = V_T^S$ and is a multiple of the conductor of $H_{T\,[p]}^S$, so that $\mathrm{rk}_p(\mathcal{C}\ell_T^S) = \mathrm{rk}_p(\mathcal{C}\ell_{\mathfrak{m}}^S)$. By I.4.5, (ii) applied to $\mathfrak{n} = 1$ and $\delta_\infty = \Delta_\infty$, we obtain:

$$\begin{aligned}\mathrm{rk}_p(\mathcal{C}\ell_T^S) &= \mathrm{rk}_p(\mathcal{C}\ell^{S_0\,\mathrm{ord}}) + \sum_{v\in T}\mathrm{rk}_p(U_v) + \delta_{2,p}|\Delta_\infty| \\ &\quad -\mathrm{rk}_p(Y_T^{S_0\,\mathrm{ord}}/K_T^{\times p}) + \mathrm{rk}_p(V_T^S/K_T^{\times p}) \\ &= \mathrm{rk}_p(V_T^S/K_T^{\times p}) + \sum_{v\in T}\mathrm{rk}_p(U_v) - |S_0| - r_1 - r_2 + 1 - \delta + \delta_{2,p}|\Delta_\infty|\end{aligned}$$

(using (i)). Since $\mathrm{rk}_p(U_v) = \delta_v$ (resp. $\delta_v + [K_v : \mathbb{Q}_p]$) if $v \nmid p$ (resp. $v|p$) by I.3.1.1, we obtain Šafarevič's formula with decomposition.

(iii) We have $\alpha \in V_T^S$ if and only if $i_v(\alpha) \in K_v^{\times p}$ for each $v \in T \cup \Delta_\infty$ and if $(\alpha) = \mathfrak{a}^p \mathfrak{a}_{S_0}$; this gives the $T \cup \Delta_\infty$-splitting and the $Pl_p \cup S_0$-ramification (see I.6.3); the equality $Pl_p = T_p \cup S_p$ implies the S_0-ramification. The converse is trivial after noting that if $\alpha K^{\times p}$ is an element of the radical of $H_{S_0}^{T \cup \Delta_\infty}{}_{[p]}$, we may assume that α is prime to T. The rank formula of (ii) then gives the result.

More generally, set $\Delta_p := Pl_p \setminus (T_p \cup S_p)$ and consider:

$$\mathfrak{m}^* := \prod_{v \in S_0 \setminus S_p} \mathfrak{p}_v \prod_{v \in S_p} \mathfrak{p}_v^{pe_v+1} \prod_{v \in \Delta_p} \mathfrak{p}_v^{pe_v},$$

where, for $v|p$, e_v denotes the ramification index of v in $K/\mathbb{Q}(\mu_p)$. Let us check that $K\left(\sqrt[p]{V_T^S}\right)$ is the maximal elementary p-subextension of $K_{(\mathfrak{m}^*)}{}^{T \cup \Delta_\infty}$. If $\alpha \in V_T^S$, the v-conductor computations made in 1.6.3 show that if v is tame (i.e., if $v \in S_0 \setminus S_p$) the v-conductor of $K(\sqrt[p]{\alpha})/K$ is $\mathfrak{f}_v = (1)$ or $\mathfrak{p}_v$, and that otherwise (i.e., if $v \in Pl_p \setminus T_p = S_p \cup \Delta_p$) then $\mathfrak{f}_v = \mathfrak{p}_v^{pe_v+1-r}$, where $r = 0$ is equivalent to $\mathrm{v}(\alpha) \not\equiv 0 \bmod (p)$; we thus obtain the inclusion:

$$K\left(\sqrt[p]{V_T^S}\right) \subseteq K_{(\mathfrak{m}^*)}{}^{T \cup \Delta_\infty}.$$

If $K(\sqrt[p]{\alpha}) \subseteq K_{(\mathfrak{m}^*)}{}^{T \cup \Delta_\infty}$, analogous considerations show that $\alpha \in V_T^S$. We thus obtain (using $\mu_p \subset K$) the formula that we have already mentioned:

$$\mathrm{rk}_p(\mathcal{C}\ell_T^{S_0 \cup S_\infty}) - \mathrm{rk}_p(\mathcal{C}\ell_{\mathfrak{m}^*}^{T \cup \Delta_\infty}) = \\ |T| - |S_0| + \sum_{v \in T_p} [K_v : \mathbb{Q}_p] - r_1 - r_2 + \delta_{2,p}|\Delta_\infty|.$$

(iv) For $p = 2$, $T = S = \emptyset$, we have $\mathfrak{m}^* = (4)$ and:

$$\mathrm{rk}_2(\mathcal{C}\ell^{\mathrm{res}}) - \mathrm{rk}_2(\mathcal{C}\ell_{(4)}^{\mathrm{ord}}) = -r_2 \ ;$$

under the assumption of the question, we thus obtain the stronger result:

$$r_2 = 0 \ \text{ and } \ \mathrm{rk}_2(\mathcal{C}\ell^{\mathrm{res}}) = 0. \qquad \square$$

The formulas of (iii) are only a particular case of the reflection theorem whose statement we are going to give below. However, they already show the symmetry which, in the Kummer case, roughly speaking exchanges ramification and decomposition, except that for $p = 2$ and the places at infinity, we obtain for instance (assuming that $T_2 \cup S_2 = Pl_2$):

$$\mathrm{rk}_2(\mathcal{C}\ell_T^{S_0\,\mathrm{res}}) - \mathrm{rk}_2(\mathcal{C}\ell_{S_0}^{T\,\mathrm{ord}}) = |T| - |S_0| + \sum_{v \in T_2} [K_v : \mathbb{Q}_2] - r_2.$$

5.4.2 Reflection Principle. The most general statement assumes the following definitions and facts, borrowed from the language of group representations (use [Se4] and in particular Paragraph 12 for rationality questions; see also 5.4.9.1 for some complements), and which we only recall briefly:

• Let g be a finite group of order prime to p. We denote by $\mathfrak{X}_p(g)$ the set of $\mathbb{F}_p$-irreducible characters of g, and for $\chi \in \mathfrak{X}_p(g)$ we set:

$$e_\chi := \frac{\psi(1)}{|g|} \sum_{s \in g} \chi(s^{-1})\, s,$$

where ψ is an absolutely irreducible character such that χ is equal to the sum of the distinct $\mathbb{F}_p$-conjugates of ψ (which we denote by $\psi|\chi$): an $\mathbb{F}_p$-conjugate of ψ is of the form ψ^{p^i}, $i \geq 0$, where $\psi^{p^i}(s) := \psi(s^{p^i})$ for all $s \in g$. We thus obtain a fundamental system of central orthogonal idempotents of the algebra $\mathbb{F}_p[g]$, thanks to the assumption that $p \nmid |g|$.

We denote by V_χ the $\mathbb{F}_p$-irreducible representation with character χ. If g is commutative, $\psi(1) = 1$, V_χ is an $\mathbb{F}_p$-vector space of dimension equal to the order of p modulo the order of ψ.

• For any $\mathbb{Z}[g]$ or $\mathbb{Z}_p[g]$-module M of finite type and any $\chi \in \mathfrak{X}_p(g)$ we set:

$$M_\chi := (M \otimes \mathbb{F}_p)^{e_\chi} \simeq (M/M^p)^{e_\chi},$$

and we call χ-rank of M the integer $r := \mathrm{rk}_\chi(M)$ such that:

$$M_\chi \simeq r\, V_\chi := \bigoplus_{i=1}^{r} V_\chi.$$

Therefore, we have $\mathrm{rk}_p(M_\chi) = \chi(1)\mathrm{rk}_\chi(M)$.

• Assume that g, of order prime to p, is an automorphism group of K (K containing μ_p), and let $k := K^g$. If T and S are sets of places of K stable under g, we denote by T_k and S_k the sets of places of k below those of T and S. Finally, for any place u of k we denote by abuse of notation by d_u the decomposition group, in K/k, of a place v of K above u (thus d_u is only defined up to conjugation).

• Let ω be the Teichmüller character, i.e., the character defined by the action of g on μ_p (if $s \in g$, $\omega(s)$ is the unique element $a \in \mathbb{F}_p^\times$ such that $s(\zeta) = \zeta^a$ for all $\zeta \in \mu_p$). If $\chi \in \mathfrak{X}_p(g)$ we set:

$$\chi^* := \omega\chi^{-1},$$

where $\chi^{-1}(s) := \chi(s^{-1})$ for all $s \in g$; we still have $\chi^* \in \mathfrak{X}_p(g)$ and this defines the fundamental involution attached to the reflection principle (the mirror involution).

• We then define for all $\chi \in \mathfrak{X}_p(g)$ (with $\psi|\chi$) (see 5.4.9.1):

$$\rho_\chi(T,S) := \psi(1)r_2(k) + \sum_{u \in Pl^{\mathrm{r}}_{k,\infty}} \rho_{u,\chi} + \sum_{u \in T_k} \rho_{u,\chi} + \delta_{\omega,\chi} - \delta_{1,\chi}$$
$$- \sum_{u \in S_{0,k}} \rho_{u,\chi^*} - \psi(1) \sum_{u \in S_{p,k} \cup \Delta_{p,k}} [k_u : \mathbb{Q}_p] - \delta_{2,p}\psi(1)|S_{\infty,k}|$$

$$= \sum_{u\in T_k} \rho_{u,\chi} + \psi(1) \sum_{u\in T_{p,k}} [k_u : \mathbb{Q}_p] - \sum_{u\in S_{0,k}} \rho_{u,\chi^*} + \delta_{\omega,\chi} - \delta_{1,\chi}$$
$$- \psi(1) r_2(k) - \sum_{u\in Pl^{\mathrm{r}}_{k,\infty}} \rho_{u,\chi^*} + \delta_{2,p}\psi(1)|\Delta_{\infty,k}|,$$

where the $\delta_{a,b}$ denote Kronecker symbols and where:

$$\rho_{u,\chi} := \frac{1}{|d_u|} \sum_{t\in d_u} \psi(t), \quad \rho_{u,\chi^*} := \frac{1}{|d_u|} \sum_{t\in d_u} \omega\psi^{-1}(t),$$

$$\Delta_{p,k} := Pl_{k,p}\backslash(T_{p,k} \cup S_{p,k}), \ \Delta_{\infty,k} := Pl^{\mathrm{rnc}}_{k,\infty}\backslash S_{\infty,k},$$

where $Pl^{\mathrm{rnc}}_{k,\infty}$ is the set of real places of k noncomplexified in K. Be careful to distinguish between $Pl^{\mathrm{r}}_{k,\infty}$ and $Pl^{\mathrm{r}}_{\infty,k}$; in particular, we have the equality $|S_{\infty,k}| + |\Delta_{\infty,k}| = r_1(k) - r_1^{\mathrm{c}}(k)$, where $r_1^{\mathrm{c}}(k)$ is the number of real places of k which are complexified in K.

5.4.3 Remark. It is now important to comment on the relationship between Kummer theory and class field theory which will give the reflection theorem with characters. We use the notations of (Ch. I; § 6), where the symbol * also denotes the dual of a group. Let L/K be a p-elementary Kummer extension of radical W and Galois group A. Then we have the "Spiegelungsrelation", which comes directly from I.6.2, in view of the g-module action on a dual, and which can be stated as follows for any $\chi \in \mathfrak{X}_p(g)$:

$$W_{\chi^*} \simeq (A^*)_{\chi^*} := \mathrm{Hom}(A, \mu_p)_{\chi^*} \simeq (A_\chi)^* \ \ ^{32}$$

(canonical isomorphisms of g-modules), and yields the relation:

$$\mathrm{rk}_{\chi^*}(W) = \mathrm{rk}_\chi(A).$$

More precisely, we remark that if L_χ is the subfield of L with radical W_{χ^*}, then $\mathrm{Gal}(L/L_\chi) = \bigoplus_{\chi'\neq\chi} A_{\chi'}$ yielding $\mathrm{Gal}(L_\chi/K) \simeq A_\chi$: from I.6.2.1, we check that $W_{\chi^*}^{\perp} := \{a \in A, \ \lambda(W_{\chi^*}, a) = 1\} = \bigoplus_{\chi'\neq\chi} A_{\chi'}$ since $\lambda(\overline{\alpha}^{e_\chi *}, a) = \lambda(\overline{\alpha}, a^{e_\chi}) = 1$ for all $\overline{\alpha} \in W$ if and only if $a^{e_\chi} = 1$.

We suppose that K is given together with sets of places T and S; we do not assume that $Pl_p = T_p \cup S_p$. This leads to the context of Exercise 5.4.1, (iii), for which we put $\mathfrak{m}^* := \prod_{v\in S_0\backslash S_p} \mathfrak{p}_v \prod_{v\in S_p} \mathfrak{p}_v^{pe_v+1} \prod_{v\in\Delta_p} \mathfrak{p}_v^{pe_v}$, with $\Delta_p := Pl_p\backslash(T_p \cup S_p)$. The reflection theorem then consists in the application of the above to the extension $L := K_{(\mathfrak{m}^*)^{T\cup\Delta_\infty}[p]}$ for which the χ^*-component W_{χ^*} of the radical $W = V_T^S/K_T^{\times p}$ will be computed using the χ^*-component of the class group $\mathcal{C}\ell_T^S$ (see below), the χ-component of A_χ then being nothing else than the χ-component of $\mathcal{C}\ell_{\mathfrak{m}^*}^{T\cup\Delta_\infty}$ under the isomorphism of class field theory. □

5.4.4 Proposition. *Let K be any number field together with sets of places T and S, and p a prime. We have the exact sequences of $\mathbb{F}_p$-vector spaces:*

[32] Use I.6.1.2 to check that $h^{e_\chi *}(a) = h(a^{e_\chi})$ for all $h \in A^*$, $a \in A$; then associate with $h^{e_\chi *}$ the restriction of h to A_χ.

$$1 \longrightarrow E^{S_0\,\mathrm{ord}}/(E^{S_0\,\mathrm{ord}})^p \longrightarrow Y_T^{S_0\,\mathrm{ord}}/K_T^{\times p} \longrightarrow {}_p\mathcal{C}\ell^{S_0\,\mathrm{ord}} \longrightarrow 1,$$

$$1 \longrightarrow Y_T^{S_0\,\mathrm{ord}}/V_T^S \longrightarrow \bigoplus_{v\in T} U_v/(U_v)^p \bigoplus_{v\in\Delta_\infty} (\{\pm 1\})_p \longrightarrow X \longrightarrow 1,$$

where $X := \mathrm{Ker}\big(\mathcal{C}\ell_T^S/(\mathcal{C}\ell_T^S)^p \longrightarrow \mathcal{C}\ell^{S_0\,\mathrm{ord}}/(\mathcal{C}\ell^{S_0\,\mathrm{ord}})^p\big)$.

Proof. The first exact sequence is given in the proof of 5.4.1, (i). For the second one, see the proof of I.4.5, (ii) with $\mathfrak{n} = 1$, $\delta_\infty = \Delta_\infty$, and with $\mathfrak{m} = \prod_{v\in T} \mathfrak{p}_v^{m_v}$ sufficiently large in order to have $U_v^{m_v} \subseteq (U_v)^p$ for all $v \in T$, $\mathcal{C}\ell_{\mathfrak{m}}^S/(\mathcal{C}\ell_{\mathfrak{m}}^S)^p = \mathcal{C}\ell_T^S/(\mathcal{C}\ell_T^S)^p$, and $Y_{T,\mathfrak{m}}^S = V_T^S$ (see 5.4.1, (ii)). □

Suppose now that K is given together with a group of automorphisms g of order prime to p. We do not assume that $\mu_p \subset K$. Then, the above exact sequences give immediately a generalization of Šafarevič's formula, with characters (noting that ${}_p\mathcal{C}\ell^{S_0\,\mathrm{ord}}$ and $\mathcal{C}\ell^{S_0\,\mathrm{ord}}/(\mathcal{C}\ell^{S_0\,\mathrm{ord}})^p$ have same character):

$$\mathrm{rk}_{\chi^*}(\mathcal{C}\ell_T^S) - \mathrm{rk}_{\chi^*}(V_T^S) = \mathrm{rk}_{\chi^*}\Big(\bigoplus_{v\in T} U_v \bigoplus_{v\in\Delta_\infty} \{\pm 1\}\Big) - \mathrm{rk}_{\chi^*}(E^{S_0\,\mathrm{ord}}).$$

The right hand side is a straightforward computation (see 5.4.9.1) using representation theory in the context of 2.3 and the S-unit Dirichlet–Herbrand Theorem I.3.7 (see in 5.4.7 the value of this expression which is a little more complicated than $\rho_\chi(T,S)$ given above corresponding to the case $\mu_p \subset K$). If $\mu_p \subset K$, we can use the Kummer interpretation $\mathrm{rk}_{\chi^*}(W) = \mathrm{rk}_\chi(A)$ of the Remark 5.4.3, with $W = V_T^S/K_T^{\times p}$ and $A = \mathcal{C}\ell_{\mathfrak{m}^*}^{T\cup\Delta_\infty}$, giving the reflection theorem for which we recall the main notations.

Notations. For a number field K containing μ_p, given together with sets of places T and $S = S_0 \cup S_\infty$, we put:

$$T_p := T \cap Pl_p,\ S_p := S \cap Pl_p,\ \Delta_p := Pl_p \setminus (T_p \cup S_p),\ \Delta_\infty := Pl_\infty^{\mathrm{r}} \setminus S_\infty,$$

$$T^* := T \cup \Delta_\infty,\ S^* := S_0 \cup \Delta_p,\ \mathfrak{m}^* := \prod_{v\in S_0\setminus S_p} \mathfrak{p}_v \prod_{v\in S_p} \mathfrak{p}_v^{pe_v+1} \prod_{v\in\Delta_p} \mathfrak{p}_v^{pe_v},$$

where, for $v|p$, e_v denotes the ramification index of v in $K/\mathbb{Q}(\mu_p)$. We use also the notations given in Paragraph 5.4.2. □

5.4.5 Theorem (of T-S-reflection [Gr10, Ch. I, Th. 5.18] (1998)). *Let K be a number field containing the group μ_p of pth roots of unity, and g an automorphism group of K of order prime to p. We assume that T and S are g-invariant sets.*
Then for all $\chi \in \mathfrak{X}_p(g)$, we have:

$$\mathrm{rk}_{\chi^*}(\mathcal{C}\ell_T^S) - \mathrm{rk}_\chi(\mathcal{C}\ell_{\mathfrak{m}^*}^{T^*}) = \rho_\chi(T,S),$$

and if, in addition, $\Delta_p = \emptyset$, then $\mathcal{C}\ell_{\mathfrak{m}^*}^{T^*} = \mathcal{C}\ell_{S^*}^{T^*}$ and we obtain:

$$\mathrm{rk}_{\chi^*}(\mathcal{C}\ell_T^{S_0\cup S_\infty}) - \mathrm{rk}_\chi(\mathcal{C}\ell_{S_0}^{T\cup\Delta_\infty}) = \rho_\chi(T,S).$$ □

When $\Delta_p = \emptyset$, reflection is perfect in that the operation sending (T, S) to (S^*, T^*) is an involution. When $\Delta_p \neq \emptyset$, we only have the inequality $\mathrm{rk}_\chi(\mathcal{C}\ell_{\mathfrak{m}^*}^{T^*}) \leq \mathrm{rk}_\chi(\mathcal{C}\ell_{S^*}^{T^*})$ since $\mathfrak{m}^*$ is not necessarily equal to the conductor of $H_{S^*}^{T^*}{}_{[p]}$ (the maximal p-elementary subextension of $H_{S^*}^{T^*}$). A simple sufficient condition for equality is that $\rho_{u,\chi^*} = 0$ for all $u \in \Delta_{p,k}$.

Similarly, using the inequality:

$$\mathrm{rk}_\chi(\mathcal{C}\ell_{\mathfrak{m}^*}^{T^*}) \geq \mathrm{rk}_\chi(\mathcal{C}\ell_{S_0}^{T^*}),$$

which easily yields, using the involution $(T, S, \chi) \mapsto (S_0, T \cup \Delta_\infty, \chi^*)$ for the upper bound:

$$\rho_\chi(T, S) \leq \mathrm{rk}_{\chi^*}(\mathcal{C}\ell_T^S) - \mathrm{rk}_\chi(\mathcal{C}\ell_{S_0}^{T\cup\Delta_\infty}) \leq -\rho_{\chi^*}(S_0, T \cup \Delta_\infty),$$

we obtain classical inequalities (optimal for $p \neq 2$) which we indicate in the case $T = S_0 = \emptyset$ (for the proof of the specific result when $p = 2$, see 5.4.9).

5.4.6 Corollary (classical "Spiegelungssätze": $k = \mathbb{Q}$). *Let K be a Galois extension of $\mathbb{Q}$, containing μ_p, of degree not divisible by p, and let $\chi \in \mathfrak{X}_p(\mathrm{Gal}(K/\mathbb{Q}))$. For $\chi \neq 1,\ \omega$, we have the following inequalities:*

(i) Case $p \neq 2$ (Leopoldt's "Spiegelungssatz" [Le2] (1958)):

$$\frac{\psi(c) - \psi(1)}{2} \leq \mathrm{rk}_{\chi^*}(\mathcal{C}\ell) - \mathrm{rk}_\chi(\mathcal{C}\ell) \leq \frac{\psi(c) + \psi(1)}{2},$$

where c is the restriction to K of complex conjugation and $\psi|\chi$; if in addition $K/\mathbb{Q}$ is abelian and χ is even (i.e., $\psi(c) = 1$), we have:

$$0 \leq \mathrm{rk}_{\chi^*}(\mathcal{C}\ell) - \mathrm{rk}_\chi(\mathcal{C}\ell) \leq 1.$$

(ii) Case $p = 2$ (Armitage–Fröhlich–Serre, Taylor, Oriat [Or1] (1976)):

$$0 \leq \mathrm{rk}_{\chi^{-1}}(\mathcal{C}\ell^{\mathrm{res}}) - \mathrm{rk}_{\chi^{-1}}(\mathcal{C}\ell^{\mathrm{ord}}) + \mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{res}}) - \mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{ord}}) \leq \psi(1)\ ;$$

if $K/\mathbb{Q}$ is abelian, then when $\chi \neq \chi^{-1}$ we have the following two possibilities:

$$\mathrm{rk}_{\chi^{-1}}(\mathcal{C}\ell^{\mathrm{res}}) = \mathrm{rk}_{\chi^{-1}}(\mathcal{C}\ell^{\mathrm{ord}}) \quad \textit{and} \quad \mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{res}}) = \mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{ord}}) + 1,$$
$$\mathrm{rk}_{\chi^{-1}}(\mathcal{C}\ell^{\mathrm{res}}) = \mathrm{rk}_{\chi^{-1}}(\mathcal{C}\ell^{\mathrm{ord}}) + 1 \quad \textit{and} \quad \mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{res}}) = \mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{ord}}),$$

and when $\chi = \chi^{-1}$, we have the equality:

$$\mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{res}}) = \mathrm{rk}_\chi(\mathcal{C}\ell^{\mathrm{ord}}). \qquad \square$$

5.4.6.1 Remark. If $\mathcal{C}$ is (for example) a generalized p-class group of K, the χ-component $\mathcal{C}^{e_\chi}$ depends only on the faithful character χ' corresponding to χ and on the subfield K' of K fixed under the kernel of χ; in other words, we have the following relation:

$$\mathcal{C}^{e_\chi} \simeq (\mathrm{N}_{K/K'}\mathcal{C})^{e_{\chi'}} = \mathcal{C}'^{e_{\chi'}},$$

in which the analogous generalized p-class group $\mathcal{C}'$ of K' enters only via its χ'-component. All this is valid only in the semi-simple case $p \nmid |g|$. For the proof, use the relation $(\mathrm{N} \circ j)(\mathcal{C}') = \mathcal{C}'^{[K:K']} = \mathcal{C}'$, yielding the surjectivity of $\mathrm{N} := \mathrm{N}_{K/K'}$ and the injectivity of $j := j_{K/K'}$.

For instance, this applies to $\mathcal{C} = (\mathcal{A}_{\mathfrak{m}}^{\mathrm{res}}(S))_p$, in the p-Sylow of $\mathcal{C}\ell_{\mathfrak{m}}^S := \mathcal{C}\ell_{\mathfrak{m}}^{\mathrm{res}}/\mathcal{A}_{\mathfrak{m}}^{\mathrm{res}}(S)$, whose χ-component may be simplified according to the decomposition of the $v \in S$ in K'/k, $k = K^g$ (e.g., $\chi \neq 1$ and v nonsplit in K'/k). □

5.4.6.2 Example 1 (case of the Scholz theorem [Scholz2], $p = 3$). Let $K = \mathbb{Q}(\sqrt{d}, \sqrt{-3})$, $d > 0$, $d \notin \mathbb{Q}^{\times 2}$, and $\mathcal{C}_K := (\mathcal{C}\ell_K)_3$. We have $g = \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. If χ is the quadratic character whose kernel fixes $\mathbb{Q}(\sqrt{d})$, then the kernel of χ^* fixes $\mathbb{Q}(\sqrt{-3d})$; thus $\mathcal{C}_K^{e_\chi}$ (for instance) is isomorphic to $\mathcal{C}_{\mathbb{Q}(\sqrt{d})}^{e_{\chi'}} \simeq \mathcal{C}_{\mathbb{Q}(\sqrt{d})}$ since $\mathbb{Q}(\sqrt{d})$ has only two characters (χ' and 1) for which $\mathcal{C}_{\mathbb{Q}(\sqrt{d})} = \mathcal{C}_{\mathbb{Q}(\sqrt{d})}^{e_{\chi'}} \oplus \mathcal{C}_{\mathbb{Q}(\sqrt{d})}^{e_1}$ with (in a similar way) $\mathcal{C}_{\mathbb{Q}(\sqrt{d})}^{e_1} \simeq \mathcal{C}_{\mathbb{Q}}^{e_{1'}} = 1$! Of course, $\mathcal{C}_K^{e_{\chi^*}} \simeq \mathcal{C}_{\mathbb{Q}(\sqrt{-3d})}$. □

In general, the $\mathcal{C}_K^{e_\chi}$ are only particular components of the p-class groups of the subfields of K.

5.4.6.3 Example 2. Let $K = \mathbb{Q}(\mu_p)$, $p \neq 2$, and let $g = \mathrm{Gal}(K/\mathbb{Q})$. We easily obtain from 5.4.5 (with $S = Pl_p$, $T = \emptyset$, $\chi = 1$):

$$\mathrm{rk}_\omega\left(\mathcal{C}\ell_{\mathbb{Q}(\mu_p)}^{Pl_p}\right) = 0$$

(since the unit character 1 leads to invariants of $\mathbb{Q}$, we have $\mathrm{rk}_1(\mathcal{C}\ell_{\mathbb{Q}(\mu_p),Pl_p}) = \mathrm{rk}_p(\mathcal{C}\ell_{\mathbb{Q},\{p\}}) = 1$ [33], and we check that $\rho_1(\emptyset, Pl_p) = -1$); but $\mathcal{A}(Pl_p) = 1$ in $\mathbb{Q}(\mu_p)$ since $Pl_p = \{v\}$ with $\mathfrak{p}_v = (1-\zeta)$. Hence:

$$\mathrm{rk}_\omega\left(\mathcal{C}\ell_{\mathbb{Q}(\mu_p)}\right) = 0$$

for all prime numbers p. □

For additional concrete examples, especially in the case $p = 2$, see [Gr10, Ch. II]. For some arithmetical interpretations of the Spiegelungssatz, see 5.4.9.2.

To be complete on this representation-theoretic aspect, we also give the generalization with characters of Šafarevič's formula proved in 5.4.1 which does not need the assumption $\mu_p \subset K$.

[33] The maximal abelian p-ramified pro-p-extension of $\mathbb{Q}$ is, for $p \neq 2$, the cyclotomic $\mathbb{Z}_p$-extension.

5.4.7 Proposition (Šafarevič's formula with characters). *Let p be a prime number. Let g be an automorphism group of K of order prime to p, with fixed field k. Let T and $S = S_0 \cup S_\infty$ be two disjoint finite g-invariant sets of finite and noncomplex places of K.*
Then for any $\chi \in \mathfrak{X}_p(g)$ we have:

$$\mathrm{rk}_\chi(\mathcal{C}\ell_T^S) = \mathrm{rk}_\chi(V_T^S/K_T^{\times p}) + \psi(1) \sum_{u \in T_{p,k}} [k_u : \mathbb{Q}_p] + \sum_{u \in T_k} \delta_u \rho_{u,\omega_u\chi^{-1}}$$
$$- \delta_{\omega,\chi}\delta - \sum_{u \in Pl^{\mathrm{r}}_{k,\infty} \cup S_{0,k}} \rho_{u,\chi} + \delta_{1,\chi} - \psi(1) r_2(k) + \delta_{2,p}\psi(1)|\Delta_{\infty,k}|,$$

where:

$$V_T^S := \{\alpha \in K_T^{\times p} K_{T,\Delta_\infty}^{\times}, \quad (\alpha) = \mathfrak{a}^p \mathfrak{a}_{S_0},$$
$$\mathfrak{a} \in I_T, \ \mathfrak{a}_{S_0} \in \langle\, S_0 \,\rangle, \quad i_v(\alpha) \in K_v^{\times p} \quad \forall v \in T\},$$

where the $\delta_{a,b}$ denote Kronecker symbols, where ω_u is the local Teichmüller character (possibly trivial) given by the action of $d_u \simeq \mathrm{Gal}(K_v/k_u)$ on $\mu_p(K_v)$ (for v above u), $\delta_u := 1$ or 0 according as K_v contains μ_p or not, and $\delta := 1$ or 0 according as K contains μ_p or not. □

5.4.8 Exercise. Let K be a number field containing μ_n for some integer $n \geq 2$; assume that K is given together with sets of places T and S such that $T \cup S_0$ contains all the places above the prime divisors of n. Consider:

$$V_T^S := \{\alpha \in K_T^{\times n} K_{T,\Delta_\infty}^{\times}, \quad (\alpha) = \mathfrak{a}^n \mathfrak{a}_{S_0},$$
$$\mathfrak{a} \in I_T, \ \mathfrak{a}_{S_0} \in \langle\, S_0 \,\rangle, \quad i_v(\alpha) \in K_v^{\times n} \quad \forall v \in T\}.$$

Show that the norm group of $L := K\Big(\sqrt[n]{V_T^S}\Big)$ is:

$$N = P_{S_0,\mathfrak{n},S_\infty} \cdot \langle\, T \,\rangle \cdot I_{S_0}^n =: P_{S_0,\mathfrak{n},\mathrm{pos}} \langle\, T \cup \Delta_\infty \,\rangle \cdot I_{S_0}^n,$$

for any sufficiently large modulus $\mathfrak{n} \in \langle\, S_0 \,\rangle_{\mathbb{N}}$, where $\Delta_\infty := Pl_\infty^{\mathrm{r}} \setminus S_\infty$.

Answer. Using arguments analogous to those of 5.4.1, (iii), one can show that L is the maximal S_0-ramified $T \cup \Delta_\infty$-split extension of K, with exponent dividing n. It is a finite extension. Since $N = P_{S_0,\mathfrak{n},S_\infty} \cdot \langle\, T \,\rangle \cdot \mathrm{N}_{L/K}(I_{L,S_0})$, for any $\mathfrak{n}$ multiple of the conductor of L/K it is clear that:

$$N_0 := P_{S_0,\mathfrak{n},S_\infty} \cdot \langle\, T \,\rangle \cdot I_{S_0}^n \subseteq N \ ;$$

since N_0 corresponds to an S_0-ramified $T \cup \Delta_\infty$-split abelian extension with exponent dividing n, the maximality of L gives the result. □

This Kummer situation is the starting point for the proof of the existence theorem of global class field theory; for this, one shows that if K is an arbitrary number field and M an abelian extension of exponent n of K then,

for $K' := K(\mu_n)$, we have (for suitable T and S and with self-explanatory notations):

$$M\,K' \subseteq K'\Big(\sqrt[n]{V_{T'}^{S'}}\Big)\ ;$$

we then descend to the extension M/K thanks to the type of reasoning used in 3.6, (ii). Even though we have assumed the truth of the existence theorem, this aspect is still interesting for us since it can be used algorithmically to find M concretely starting from the class field data (conductor, Artin group); this is one of the objectives of [j, Coh2, Ch. 5] to which we refer.

The reader will have noted that we are in a reflection situation and that if we want to come back to the usual situation, we must start from the radical defined by $V_{S_0}^{T\cup\Delta_\infty}$.

(5.4.9) Additional Material. In 5.4.9.1, we will go into more details about the computation of $\mathrm{rk}_{\chi^*}\Big(\bigoplus_{v\in T} U_v \bigoplus_{v\in\Delta_\infty}\{\pm1\}\Big) - \mathrm{rk}_{\chi^*}(E^{S_0\,\mathrm{ord}})$, and in 5.4.9.2, we will give some comments on the interpretation of the classical reflection theorem. The notations are given in 5.4.2 and 5.4.5.

(5.4.9.1) p-Ranks Computations. We use the following properties of representation theory of g over $\mathbb{F}_p$, in the semi-simple case (i.e., $p\nmid|g|$):

(i) In the exact sequence of $\mathbb{Z}_p[g]$-modules $1\to N\to M\to M/N\to 1$ we suppose that $N\cap M^p = N^p$; then this yields the exact sequence:

$$1\longrightarrow N/N^p\longrightarrow M/M^p\longrightarrow M/M^pN\longrightarrow 1,$$

and by semi-simplicity: $M\otimes_{\mathbb{Z}_p}\mathbb{F}_p \simeq N\otimes_{\mathbb{Z}_p}\mathbb{F}_p \oplus (M/N)\otimes_{\mathbb{Z}_p}\mathbb{F}_p$ (isomorphism of representations).

(ii) If the $\mathbb{Z}_p[g]$-module M is a free $\mathbb{Z}_p$-module of finite type, the $\mathbb{F}_p$-representation $M\otimes_{\mathbb{Z}_p}\mathbb{F}_p \simeq M/M^p$ and the $\mathbb{Q}_p$-representation $M\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ have the same character (see [Se4, §§ 14-16]).

(iii) If M is a *finite* $\mathbb{Z}_p[g]$-module then the $\mathbb{F}_p$-representations M/M^p and ${}_pM := \{x\in M,\ x^p=1\}$ are isomorphic: from the above reference, we know that, in the semi-simple case, the representation theories over $\mathbb{Z}_p$ and $\mathbb{F}_p$ are "the same" by reduction modulo p, so that for any $\chi\in\mathfrak{X}_p(g)$ we can write the exact sequence of $\mathbb{Z}_p[g]$-modules:

$$1\longrightarrow ({}_pM)^{e_\chi}\longrightarrow M^{e_\chi}\xrightarrow{\ p\ }(M^{e_\chi})^p = (M^p)^{e_\chi}\longrightarrow 1$$

(the idempotents e_χ being those of $\mathbb{Z}_p[g]$); since M is finite, we get:

$$|({}_pM)_\chi| := |({}_pM)^{e_\chi}| = |M^{e_\chi}|\,|(M^p)^{e_\chi}|^{-1} = |(M/M^p)^{e_\chi}| =: |(M/M^p)_\chi|,$$

which proves that $(M/M^p)_\chi$ and $({}_pM)_\chi$ are isomorphic.

(iv) Let d be a subgroup of g and V_d the permutation representation of g modulo d ($V_d \simeq \mathbb{F}_p[g]\sum_{t\in d} t$ for instance); then the character of V_d is $\mathrm{Ind}_d^g(1_d) =: \sum_{\chi\in\mathfrak{X}_p(g)} \rho_\chi\,\chi$, where we recall that $\rho_\chi := \frac{1}{|d|}\sum_{t\in d}\psi(t)$, $\psi|\chi$. If d is normal in g, V_d is the regular representation of g/d, then $\rho_\chi = \psi(1)$ (resp. 0) if $d \subseteq \mathrm{Ker}(\chi)$ (resp. $d \not\subseteq \mathrm{Ker}(\chi)$).

(v) Let d be a subgroup of g and W a representation of d whose character is equal to the restriction of the Teichmüller character ω (since $\mu_p \subset K$, then μ_p is such a representation). Then, the character of the representation V of g induced by W is $(\mathrm{Ind}_d^g(1_d))^*$, and $\mathrm{rk}_{\chi^*}(V) = \rho_\chi$: indeed, the s_i denoting a complete system of representatives of g/d, by definition (see [Se4, § 3.3, Th. 12]) we have for all $s \in g$:

$$\begin{aligned}\mathrm{Ind}_d^g(\omega)(s) &= \sum_{\substack{s_i\in g/d\\ s_i^{-1}ss_i\in d}} \omega(s_i^{-1}ss_i) = \sum_{\substack{s_i\in g/d\\ s_i^{-1}ss_i\in d}} \omega(s)\\ &= \omega(s)\,\mathrm{Ind}_d^g(1_d)(s) = \omega(s)\,\mathrm{Ind}_d^g(1_d)(s^{-1}),\end{aligned}$$

giving the first part of the claim; then, $\mathrm{rk}_{\chi^*}(V)$ is given by the scalar product $\langle\,(\mathrm{Ind}_d^g(1_d))^*, \psi^*\,\rangle$ with $\psi^* := \omega\psi^{-1}$ (note that ψ^* is also absolutely irreducible), and an elementary computation yields $\langle\,(\mathrm{Ind}_d^g(1_d))^*, \psi^*\,\rangle = \langle\,\mathrm{Ind}_d^g(1_d), \psi\,\rangle$. Therefore $\mathrm{rk}_{\chi^*}(V) = \rho_\chi$.

Let $u \in Pl_{p,k}$, and consider the induced representation $\bigoplus_{v|u} U_v \otimes \mathbb{F}_p$ of g; from (i) with $N = \bigoplus_{v|u}\mathrm{tor}(U_v)$ we have:

$$\bigoplus_{v|u} U_v \otimes \mathbb{F}_p \simeq \bigoplus_{v|u}\mathrm{tor}(U_v)\otimes\mathbb{F}_p \,\oplus\, \bigoplus_{v|u}(U_v/\mathrm{tor}(U_v))\otimes\mathbb{F}_p.$$

Using the log map defined in III.2.2.1, which is a g-module homomorphism, injective on $\bigoplus_{v|u}(U_v/\mathrm{tor}(U_v))$, we see from (ii) that the character of $\bigoplus_{v|u}(U_v/\mathrm{tor}(U_v))\otimes\mathbb{F}_p$ is the character of the $\mathbb{Q}_p$-representation $\bigoplus_{v|u} K_v$ which is $[k_u : \mathbb{Q}_p]$ times the regular representation. The corresponding χ^*-rank is thus $[k_u : \mathbb{Q}_p]\psi^*(1) = [k_u : \mathbb{Q}_p]\psi(1)$.

Since $\mu_p \subset K$, $\bigoplus_{v|u}\mathrm{tor}(U_v)\otimes\mathbb{F}_p$ is induced by $\mathrm{tor}(U_v)\otimes\mathbb{F}_p$ whose character is ω; from (v), the character of the above representation of g is $(\mathrm{Ind}_{d_u}^g(1_{d_u}))^*$, where we recall that d_u is the decomposition group in K/k of a fixed place $v|u$, and the χ^*-rank is $\rho_{u,\chi}$.

Let $u \in Pl_{\mathrm{ta}}$. In this case $U_v^1 \otimes \mathbb{F}_p = 1$ and the character of $\bigoplus_{v|u} U_v \otimes \mathbb{F}_p$ is the character of the torsion part giving a χ^*-rank equal to $\rho_{u,\chi}$.

Let $u \in Pl^{\mathrm{r}}_{k,\infty}$. In this case, $\bigoplus_{v|u}\{\pm 1\}\otimes\mathbb{F}_p$ is nontrivial only for $p = 2$ and gives the regular representation since $d_u = 1$ (by assumption $|g|$ is odd); this yields a χ^*-rank equal to $\delta_{2,p}\psi(1)$.

We now compute the χ^*-rank of $E^{S_0\,\mathrm{ord}}$ which is given by the Dirichlet–Herbrand Theorem I.3.7. We have:

$$\mathrm{rk}_{\chi^*}(E^{S_0\,\mathrm{ord}}) = \sum_{u\in Pl_{k,\infty}} \rho_{u,\chi^*} + \sum_{u\in S_{0,k}} \rho_{u,\chi^*} + \delta_{\omega,\chi^*} - \delta_{1,\chi^*}.$$

We remark that if u is a complex infinite place of k or a real infinite place of k, totally split in K/k, then $\rho_{u,\chi^*} = \psi(1)$ since $d_u = 1$; if u is a real infinite place of k, complexified in K/k, then $\rho_{u,\chi^*} = \frac{1}{2}(\psi(1)+\psi(c_u))$ where c_u generates d_u. Note that $\delta_{\omega,\chi^*} = \delta_{1,\chi}$ and $\delta_{1,\chi^*} = \delta_{\omega,\chi}$.

We have obtained:

$$\mathrm{rk}_{\chi^*}\Big(\bigoplus_{v\in T} U_v \bigoplus_{v\in\Delta_\infty}\{\pm1\}\Big) = \sum_{u\in T_k}\rho_{u,\chi} + \sum_{u\in T_{p,k}}[k_u:\mathbb{Q}_p]\psi(1) + \delta_{2,p}\psi(1)|\Delta_{\infty,k}|,$$

and:

$$\mathrm{rk}_{\chi^*}(E^{S_0\,\mathrm{ord}}) = r_2(k)\psi(1) + \sum_{u\in Pl^{\mathrm{r}}_{k,\infty}\cup S_{0,k}} \rho_{u,\chi^*} + \delta_{1,\chi} - \delta_{\omega,\chi}.$$

This yields the second expression of $\rho_\chi(T,S)$ given at the end of 5.4.2.

Note. We have $\sum_{u\in Pl_{k,\infty}}(\rho_{u,\chi}+\rho_{u,\chi^*}) = \psi(1)[k:\mathbb{Q}] + \delta_{2,p}\psi(1)r_1(k)$: we check that $\rho_{u,\chi}+\rho_{u,\chi^*} = \frac{1}{2}(\psi(1)+\psi(c_u)+\psi(1)+\psi(c_u)\omega(c_u))$; if $c_u = 1$, this sum is equal to $2\psi(1)$; otherwise, if $c_u \neq 1$ (which supposes $p\neq 2$), $\omega(c_u) = -1$, and this sum is equal to $\psi(1)$; let $r_1^{\mathrm{c}}(k) := |Pl^{\mathrm{rc}}_{k,\infty}|$; $\sum_{v\in Pl_{k,\infty}}(\rho_{u,\chi}+\rho_{u,\chi^*}) - \psi(1)[k:\mathbb{Q}] = \psi(1)\big(2\big(r_2(k)+r_1(k)-r_1^{\mathrm{c}}(k)\big)+r_1^{\mathrm{c}}(k)\big)-\psi(1)\big(r_1(k)+2r_2(k)\big) = \psi(1)\big(r_1(k)-r_1^{\mathrm{c}}(k)\big) = \delta_{2,p}\psi(1)r_1(k)$. Finally we use the relation $[k:\mathbb{Q}] = r_1(k)+2r_2(k) = \sum_{u|p}[k_u:\mathbb{Q}_p]$ to obtain the first expression of $\rho_\chi(T,S)$ (note that $r_1^{\mathrm{c}}(k) = 0$ if $p=2$ since $|g|$ is odd, and $r_1^{\mathrm{c}}(k) = r_1(k)$ if $p\neq 2$ since $K\supset\mu_p$ is totally complex).

(5.4.9.2) Interpretation of the Reflection Theorem for Usual Class Groups. We consider the case where $\mu_p =: \langle\,\zeta\,\rangle \subset K$, $T=\emptyset$, $S = S_\infty \subseteq Pl^{\mathrm{r}}_\infty$; then the reflection theorem becomes for any $\chi\in\mathfrak{X}_p(g)$:

$$\mathrm{rk}_{\chi^*}(\mathcal{C}\ell^{S_\infty}) - \mathrm{rk}_\chi(\mathcal{C}\ell^{\Delta_\infty}_{\mathfrak{m}^*}) = \rho_\chi(\emptyset, S_\infty), \tag{1}$$

where $\mathfrak{m}^* := \prod_{v|p}\mathfrak{p}_v^{pe_v} = p(1-\zeta)$ is the modulus of p-primarity of K which characterizes the non-ramification at p of Kummer extensions of degree p (review I.6.3), and where $\Delta_\infty := Pl^{\mathrm{r}}_\infty\setminus S_\infty$.

We can take the χ-parts of the exact sequences given in the proof of I.4.5, (ii) (beware that the notations are permuted because of the reflection situation: $\mathfrak{m}\mapsto\mathfrak{m}^*$, $T\mapsto Pl_p$, $S_\infty\mapsto\Delta_\infty$, $\Delta_\infty\mapsto S_\infty$); then since $(U_v/U_v^1)_p = 1$ for $v|p$, taking $\mathfrak{n}=1$, $\Sigma_\infty\subseteq S_\infty$, we obtain:

$$\begin{aligned}&\mathrm{rk}_\chi(\mathcal{C}\ell^{\Delta_\infty}_{\mathfrak{m}^*}) - \mathrm{rk}_\chi(\mathcal{C}\ell^{\Delta_\infty\cup\Sigma_\infty}) = \\ &\mathrm{rk}_\chi\Big(\bigoplus_{v|p} U_v^1/(U_v^1)^p U_v^{pe_v} \bigoplus_{v\in\Sigma_\infty}\{\pm1\}\Big) - \mathrm{rk}_\chi\big(Y_{Pl_p}^{\Delta_\infty\cup\Sigma_\infty}/Y_{Pl_p,\mathfrak{m}^*}^{\Delta_\infty}\big),\end{aligned} \tag{2}$$

where we recall that:

$$\begin{aligned} Y^{\rm ord}_{Pl_p} &:= \{\alpha \in K^\times_{Pl_p},\ \ (\alpha) = \mathfrak{a}^p\},\\ Y^{\Delta_\infty \cup \Sigma_\infty}_{Pl_p} &:= \{\alpha \in Y^{\rm ord}_{Pl_p},\ \ i_v(\alpha) > 0\ \forall v \in S_\infty \setminus \Sigma_\infty\},\\ Y^{\Delta_\infty}_{Pl_p,\mathfrak{m}^*} &:= \{\alpha \in Y^{\rm ord}_{Pl_p},\ \ i_v(\alpha) \in (U^1_v)^p U_v^{pe_v}\ \forall v|p,\ \ i_v(\alpha) > 0\ \forall v \in S_\infty\} \end{aligned}$$

(the subgroup of p-primary "Δ_∞-pseudo-units"); this group will be denoted $Y^{\Delta_\infty}_{\rm prim}$ (and for simplicity, the indices Pl_p will be omitted). Recall that $Y^{\rm ord} = K^{\times p} Y^{\rm ord}_{Pl_p}$ is given by the exact sequence:

$$1 \longrightarrow E^{\rm ord}/(E^{\rm ord})^p \longrightarrow Y^{\rm ord}/K^{\times p} \longrightarrow {}_p\mathcal{C}\ell^{\rm ord} \longrightarrow 1, \tag{3}$$

where $({}_p\mathcal{C}\ell^{\rm ord})_\chi \simeq \mathcal{C}\ell^{\rm ord}_\chi$ by (iii). Thus we easily obtain from (1) and (2):

$$\begin{aligned} &{\rm rk}_{\chi^*}(\mathcal{C}\ell^{S_\infty}) - {\rm rk}_\chi(\mathcal{C}\ell^{\Delta_\infty \cup \Sigma_\infty}) = \rho_\chi(\emptyset, S_\infty)\\ &+{\rm rk}_\chi\Big(\bigoplus_{v|p} U^1_v/(U^1_v)^p U_v^{pe_v} \bigoplus_{v \in \Sigma_\infty} \{\pm 1\}\Big) - {\rm rk}_\chi\big(Y^{\Delta_\infty \cup \Sigma_\infty}/Y^{\Delta_\infty}_{\rm prim}\big). \end{aligned}$$

We now compute the χ-rank of $\bigoplus_{v|p} U^1_v/(U^1_v)^p U_v^{pe_v}$. Consider the exact sequences:

$$1 \longrightarrow U_v^{pe_v}/U_v^{pe_v} \cap (U^1_v)^p \longrightarrow U^1_v/(U^1_v)^p \longrightarrow U^1_v/(U^1_v)^p U_v^{pe_v} \longrightarrow 1,$$

and:

$$1 \longrightarrow U_v^{pe_v} \cap (U^1_v)^p \longrightarrow U_v^{pe_v} \xrightarrow{\ \tau\ } \mu_p \longrightarrow 1,$$

where the map τ associates with $\alpha = 1 + p(1-\zeta)\eta$ the root of unity ζ^t with $t := {\rm tr}_{F_v/\mathbb{F}_p}(\overline{\eta})$ (see I.6.3.5).

If $s \in d_u$, $s(\alpha) = 1 + p(1-\zeta^{\omega(s)})s(\eta) = 1 + p(1-\zeta)\frac{1-\zeta^{\omega(s)}}{1-\zeta} s(\eta) \equiv 1 + p(1-\zeta)\omega(s)s(\eta) \bmod p(1-\zeta)\mathfrak{p}_v$, thus ${\rm tr}_{F_v/\mathbb{F}_p}\big(\overline{\omega(s)}\ \overline{s(\eta)}\big) = \overline{\omega(s)}{\rm tr}_{F_v/\mathbb{F}_p}(\overline{\eta})$ since $\overline{\omega(s)} \in \mathbb{F}_p$; therefore τ is an homomorphism of d_u-modules and the character of the representation $\bigoplus_{v|u} U_v^{pe_v}/U_v^{pe_v} \cap (U^1_v)^p$ is induced by ω; then, using 5.4.9.1, (v), we get:

$$\begin{aligned} {\rm rk}_\chi\Big(\bigoplus_{v|u} U^1_v/(U^1_v)^p U_v^{pe_v}\Big) &= {\rm rk}_\chi\Big(\bigoplus_{v|u} U^1_v/(U^1_v)^p\Big) - {\rm rk}_\chi\Big(\bigoplus_{v|u} U_v^{pe_v}/U_v^{pe_v} \cap (U^1_v)^p\Big)\\ &= \rho_{u,\chi^*} + [k_u : \mathbb{Q}_p]\psi(1) - \rho_{u,\chi^*} = [k_u : \mathbb{Q}_p]\psi(1), \end{aligned}$$

and we get:

$$\begin{aligned} &{\rm rk}_{\chi^*}(\mathcal{C}\ell^{S_\infty}) - {\rm rk}_\chi(\mathcal{C}\ell^{\Delta_\infty \cup \Sigma_\infty})\\ &\quad = \rho_\chi(\emptyset, S_\infty) + \sum_{u|p} [k_u : \mathbb{Q}_p]\psi(1) + \delta_{2,p}\psi(1)|\Sigma_{\infty,k}| - {\rm rk}_\chi\big(Y^{\Delta_\infty \cup \Sigma_\infty}/Y^{\Delta_\infty}_{\rm prim}\big)\\ &\quad = \rho_\chi(\emptyset, S_\infty) + \psi(1)\big([k : \mathbb{Q}] + \delta_{2,p}|\Sigma_{\infty,k}|\big) - {\rm rk}_\chi\big(Y^{\Delta_\infty \cup \Sigma_\infty}/Y^{\Delta_\infty}_{\rm prim}\big). \end{aligned}$$

Using the expression of $\rho_\chi(\emptyset, S_\infty)$ and the relation $[k:\mathbb{Q}] = r_1(k) + 2r_2(k)$, we finally obtain:

$$\mathrm{rk}_{\chi^*}(\mathcal{C}\ell^{S_\infty}) - \mathrm{rk}_\chi(\mathcal{C}\ell^{\Delta_\infty \cup \Sigma_\infty}) = \delta_{\omega,\chi} - \delta_{1,\chi} - \sum_{u \in Pl^r_{k,\infty}} \rho_{u,\chi^*}$$

$$+\psi(1)\big(r_1(k) + r_2(k) + \delta_{2,p}|\Delta_{\infty,k} \cup \Sigma_{\infty,k}|\big) - \mathrm{rk}_\chi\big(Y^{\Delta_\infty \cup \Sigma_\infty}/Y^{\Delta_\infty}_{\mathrm{prim}}\big)\ ; \quad (4)$$

since $\mathrm{rk}_\chi\big(Y^{\Delta_\infty \cup \Sigma_\infty}/Y^{\Delta_\infty}_{\mathrm{prim}}\big)$ is the χ-rank of the diagonal image of $Y^{\Delta_\infty \cup \Sigma_\infty}$ in $\bigoplus_{v|p} U^1_v/(U^1_v)^p U_v^{pe_v} \bigoplus_{v \in \Sigma_\infty} \{\pm 1\}$, we have the inequality:

$$\mathrm{rk}_\chi\big(Y^{\Delta_\infty \cup \Sigma_\infty}/Y^{\Delta_\infty}_{\mathrm{prim}}\big) \le \psi(1)\big([k:\mathbb{Q}] + \delta_{2,p}|\Sigma_{\infty,k}|\big). \quad (4')$$

We will explain the interest of such formulas (4), (4′), by giving two classical examples which are not always well understood since, in general, in (4) the term $\psi(1)\big([k:\mathbb{Q}]+\delta_{2,p}|\Sigma_{\infty,k}|\big) - \mathrm{rk}_\chi\big(Y^{\Delta_\infty \cup \Sigma_\infty}/Y^{\Delta_\infty}_{\mathrm{prim}}\big)$ is replaced by 0 (for a lower bound) or by $\psi(1)\big([k:\mathbb{Q}] + \delta_{2,p}|\Sigma_{\infty,k}|\big)$ (for an upper bound), giving again the Leopoldt's Spiegelungssatz 5.4.6, (i) with inequalities.

For $p = 2$, to obtain the inequalities 5.4.6, (ii), we substract the equality (4) with $S_\infty = Pl^r_\infty$ from the equality (4) with $S_\infty = \emptyset$ ($\Sigma_\infty = \emptyset$ in each case); then we check that $\mathrm{rk}_\chi(Y^{\mathrm{ord}}/Y^{\mathrm{ord}}_{\mathrm{prim}}) - \mathrm{rk}_\chi(Y^{\mathrm{res}}/Y^{\mathrm{res}}_{\mathrm{prim}})$ is the χ-rank of the quotient of the images of Y^{ord} and Y^{res} in $\bigoplus_{v|p} U^1_v/(U^1_v)^p U_v^{pe_v}$.

Analysis of the Theorem of Scholz. We refer to 5.4.6.1 and 5.4.6.2 to review that $\mathrm{rk}_\chi(\mathcal{C}\ell) = \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big)$, $\mathrm{rk}_{\chi^*}(\mathcal{C}\ell) = \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big)$.

Let $E =: \langle\, \varepsilon, \zeta \,\rangle$, where ε is the fundamental unit of $\mathbb{Q}(\sqrt{d}\,)$; to simplify, we merge the notation of an element with that of its class modulo $K^{\times 3}$. Thus:

$$(E/E^3)_\chi = \langle\, \varepsilon \,\rangle, \quad (E/E^3)_{\chi^*} = 1,$$

$$(E/E^3)_\omega = \langle\, \zeta \,\rangle, \quad (E/E^3)_1 = 1\ ;$$

Formulas (4), (4′) yield (since $\rho_{\infty,\chi^*} = 0$):

$$\mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big) - \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big) = 1 - \mathrm{rk}_3\big(Y_{\mathbb{Q}(\sqrt{d})}/Y_{\mathbb{Q}(\sqrt{d}),\mathrm{prim}}\big),$$

with $\mathrm{rk}_3\big(Y_{\mathbb{Q}(\sqrt{d})}/Y_{\mathbb{Q}(\sqrt{d}),\mathrm{prim}}\big) \le 1$. Let:

$$Y_{\mathbb{Q}(\sqrt{d})}/\mathbb{Q}(\sqrt{d}\,)^{\times 3} =: \langle\, y_1, \ldots, y_r, \varepsilon \,\rangle,$$

where r is the 3-rank of the class group of $\mathbb{Q}(\sqrt{d}\,)$ (see (3)); we have:

$$\mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big) - \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big) = 1$$

if and only if the y_i as well as ε are 3-primary; otherwise $Y_{\mathbb{Q}(\sqrt{d}),\mathrm{prim}}$ is of index 3 in $Y_{\mathbb{Q}(\sqrt{d})}$ and we have:

$$\mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big) = \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big).$$

If we only know that ε is 3-primary, then we have:

$$0 \le \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big) - \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big) \le 1\ ;$$

oterwise, if we know that ε *is not* 3-primary, then:

$$\mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big) = \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big).$$

Symmetrically, we can start from the character χ^* and write (with $\rho_{\infty,\chi} = 1$):

$$\mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big) - \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big) = -\mathrm{rk}_3\big(Y_{\mathbb{Q}(\sqrt{-3d})}/Y_{\mathbb{Q}(\sqrt{-3d}),\mathrm{prim}}\big),$$

with $\mathrm{rk}_3\big(Y_{\mathbb{Q}(\sqrt{-3d})}/Y_{\mathbb{Q}(\sqrt{-3d}),\mathrm{prim}}\big) \le 1$, then we can put, in an analogous manner, $Y_{\mathbb{Q}(\sqrt{-3d})}/\mathbb{Q}(\sqrt{-3d}\,)^{\times 3} = \langle\, y'_1, \ldots, y'_{r'} \,\rangle$, where r' is the 3-rank of the class group of $\mathbb{Q}(\sqrt{-3d}\,)$, which gives the following reasoning. We have:

$$\mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big) = \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big)$$

if and only if all the y'_i are 3-primary, otherwise $Y_{\mathbb{Q}(\sqrt{-3d}),\mathrm{prim}}$ is of index 3 in $Y_{\mathbb{Q}(\sqrt{-3d})}$ and this yields:

$$\mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{d})}\big) - \mathrm{rk}_3\big(\mathcal{C}\ell_{\mathbb{Q}(\sqrt{-3d})}\big) = -1.$$

This methodology was initiated in: Bull. Soc. Math. France 100 (1972), 177–193; in this paper we gave many numerical examples.

Analysis of a Result of Hecke. We are now concerned with the case $K = \mathbb{Q}(\mu_p)$, $p \ne 2$, with $g = \mathrm{Gal}(K/\mathbb{Q})$. For an even character $\chi \ne 1$ (i.e., $\chi = \omega^k$, k even, $1 < k < p-1$), we have $\chi^* = \omega\chi^{-1} = \omega^{1-k} \ne \omega$. Since $\rho_{\infty,\chi^*} = 0$, formulas (4), (4′) yield:

$$\mathrm{rk}_{\chi^*}(\mathcal{C}\ell) - \mathrm{rk}_\chi(\mathcal{C}\ell) = 1 - \mathrm{rk}_\chi\big(Y/Y_{\mathrm{prim}}\big),$$

with $\mathrm{rk}_\chi\big(Y/Y_{\mathrm{prim}}\big) \le 1$. Let $(E/E^p)_\chi =: \langle\, \varepsilon_\chi E^p \,\rangle$ denoted $\langle\, \varepsilon_\chi \,\rangle$, and let:

$$\big(Y/K^{\times p}\big)_\chi =: \langle\, y_1, \ldots, y_{r_\chi}, \varepsilon_\chi \,\rangle,$$

where r_χ is the χ-rank of the class group, and where all the numbers are prime to p. Then:

$$\mathrm{rk}_{\chi^*}(\mathcal{C}\ell) - \mathrm{rk}_\chi(\mathcal{C}\ell) = 1$$

if and only if all the elements $y_1, \ldots, y_{r_\chi}, \varepsilon_\chi$ are p-primary, otherwise, $\big(Y_{\mathrm{prim}}/K^{\times p}\big)_\chi$ is of index p in $\big(Y/K^{\times p}\big)_\chi$ and the p-ranks are equal.

If ε_χ is p-primary, we only have $0 \le \mathrm{rk}_{\chi^*}(\mathcal{C}\ell) - \mathrm{rk}_\chi(\mathcal{C}\ell) \le 1$, otherwise $\mathrm{rk}_{\chi^*}(\mathcal{C}\ell) = \mathrm{rk}_\chi(\mathcal{C}\ell)$.

The result of Hecke (1910) was (with classical notations) the inequality $\mathrm{rk}_p(\mathcal{C}\ell^+) \leq \mathrm{rk}_p(\mathcal{C}\ell^-)$ that we easily obtain from (4) by summation over the even $\chi \neq 1$; the use of (4′) yields $0 \leq \mathrm{rk}_p(\mathcal{C}\ell^-) - \mathrm{rk}_p(\mathcal{C}\ell^+) \leq \frac{p-3}{2}$. Some insights into representation aspects were given by Pollaczek (1924) after Kummer.

If we start from the odd character $\chi^* \neq \omega$, we obtain, since $\rho_{\infty,\chi} = 1$:

$$\mathrm{rk}_\chi(\mathcal{C}\ell) - \mathrm{rk}_{\chi^*}(\mathcal{C}\ell) = -\mathrm{rk}_{\chi^*}\big(Y/Y_{\mathrm{prim}}\big)\ ;$$

then if $\big(Y/K^{\times p}\big)_{\chi^*} =: \langle\, y'_1, \ldots, y'_{r_{\chi^*}} \,\rangle$, the reasoning is the same, but with pseudo-units (which are not units) comming from an odd component.

We do not know examples with $r_\chi \geq 1$ (see [(c), Wa, Ch. 8, § 3]). To find an $r_\chi \geq 1$, we must check that $r_{\chi^*} \geq 1$ and (when it is the case) that y'_{χ^*} (generator of $(Y/K^{\times p})_{\chi^*}$ when $r_{\chi^*} = 1$) is p-primary (the case $r_{\chi^*} \geq 2$ automatically yields $r_\chi \geq 1$); the first condition is equivalent to the triviality modulo (p) of the generalized Bernoulli number b_{χ^*} or to the p-primarity of the cyclotomic unit η_χ, giving a probability equal to $\frac{1}{p}$;[34] the second condition (when the first one is realized with $r_{\chi^*} = 1$) has also a probability equal to $\frac{1}{p}$. If we assume that these two conditions are independent, this gives the probability $\frac{1}{p^2}$ (for χ fixed). We have neglected the case $r_{\chi^*} \geq 2$ whose probability is less than $\frac{1}{p^2}$ (the principal theorem of Ribet–Mazur–Wiles–Kolyvagin implies that $|\mathcal{C}\ell_K^{e_{\chi^*}}| = |b_{\chi^*}|_p^{-1}$, but if $b_{\chi^*} \equiv 0 \bmod (p^2)$, $\mathcal{C}\ell_K^{e_{\chi^*}}$ may be cyclic), so that we can consider the probability $\frac{2}{p^2}$ as a wide upper bound.

This heuristic reasoning, involving *congruences*, is more convincing than the direct interpretation $r_\chi \geq 1$ if and only if $p \,|\, (\langle\, \varepsilon_\chi \,\rangle : \langle\, \eta_\chi \,\rangle)$ (principal theorem of Ribet–Mazur–Wiles–Kolyvagin–Greither), since we do not know efficient heuristics for global p-powers; the above gives for $p \,|\, (\langle\, \varepsilon_\chi \,\rangle : \langle\, \eta_\chi \,\rangle)$ a probability less than $\frac{2}{p^2}$ (see [Scho2] for the non-p-parts of the class goup).

But there are $n := \frac{p-3}{2}$ even characters $\neq 1$ for $p \geq 3$; perhaps they do not have the same "weight" because of the subfields of "small" degree whose p-class number can be limited. To be more precise, we may estimate the index of irregularity $i(p)$ (i.e., the number of odd characters χ^* giving $r_{\chi^*} \geq 1$): it seems clear that the density of prime numbers p, for which $i(p) \geq 1$, exists (its

[34] The equivalence of these two conditions is classical and comes from the congruence properties of p-adic L-functions. Let $\mu_p =: \langle\, \zeta \,\rangle$, and for any $a \in \mathbb{Z}$ prime to p, let $\sigma_a \in g$ be such that $\sigma_a(\zeta) = \zeta^a$. By definition, we have $b_{\chi^*} := \frac{1}{p} \sum_{a=1}^{p-1} \chi^*(\sigma_a^{-1}) a \in \mathbb{Z}_p$, and $\eta_\chi := (1-\zeta)^{e_\chi}$ seen in $(E/E^p)_\chi$, with the idempotent $e_\chi := \frac{1}{p-1} \sum_{a=1}^{p-1} \chi(\sigma_a^{-1}) \sigma_a \in \mathbb{Z}_p[g]$; for $u = p$, $e_v = 1$, $\varphi \notin \{1, \omega\}$, we have $(U_v^1/(U_v^1)^p U_v^p)_\varphi \simeq \mathbb{F}_p$; since η_χ is p-primary if and only if its image in $(U_v^1/(U_v^1)^p U_v^p)_\chi$ is trivial, this gives one possibility out of p. In an analogous way, the p-primarity of y'_{χ^*} only depends on its image in $(U_v^1/(U_v^1)^p U_v^p)_{\chi^*}$.

value is discussed in [(c), Wa, Ch. 5, § 3] after the Theorem 5.17; see [Ri4] and [BCEMS] for some numerical computations). In this context, the probability that $i(p) = i \geq 0$ is $\mathsf{C}_n^i \Big(1 - \frac{1}{p}\Big)^{n-i} \Big(\frac{1}{p}\Big)^i$, for $p \geq 3$.

Since these values are in accordance with all numerical data, this "proves" that the above phenomena can be neglected[35], which yields a number of favourable cases $p < B$ around $\sum\limits_{p<B} \sum\limits_{i=0}^{n} \mathsf{C}_n^i \Big(1 - \frac{1}{p}\Big)^{n-i} \Big(\frac{1}{p}\Big)^i \Big(1 - \Big(1 - \frac{2}{p}\Big)^i\Big) = \sum\limits_{p<B} \Big(1 - \Big(1 - \frac{2}{p^2}\Big)^n\Big) < \sum\limits_{p<B} \frac{2n}{p^2} < \sum\limits_{p<B} \frac{1}{p} < \log(\log(B))$ (of course, it is then equivalent to use directly the probability that $p \,|\, (\langle\, \varepsilon_\chi \,\rangle : \langle\, \eta_\chi \,\rangle)$ for *at least* one character χ). See in [Th2] a criterion for the p-triviality of this index.

In conclusion, the classical Kummer–Vandiver conjecture is probably false for probabilistic reasons[36] (see [Iw5] for another approach with Gauss sums).

c) Class Field Theory Over $\mathbb{Q}$

We come back to ray class fields by looking at the case where the base field is $\mathbb{Q}$.

5.5 Ray Class Fields on the Field of Rational Numbers. If $K = \mathbb{Q}$, any modulus is of the form $m\mathbb{Z}$ for $m \geq 1$, and the ray class field $\mathbb{Q}_{(m)}{}^{\rm res}$ is simply the cyclotomic field $\mathbb{Q}(\mu_m)$ of mth roots of unity (see 5.5.1). Note that (except for $m = 1,\ 2$, where $\mathbb{Q}_{(m)}{}^{\rm res} = \mathbb{Q}$), the place at infinity of $\mathbb{Q}$ is complexified in $\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}$; the maximal real subfield of $\mathbb{Q}_{(m)}{}^{\rm res}$ is the field $\mathbb{Q}_{(m)}{}^{\{\infty\}} =: \mathbb{Q}_{(m)}{}^{\rm ord} =: \mathbb{Q}_{(m)}{}^{\rm nc}$.

The case of ray class fields over $\mathbb{Q}$ gives the simplest example in which $m\mathbb{Z}$ is not always equal to the conductor of $\mathbb{Q}_{(m)}{}^{\rm res}$: indeed, $m\mathbb{Z}$ (or simply m) is the conductor of $\mathbb{Q}_{(m)}{}^{\rm res}$ if and only if m is odd or divisible by 4 (this follows from 5.1.1.2).

Using classical properties of cyclotomic fields (see [c, Wa, Ch. 2]), we can now prove that $\mathbb{Q}_{(m)}{}^{\rm res} = \mathbb{Q}(\mu_m)$.

5.5.1 Proposition. *For any rational integer $m \geq 1$, we have:*

$$\mathbb{Q}_{(m)}{}^{\rm res} = \mathbb{Q}(\mu_m).$$

Proof. With the computation that we will give in 5.5.2, we already have:

$$\mathrm{Gal}(\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}),$$

[35] However, see [Sou] giving some insights into this aspect.

[36] A more precise computation involving the Cohen–Lenstra–Martinet heuristics on class groups would certainly give less than $c\log(\log(B))$ with $c < 1$. Moreover, discarding the small primes, we would obtain $c\log(\log(B)) - c'$, $c' > 1$, which explains that only very large p can disprove the conjecture.

so an inclusion will be sufficient. We will check that $\mathbb{Q}(\mu_m) \subseteq \mathbb{Q}_{(m)}{}^{\mathrm{res}}$; for this we may assume that m is a conductor. By 4.1.1, we are reduced to compute the conductor of $\mathbb{Q}(\mu_{\ell^n})$ where ℓ^n is the ℓ-part of m ($n \geq 1$, $n \geq 2$ if $\ell = 2$). Then, since ℓ is the only ramified place, we see from 4.2.1 that this conductor is that of $\mathbb{Q}_\ell(\mu_{\ell^n})$. Part (i) of Exercise 3.4.3 computes the norm group, and hence the conductor, equal to ℓ^n. □

5.5.2 Remark. At the level of generalized class groups and of the Artin map, we do not obtain directly the classical isomorphism:

$$\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times.$$

Indeed, if we denote by T the support of $m\mathbb{Z}$ we obtain:

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}_{(m)}{}^{\mathrm{res}}/\mathbb{Q}) &\simeq I_T/P_{T,m\mathbb{Z},\mathrm{pos}}\\ &= \{a\mathbb{Z},\ a \in \mathbb{Q}_T^\times\}/\{u\mathbb{Z},\ u \in \mathbb{Q}_T^\times,\ u \equiv 1 \bmod m\mathbb{Z},\ u > 0\}\ ;\end{aligned}$$

now consider the map (which is well defined):

$$\begin{array}{ccc} I_T & \longrightarrow & (\mathbb{Z}/m\mathbb{Z})^\times\ ;\\ a\mathbb{Z} & \longmapsto & |a| + m\mathbb{Z}\end{array}$$

its kernel is the set of the $a\mathbb{Z}$, $a \in \mathbb{Q}_T^\times$ such that $|a| \equiv 1 \bmod m\mathbb{Z}$, hence is equal to $P_{T,m\mathbb{Z},\mathrm{pos}}$; since surjectivity is trivial, we obtain the expected isomorphism (which is specific to the base field $\mathbb{Q}$).

We recover the Artin map:

$$I_T/P_{T,m\mathbb{Z},\mathrm{pos}} \longrightarrow \mathrm{Gal}(\mathbb{Q}_{(m)}{}^{\mathrm{res}}/\mathbb{Q}),$$

which sends $\ell\mathbb{Z} =: (\ell)$, with ℓ positive prime number not dividing m, to the Frobenius:

$$\left(\frac{\mathbb{Q}_{(m)}{}^{\mathrm{res}}/\mathbb{Q}}{(\ell)}\right)$$

(which acts via $\zeta \longrightarrow \zeta^\ell$ for any $\zeta \in \mu_m$), by composing the above isomorphism:

$$I_T/P_{T,m\mathbb{Z},\mathrm{pos}} \longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times,$$

with the one sending $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$ for $a \in \mathbb{Q}_T^\times$ to the Artin symbol:

$$\left(\frac{\mathbb{Q}_{(m)}{}^{\mathrm{res}}/\mathbb{Q}}{(b)}\right),$$

where b is a *positive representative* of $a + m\mathbb{Z}$ (and not $|a|$!). More generally, we would like to insist on the fact that a Frobenius $\left(\frac{L^{\mathrm{ab}}/K}{v}\right)$, or $\left(\frac{L^{\mathrm{ab}}/K}{\mathfrak{p}_v}\right)$, involves $q_v := |F_v|$, in other words a positive generator of $\mathrm{N}\mathfrak{p}_v$ (and similarly, by multiplicativity for the Artin symbol); for instance, for $m = 7$, $\left(\frac{\mathbb{Q}_{(7)}{}^{\mathrm{res}}/\mathbb{Q}}{(-2)}\right)$

would be the Frobenius of 2, of order 3, while, choosing 5 as representative of the class of -2 modulo (7), $\left(\frac{\mathbb{Q}_{(7)}{}^{\rm res}/\mathbb{Q}}{(5)}\right)$ is the Frobenius of 5, of order 6, which is indeed the automorphism $\zeta \to \zeta^{-2}$. Going from $a \in \mathbb{Q}_T^\times$ to $b > 0$ is not necessary if we set:

$$\left(\frac{\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}}{a}\right) := \left(\frac{\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}}{(a)}\right)$$

for any $a > 0$ prime to m, and:

$$\left(\frac{\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}}{-1}\right) := \left(\frac{\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}}{\infty}\right) = c$$

(complex conjugation), but this is a trick only valid for the base field $\mathbb{Q}$. □

5.6 Class Field Theory Correspondence. Thus, in the case of the base field $\mathbb{Q}$, the class field theory correspondence is the well-known Kronecker–Weber theorem, of which a direct proof is not too difficult (such a proof is given in [c, Wa, Ch. 14] and in [Neum1]). In other words, in the cyclotomic field $\mathbb{Q}(\mu_m)$, there is a bijective Galois correspondence between the set of subfields and the set of subgroups of $(\mathbb{Z}/m\mathbb{Z})^\times$.

5.6.1 Artin Group of Abelian Extensions of $\mathbb{Q}$. If L is an abelian extension of $\mathbb{Q}$ with conductor $f\mathbb{Z}$, for which we know $H := {\rm Gal}(\mathbb{Q}_{(f)}{}^{\rm res}/L)$ as a subgroup of $(\mathbb{Z}/f\mathbb{Z})^\times$, then (denoting by R the support of f) the Artin group of $L/\mathbb{Q}$ is equal to:

$$A_{L/\mathbb{Q}} = \{a\mathbb{Z},\ a \in \mathbb{Q}_R^\times,\ a > 0,\ a + f\mathbb{Z} \in H\}.$$

It indeed contains $P_{R,f\mathbb{Z},{\rm pos}}$.

5.6.2 Decomposition Law of Prime Numbers in $\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}$. By 5.2, we need not consider prime divisors ℓ of m since the inertia field is $\mathbb{Q}_{(n)}{}^{\rm res}$, where n is the largest divisor of m prime to ℓ.

The residue degree of ℓ is then the order of the class $\ell + m\mathbb{Z}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$ and the decomposition field is the field fixed under $\langle\, \ell + m\mathbb{Z}\,\rangle$. Thus, ℓ is totally split in $\mathbb{Q}_{(m)}{}^{\rm res}/\mathbb{Q}$ if and only if $\ell \equiv 1 \bmod m\mathbb{Z}$.

If the conductor of an abelian extension L is $f\mathbb{Z}$, the residue degree of $\ell \nmid f$ in $L/\mathbb{Q}$ is then the order of $\ell + f\mathbb{Z}$ modulo H.

5.6.3 Abelian Closure of $\mathbb{Q}$. The Galois group of $\overline{\mathbb{Q}}^{\rm ab} = \mathbb{Q}(\mu)$ (the field generated by all the roots of unity) is:

$$\overline{G}^{\rm ab} \simeq \varprojlim_{m \geq 1} (\mathbb{Z}/m\mathbb{Z})^\times \simeq \widehat{\mathbb{Z}}^\times = \prod_{p\,{\rm prime}} \mathbb{Z}_p^\times,$$

whose structure is well known (we will find again this result in III.4.1.11 in an idelic way). The inertia groups correspond to each $\mathbb{Z}_p^\times$.

Since $\mathrm{Gal}(\mathbb{Q}_{(m)}^{\mathrm{res}}/\mathbb{Q})$ is the direct sum of the inertia groups of the ramified primes, it is clear that it may be convenient to use duality to express the class field theory correspondence and the law of decomposition of the places. This leads to the notion of Dirichlet characters. We leave this to the reader (see [c, Wa, Ch. 3]).

d) Congruence Groups

Before coming back to generalized class groups, we explain in this short subsection a classical formalism which is necessary when we cannot take quotients by a suitable ray group, situation which we avoid since we assume the Artin reciprocity law (or any equivalent statement) from the start.

The notion of congruence groups, used instead of idèle class groups or generalized class groups, introduced without any knowledge of the existence of a norm or Artin conductor, is the following. Consider the groups $N_{\mathfrak{m}}$ (the congruence groups) which are the subgroups of I_T containing $P_{T,\mathfrak{m},\mathrm{pos}}$, where $\mathfrak{m}$ is a modulus of K with support $T \subset Pl_0$; we then define an equivalence relation by:

$$N_{\mathfrak{m}_1} \sim N_{\mathfrak{m}_2},$$

for $\mathfrak{m}_1$, $\mathfrak{m}_2$ with supports $T_1,\ T_2$, if and only if:

$$N_{\mathfrak{m}_2} \cap I_{T_1} = N_{\mathfrak{m}_1} \cap I_{T_2}.$$

In this context, class field theory consists in proving that there exists a bijective Galois correspondence between finite abelian extensions of K and equivalence classes of congruence groups; the conductor (of the extension corresponding to the class) is then the g.c.d. of the $\mathfrak{m}$ belonging to the class. From the point of view that we have adopted here, this fact is quite clear for the following reason: if $\mathfrak{f}$ is the conductor of the abelian extension L/K and if $\mathfrak{m}$, built on T, is a multiple of $\mathfrak{f}$, the congruence group relative to $\mathfrak{m}$ is the Takagi group:

$$N_{\mathfrak{m}} := P_{T,\mathfrak{m},\mathrm{pos}}\mathrm{N}_{L/K}(I_{L,T}).$$

The equivalence relation is a simple translation of the invariance of the quotients $I_T/N_{\mathfrak{m}}$ when $\mathfrak{m}$ ranges over all the multiples of $\mathfrak{f}$ (see 4.3.2, 4.4.1).

However, this point of view can be convenient to define a priori subgroups of I_T (containing $P_{T,\mathfrak{m},\mathrm{pos}}$), for instance by asking that certain ideals should be norms; we must then algorithmically compute the conductor of this congruence group and find the structure of the corresponding quotient group. This is the point of view used in [j, Coh2, Ch. 3 and 4].

e) Norm Action on Generalized Class Groups

Let L/K be a finite extension of number fields. It is useful to give the action of the arithmetic norm for L/K on generalized class groups, using the fact that it corresponds to restriction of automorphisms under the Artin map. By perversity, we are going to start by looking at class groups in idelic terms (in fact this is technically simpler).

Notation and assumption. Let $\mathfrak{m} \in \langle T \rangle_{\mathbb{N}}$, and let $\mathfrak{m}'$ be a modulus of L built from the set of places of L above those of T, such that:

$$\mathrm{N}_{L/K}(U^{\mathrm{res}}_{L,\mathfrak{m}'}) \subseteq K^{\times} U^{\mathrm{res}}_{K,\mathfrak{m}},$$

where $\mathrm{N}_{L/K}$ is the norm map from J_L to J_K. □

We then have:

5.7 Proposition. *For any finite set S of places of K, disjoint from T, we have the following commutative diagram, where S' denotes the set of places of L above those of S:*

$$\begin{array}{ccc} \mathcal{C}\ell^{S'}_{L,\mathfrak{m}'} & \xrightarrow{\quad\rho_L\quad} & \mathrm{Gal}(L_{(\mathfrak{m}')}{}^{S'}/L) \\ \Big\downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \Big\downarrow{\scriptstyle \mathit{restriction}} \\ \mathcal{C}\ell^{S}_{K,\mathfrak{m}} & \xrightarrow{\quad\rho_K\quad} & \mathrm{Gal}(K_{(\mathfrak{m})}{}^{S}/K) \end{array}$$

Proof. In the idelic formulation (see I.5.1):

$$\mathcal{C}\ell^{\mathrm{res}}_{L,\mathfrak{m}'} \simeq J_L/L^{\times} U^{\mathrm{res}}_{L,\mathfrak{m}'}, \quad \mathcal{C}\ell^{\mathrm{res}}_{K,\mathfrak{m}} \simeq J_K/K^{\times} U^{\mathrm{res}}_{K,\mathfrak{m}} \ ;$$

by assumption we have the inclusion $\mathrm{N}_{L/K}(L^{\times} U^{\mathrm{res}}_{L,\mathfrak{m}'}) \subseteq K^{\times} U^{\mathrm{res}}_{K,\mathfrak{m}}$ or, equivalently, $\mathrm{N}_{L/K}(P_{L,T,\mathfrak{m}',\mathrm{pos}}) \subseteq P_{K,T,\mathfrak{m},\mathrm{pos}}$, showing that $\mathrm{N}_{L/K}$ is defined as a map from $\mathcal{C}\ell^{\mathrm{res}}_{L,\mathfrak{m}'}$ to $\mathcal{C}\ell^{\mathrm{res}}_{K,\mathfrak{m}}$ and is also given by:

$$\mathrm{N}_{L/K}(a\ell^{\mathrm{res}}_{L,\mathfrak{m}'}(\mathfrak{a}')) := a\ell^{\mathrm{res}}_{K,\mathfrak{m}}(\mathrm{N}_{L/K}(\mathfrak{a}')),$$

for any ideal $\mathfrak{a}'$ of L prime to T. Furthermore, applying norm lifting Theorem 4.7.2 to the extension $M := K_{(\mathfrak{m})^{\mathrm{res}}}$ and to the norm group $N := K^{\times} U^{\mathrm{res}}_{K,\mathfrak{m}}$, the idèle group corresponding to $LK_{(\mathfrak{m})^{\mathrm{res}}}$ on L, is equal to $\mathrm{N}^{-1}_{L/K}(K^{\times} U^{\mathrm{res}}_{K,\mathfrak{m}})$ which contains $L^{\times} U^{\mathrm{res}}_{L,\mathfrak{m}'}$, once again by assumption; thus, we have:

$$LK_{(\mathfrak{m})^{\mathrm{res}}} \subseteq L_{(\mathfrak{m}')^{\mathrm{res}}},$$

and hence the restriction:

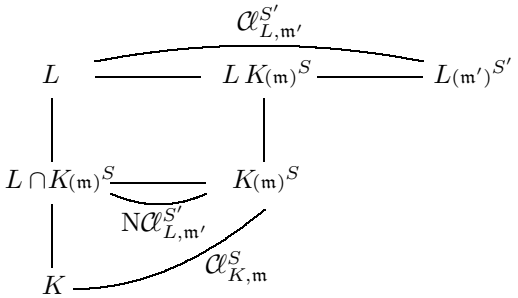
$$\mathrm{Gal}(L_{(\mathfrak{m}')}{}^{\mathrm{res}}/L) \longrightarrow \mathrm{Gal}(K_{(\mathfrak{m})}{}^{\mathrm{res}}/K)$$

makes sense.

Finally, since $\mathrm{N}_{L/K}\Big(\bigoplus_{w\in S'} L_w^\times\Big) \subseteq \bigoplus_{v\in S} K_v^\times$ (i.e., $\mathrm{N}_{L/K}(\langle\, S'\,\rangle) \subseteq \langle\, S\,\rangle$) and using the decomposition properties 1.2.5, all the above statements are still valid in terms of S and S'-splitting.

The above diagram is thus well defined, and its commutativity again comes from applying 4.5, (iv) to the extension $L_{(\mathfrak{m}')}{}^{S'}/K$. □

5.7.1 Corollary. *We have the diagram:*



where $\mathrm{Gal}(K_{(\mathfrak{m})}{}^S/L\cap K_{(\mathfrak{m})}{}^S) \simeq \mathrm{N}_{L/K}(\mathcal{C}\ell^{S'}_{L,\mathfrak{m}'})$. *In particular the norm map is surjective if and only if* L *and* $K_{(\mathfrak{m})}{}^S$ *are linearly disjoint over* K*; when this is the case,* $|\mathcal{C}\ell^{S}_{K,\mathfrak{m}}|$ *divides* $|\mathcal{C}\ell^{S'}_{L,\mathfrak{m}'}|$. □

5.7.2 Remarks. (i) We also have:

$$\mathrm{Gal}(L_{(\mathfrak{m}')}{}^{S'}/L\,K_{(\mathfrak{m})}{}^S) \simeq {}_{\mathrm{N}}\mathcal{C}\ell^{S'}_{L,\mathfrak{m}'}$$

(the kernel of the arithmetic norm $\mathrm{N}_{L/K}$), equal to:

$$\{\sigma\ell^{S'}_{L,\mathfrak{m}'}(\mathfrak{a}'),\ \ \mathfrak{a}' \text{ prime to } T,\ \sigma\ell^{S}_{K,\mathfrak{m}}(\mathrm{N}_{L/K}(\mathfrak{a}')) = 1\}.$$

(ii) Going to the limit but keeping T and S fixed (see 5.3), we obtain a similar diagram, in which $\mathrm{N}_{L/K} : J_L \longrightarrow J_K$ yields:

$$\mathrm{N}_{L/K} : \mathcal{C}\ell^{S'}_{L,T'} := \varprojlim_{\mathfrak{m}\in\langle\, T\,\rangle_{\mathbb{N}}} J_L/L^\times U^{\mathrm{res}}_{L,(\mathfrak{m})} \longrightarrow \mathcal{C}\ell^{S}_{K,T} := \varprojlim_{\mathfrak{m}\in\langle\, T\,\rangle_{\mathbb{N}}} J_K/K^\times U^{\mathrm{res}}_{K,\mathfrak{m}},$$

where, to simplify, we have chosen $\mathfrak{m}' := (\mathfrak{m})$, the modulus obtained by extending $\mathfrak{m}$ to L, which is always suitable. □

5.7.3 Remarks. (i) Without any difficulty we can even go completely to the limit on T (for instance with $S = \emptyset$) so as to obtain the corresponding abelian closures $\overline{K}^{\mathrm{ab}}$ and $\overline{L}^{\mathrm{ab}}$, the norm, still coming from $\mathrm{N}_{L/K} : J_L \longrightarrow J_K$, giving:

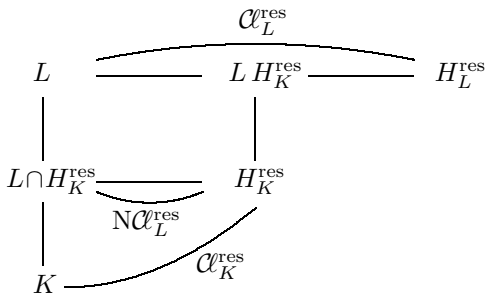
$$\mathrm{N}_{L/K} : C_L/D_L \longrightarrow C_K/D_K.$$

In this case, since $D_K = D_K^{[L:K]} \subset \mathrm{N}_{L/K}(C_L)$ by divisibility (see III.4.15.1, (i)), we get:

$$\mathrm{N}_{L/K}(C_L/D_L) = \mathrm{N}_{L/K}(C_L)/D_K \simeq \mathrm{Gal}(\overline{K}^{\mathrm{ab}}/L^{\mathrm{ab}}),$$

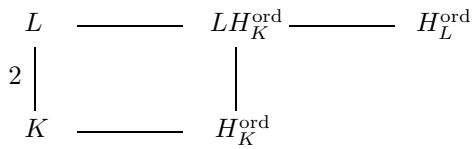
and the norm is surjective if and only if $L^{\mathrm{ab}} = K$. But this is nothing else than class field theory in L/K (see 3.7).

(ii) The usual particular cases ($T = \emptyset$, $S = \emptyset$, and $S = Pl_\infty^{\mathrm{r}}$) can be represented by an analogous diagram of finite extensions, such as:



Here $L \cap H_K^{\mathrm{res}}/K$ is the maximal abelian subextension of L/K which is unramified (at the finite places), and the norm map is surjective if and only if this extension reduces to K. For the ordinary sense, we replace everywhere "res" by "ord"; $L \cap H_K^{\mathrm{ord}}/K$ is then the maximal abelian subextension which is unramified and noncomplexified, whose Galois group measures the surjectivity defect of the norm on the ordinary class group of L. □

5.7.4 Example. Assume that L is a quadratic extension of K and that there exists a finite ramified place in L/K or a real place of K which is complexified in L; consider the ordinary sense ($T = \emptyset$, $S = Pl_\infty^{\mathrm{r}}$):



Since L/K is ramified or complexified in at least one place, we have $L \cap H_K^{\mathrm{ord}} = K$; hence the ordinary class number of K divides the ordinary class number of L. Thus, we have the exact sequence:

$$1 \longrightarrow {}_{\mathrm{N}}\mathscr{C}\ell_L^{\mathrm{ord}} \longrightarrow \mathscr{C}\ell_L^{\mathrm{ord}} \xrightarrow{\mathrm{N}_{L/K}} \mathscr{C}\ell_K^{\mathrm{ord}} \longrightarrow 1,$$

which is a simple translation of the classical equality (with notations which are themselves classical):

$$h_L = h_L^*\ h_K,$$

in which h_L^* is called the relative class number. □

5.7.5 Remark. Note that this result is often stated for a field with complex conjugation (or a CM field), in other words a totally complex field L which is a quadratic extension of a totally real field K; in this context, h_L^* and h_K are often denoted h_L^- and h_L^+ (relative class number and real class number), but this notation is ambiguous since we do not necessarily have $\mathcal{C}\ell_L = \mathcal{C}\ell_L^+ \oplus \mathcal{C}\ell_L^-$, in the usual Galois meaning for which $\mathcal{C}\ell_L^\pm := \{cl(\mathfrak{a}) \in \mathcal{C}\ell_L,\ cl(\mathfrak{a}^c) = cl(\mathfrak{a})^{\pm 1}\}$, c denoting complex conjugation (the obstruction coming from the 2-Sylow subgroups; see [Scho3], [Scho4]).

This is particularly interesting in the case of cyclotomic fields $L = \mathbb{Q}(\mu_m)$, since in this case, although $\mathbb{Q}(\mu_m)/\mathbb{Q}(\mu_m)^{\rm nc}$ is unramified as soon as m (assumed to be a nontrivial conductor) is not a prime power, we always have the relation "$h = h^-\ h^+$" (this nonramification property is proved in III.1.4.2 but can be checked in an elementary way). □

f) The Principal Ideal Theorem — Hilbert Towers

5.8 The Principal Ideal Theorem in the Tame Case. Let K be a number field together with sets of places T and S. For the tame modulus $\mathfrak{m} = \prod_{v \in T} \mathfrak{p}_v$, we consider the S-split ray class field $K' := K_{(\mathfrak{m})^S}$, and we denote by T' and S' the sets of places of K' above those of T and S. Let $K'' := K'_{(\mathfrak{m}')^{S'}}$ for $\mathfrak{m}' = \prod_{v' \in T'} \mathfrak{p}_{v'}$ be the analogous ray class field over K'. By 3.6, it is a Galois extension of K.

5.8.1 Lemma 1. *The maximal abelian subextension $K''^{\rm ab}$ of K'' in K''/K is equal to K'.*

Proof. Set $L := K''^{\rm ab} \supseteq K'$. The extension K''/K is T-tamely ramified (use 5.2.2, (ii) for the extensions K'/K and K''/K', and multiplicativity of ramification indices); it follows that L/K is also T-tamely ramified and, once again using 5.2.2, (ii), we have $L \subseteq K'$, proving equality. □

If $G' := {\rm Gal}(K'/K)$ and $G'' := {\rm Gal}(K''/K)$, we have:

$$G' = G''^{\rm ab} \text{ and } {\rm Gal}(K''/K') = [G'', G''].$$

We now state a purely algebraic but nontrivial classical result [37] which was the prelude to further development of the subject which, after Suzuki in [Su], [i, Miy0, Suzuki], has been renewed by Gruenberg–Weiss in [GW] whose main result we give a little later.

[37] Works of Artin–Furtwängler (1930), Magnus (1934), Iyanaga (1930, 1934); see [d, AT, Ch. 13, § 4] and [c, Neu1, Ch. VI, 7.6].

5.8.2 Lemma 2. *Let G be a finite group whose commutator subgroup $[G\,,\,G]$ is commutative. Then the transfer map from G to $[G\,,\,G]$ is trivial.* □

It then immediately follows, from property 4.5, (v) of the Artin map, that for a number field K given together with sets of places T and S, we have:

5.8.3 Theorem (principal ideal). *For $\mathfrak{m} = \prod_{v\in T} \mathfrak{p}_v$, consider the S-split ray class field $K' := K_{(\mathfrak{m})^S}$, and denote by T' and S' the sets of places of K' above those of T and S.*
Then for the ideal extension map $j_{K'/K} : I_{K,T} \longrightarrow I_{K',T'}$, we have the inclusion $j_{K'/K}(I_{K,T}) \subset P_{K',T',\mathfrak{m}',\mathrm{pos}}\langle S'\rangle$ where $\mathfrak{m}' = \prod_{v'\in T'} \mathfrak{p}_{v'}$. In other words, the natural map $j_{K'/K} : \mathcal{C}\ell^S_{K,\mathfrak{m}} \longrightarrow \mathcal{C}\ell^{S'}_{K',\mathfrak{m}'}$ is zero. □

When $T = \emptyset$ and $S = Pl^{\mathrm{r}}_\infty$ (for instance), the field K' is the ordinary Hilbert class field H^{ord}_K, and we obtain the famous result (which was conjectured by Hilbert from the very beginning of the theory), called the principal ideal theorem, which states that the extension to H^{ord}_K of an ideal of K is principal.

This theorem does not say precisely how this principalization takes place; historically (see for instance Olga Taussky's account in [i, Tau]), the Hilbert Theorem 94 asserted that in any unramified cyclic extension M of K, the capitulation kernel (i.e., the kernel of the transfer map for M/K or that of extension of classes from K to M) is of order a multiple of $[M : K]$. Many partial results were then given (for instance those of Tannaka–Terada, Furuya, Thiébaud), and we refer to [Miy3] and [i, Miy0, Suzuki] for a detailed account of the main results on these problems, which seem to have reached their optimal formulation with the results of [GW] which we simply state in a less general situation.

5.8.4 Definition (Gruenberg–Weiss). Let G be a finite abelian group. We say that a finite abelian group X is a transfer kernel for G if there exists an exact sequence of the form $1 \to A \longrightarrow H \longrightarrow G \to 1$, with A a finite abelian group, such that:

$$X \simeq \mathrm{Ker}\,(\mathrm{Ver} : H/[H,H] \longrightarrow A),$$

where as usual Ver denotes the transfer map (see 1.4.1). □

5.8.5 Theorem (Gruenberg–Weiss [GW] (2000)). *Let X be a finite abelian group of exponent dividing $|G|$.*
Then X is a transfer kernel for G if and only if $|G|$ divides $|X|$. □

We apply this to the following data: L/K is a subextension of H^{ord}_K/K, $H = \mathrm{Gal}(H^{\mathrm{ord}}_L/K)$, $A = \mathrm{Gal}(H^{\mathrm{ord}}_L/L)$, $G = \mathrm{Gal}(L/K)$, so the exact sequence:

$$1 \longrightarrow X \longrightarrow \mathcal{C}\ell_K^{\mathrm{ord}} \simeq H/[H,H] \xrightarrow{\mathrm{Ver}} A \simeq \mathcal{C}\ell_L^{\mathrm{ord}},$$

implies that $|G|$ divides $|X|$ (i.e., in more colorful terms, the capitulation kernel in L/K is of order a multiple of $|G| = [L : K]$). The condition that the exponent of X is a divisor of $|G|$ is here trivially satisfied since $\mathrm{N}_{L/K} \circ j_{L/K} = [L : K]$ in $\mathcal{C}\ell_K^{\mathrm{ord}}$. For $L = H_K^{\mathrm{ord}}$ we find again the principal ideal theorem.

More generally:

5.8.6 Corollary. *Let L/K be an abelian T-tamely ramified S-split extension. Then for $\mathfrak{m} = \prod_{v \in T} \mathfrak{p}_v$ and $\mathfrak{m}' = \prod_{v' \in T'} \mathfrak{p}_{v'}$ in L, the capitulation kernel:*

$$\mathrm{Ker}\Big(\mathcal{C}\ell_{K,\mathfrak{m}}^{S} \longrightarrow \mathcal{C}\ell_{L,\mathfrak{m}'}^{S'}\Big)$$

has order a multiple of $[L : K]$.

Proof. Replace H_K^{ord} and H_L^{ord} by $K_{(\mathfrak{m})}{}^{S}$ and $L_{(\mathfrak{m}')}{}^{S'}$ respectively. □

5.9 Hilbert Towers. Of course the ideals of H_K^{ord} are not necessarily principal and one may ask if, by iteration, the tower of number fields:

$$K^{(0)} := K \subseteq K^{(1)} \subseteq \cdots \subseteq K^{(\infty)} := \bigcup_{i \geq 1} K^{(i)},$$

inductively defined by $K^{(i+1)} := H_{K^{(i)}}^{\mathrm{ord}}$, is finite or not (finiteness being equivalent to the existence of $n_0 \geq 0$ such that the class group of $K^{(n_0)}$ is trivial). The field $K^{(\infty)}$ is called the Hilbert class fields tower (in the ordinary sense). In a similar way, for any prime number p, we define the p-Hilbert class fields tower $K^{(\infty)}{}_{(p)} := \bigcup_{i \geq 1} K^{(i)}{}_{(p)} \subseteq K^{(\infty)}$, with $K^{(i+1)}{}_{(p)} := H_{K^{(i)}{}_{(p)}}^{\mathrm{ord}}(p)$, and ask for the same question. The notation $K^{(\infty)}{}_{(p)}$ is legitimate since the maximal pro-p-subextension of $K^{(\infty)}$ is solvable and thus coincide with the p-tower and even with the maximal unramified (noncomplexified) pro-p-extension M of K (hint: let $M_0 := K \subseteq M_1 \subseteq \cdots \subseteq \bigcup_{i \geq 1} M_i = M$ with M_{i+1}/M_i abelian; for the inclusion $M \subseteq K^{(\infty)}{}_{(p)}$, prove by induction that $M_i \subseteq K^{(i)}{}_{(p)}$).

This second problem, which is just as famous, was solved in the negative in 1964, thanks to a group-theoretical result of Šafarevič. [38]

5.9.1 Theorem (Golod–Šafarevič–Gaschütz–Vinberg). *Let G be a pro-p-group of finite rank (i.e., with a finite number of generators); let $d(G)$ and $r(G)$ be respectively the minimal number of generators and of relations defining the group G.* [39]

If G is a finite group, then we have $r(G) > \frac{1}{4}\,(d(G))^2$.

[38] See in [d, CF, Ch. IX], [g, Se3, Ch. I, Ann. 3; NSW, Ch. III, § 9], the Golod–Šafarevič theorem which was later improved in a number of ways such as the Gaschütz–Vinberg theorem and some results of Koch.

[39] [e, Ko3, Ch. 3, §§ 1.16, 2.7].

It is then sufficient to exhibit an example for which $d(G)$ is sufficiently large compared with $r(G)$, for $G := \mathrm{Gal}(K^{(\infty)_{(p)}}/K)$, which class field theory easily gives (see Exercise 5.9.5).

Note. We will introduce the notation $\overline{H}_{T(p)}^{S}$ for the maximal T-ramified S-split pro-p-extension of K; as in the case $T = \emptyset$, $S = Pl_\infty^r$ (the p-Hilbert class fields tower $K^{(\infty)_{(p)}}$ in the ordinary sense), $\overline{H}_{T(p)}^{S}$ is also the p-tower of the successive maximal T-ramified S-split abelian pro-p-extensions defined in 5.3, and the maximal pro-p-subextension of the corresponding tower $\overline{H}_T^S$ (same proof). The groups $\mathcal{G}_T^S := \mathrm{Gal}(\overline{H}_{T(p)}^{S}/K)$ will be studied in the Appendix. Warning: $\overline{H}_T^S$ may be strictly contained in the maximal T-ramified S-split Galois extension of K (e.g., take $k/\mathbb{Q}$ with Galois group A_5 and let T be the set of ramified primes in $k/\mathbb{Q}$; then $k \cap \overline{H}_T = \mathbb{Q}$ with $\overline{H}_T \neq \mathbb{Q}$).

The above result (existence of infinite class fields towers) thus showed the complexity of the unramified Galois closure of a number field, and showed that the historical utopia of finding a finite extension of K whose principality would reduce computations in K to ordinary element arithmetic was doomed (see in 5.9.3 the proof that the existence of such an extension is equivalent to the finiteness of the class fields tower).

Many infinite Hilbert class fields towers have been constructed (for instance by Matsumura [Mat], Martinet [Mar1], Schmithals [Schm], Schoof [Scho1], Maire [Mai1]). Recently, tamely ramified class fields towers (or p-towers) have also been studied in [Mai1], both for number fields and for function fields, and have renewed the study of the Martinet constants on number field discriminants, for which upper bounds are obtained from infinite towers (see in the introduction of [HM1] a good historical review of the subject). It is in the same paper [HM1] that Hajir–Maire give improvements on these constants, in this wider context, and for which many interesting questions can be asked (see [HM2, HM3], [HM4] for additional results). We will give in 5.9.4, (iii) a detailed example after [HM2] of such a computation, showing also some links with genera theory.

Note (Martinet's constants). Let K be a number field of signature (r_1, r_2). The infinity type of K is the rational number $\frac{r_1}{[K:\mathbb{Q}]}$ and its root discriminant is $\mathrm{rd}_K := (\mathrm{d}_{K/\mathbb{Q}})^{1/[K:\mathbb{Q}]}$, where $\mathrm{d}_{K/\mathbb{Q}}$ is the absolute value of the discriminant of $K/\mathbb{Q}$. For fixed $t \in \mathbb{Q} \cap [0, 1]$ and integers $n \geq 1$ such that number fields of degree n and infinity type t exist (i.e., such that $tn \in \mathbb{N}$ and $tn \equiv n \bmod (2)$), we let (after [Mar1], [HM1, § 1.1]):

$$\alpha_n(t) := \min_K \{\mathrm{rd}_K,\ [K:\mathbb{Q}] = n,\ \tfrac{r_1}{[K:\mathbb{Q}]} = t\},$$
$$\alpha(t) := \liminf_n \alpha_n(t).$$

Let T be a finite set of finite places of K and let $K =: K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty := \bigcup_{i \geq 1} K_i$ be a tower of T-tamely ramified, noncomplexified extensions of K (the non-

complexification insures that the infinity type is constant in the tower). Then, if K_∞/K is infinite, we easily obtain $\alpha(t) \leq \mathrm{rd}_K \,.\, \prod_{v\in T}(\mathrm{N}\mathfrak{p}_v)^{1/[K:\mathbb{Q}]}$.

In the nontame case for p-towers, the moduli $\mathfrak{m}$ (with fixed support T such that $T_p \neq \emptyset$) can take an infinite number of values, and the only canonical tower is then that of the $H_T^{S(p)}$ (see 5.3) which are, in general, infinite extensions of the base field; in addition, we will see in Section 2 of Chapter IV that, in this context, the transfer map is on the contrary injective (under the assumption that $Pl_p \subseteq T$, $S_0 = \emptyset$, for the ordinary sense, and assuming the Leopoldt conjecture for p). It is however possible to ask that ramification is bounded by observing that because of the reciprocity law we have a correspondence between the natural filtration of the local unit groups with that of higher ramification groups (in upper numbering); this is the study which has been started in [HM3]. Hence this is quite a different context (even though the problem of principalization under extensions can be asked in complete generality), and which leads to difficult questions related to the theory of pro-p-groups (for instance the conjecture of Fontaine–Mazur stated in [g, NSW, Ch. X, § 8]) which we will not describe (see [Haj] for an introduction to these problems in the particular case of p-Hilbert towers).

5.9.2 Remarks. (i) The Hilbert class field is a particular solution to the principalization problem of the ideal group of a field K; we will not expand on this, but it is clear that the classes of K can principalize in many other abelian extensions of K, and we now have quite a precise understanding of the ideal extension map for the extension $\overline{K}^{\mathrm{ab}}/K$ (see [Gr9], [Kur], [Bos]). For instance, from the above papers we can state the following results:

(α) Let $K/\mathbb{Q}$ be a real abelian extension of degree prime to $p \neq 2$. For any $\mathbb{Q}_p$-irreducible character χ of $g := \mathrm{Gal}(K/\mathbb{Q})$, let $\mathcal{C}\ell_\chi := (\mathcal{C}\ell_K)_p^{e_\chi}$ where $e_\chi \in \mathbb{Z}_p[g]$ is the corresponding idempotent. Let $\psi|\chi$; ψ is of degree 1, of order m_χ prime to p, and $\mathbb{Z}_p[g]e_\chi \simeq \mathbb{Z}_p[\mu_{m_\chi}] =: R_\chi$; put $\mathcal{C}\ell_\chi \simeq \bigoplus_{i=1}^{r_\chi} R_\chi/p^{n_{\chi,i}}R_\chi$.

Then there exist infinitely many abelian extensions $M/\mathbb{Q}$ such that $\mathrm{Gal}(KM/K) \simeq \bigoplus_\chi \bigoplus_{i=1}^{r_\chi} \mathbb{Z}/p^{n_{\chi,i}}\mathbb{Z}$ and $j_{KM/K}((\mathcal{C}\ell_K)_p) = 1$.

(β) Let k be a non-totally real number field; then for all finite extension K of k there exists an abelian extension M of k such that $j_{KM/K}(\mathcal{C}\ell_K^{\mathrm{ord}}) = 1$.

(γ) For any totally real number field K there exists a real abelian extension M of $\mathbb{Q}$ such that $j_{KM/K}(\mathcal{C}\ell_K^{\mathrm{ord}}) = 1$.

In a forthcoming paper, Bosca proves (β) and (γ) in a unified way: "if K/k is totally split at a (real or complex) infinite place, then the ordinary class group of K principalizes in an abelian compositum of K/k". In [Bos], we also find analogous results for the logarithmic class group defined in (Ch. III, § 7).

In addition, if we do not request any Galois conditions, it is easy to principalize $\mathcal{C}\ell_K^{\rm ord}$ in a brutal way; setting $\mathcal{C}\ell_K^{\rm ord} = \langle\, \mathcal{C}\ell^{\rm ord}(\mathfrak{a}_i)\,\rangle_{1\le i\le r}$, we simply consider:

$$L := K(\,\sqrt[n_1]{\alpha_1}, \dots,\, \sqrt[n_r]{\alpha_r}\,),$$

where $\mathfrak{a}_i^{n_i} = (\alpha_i),\ \alpha_i \in K^\times,\ 1 \le i \le r$, but this is far from class field theory considerations.

(ii) Finally, concerning the construction of unramified extensions (for instance), we have only mentioned the abelian case (Hilbert class fields) or briefly the soluble case (p-Hilbert class fields towers); however, it is important to note that a *principal* number field can have an *infinite* unramified extension (Galois or non-Galois) (see various examples in [Mai3]; we reproduce such an example in Exercise 5.9.7). □

5.9.3 Proposition. *Let K be a number field and let L be an arbitrary finite extension of K such that $\mathcal{C}\ell_L^{\rm ord} = 1$.*
Then L contains the (finite) ordinary Hilbert class fields tower of K.

Proof. Consider the extension $H_K^{\rm ord}L$ of L which is abelian, unramified and noncomplexified (see II.1.2.5), hence equal to L.

By induction, seen as an extension of $K^{(i)}$, L contains $K^{(i+1)}$, hence we have $K^{(\infty)} =: K^{(n_0)} \subseteq L$. □

The extension $L := K^{(n_0)}$ is the minimal solution to the problem "$\mathcal{C}\ell_L^{\rm ord} = 1$".

Note that if there are several floors in the tower, then $K^{(\infty)} = \overline{H}_K^{\rm ord}$ is not contained in $L^{\rm ab}$.

There is an analogous result with sets T and S for the corresponding tower $\overline{H}_{K,T}^{S}$, relative to the existence of L such that $\mathcal{C}\ell_{L,T'}^{S'} = 1$.

5.9.4 Examples (from [Mai1] and [HM2, § 3.2] (1999/2000)). (i) The field $\mathbb{Q}(\sqrt{53\times 131}\,)$ has an infinite restricted Hilbert class fields tower but a finite ordinary Hilbert class fields tower (see Exercise 5.9.6).

(ii) The number field (totally complex of degree 10):

$$\mathbb{Q}(\xi,\, \sqrt{-36\xi^4 + 125\xi^3 - 221\xi^2 + 182\xi - 80}\,),$$

where ξ is a root of the polynomial:

$$X^5 - 2X^4 + 3X^3 - 3X^2 - X + 1,$$

has an infinite 2-class fields tower whose root discriminant is equal to $84.37\cdots$ (see Exercise 5.9.8).

(iii) The number field $\mathbb{Q}(\theta)$ (totally complex of degree 12), where θ is a root of the polynomial:

$$X^{12} + 339X^{10} - 19752X^8 - 2188735X^6 + 284236829X^4$$
$$+4401349506X^2 + 15622982921,$$

has an infinite 2-tower of number fields (tamely ramified at a place dividing 3) with root discriminant bounded by $82.2\cdots$.

I thank F. Hajir and C. Maire for the authorization to reproduce the details for this example and to use their source text (the notations being the same as ours). We will see that cohomological computations of the Appendix and genera theory (Chapter IV) are needed for the proof.

"The number field arithmetic which is at the heart of our construction takes place in degree 6 number fields; computer packages such as PARI and KANT make it easy to carry out these calculations. However, we would like to present the examples in such a way that a reader armed with an ordinary calculator can verify all of our claims. To this end, we provide (at the cost of lengthening the presentation slightly) much supplementary data and a method for verifying each step in the reasoning. We also provide some data (such as class number, generators for the unit group) whose validity need not be verified but which would aid the reader who wishes to check our claims independently.

Let $k = \mathbb{Q}(\xi)$ where ξ is a root of $f = x^6 + x^4 - 4x^3 - 7x^2 - x + 1$. The prime factorization of the discriminant of f is $\mathrm{d}_f = -23\cdot 35509$; thus, $\mathrm{d}_f = \mathrm{d}_k$ is also the discriminant of k, and $Z_k = \mathbb{Z}[\xi]$.

The roots of f are:

$$\xi_1 = -0.76166245384468100791784609\cdots$$
$$\xi_2 = -0.69953796284372129907057255\cdots$$
$$\xi_3 = +0.29522571317729963668939709\cdots$$
$$\xi_4 = +1.83015782341636731046020011\cdots$$
$$\xi_5 = -0.33209155995263232008058928\cdots$$
$$+1.83394227605082629317069415\cdots\sqrt{-1}$$
$$\xi_6 = -0.33209155995263232008058928\cdots$$
$$-1.83394227605082629317069415\cdots\sqrt{-1}.$$

Thus, k has signature $(4,1)$. The restricted class number of k is 1. The unit group of k is generated by $\{\xi,\ 4\xi^5 - 3\xi^4 + 6\xi^3 - 20\xi^2 - 13\xi + 6,\ 6\xi^5 - 4\xi^4 + 9\xi^3 - 30\xi^2 - 21\xi + 8,\ -\xi^5 + \xi^4 - 2\xi^3 + 6\xi^2 + \xi - 1,\ -1\}$.

Generators for some Z_k-ideals of small norm are listed in the table below where $\pi_r = a_5\xi^5 + a_4\xi^4 + a_3\xi^3 + a_2\xi^2 + a_1\xi + a_0$ generates a prime ideal $\pi_r Z_k$ of norm r, and the coefficients of h_{π_r}, the minimal polynomial of π_r, are listed in descending powers.

π_r	$a_5, a_4, a_3, a_2, a_1, a_0$	h_{π_r}
π_3	$-6, 4, -9, 30, 21, -7$	$1, 0, -5, 2, 5, -5, 3$
π_7	$-9, 6, -13, 44, 31, -12$	$1, 1, -29, 98, 624, -449, -7$
π_{13}	$-7, 5, -11, 36, 23, -9$	$1, 3, -4, -24, -23, 7, 13$
π_{19}	$5, -4, 8, -26, -15, 6$	$1, 11, 50, 120, 151, 89, 19$
π'_{19}	$5, -3, 7, -24, -20, 6$	$1, -3, -10, 13, 29, -8, -19$
π_{23}	$-5, 4, -8, 26, 15, -9$	$1, 7, 20, 30, 16, -20, -23$
π'_{23}	$6, -4, 9, -30, -22, 6$	$1, 6, 11, 0, -30, -46, -23$
π_{29}	$11, -8, 17, -56, -35, 16$	$1, -7, 3, 52, -82, 55, -29$
π_{31}	$7, -5, 11, -36, -22, 7$	$1, 9, 22, 13, -15, -38, -31$

The fact that $19Z_k$ has two prime factors of residue degree 1 can be seen, for instance, from the factorization of f over $\mathbb{F}_{19}$: $f(x) \equiv (x+7)(x-2)$ $(x^4 + 14x^3 + 2x^2 + 11x + 4) \bmod 19$. Similarly, f factors over $\mathbb{F}_{23}$ as $f(x) \equiv (x+10)^2(x-5)(x^3 + 8x^2 + 19x + 4) \bmod 23$. To see that the pairs π_{19}, π'_{19} and π_{23}, π'_{23} generate different prime ideals, one can check that the minimal polynomials of π_{19}/π'_{19} and π_{23}/π'_{23} are not integral.

The element $\eta = -671\xi^5 + 467\xi^4 - 994\xi^3 + 3360\xi^2 + 2314\xi - 961$ of Z_k is totally negative. Its minimal polynomial is $g(y) = y^6 + 339y^5 - 19752y^4 - 2188735y^3 + 284236829y^2 + 4401349506y + 15622982921$. The ideal (η) factors into eight prime ideals of Z_k; in fact, one can check that $\eta = \pi_7\pi_{13}\pi_{19}\pi'_{19}\pi_{23}\pi'_{23}\pi_{29}\pi_{31}$. We let $K = k(\sqrt{\eta}\,)$, a totally complex field of degree 12. A defining polynomial for K is $g(y^2)$. We note that η is congruent to a square modulo $4Z_k$; explicitly, $\eta = \beta^2 + 4\gamma$ with $\beta = \xi^5 + \xi^4 + \xi^3 + 1$ and $\gamma = -173\xi^5 + 112\xi^4 - 270\xi^3 + 815\xi^2 + 576\xi - 237$. Thus, the relative discriminant $\mathrm{d}_{K/k}$ is simply (η), and K/k is complexified at the four real infinite places of k, ramified at the eight primes dividing η, and nowhere else. The root discriminant of K is:

$$\begin{aligned}\mathrm{rd}_K &= \mathrm{rd}_k.(\mathrm{N}_{K/k}\mathrm{d}_{K/k})^{1/12} \\ &= (23 \cdot 35509)^{1/6}(7 \cdot 13 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31)^{1/12} = 68.363\cdots\end{aligned}$$

Consider $t := \{\mathfrak{p}\}$ for the prime $\mathfrak{p} = \pi_3 Z_k$ of k above 3; $\mathfrak{p}$ is inert in K/k. We put $T = \{\mathfrak{p}Z_K\}$."

Now we leave the text of [HM2] and give a direct (but similar) reasoning for the infiniteness of the group $\mathcal{G}_{K,T} = \mathcal{G}^{\mathrm{res}}_{K,T} = \mathcal{G}^{\mathrm{ord}}_{K,T} := \mathrm{Gal}(\overline{H}_{K,T(2)}/K)$ whose abelianization is isomorphic to $(\mathcal{C}\ell_{K,T})_2$. Suppose that $\mathcal{G}_{K,T}$ is finite.

Recall that $d := d(\mathcal{G}_{K,T}) = \mathrm{rk}_2(H^1(\mathcal{G}_{K,T}, \mathbb{Z}/2\mathbb{Z})) = \mathrm{rk}_2(\mathcal{C}\ell_{K,T})$, and that $r := r(\mathcal{G}_{K,T}) = \mathrm{rk}_2(H^2(\mathcal{G}_{K,T}, \mathbb{Z}/2\mathbb{Z}))$. Then, from Corollary 3.8.2 of the Appendix with $E^S_{\mathfrak{m}} = E_{K,\mathfrak{p}Z_K}$, we obtain:

$$d < 2 + 2\sqrt{6} < 6.9$$

since $r_1 = 0$, $r_2 = 6$, and $-1 \not\equiv 1 \bmod \mathfrak{p}Z_K$.

Now we apply Corollary IV.4.5.1 to the extension K/k for the sets t and $s = Pl^{\rm r}_{k,\infty}$; since all elements of s are complexified in K, this gives:

$$1 \longrightarrow E^{\rm ord}_{k,\mathfrak{p}}/E^{\rm ord}_{k,\mathfrak{p}} \cap {\rm N}_{K/k}(J_K) \xrightarrow{\nu} \Omega^s_t(K/k) \xrightarrow{\pi} ({\rm Gal}(H_{K/k,t}/K\, H^{\rm ord}_{k,t}))_2 \longrightarrow 1,$$

where:

$$E^{\rm ord}_{k,\mathfrak{p}} := \{\varepsilon \in E^{\rm ord}_k,\ \ \varepsilon \equiv 1 \bmod \mathfrak{p}\},$$

$$\Omega^s_t(K/k) \simeq \Big\{(\sigma_u)_{u\notin t} \in \bigoplus_{u\in s} D_v(K/k) \bigoplus_{u\notin t\cup s} I_u(K/k),\ \prod_{u\notin t}\sigma_u = 1\Big\} \simeq (\mathbb{Z}/2\mathbb{Z})^{11}$$

since, in K, four real infinite places of k are complexified and eight finite places of k are ramified. Since $d = {\rm rk}_2({\rm Gal}(H_{K,T}/K)) \geq {\rm rk}_2({\rm Gal}(H_{K/k,t}/K\, H^{\rm ord}_{k,t}))$, we have:

$$d \geq {\rm rk}_2(\Omega^s_t(K/k)) - {\rm rk}_2(E^{\rm ord}_{k,\mathfrak{p}}) = 11 - 4 = 7$$

because the numerical data above show that ${\rm rk}_2(E^{\rm ord}_{k,\mathfrak{p}}) = 4$, a contradiction.

Therefore, K has an infinite 2-tower of number fields (tamely ramified at a place dividing 3, unramified elsewhere) with a root discriminant bounded by ${\rm rd}_K \times 9^{1/12} = 82.1\cdots$, giving $\alpha(0) < 82.2\cdots$.

Note that the classical reasoning with class groups (i.e., $t = \emptyset$) and corresponding genera theory does not succeed in this case. □

5.9.5 Exercise (Golod–Šafarevič's first example). Show that the 2-class fields tower of $K = \mathbb{Q}(\sqrt{-2\times 3\times 5\times 7\times 11\times 13}\,)$ is infinite (hint: use the Example of Corollary IV.4.5.1 in $K/\mathbb{Q}$, and Corollary 3.8.2 of the Appendix). □

5.9.6 Exercise. Consider the fields $k = \mathbb{Q}(\sqrt{-131}\,)$ whose class number is 5, and put $K = \mathbb{Q}(\sqrt{53\times 131}\,)$. Let $M = H_k(\sqrt{-53}\,)$, where H_k is the Hilbert class field of k. Note that $\mathcal{C}\ell^{\rm res}_K \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and $\mathcal{C}\ell^{\rm ord}_K \simeq \mathbb{Z}/2\mathbb{Z}$.

(i) Check that 53 is totally split in $H_k/\mathbb{Q}$ and that 2 is totally split in H_k/k.

(ii) Deduce that ${\rm rk}_2(\mathcal{C}\ell_M) \geq 9$ (apply IV.4.5.1 in M/H_k).

(iii) Prove that the 2-class fields tower of M is infinite. Therefore, the class fields tower of K, in the restricted sense, is infinite since M/K is unramified (but not necessarily its 2-class fields tower!).

(iv) Using Corollary 3.8.1 of the Appendix, show that the class fields tower of K in the ordinary sense is finite. Therefore, it is $K(\sqrt{53}\,)$.

For generalizations of such examples, see [Mai1]. □

5.9.7 Exercise (after [Mai3] using PARI). Consider the totally real field F associated to the irreducible polynomial:

$$X^7 - 3X^6 - 13X^5 + 28X^4 + 42X^3 - 47X^2 - 31X + 12,$$

whose discriminant is the prime number $\ell = 17380678572159893$ (the Galois group of the Galois closure of $F/\mathbb{Q}$ is S_7).

Let $q = 1051$, $r = 16747$, $K = \mathbb{Q}(\sqrt{\ell\,.\,q\,.\,r}\,)$, and $M = FK$.

(i) Check the decomposition of ℓ, q, r in $F/\mathbb{Q}$ (hint: ℓ splits into five places of residue degree 1 and one place of ramification index 2; q splits into six places; r is totally split).

(ii) Deduce that M has an infinite 2-Hilbert class fields tower $\overline{H}_M^{\mathrm{ord}}{}^{(2)}$ and that M/K is unramified. Therefore, the Galois closure of $\overline{H}_M^{\mathrm{ord}}{}^{(2)}$ over K is an infinite unramified Galois extension of K.

(iii) Prove that the Hilbert tower $\overline{H}_K^{\mathrm{ord}}$ of K is equal to the genus field $\mathbb{Q}(\sqrt{\ell}, \sqrt{q\,.\,r}\,)$ of K (hint: check that the fields $\mathbb{Q}(\sqrt{\ell}\,)$ and $\mathbb{Q}(\sqrt{q\,.\,r}\,)$ are principal and that the class number of K is equal to 2). Note that the genus field of K is thus principal and admits an infinite unramified extension.

For other similar constructions, see [Mai3]. □

5.9.8 Exercise (after [HM2] using PARI). Consider the Example 5.9.4, (ii). Let $k = \mathbb{Q}(\xi)$, $K = k(\sqrt{\eta}\,)$, with $\eta = -36\xi^4 + 125\xi^3 - 221\xi^2 + 182\xi - 80$. Show that the discriminant of k is -31391, that its signature is (3, 1), that η is totally negative and such that $(\eta) = \pi_7\pi_7'\pi_{11}\pi_{11}'\pi_{13}\pi_{19}\pi_{19}'\pi_{23}\pi_{29}$, with the principle of notations of the Example 5.9.4, (iii). Deduce that K/k is ramified at nine finite places and complexified at three real places, so that $d \geq 7$. Conclude that the 2-Hilbert tower of K cannot be finite. □

In the totally complex case, the historical example of Martinet (published in 1978 in [Mar1]) yields a root discriminant less than 92.4 in the following way. Consider $k = \mathbb{Q}(\mu_{11}, \sqrt{2}\,)^{\mathrm{nc}}$, a totally real field of degree 10 in which 23 is totally split, and use $K/k = k(\sqrt{-23}\,)/k$ which is ramified at ten places $v|23$ and complexified at ten real places.

§6 The Hasse Principle — For Norms — For Powers

6.1 An Index Computation. The equality:

$$(J_K : K^{\times}\mathrm{N}_{L/K}(J_L)) = [L^{\mathrm{ab}} : K],$$

which comes from the fundamental properties of the global reciprocity map for a finite extension L/K will allow us to give a nontrivial example of the local-global principle mentioned in the Introduction, the Hasse norm theorem. For this, we will interpret this index as a product of suitable norm indices; this computation, which is useful in practice only when L/K is a *cyclic* extension, involves interesting arithmetic invariants (such as the order of the group of ambiguous classes). For a cohomological approach see [d, Lang1, Ch. IX].

6.1.1 Notations. Let L/K be a cyclic extension with Galois group $G =: \langle\,\sigma\,\rangle$, and write $\mathrm{N}_{L/K} =: \mathrm{N}$. Recall that for $S = \emptyset$, $U^S = U$, $E^S = E$, and $\mathcal{C}\ell^S = \mathcal{C}\ell$ denote respectively the group of unit idèles in the restricted sense

(U^{res}), the group of units in the restricted sense (E^{res}), and the restricted class group $(\mathcal{C}\ell^{\mathrm{res}})$ of K. In the computations below, to simplify notations we omit these superscripts. □

Finally, it will be necessary to check that each of the indices that we will write below is finite (in particular by using the fact that $J_L/L^\times U_L \simeq \mathcal{C}\ell_L$ and $J_K/K^\times U_K \simeq \mathcal{C}\ell_K$ are finite).

Because of the inclusions $K^\times \mathrm{N}(U_L) \subseteq K^\times \mathrm{N}(J_L) \subseteq J_K$, we have the equality:

$$(J_K : K^\times \mathrm{N}(J_L)) = \frac{(J_K : K^\times \mathrm{N}(U_L))}{(K^\times \mathrm{N}(J_L) : K^\times \mathrm{N}(U_L))}$$

(the finiteness of the numerator comes from that of $J_K/K^\times U_K \simeq \mathcal{C}\ell_K$ and from that of $U_K/\mathrm{N}(U_L)$ by local class field theory 1.4.3). We have the exact sequence:

$$1 \longrightarrow K^\times \cap \mathrm{N}(J_L)/K^\times \cap \mathrm{N}(L^\times U_L) \longrightarrow \mathrm{N}(J_L)/\mathrm{N}(L^\times U_L) \longrightarrow K^\times \mathrm{N}(J_L)/K^\times \mathrm{N}(U_L) \longrightarrow 1,$$

since the kernel is equal to:

$$\begin{aligned} K^\times \mathrm{N}(U_L) \cap \mathrm{N}(J_L)/\mathrm{N}(L^\times U_L) &\simeq (K^\times \cap \mathrm{N}(J_L))\mathrm{N}(U_L)/\mathrm{N}(L^\times U_L) \\ &\simeq K^\times \cap \mathrm{N}(J_L)/K^\times \cap \mathrm{N}(L^\times U_L)\ ; \end{aligned}$$

thus, $\mathrm{N}(J_L)/\mathrm{N}(L^\times U_L)$ being finite as a quotient of $\mathcal{C}\ell_L$, we obtain the formula:

$$(J_K : K^\times \mathrm{N}(J_L)) = \frac{(J_K : K^\times \mathrm{N}(U_L))(K^\times \cap \mathrm{N}(J_L) : K^\times \cap \mathrm{N}(L^\times U_L))}{(\mathrm{N}(J_L) : \mathrm{N}(L^\times U_L))}\ ;$$

furthermore, the exact sequence:

$$1 \longrightarrow {}_{\mathrm{N}}J_L\, L^\times U_L \longrightarrow J_L \longrightarrow \mathrm{N}(J_L)/\mathrm{N}(L^\times U_L) \longrightarrow 1,$$

where ${}_{\mathrm{N}}J_L := \{\boldsymbol{x} \in J_L,\ \mathrm{N}\boldsymbol{x} = 1\}$, allows us to interpret the finite index $(\mathrm{N}(J_L) : \mathrm{N}(L^\times U_L))$ in the form:

$$(J_L : {}_{\mathrm{N}}J_L\, L^\times U_L) = \frac{(J_L : J_L^{1-\sigma} L^\times U_L)}{({}_{\mathrm{N}}J_L L^\times U_L : J_L^{1-\sigma} L^\times U_L)}.$$

It is here that class groups enter since, in the exact sequence:

$$1 \longrightarrow J_L^{1-\sigma} L^\times U_L/L^\times U_L \longrightarrow J_L/L^\times U_L \longrightarrow J_L/J_L^{1-\sigma} L^\times U_L \longrightarrow 1,$$

$J_L/L^\times U_L \simeq \mathcal{C}\ell_L$ and $J_L^{1-\sigma} L^\times U_L/L^\times U_L \simeq (\mathcal{C}\ell_L)^{1-\sigma}$; we thus have:

$$1 \longrightarrow (\mathcal{C}\ell_L)^{1-\sigma} \longrightarrow \mathcal{C}\ell_L \longrightarrow J_L/J_L^{1-\sigma} L^\times U_L \longrightarrow 1$$

and thanks to:

$$1 \longrightarrow (\mathcal{C}\ell_L)^G \longrightarrow \mathcal{C}\ell_L \longrightarrow (\mathcal{C}\ell_L)^{1-\sigma} \longrightarrow 1,$$

this allows us to write:

$$(J_L : J_L^{1-\sigma} L^\times U_L) = |(\mathcal{C}\ell_L)^G|,$$

which is equal to the number of invariant classes for the cyclic extension L/K (also called the number of ambiguous classes); the (delicate) computation of $|(\mathcal{C}\ell_L)^G|$ yields the following result.

6.1.2 Lemma. *For any cyclic extension L/K with Galois group G, we have:*

$$|(\mathcal{C}\ell_L)^G| = \frac{|\mathcal{C}\ell_K| \prod\limits_{v \in Pl_0} e_v}{[L:K]\ (E_K : E_K \cap \mathrm{N}L^\times)},$$

where e_v is the ramification index of v in L/K. [40] □

Therefore, we have obtained:

$$(J_K : K^\times \mathrm{N}(J_L)) = \frac{(J_K : K^\times \mathrm{N}(U_L))}{|(\mathcal{C}\ell_L)^G|} \times (K^\times \cap \mathrm{N}(J_L) : K^\times \cap \mathrm{N}(L^\times U_L))({}_{\mathrm{N}}J_L\, L^\times U_L : J_L^{1-\sigma} L^\times U_L)\ ;$$

however, we can write:

$$\begin{aligned}(J_K : K^\times \mathrm{N}(U_L)) &= (J_K : K^\times U_K)(K^\times U_K : K^\times \mathrm{N}(U_L)) \\ &= |\mathcal{C}\ell_K| \frac{(U_K : \mathrm{N}(U_L))}{(E_K : E_K \cap \mathrm{N}(U_L))},\end{aligned}$$

since we have the exact sequence:

$$1 \longrightarrow E_K/E_K \cap \mathrm{N}(U_L) \longrightarrow U_K/\mathrm{N}(U_L) \longrightarrow K^\times U_K/K^\times \mathrm{N}(U_L) \longrightarrow 1.$$

By local class field theory (see 1.4.3, (ii)), the numerator is:

$$(U_K : \mathrm{N}(U_L)) = \prod_{v \in Pl_0} e_v,$$

and the denominator can be written in the form:

$$(E_K : E_K \cap \mathrm{N}(U_L)) = \frac{(E_K : E_K \cap \mathrm{N}L^\times)}{(E_K \cap \mathrm{N}(U_L) : E_K \cap \mathrm{N}L^\times)},$$

the inclusion $E_K \cap \mathrm{N}L^\times \subseteq E_K \cap \mathrm{N}(U_L)$ being an easy consequence of 2.5.4 (we have here $E_K \cap \mathrm{N}(U_L) = E_K \cap \mathrm{N}(J_L)$). Thus, the index $(J_K : K^\times \mathrm{N}(U_L))$ can be written:

[40] Recall that classes and units are taken in the restricted sense; for the ordinary sense, see 6.2.3.

$$(J_K : K^\times \mathrm{N}(U_L)) = \frac{|\mathcal{O}_K| \prod_{v \in Pl_0} e_v}{(E_K : E_K \cap \mathrm{N}L^\times)} (E_K \cap \mathrm{N}(U_L) : E_K \cap \mathrm{N}L^\times)$$
$$= |(\mathcal{O}_L)^G| \ [L : K] \ (E_K \cap \mathrm{N}(U_L) : E_K \cap \mathrm{N}L^\times)$$

using 6.1.2. Coming back to the expression for $(J_K : K^\times \mathrm{N}J_L)$, we obtain:

$$(J_K : K^\times \mathrm{N}J_L) = [L : K] \ (E_K \cap \mathrm{N}U_L : E_K \cap \mathrm{N}L^\times) \times$$
$$(K^\times \cap \mathrm{N}(J_L) : K^\times \cap \mathrm{N}(L^\times U_L))({}_{\mathrm{N}}J_L \, L^\times U_L : J_L^{1-\sigma} L^\times U_L) \ ;$$

this index being equal to $[L : K]$ (by the fundamental equality of global class field theory), we therefore obtain:

(i) $E_K \cap \mathrm{N}(U_L) = E_K \cap \mathrm{N}L^\times$,
(ii) $K^\times \cap \mathrm{N}(J_L) = K^\times \cap \mathrm{N}(L^\times U_L)$,
(iii) ${}_{\mathrm{N}}J_L \, L^\times U_L = J_L^{1-\sigma} L^\times U_L$.

Statement (iii) does not tell us much since ${}_{\mathrm{N}}J_L = J_L^{1-\sigma}$ by the Hilbert Theorem 90 for the idèle group in a cyclic extension; this fact has an analog for an arbitrary Galois extension L/K and can be written $H^1(G, J_L) = 1$ (see 2.4). But one checks that (ii) can be written:

$$K^\times \cap \mathrm{N}(J_L) = K^\times \cap \mathrm{N}(L^\times U_L)$$
$$= \mathrm{N}L^\times \, (E_K \cap \mathrm{N}(U_L))$$
$$= \mathrm{N}L^\times \ (E_K \cap \mathrm{N}L^\times) \ \text{(by (i))}$$
$$= \mathrm{N}L^\times.$$

Thus we have proved the following result.

6.2 Theorem (Hasse's norm theorem (1930)). *Let L/K be a cyclic extension of number fields.*
Then a necessary and sufficient condition for an $x \in K^\times$ to be the norm of an element of $L^\times$ is that x be a local norm everywhere for L/K or, equivalently, $i_v(x) =: \mathrm{N}_{L_v/K_v}(y_v)$, $y_v \in L_v^\times$, for all $v \in Pl$.
The product formula tells us that this is equivalent to $\left(\frac{x \, , \, L/K}{v}\right) = 1$ for all noncomplex places v except an arbitrarily chosen one. □

6.2.1 Remark. Since by 4.4.3 we know how to compute the Hasse symbols $\left(\frac{x \, , \, L/K}{v}\right)$, in the cyclic case it is numerically possible to know whether or not $x \in \mathrm{N}_{L/K}(L^\times)$; for this, we can omit the computation at an arbitrary place v_0. Recall also that it is sufficient to check this for the (finite) places which are ramified in L/K (except one), as soon as we know that $\mathrm{v}(x) \equiv 0 \bmod (f_v)$ for every place v (in particular for $v \in Pl_\infty^{\mathrm{r}}$), where f_v is the residue degree of v for L/K (see 1.4.3).

Note that Hasse's theorem does not give us the solution $y \in L^\times$ such that $\mathrm{N}_{L/K}(y) = x$, but note that if y_0 is one of them, the others will be given by

$y = y_0\, z^{1-\sigma}$, $z \in L^\times$. For an algorithmic point of view, see [Sim] or [j, Coh2, Ch. 7, § 5] where S-unit groups play a fundamental role. □

6.2.2 Exercise. Let L be a totally imaginary number field. It is known (claimed by Hilbert (1902), proved by Siegel (1919)) that -1 is the sum of 1, 2, or 4 squares in L (with evident condition of minimality). Thus, if we suppose that $\sqrt{-1} \notin L$, -1 is the sum of 2 squares if and only if it is a norm in $L(\sqrt{-1}\,)/L$.

Prove that this is the case if and only if for all $w|2$ the local degree $[L_w : \mathbb{Q}_2]$ is even (hint: use the Hasse norm Theorem 6.2 in $L(\sqrt{-1}\,)/L$, and show that -1 is a local norm at the odd places of L; for $w|2$, use the norm residue symbols $(-1, L_w(\sqrt{-1}\,)/L_w)$, then the local norm lifting Theorem 1.5.4 for $K_v = \mathbb{Q}_2$, $M = \mathbb{Q}_2(\sqrt{-1}\,)$, and finally 1.6.5).

We can omit a place $w_0|2$ and deduce that the corresponding local degree is even ! This is not surprising since here the product formula looks like:

$$\sum_{w|2} [L_w : \mathbb{Q}_2] = [L : \mathbb{Q}] = 2r_2(L) \equiv 0 \bmod (2).$$

For instance, there is nothing to do for the field L generated by a root of $X^4 + 2X + 2$. □

6.2.3 Remark (Chevalley's ambiguous class formula (1933)). Classically, the above index computations are done in the ordinary sense (U^{ord}, E^{ord}, and $\mathcal{C}\ell^{\mathrm{ord}}$), which lead to a formula involving $|(\mathcal{C}\ell_L^{\mathrm{ord}})^G|$, which itself involves the "ramification" of real infinite places, and which for us can be written (still for a cyclic extension L/K):

$$|(\mathcal{C}\ell_L^{\mathrm{ord}})^G| = \frac{|\mathcal{C}\ell_K^{\mathrm{ord}}| \prod\limits_{v \in Pl_0} e_v \prod\limits_{v \in Pl_\infty^{\mathrm{r}}} f_v}{[L : K]\ (E_K^{\mathrm{ord}} : E_K^{\mathrm{ord}} \cap \mathrm{N}_{L/K}(L^\times))}.$$

This formula occurs for the first time in complete generality in [h, Che1] and relies on work of Herbrand on the unit group, more precisely on the computation of the Herbrand quotient of E_L (see for instance [d, Lang1, Ch. IX, § 1]), which is given by the formula:

$$\frac{(E_K : \mathrm{N}_{L/K}(E_L))}{({}_{\mathrm{N}}E_L : E_L^{1-\sigma})} = \frac{2^{r_1^{\mathrm{c}}}}{[L : K]},$$

where r_1^{c} is the number of real places of K complexified in L, and which is the key of Chevalley's formula.

It has been extended to the case of S-decomposition in [Ja2]. □

We also give without proof a more general formula which allows to perform computations of invariant classes in cyclic extensions (see [Gr8]).

6.2.4 Proposition (invariant class formula with unramified modulus). *Let L/K be a cyclic extension of number fields with Galois group G, and let $\mathfrak{m} = \prod_{v\in T} \mathfrak{p}_v^{m_v}$, $m_v \geq 0$, T disjoint from the set of places which are ramified in L/K. Let $\mathfrak{m}'$ be the extension of $\mathfrak{m}$ to L. Let $\mathcal{C}' := I' P_{L,T,\mathfrak{m}',\mathrm{pos}}/P_{L,T,\mathfrak{m}',\mathrm{pos}} \subseteq \mathcal{C}\ell^{\mathrm{res}}_{L,\mathfrak{m}'}$, where I' is an arbitrary sub-G-module of $I_{L,T}$. We then have:*

$$|(\mathcal{C}\ell^{\mathrm{res}}_{L,\mathfrak{m}'}/\mathcal{C}')^G| = \frac{|\mathcal{C}\ell^{\mathrm{res}}_{\mathfrak{m}}| \prod_{v\in Pl_0} e_v}{[L:K]\ |\mathrm{N}_{L/K}(\mathcal{C}')|\ (\Lambda : \Lambda \cap \mathrm{N}_{L/K}(L^\times))},$$

where $\Lambda := \{x \in K^\times_{T,\mathfrak{m},\mathrm{pos}},\ (x) \in \mathrm{N}_{L/K}(I')\}$. □

6.2.5 Remarks. (i) Recall that the action of $\mathrm{N}_{L/K}$ on $\mathcal{C}\ell^{\mathrm{res}}_{L,\mathfrak{m}'}$ is given in 5.7, and implies that $\mathrm{N}_{L/K}(\mathcal{C}')$ makes sense.

(ii) By the Hasse norm Theorem 6.2, the term $(\Lambda : \Lambda \cap \mathrm{N}_{L/K}(L^\times))$ is of a *local nature*; it can be written $(\Lambda : \Lambda \cap \mathrm{N}_{L/K}(J_L))$ and depends only on the norm residue symbols at the ramified places since the condition $(x) \in \mathrm{N}_{L/K}(I')$ defining Λ implies that these norm conditions are already satisfied at the unramified places (by 1.4.3).

This remark is of course valid for $E_K \cap \mathrm{N}_{L/K}(L^\times) = E_K \cap \mathrm{N}_{L/K}(J_L)$ in the various ambiguous class formulas.

(iii) We obtain an expression for $|(\mathcal{C}\ell^{S'}_{L,\mathfrak{m}'})^G|$, where $S' \subset Pl_L$ is stable under G, by choosing for $\mathcal{C}'$ the G-module $\langle\, \mathcal{C}\ell^{\mathrm{res}}_{L,\mathfrak{m}'}(S') \,\rangle$ (in the sense explained in I.4.4.1, (ii)). □

The Hasse principle is a key tool in the proof of the Hasse–Minkowski theorem on quadratic forms over number fields (see also the direct proofs of [a, BŠa; D; Se1]). The three-variable case is the object of Exercise 6.4 which can also be found in [d, CF, Exer. 4] and which is given in all the books dealing with the Hasse principle. The four-variable case is solved in 7.3.2.

When L/K is not cyclic, the Hasse principle is in general not true and its defect group, which is essentially given in cohomological terms, is in fact an algebraic invariant, related to the family of decomposition groups of ramified places. To be complete on this, we simply give the following results of Scholz-Tate involving Schur multipliers. [41]

Let L/K be Galois with Galois group G; for any noncomplex place v of K we denote by w a place of L above v, fixed arbitrarily, and we denote by D_w the decomposition group of w in L/K.

6.2.6 Proposition. *We have a canonical isomorphism (where $H^{-3} := H_2$):*

$$K^\times \cap \mathrm{N}_{L/K}(J_L)/\mathrm{N}_{L/K}(L^\times) \simeq H^{-3}(G,\mathbb{Z}) \Big/ \mathrm{Inf}\left(\bigoplus_v H^{-3}(D_w,\mathbb{Z})\right),$$

[41] See [d, CF, Ch. VII, § 11.4], [Scholz1], [Jeh], as well as the work of Razar [Ra] which is the culmination of several approaches (Garbanati, Gerth, Gurak, ...).

where, for $(\alpha_w)_v \in \bigoplus_v H^{-3}(D_w, \mathbb{Z})$, *we put* $\mathrm{Inf}((\alpha_w)_v) := \prod_v \mathrm{Inf}_w(\alpha_w)$, Inf_w *denoting the inflation map* $H^{-3}(D_w, \mathbb{Z}) \longrightarrow H^{-3}(G, \mathbb{Z})$. □

6.2.7 Remarks. (i) Since the group G is finite, by duality (see 2.4.1, (ii)), we can express that the dual of $K^\times \cap \mathrm{N}_{L/K}(J_L)/\mathrm{N}_{L/K}(L^\times)$ is isomorphic to:

$$\mathrm{Ker}\Big(\mathrm{Res} : H^2(G, \mathbb{Q}/\mathbb{Z}) \longrightarrow \bigoplus_v H^2(D_w, \mathbb{Q}/\mathbb{Z})\Big),$$

where $\mathrm{Res} := (\mathrm{Res}_w)_v$ is the family of restriction maps. Since $\mathbb{Q}$ is uniquely divisible, its cohomology is trivial and we may replace the $H^2(\bullet, \mathbb{Q}/\mathbb{Z})$ by the $H^3(\bullet, \mathbb{Z})$. When v is unramified in L/K, D_w is cyclic (generated by the Frobenius of w), and $H^3(D_w, \mathbb{Z}) = H^1(D_w, \mathbb{Z}) = 1$, so that only the finite ramified places enter in the definition of Inf and of Res.

(ii) Finally, when L/K is abelian, Razar has shown in [Ra] that we may replace $H^{-3}(G, \mathbb{Z})$ and $H^{-3}(D_w, \mathbb{Z})$ by $\bigwedge^2 G$ and $\bigwedge^2 D_w$, respectively, which in this case enables us to perform explicit computations and to immediately construct counterexamples to the Hasse principle (the simplest being $\mathbb{Q}(\sqrt{13}, \sqrt{17})/\mathbb{Q}$ of Scholz, for which -1 is a local norm everywhere without being a global norm; see [Scholz1] or [d, CF, Ch. VII, § 11.4]).

(iii) For example, if L/K is abelian and if there exists a place v of K such that $D_w = G$, then the Hasse principle for the norm is true in L/K.

In the case where $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, the Hasse principle for the norm holds in L/K if and only if there exists v such that $D_w = G$. □

We will again meet the default group $K^\times \cap \mathrm{N}_{L/K}(J_L)/\mathrm{N}_{L/K}(L^\times)$ in the section dealing with central class fields (Ch. IV, § 4, (c), and Exercise IV.4.10). This group is also called the knot group of the extension L/K, notion which was introduced and studied by Scholz, then by Jehne.

6.3 Local-Global Principle for Powers. Starting with Chapter III, we will come back to the fine study of the elementary parts of class field theory so as to obtain the structure of $\mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K)$, and deduce a number of little-known consequences. Meanwhile, in the following Theorem 6.3.3 the reader will find the solution of an important local-global problem (the local-global principle for powers) which only relies on the surjectivity of the Artin map and on simple Kummer theory arguments which can found for the first time in [SchFK] and in [Che5, I], and which should not be considered as a result of class field theory, although it is an essential tool for it.[42] This result will be crucial to explain in detail certain elements of the structure of $\mathrm{Gal}(\overline{K}^{\mathrm{ab}}/K)$ (for instance by means of the Schmidt–Chevalley Theorem III.4.3 and the Grunwald–Wang Theorem III.4.16.4); note that it is the starting point for the p-adic class field theory of Jaulent and for the study of the connected component of the unit element of C done by Artin–Tate and Weil. Finally,

[42] See [d, AT, Ch. X, § 1]; see also [e, Ko3, Ch. 2, § 1.12, Th. 2.21].

we mention that it exhibits the famous special case (which is an obstruction at 2 of the corresponding Hasse principle), which shows once more to those who are not yet convinced, that 2 is the most "interesting" prime number.

6.3.1 Notations. Let K be a number field [43], and let p^e for some $e \geq 1$ be a fixed power of a prime number p. We set (in a suitable algebraic closure):

$$\mu_{p^e} =: \langle\, \zeta_e \,\rangle \quad \text{and} \quad \mu_{p^k} =: \langle\, \zeta_k \,\rangle, \quad \text{where} \quad \zeta_k := \zeta_e^{p^{e-k}},$$

for $0 \leq k \leq e$. Denote by K' the field $K(\mu_{p^e})$, and set $G' := \mathrm{Gal}(K'/K)$ which is isomorphic to a subgroup of $(\mathbb{Z}/p^e\mathbb{Z})^\times$. □

6.3.2 Theorem. *Let $x \in K^\times$ be such that $x =: x'^{p^e}$, $x' \in K'^\times$.*
Then $x = y^{p^e}$ for an $y \in K^\times$, except in the following exceptional case:

- $p = 2, \quad e \geq 2,$
- $K \cap \mathbb{Q}(\mu_{2^e}) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, *for* $2 \leq n \leq e$,
- $x = (-1)^{2^{e-n}} x_0 \,.\, y^{2^e}$, *with* $x_0 := (2 + \zeta_n + \zeta_n^{-1})^{2^{e-1}}$ *and* $y \in K^\times$.

In this case, $(-1)^{2^{e-n}} x_0 = (1 + \zeta_n)^{2^e}$. □

6.3.3 Theorem (local-global principle for powers). *Let Σ be a finite set of places of K. Let $x \in K^\times$ be such that $i_v(x) \in K_v^{\times p^e}$ for all places $v \notin \Sigma$. Then $x = y^{p^e}$ for an $y \in K^\times$, except in the following Σ-special case:*

- $p = 2, \quad e \geq 3,$
- $K \cap \mathbb{Q}(\mu_{2^e}) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, *for* $2 \leq n < e$,
- *for all places* $v \in Pl_2 \backslash (\Sigma \cap Pl_2)$, K_v *contains one of the numbers:*

$$1 + \zeta_n, \quad \zeta_{n+1} + \zeta_{n+1}^{-1}, \quad \sqrt{-1}\,(\zeta_{n+1} + \zeta_{n+1}^{-1}),$$

- $x = x_0 \,.\, y^{2^e}$, *with* $x_0 := (2 + \zeta_n + \zeta_n^{-1})^{2^{e-1}}$ *and* $y \in K^\times$. □

We give detailed proofs by the way of the following exercise in which the reader will find many other properties and examples, as well as the study of an idèle $\boldsymbol{s}$ such that $i(x_0) = \boldsymbol{s}^{2^e}$ in the special case (i.e., the Σ-special case above for $\Sigma = \emptyset$). The notations are those of 6.3.1.

6.3.4 Exercise. Let $x \in K^\times$ be such that $x =: x'^{p^e}$, for an $x' \in K'^\times$.

(α) (case $p \neq 2$). In this case, $G' =: \langle\, \sigma \,\rangle$ is cyclic.

(i) Show that $H^1(G', \mu_{p^e}) = 1$ (since μ_{p^e} is finite, its Herbrand quotient [44] is trivial and we have $|H^1(G', \mu_{p^e})| = |\mu_{p^e}^{G'} / \mathrm{N}_{K'/K}(\mu_{p^e})|$; thus, one can show the equality $\mu_{p^e}^{G'} = \mathrm{N}_{K'/K}(\mu_{p^e})$, but one can also show by a direct computation that ${}_{\mathrm{N}}\mu_{p^e} = \mu_{p^e}^{1-\sigma}$, where ${}_{\mathrm{N}}\mu_{p^e}$ is the kernel of $\mathrm{N}_{K'/K}$ in μ_{p^e}).

[43] Result 6.3.2 is valid for any field of characteristic equal to 0; in particular it will be used for the completions of the field K.

[44] [d, Lang1, Ch. IX, § 1], [d, Se2, Ch. VIII, § 4].

(ii) From the equality $x = x'^{p^e}$ and the above results, deduce that $x = y^{p^e}$ for $y \in K^\times$.

(β) (case $p = 2$, $e \geq 2$). In this case, G' is isomorphic to a subgroup of $\langle -\overline{1} \rangle \oplus \langle \overline{5} \rangle$ in $(\mathbb{Z}/2^e\mathbb{Z})^\times$. Set $Q := K \cap \mathbb{Q}(\mu_{2^e})$.

(i) Show that $x \in K^{\times 2^e}$ is still true if K contains $\mathbb{Q}(\mu_4)$ or if for some $n \geq 3$, Q is equal to the subfield Q'_{n-2} of $\mathbb{Q}(\mu_{2^n})$, of relative degree equal to 2, different from $Q_{n-2} := \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ (see Fig. 6.1) (thus there will only remain the case where $Q = Q_{n-2}$ for some $n \geq 2$).

(ii) Show that in all other cases, we have $x \in \langle -1 \rangle K^{\times 2^{e-1}}$.

From now on, we assume that $Q = Q_{n-2}$ for $e \geq n \geq 2$; in particular $K_1 := K(\sqrt{-1})$ is a quadratic extension of K containing μ_{2^n} and not $\mu_{2^{n+1}}$.

(iii) Show that, if the set of counterexamples (to $x \in K^{\times 2^e}$) is not empty, it is of the form $x_0 K^{\times 2^e}$ for an arbitrary solution x_0 (by abuse of language we will say that the counterexample is unique).

(iv) Show that, for all $n \geq 2$:

$$x_n := (1 + \zeta_n)^{2^n} \in Q_{n-2}^\times \cap (\mathbb{Q}(\mu_{2^n}))^{\times 2^n}, \text{ where } Q_{n-2} := \mathbb{Q}(\zeta_n + \zeta_n^{-1}),$$

and that it is also an element of $-Q_{n-2}^{\times 2^{n-1}}$.

(v) Conclude by giving a characterization of the cases where K contains a counterexample, and give its value. This will prove Theorem 6.3.2.

(γ) (Hasse principle for powers). In this question, p is once again an arbitrary prime number and e an integer which is ≥ 1. Let Σ be a finite set of noncomplex places of K, and let $x \in K^\times$ be such that $i_v(x) \in K_v^{\times p^e}$ for all places v not belonging to Σ. Consider the Kummer extension $K'(\sqrt[p^e]{x})/K'$.

(i) Check that there exists a place v'_0 of K', unramified in $K'(\sqrt[p^e]{x})/K'$, which is not above a place of Σ, whose Frobenius in $K'(\sqrt[p^e]{x})/K'$ is a generator (density Theorem 4.6).

(ii) Deduce that $x \in K'^{\times p^e}$, and then that $x \in K^{\times p^e}$, except perhaps in the case $p = 2$, for a particular case which one asks to characterize: it is the Σ-special case, where nonetheless we have $x \in K^{\times 2^{e-1}}$.

(iii) Let ${}_{p^e}J$ (resp. ${}_{p^e}C$) be the set of idèles (resp. of idèle classes) of order a divisor of p^e, and let $\mathscr{A}$ be the canonical map $J \longrightarrow C$. Deduce from the above that ${}_{p^e}C = \mathscr{A}({}_{p^e}J)$ except in the Σ-special case for $\Sigma = \emptyset$ (then simply called the special case), in which case ${}_{2^e}C = \langle \mathscr{A}(\boldsymbol{s}) \rangle . \mathscr{A}({}_{2^e}J)$, with $\mathscr{A}(\boldsymbol{s}^2) \in \mathscr{A}({}_{2^{e-1}}J)$, $\mathscr{A}(\boldsymbol{s}) \notin \mathscr{A}({}_{2^e}J)$ for a suitable idèle $\boldsymbol{s}$ (see the data in the proof of (ii) above). In other words, ${}_{2^e}C/\mathscr{A}({}_{2^e}J)$ has order 2 in the special case.

Answer. For statements (α) and (β), we may assume that $\mu_{p^e} \not\subset K$; note also that $\mu_{p^e}^{G'} = \mu_p(K)$ is of the form μ_{p^k} for $0 \leq k < e$, with $k \geq 1$ for $p = 2$.

(α) (i) If $k = 0$, the result is trivial. If $k \geq 1$, $K \cap \mathbb{Q}(\mu_{p^e}) = \mathbb{Q}(\mu_{p^k})$ (indeed, between $\mathbb{Q}(\mu_{p^k})$ and $\mathbb{Q}(\mu_{p^e})$ there exist only the fields $\mathbb{Q}(\mu_{p^{k+i}})$ for $0 \leq i \leq e - k$ since $k \geq 1$), G' has order p^{e-k}, and we have:

$$\mathrm{Irr}(\zeta_e, K) = X^{p^{e-k}} - \zeta_k,$$

hence $\mu_{p^k} \subseteq \mathrm{N}_{K'/K}(\mu_{p^e})$.

(ii) If $x = x'^{p^e}$, we have $1 = (x'^{1-\sigma})^{p^e}$, hence $x'^{1-\sigma} =: \zeta' \in {}_{\mathrm{N}}\mu_{p^e}$; since $H^1(G', \mu_{p^e}) = 1$ (i.e., ${}_{\mathrm{N}}\mu_{p^e} = \mu_{p^e}^{1-\sigma}$), there exists $\xi \in \mu_{p^e}$ such that $\zeta' = \xi^{1-\sigma}$, and there exists $y \in K^\times$ such that $x' = \xi y$. We thus have $x = y^{p^e}$.

We can also say that the exact sequence:

$$1 \longrightarrow \mu_{p^e} \longrightarrow K'^\times \xrightarrow{p^e} K'^{\times p^e} \longrightarrow 1,$$

yields, since $H^1(G', \mu_{p^e}) = 1$, the surjective map:

$$K'^{\times G} = K^\times \xrightarrow{p^e} K'^{\times p^e G} = K^\times \cap K'^{\times p^e},$$

so that $K^{\times p^e} = K^\times \cap K'^{\times p^e}$.

(β) (i) If K contains $\mathbb{Q}(\mu_4)$, we have $Q = \mathbb{Q}(\mu_{2^k})$ for $k \geq 2$, G' is cyclic of order 2^{e-k}, and we still have $\mathrm{Irr}(\zeta_e, K) = X^{2^{e-k}} - \zeta_k$ and the same result (here we find that $-\zeta_k \in \mathrm{N}_{K'/K}(\mu_{2^e})$, but $\zeta_k = (-\zeta_k)^{1+2^{k-1}}$).

The following field diagram gives the structure of $\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}$:

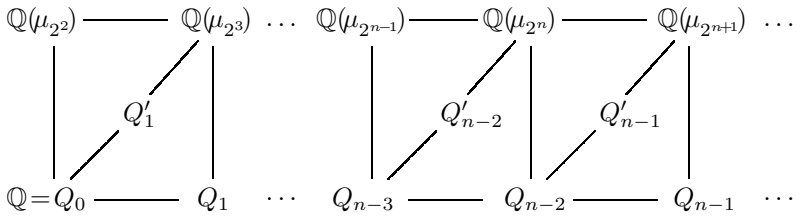


Fig. 6.1

If for some $n \geq 3$, $Q = Q'_{n-2}$ (which is the subfield of $\mathbb{Q}(\mu_{2^e})$ fixed under $\langle -\overline{5}^{2^{n-3}} \rangle$), then necessarily $n \leq e$, the group G' is cyclic of order 2^{e-n+1} and we have:

$$\mathrm{Irr}(\zeta_e, K) = X^{2^{e-n+1}} - \omega X^{2^{e-n}} - 1,$$

where $\omega := \zeta_n - \zeta_n^{-1}$, so that $\mathrm{N}_{K'/K}(\mu_{2^e}) = \langle -1 \rangle = \mu_2(K)$. In this case, we still have $x = y^{2^e}$.

(ii) If we consider the equality $x = x'^{2^e}$ in $K_1 := K(\sqrt{-1}) \subseteq K'$, fact (i) shows that there exists $y_1 \in K_1^\times$ such that $x = y_1^{2^e}$; hence, $x^2 = \mathrm{N}_{K_1/K}(x) = (\mathrm{N}_{K_1/K}(y_1))^{2^e}$, proving the existence of $y := \mathrm{N}_{K_1/K}(y_1) \in K^\times$ such that $x = \pm y^{2^{e-1}}$.

(iii) Let τ be the generator of $\mathrm{Gal}(K_1/K)$. From the following exact sequence of $\langle \tau \rangle$-modules:

$$1 \longrightarrow \mu_{2^n} \longrightarrow K_1^\times \xrightarrow{2^e} K_1^{\times 2^e} \longrightarrow 1,$$

by taking invariants under $\langle\, \tau \,\rangle$, we obtain:

$$1 \longrightarrow \mu_2 \longrightarrow K^\times \xrightarrow{2^e} K^\times \cap K_1^{\times 2^e} \longrightarrow H^1(\langle\, \tau \,\rangle, \mu_{2^n}) \longrightarrow 1$$

since $H^1(\langle\, \tau \,\rangle, K_1^\times) = 1$ (Theorem 90). Thus, the Herbrand quotient of μ_{2^n} being trivial:

$$K^\times \cap K_1^{\times 2^e}/K^{\times 2^e} \simeq {}_{\mathrm{N}}\mu_{2^n}/\mu_{2^n}^{1-\tau} \simeq \mu_2/\mathrm{N}_{K_1/K}(\mu_{2^n}),$$

and so "the" counterexample happens if and only if $\mathrm{N}_{K_1/K}(\zeta_n) = 1$, hence if and only if $\tau(\zeta_n) = \zeta_n^{-1}$, which means that $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq K$, i.e., $Q = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, which is indeed the case.

(iv) If $n \geq 2$, we have $x_n := (1+\zeta_n)^{2^n} \in Q_{n-2}^\times$ since $(1+\zeta_n^{-1})^{2^n} = (\zeta_n^{-1}(\zeta_n+1))^{2^n} = (1+\zeta_n)^{2^n}$; furthermore, we have:

$$(1+\zeta_n)^2 = 1 + \zeta_n^2 + 2\zeta_n = \zeta_n(\zeta_n^{-1} + \zeta_n + 2),$$

which shows that:

$$x_n = -y_n^{2^{n-1}}, \text{ with } y_n := 2 + \zeta_n + \zeta_n^{-1} \in Q_{n-2}^\times.$$

Note that x_n is not even a square in $Q_{n-2}^\times$

(v) Assume that K does not contain $\mathbb{Q}(\mu_4)$ and is such that $Q \neq Q'_{n-2}$ for all $n \geq 3$. We thus have:

$$Q = Q_{n-2} \text{ for some } n \geq 2.$$

Recall that $K_1^\times \cap \mu_{2^e} = \mu_{2^n}$ since $K_1 \cap \mathbb{Q}(\mu_{2^e})$ contains $\mathbb{Q}(\mu_4)$ and Q_{n-2}, hence $\mathbb{Q}(\mu_{2^n})$, the only possible quadratic extension of Q_{n-2}.

If $n = e$, by "uniqueness" the counterexample in K is equal to:

$$x := x_e = -y_e^{2^{e-1}} \text{ (equal to } (1+\zeta_e)^{2^e} \text{ in } K')$$

(indeed, if we had $x = y^{2^e}$ with $y \in K^\times$, then -1 would be a square in K, which is not the case).

If $n < e$, we have at our disposal the element $x_n \in Q_{n-2}^\times$ (see (iv)) such that:

$$x_n = -y_n^{2^{n-1}}, \; y_n \in Q_{n-2}^\times,$$

so that we can consider:

$$x := x_n^{2^{e-n}} = y_n^{2^{e-1}} \text{ (equal to } (1+\zeta_n)^{2^e} \text{ in } K') \text{ ;}$$

x is the desired counterexample in K: indeed, if $y_n^{2^{e-1}} = y^{2^e}$, $y \in K^\times$, then $y_n = \xi y^2$, $\xi \in \mu_{2^{e-1}}$; but $\xi \in K^\times$, hence $\xi = \pm 1$ so we easily obtain:

$$y = \pm(\zeta_{n+1} + \zeta_{n+1}^{-1}), \text{ if } \xi = 1,$$
$$y = \pm\sqrt{-1}\,(\zeta_{n+1} + \zeta_{n+1}^{-1}), \text{ if } \xi = -1.$$

But the field $Q_{n-2}(y) \subseteq K$ is respectively equal to Q_{n-1} and to Q'_{n-1}, which means (since here $n < e$) that $K \cap \mathbb{Q}(\mu_{2^e})$ is not equal to Q_{n-2}, a contradiction.

To summarize, the counterexample of Theorem 6.3.2 takes place if and only if:

$$K \cap \mathbb{Q}(\mu_{2^e}) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}), \quad 2 \leq n \leq e,$$

and it is given by:

$$x := (-1)^{2^{e-n}}\,(2 + \zeta_n + \zeta_n^{-1})^{2^{e-1}}$$

(equal to $(1 + \zeta_n)^{2^e}$ in K').

6.3.4.1 Examples. (i) If K does not contain $\mathbb{Q}(\mu_4)$ and if we take $e = 2$, we always obtain $Q = \mathbb{Q} = Q_0$ (i.e., $n = e = 2$), and:

$$x = x_2 = -4 = (1 + \sqrt{-1}\,)^4,$$

which is a 4th power in $K(\sqrt{-1}\,)$ but is not a square in K.

(ii) For $e = 3$, if K contains $Q_1 = \mathbb{Q}(\sqrt{2}\,)$ but does not contain $\mathbb{Q}(\sqrt{-1}\,)$, we obtain $Q = Q_1$ (i.e., $n = e = 3$), and:

$$x = x_3 = -(2 + \sqrt{2}\,)^4 = (1 + \zeta_3)^8,$$

with $\zeta_3^2 = \sqrt{-1}\,$, $\zeta_3 + \zeta_3^{-1} = \sqrt{2}$.

(iii) Finally note that, when K does not contain $\mathbb{Q}(\sqrt{2}\,)$ and $e = 3$, $Q = Q_0$, hence $n = 2$, we have:

$$x = x_2^2 = 16 = (1 + \sqrt{-1}\,)^8 = (\sqrt{2}\,)^8 = (\sqrt{-2}\,)^8,$$

which is an 8th power in $\mathbb{Q}(\mu_8)$ and only a 4th power in K. □

Note. The case $n = e \geq 2$ is the only case where there exists a counterexample with K'/K cyclic (of degree 2); we will see that the special case assumes the noncyclicity, hence $n < e$ with $n \geq 2$.

(γ) (i) Since $K'(\sqrt[p^e]{x}\,)/K'$ is cyclic, there exists an infinite number of such places by the density theorem or simply the surjectivity of the Artin map (but the finiteness assumption on Σ is essential).

(ii) Let v be the place of K below v'_0. The extension $K'(\sqrt[p^e]{x}\,)/K'$ is split at v'_0 (since $i_v(x) \in K_v^{\times p^e}$, a fortiori $i'_{v'_0}(x) \in K'^{\times p^e}_{v'_0}$), hence the Frobenius of v'_0 is equal to 1, and $K'(\sqrt[p^e]{x}\,) = K'$, hence $x \in K'^{\times p^e}$. We thus have $x \in K^{\times p^e}$, except if $p = 2$, $e \geq 2$, $Q = Q_{n-2}$ for some n such that $2 \leq n \leq e$,

and if (up to an element of $K^{\times 2^e}$) $x = (-1)^{2^{e-n}} y_n^{2^{e-1}}$. But since $e \geq 2$, in the case $x = -y_e^{2^{e-1}}$ we would have $-1 \in K_v^{\times 2}$ for all places $v \notin \Sigma$ (since $y_e^{2^{e-1}} \in K^{\times 2}$); this is impossible since $\sqrt{-1} \notin K$ (choose $v_1 \notin \Sigma$ such that the Frobenius of v_1 for $K(\sqrt{-1})/K$ is of order 2, or simply note that this is the reasoning used in (i) above for $e = 1$ with $x = -1$). We are thus in the case where (see (β), (v)):

$$Q = Q_{n-2}, \quad 2 \leq n < e,$$

which corresponds to the counterexample $x = x_n^{2^{e-n}} = y_n^{2^{e-1}}$. It follows that the extension K'/K contains the biquadratic subextension $K\mathbb{Q}(\mu_{2^{n+1}})/K$ since $e \geq n+1$. In K' we have:

$$x = (1+\zeta_n)^{2^e} = (\zeta_{n+1} + \zeta_{n+1}^{-1})^{2^e} = (\sqrt{-1}\,(\zeta_{n+1} + \zeta_{n+1}^{-1}))^{2^e},$$

so that $1+\zeta_n$, $\zeta_{n+1} + \zeta_{n+1}^{-1}$, $\sqrt{-1}\,(\zeta_{n+1} + \zeta_{n+1}^{-1})$ are generators over K of $K\mathbb{Q}(\mu_{2^n})$, KQ_{n-1}, KQ'_{n-1}, respectively.

But if v is any place of K not dividing 2, it is split in at least one of the three extensions $K\mathbb{Q}(\mu_{2^n})$, KQ_{n-1}, and KQ'_{n-1} (since v is unramified in $K\mathbb{Q}(\mu_{2^{n+1}})/K$ and $\mathrm{Gal}(K\mathbb{Q}(\mu_{2^{n+1}})/K) \simeq (\mathbb{Z}/2\mathbb{Z})^2$). It follows that for such places $i_v(x) \in K_v^{\times 2^e}$ (for instance if $v|\infty$, the splitting takes place in KQ_{n-1}/K). It follows that our initial assumption ($i_v(x) \in K_v^{\times p^e}$ for all $v \notin \Sigma$) is satisfied for x, except perhaps for the even places not belonging to Σ.

Finally, if v divides 2, $i_v(x) \in K_v^{\times 2^e}$ if and only if K_v contains one of the three quadratic extensions of Q_{n-2} in $\mathbb{Q}(\mu_{2^{n+1}})$, in other words if v splits at least partially in $K\mathbb{Q}(\mu_{2^{n+1}})/K$ (apply the results of (α) and (β) to K_v by discussing over $K_v \cap \mathbb{Q}(\mu_{2^e})$).

This defines the Σ-special case of Theorem 6.3.3, which is especially tricky:

- $p = 2, \quad e \geq 3,$
- $K \cap \mathbb{Q}(\mu_{2^e}) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, for some n such that $2 \leq n < e$,
- for all places $v \in Pl_2 \setminus \Sigma_2$, K_v contains one of the numbers:[45]

$$1+\zeta_n, \quad \zeta_{n+1} + \zeta_{n+1}^{-1}, \quad \sqrt{-1}\,(\zeta_{n+1} + \zeta_{n+1}^{-1}),$$

the defect to the Hasse principle relative to Σ being due to:

$$x \in x_0 K^{\times 2^e}, \quad \text{with} \quad x_0 = (2 + \zeta_n + \zeta_n^{-1})^{2^{e-1}},$$

where $\zeta_n = \zeta_{n+1}^2$ is a generator of μ_{2^n}.

The minimal example is for $K = \mathbb{Q}$, $e = 3$, $n = 2$, $\Sigma = Pl_2$, which is the example $x = 16$ given in 6.3.4.1, (iii).

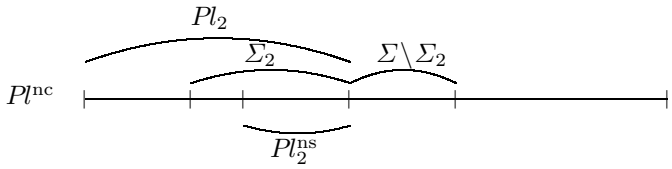
[45] where the first one may be replaced by $\sqrt{-1}$ since $Q_{n-2}(\sqrt{-1}) = \mathbb{Q}(\mu_{2^n})$.

6.3.4.2 Notation. We introduce the set $Pl_2^{\rm ns}$ of the ("nonsplit") places $v|2$ such that $\mathrm{Gal}(K_v(\mu_{2^{n+1}})/K_v)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (or, equivalently, $K_v \cap \mathbb{Q}(\mu_{2^e}) = Q_{n-2}$). □

We can say that the third condition of the Σ-special case is equivalent to the condition:

- $Pl_2^{\rm ns} \subseteq \Sigma_2$,

according to the following diagram:



This diagram means that we have (unfortunately, when $Pl_2^{\rm ns} \neq \emptyset$) discarded the places $v|2$ which would have told us (for a local reason) that x is not a 2^eth power. In other words, to choose $\Sigma_2 \supseteq Pl_2^{\rm ns}$ when $Pl_2^{\rm ns} \neq \emptyset$ is in practice artificial, and the true special case corresponds to the fields K for which:

$$K \cap \mathbb{Q}(\mu_{2^e}) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}), \quad \text{for some } n \text{ such that } 2 \leq n < e,$$

and whose places $v|2$ are all partially split in $K\mathbb{Q}(\mu_{2^{n+1}})/K$ (i.e., $Pl_2^{\rm ns} = \emptyset$).

6.3.4.3 Remark (special case: the idèle $\boldsymbol{s}$). The Hasse principle for powers consists precisely in choosing $\Sigma = \emptyset$, in which case the last condition (corresponding to the existence of the special case, hence to the fact that the principle is false) can be written:

- $Pl_2^{\rm ns} = \emptyset$.

In this case $i(2+\zeta_n+\zeta_n^{-1})^{2^n}$ is of the form $\boldsymbol{s}^{2^{n+1}}$, where $\boldsymbol{s}$ is an idèle whose components s_v are, at each place, one of the numbers (considered in K_v):

$$1+\zeta_n, \quad \zeta_{n+1}+\zeta_{n+1}^{-1}, \quad \sqrt{-1}\,(\zeta_{n+1}+\zeta_{n+1}^{-1}).$$

For any $e > n$, we also have $i(x_0) := i(2+\zeta_n+\zeta_n^{-1})^{2^{e-1}} = \boldsymbol{s}^{2^e}$. The idèle $\boldsymbol{s}$ is not unique and is clearly defined only up to some element of ${}_{2^{n+1}}J$ (this comes from the fact that if v is totally split in $K\mathbb{Q}(\mu_{2^{n+1}})/K$, we can choose the component s_v among three possibilities; this total splitting is equivalent to $\zeta_{n+1} \in K_v$).

One should keep in mind that for all $e > n$, the idèle group $\langle\, \boldsymbol{s} \,\rangle \cdot {}_{2^e}J$ does not depend on the choice of $\boldsymbol{s}$. □

(iii) Note (still in the special case with $Pl_2^{\rm ns} = \emptyset$) that $\boldsymbol{s}^2$ is of the form $\boldsymbol{\zeta}\, i(2+\zeta_n+\zeta_n^{-1})$, where $\boldsymbol{\zeta} \in {}_{2^n}J$, $\boldsymbol{\zeta} \notin {}_{2^{n-1}}J$: indeed, we have $\boldsymbol{\zeta} =: (\zeta_v)_v$ with $\zeta_v = \zeta_n$, or $\zeta_v = 1$, or $\zeta_v = -1$ since:

$$(1+\zeta_n)^2 = \zeta_n y_n, \quad (\zeta_{n+1}+\zeta_{n+1}^{-1})^2 = y_n, \quad (\sqrt{-1}\,(\zeta_{n+1}+\zeta_{n+1}^{-1}))^2 = -y_n,$$

with $y_n := 2+\zeta_n+\zeta_n^{-1}$; but by the Čebotarev theorem, we have equidistribution of all possibilities. In other words:

$$\mathscr{A}(\boldsymbol{s}) \in {}_{2^{n+1}}C, \quad \mathscr{A}(\boldsymbol{s}) \notin {}_{2^n}C.$$

Finally, for all $e > n$:

$$\mathscr{A}(\boldsymbol{s}^2) \in \mathscr{A}({}_{2^{e-1}}J), \quad \mathscr{A}(\boldsymbol{s}) \notin \mathscr{A}({}_{2^e}J)$$

(indeed, otherwise we would easily obtain $y_n \in \pm K^{\times 2}$, which is absurd).

Let $\boldsymbol{x}$ be an idèle such that $\mathscr{A}(\boldsymbol{x})^{p^e} = 1$; there exists $x \in K^\times$ such that $\boldsymbol{x}^{p^e} = i(x)$, so that $i_v(x) \in K_v^{\times p^e}$ for all noncomplex places v. Thus, in general we have $\boldsymbol{x}^{p^e} =: i(y)^{p^e}$, $y \in K^\times$, which yields $\boldsymbol{x} =: \boldsymbol{\zeta}\, i(y)$, where $\boldsymbol{\zeta} \in {}_{p^e}J$ is an idèle of the form $(\zeta_v)_v$, with $\zeta_v \in {}_{p^e}\mu(K_v)$; the result follows in this case.

The special case gives the additional solutions $\boldsymbol{x}^{2^e} = \boldsymbol{s}^{2^e}.\, i(y^{2^e})$, which proves the final result (independently of the choice of $\boldsymbol{s}$). This finishes the question (γ) and the exercise. □

For use in Exercise 6.4 on quadratic forms below, we note that we have shown that $a \in K^\times$ is a square in $K^\times$ if and only if it is a square locally at almost every place of K since troubles can start only for 8th powers.

6.3.5 Remarks. (i) The existence of a counterexample to the equality:

$$K^\times \cap K(\mu_{p^e})^{\times p^e} = K^{\times p^e}$$

(Theorem 6.3.2) should not be mistaken with a Σ-special case (Theorem 6.3.3), which is a counterexample to the Hasse principle for powers and which is relative to the choice of Σ; the former case is characterized by the following conditions:

- $p = 2, \quad e \geq 2,$
- $K \cap \mathbb{Q}(\mu_{2^e}) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, for $2 \leq n \leq e$,

and concerns $x := (-(2+\zeta_n+\zeta_n^{-1})^{2^{n-1}})^{2^{e-n}}$, which yields the minimal example $x = -4$ (for $K = \mathbb{Q}$ and $e = 2$) which is never a special case. To avoid any misunderstanding, this case has been called instead the *exceptional case*.

(ii) Note also that $\pm(2+\zeta_n+\zeta_n^{-1})^{2^{n-1}}$ is a 2^nth power in each of the three quadratic subextensions of $K\mathbb{Q}(\mu_{2^{n+1}})/K$ (the minus sign occurs only for $K\mathbb{Q}(\mu_{2^n})/K$ and the relation $(2+\zeta_n+\zeta_n^{-1})^{2^{n-1}} = -(1+\zeta_n)^{2^n}$). □

Finally, we give the following numerical example of a true special case.

6.3.6 Example. Let $K = \mathbb{Q}(\sqrt{7}\,)$, $p = 2$, and $e = 3$. Then $K \cap \mathbb{Q}(\mu_8) = \mathbb{Q}$ (i.e., $n = 2$), so that we have the exceptional case with $x = 16$ (we have

$16 = (1+\sqrt{-1}\,)^8 = (\sqrt{2}\,)^8 = (\sqrt{-2}\,)^8$ in $\mathbb{Q}(\mu_8)$). From the above, we know that $i_v(x) \in K_v^{\times 8}$ for any place not dividing 2, and for the unique place v_0 of K above 2, we have $K_{v_0} = \mathbb{Q}_2(\sqrt{7}\,) = \mathbb{Q}_2(\sqrt{-1}\,)$ (i.e., $Pl_2^{\rm ns} = \emptyset$), which implies that $i_{v_0}(x) \in K_{v_0}^{\times 8}$ (we could also have chosen $K = \mathbb{Q}(\sqrt{\pm 14}\,)$). We thus have a special case (i.e., $\Sigma = \emptyset$); therefore it is an absolute counterexample to the Hasse principle for powers. □

We will speak of the *special case* only in this type of situation.

6.3.7 Exercise. Consider the special case of Example 6.3.6 above. Let ℓ be the residue characteristic of $v \in Pl_0$. Show that the idèle $\boldsymbol{s} =: (s_v)_v$ (see 6.3.4.3) can be chosen as follows. If $\ell = 2$, $s_v = 1 + \sqrt{-1}$; if $\ell = 7$, $s_v = \sqrt{2}$; if $\ell \equiv 1 \bmod (4)$, $s_v = 1 + \sqrt{-1}$, and if $\ell \equiv -1 \bmod (4)$, $s_v = \sqrt{(-1)^{\frac{\ell+1}{4}} 2}$.

Check that $1 + \sqrt{-1}$, $\sqrt{2}$, $\sqrt{-2}$ are all possible for s_v if and only if $|F_v| \equiv 1 \bmod (8)$ (i.e., $\ell \equiv 1 \bmod (8)$, or $\ell \not\equiv 1 \bmod (8)$ and $\ell \equiv \pm 5,\ \pm 11,\ \pm 13 \bmod (28)$). □

6.3.8 Exercise (another criterion for pth powers). Let S be a finite set of noncomplex places of K such that $(\langle\, \mathcal{A}_{K'}^{\rm res}(S')\,\rangle)_p = (\mathcal{A}_{K'}^{\rm res})_p$ (in the sense of I.4.4.1, (ii)), where S' is the set of places of $K' := K(\mu_p)$ above those of S. Let $x \in K^\times$ satisfying the following conditions:

- $(x) = \mathfrak{a}^p$, for an ideal $\mathfrak{a}$ of K,
- $i_v(x) \in K_v^{\times p}$ for all $v \in S \cup Pl_p$.

Show that $x \in K^{\times p}$.

Answer. The assumption on S' in K' is equivalent to $H_{K'(p)}^{S'} = K'$. But the assumption $(x) = \mathfrak{a}^p$ implies that $K'(\sqrt[p]{x}\,)/K'$ is unramified outside p, and the assumption $i_v(x) \in K_v^{\times p}$ for all $v \in S \cup Pl_p$ implies that it is S'-split and finally unramified; thus $K'(\sqrt[p]{x}\,) \subseteq H_{K'}^{S'}$, hence $x \in K^{\times p}$ by the above and 6.3.2 for $e = 1$.

Here, the number of local conditions is finite, but the required conditions assume the knowledge of the p-class group of K'.

We can also replace the conditions $i_v(x) \in K_v^{\times p}$ for $v|p$ by the Kummer nonramification conditions for places above p (use I.6.3, (ii) in K'). □

6.3.9 Remark. Let K be a number field and p a prime. Suppose we need to prove that some $\alpha \in K^\times$ is not a pth power in K. Then it is sufficient to find a place $v \nmid p$ such that α is not congruent to a pth power modulo $\mathfrak{p}_v$. The local-global principle for powers implies that such a place always exists but it does not give a bound for the number of tests. □

6.4 Exercise (quadratic forms in three variables). For $a,\ b \in K^\times$, consider the quadratic form:

$$(q) \quad X^2 - a\,Y^2 - b\,Z^2.$$

We will say that it represents 0 in K if there exist $x,\ y,\ z \in K$ (not all zero) such that:

$$x^2 - ay^2 - bz^2 = 0.$$

Set $L = K(\sqrt{a}\,)$.

(i) Check that (q) represents 0 in K if and only if $b \in \mathrm{N}_{L/K}(L^\times)$.

(ii) Characterize the finite places of K which are ramified in L/K (see I.6.3).

(iii) Check that, for unramified places v (finite or not), the local norm condition $i_v(b) \in \mathrm{N}_{L_v/K_v}(L_v^\times)$ (where $L_v = L_w = K_v(\sqrt{a}\,)$, for any $w|v$) is equivalent to $\mathrm{v}(b) \equiv 0 \bmod (f_v)$. For a concrete use of this, note that it is necessary to check the local conditions only when $\mathrm{v}(b)$ is odd, and that then we must have $f_v = 1$, which is the case if and only if $i_v(a) \in K_v^{\times 2}$.

To apply the Hasse principle, we can now assume that we are in the case where the bad places are the finite ramified places (where one may be omitted). It is then necessary to compute the symbols $(i_v(b), L_v/K_v)$ which can be identified with the quadratic Hilbert symbols $\left(\frac{a,\,b}{v}\right)$ over K; the case of odd places corresponds to regular Hilbert symbols and is given by a formula (see 1.6.8 for $n = 2$), so there essentially remains the case of even places. These symbols are also the Hasse symbols $\left(\frac{b\,,\,L/K}{v}\right)$ that we know how to compute in terms of Frobenius' thanks to the global approach explained in 4.4.3 which thus reduces to the techniques of question (iii) since here the conductor $\mathfrak{f}_{L/K}$ is known by 1.6.3.

(iv) Let $K = \mathbb{Q}(\sqrt{2}\,)$, $a = 2 + 3\sqrt{2}$, and $b = -15(1 + \sqrt{2}\,)$; does the form (q) represent 0 in K ?

(v) Specialize all the above to $K = \mathbb{Q}$, taking into account the important simplifications that we have in this case, and show that, for $v \neq 2$, we have $\left(\frac{a,\,b}{v}\right) = \left(\frac{u}{v}\right)$ (quadratic residue symbol in $F_v^\times$), where $u = (-1)^{\mathrm{v}(a)\mathrm{v}(b)}\,a^{\mathrm{v}(b)}\,b^{-\mathrm{v}(a)}$ (a particular case of the general formula given in 1.6.8 and proved in 7.1.5). Although, because of the product formula it is not really necessary to give a formula for the Hilbert symbol at $v = (2)$, show that:

$$\left(\frac{a,\,b}{v}\right) = \Big(-1\Big)^{\frac{a'-1}{2}\frac{b'-1}{2}}\left(\frac{2}{u'}\right),$$

where $a' = 2^{-\mathrm{v}(a)}\,a,\ b' = 2^{-\mathrm{v}(b)}\,b,\ u' = a^{\mathrm{v}(b)}\,b^{-\mathrm{v}(a)} = a'^{\mathrm{v}(b)}\,b'^{-\mathrm{v}(a)}$, and where:

$$\left(\frac{2}{u'}\right) := \Big(-1\Big)^{\frac{u'^2-1}{8}},$$

for a 2-adic unit u'.

Answer. The case where a is a square in $K^\times$ being solved trivially by a direct study, we will implicitly assume that a is not a square; in this case, for any solution, z is nonzero.

(i) We write:

$$b = \frac{x^2 - ay^2}{z^2} = \mathrm{N}_{L/K}\Big(\frac{x + y\sqrt{a}}{z}\Big).$$

(ii) An odd place v is ramified if and only if $\mathrm{v}(a) \equiv 1 \bmod (2)$, an even place is ramified if and only if $\frac{a}{t^2} \equiv 1 \bmod (4)$ is not soluble for $t \in K^\times$.

(iii) This is Corollary 1.4.3: if $i_v(b) \in \mathrm{N}_{L_v/K_v}(L_v^\times) = \mathrm{N}_{L_v/K_v}(\pi_w^{\mathbb{Z}} U_w) \subset \pi_v^{f_v\mathbb{Z}} U_v$, we indeed have $\mathrm{v}(b) \equiv 0 \bmod (f_v)$ (including the case $\pi_v = -1$ and $f_v = 2$ corresponding to a complexified real place v), and the converse comes from the fact that, in the unramified case, $U_v \subseteq \mathrm{N}_{L_w/K_v}(U_w)$.

(iv) We have $(a) = (\sqrt{2}\,)(3 + \sqrt{2}\,) = \mathfrak{p}_2\mathfrak{p}_7$ (the place 2 is ramified in $K/\mathbb{Q}$ and the place 7 is split). It follows that the places of K which are ramified in L/K are the places $\mathfrak{p}_2$ and $\mathfrak{p}_7$.

Since $b = -15(1 + \sqrt{2}\,)$ has even valuation at every place except perhaps at places above ∞, 3, and 5, we must see whether or not $\mathrm{v}(b) \equiv 0 \bmod (f_v)$ is true for these places; we will simply check that if $\mathrm{v}(b) \equiv 1 \bmod (2)$, then $f_v = 1$ (splitting):

- the place ∞ splits in $K/\mathbb{Q}$ into two places v_1, v_2, and we have $i_{v_1}(b) < 0$ (i.e., $\mathrm{v}_1(b) = 1$), $i_{v_2}(b) > 0$ (i.e., $\mathrm{v}_2(b) = 0$). But we have $i_{v_1}(a) > 0$ (v_1 is split in L/K, hence $f_{v_1} = 1$);
- the place 3 is inert in $K/\mathbb{Q}$, hence $F_v = \mathbb{F}_9$, and since $a \equiv -1 \bmod (3)$, the residual image of a is a square (i.e., $i_v(a) \in K_v^{\times\,2}$, hence $f_v = 1$);
- the place 5 is also inert, $F_v = \mathbb{F}_{25}$, and we find that $a^3 \equiv 1 \bmod (5)$, hence that a is also a square at 5.

The remaining local norm conditions are for the even place $\mathfrak{p}_2$ (which we can omit), and for $v = \mathfrak{p}_7$. We can compute the Hasse symbol:

$$\left(\frac{b\,,\,L/K}{\mathfrak{p}_7}\right) = \left(\frac{-15(1+\sqrt{2}\,)\,,\,L/K}{\mathfrak{p}_7}\right).$$

In fact, it defines a regular Hilbert symbol of order 2 which we will learn how to compute in 7.1.5; with this result, we would obtain:

$$\left(\frac{a,\,b}{\mathfrak{p}_7}\right) \equiv \Big((-1)^{\mathrm{v}(a)\mathrm{v}(b)}\, a^{\mathrm{v}(b)}\, b^{-\mathrm{v}(a)}\Big)^{\frac{q_v-1}{2}} \equiv b^{-3} \equiv 1 \bmod \mathfrak{p}_7.$$

Let us nonetheless directly compute this Hasse symbol knowing that the conductor of L/K is (because of 1.6.3 which yields $r = 0$ in the computation of the 2-part of the conductor):

$$\mathfrak{f} = \mathfrak{p}_2^{2\times 2+1}\mathfrak{p}_7 = (4)\mathfrak{p}_2\mathfrak{p}_7.$$

A $\mathfrak{p}_7$-associate b' of b must satisfy (see 4.4.3, (γ)):

$$\begin{aligned} b' &\equiv b \bmod \mathfrak{p}_7 \text{ (since here } \mathrm{v}(b) = 0), \\ b' &\equiv 1 \bmod (4)\mathfrak{p}_2, \\ i_{v_2}(b') &> 0 \text{ (since only } v_2|\infty \text{ is complexified}), \end{aligned}$$

which for example yields $b' = 17 + 12\sqrt{2}$. Here b' happens to be a unit (this was not done on purpose!); the ideal $\mathfrak{b}$ (in the general formula $(b') =: \mathfrak{p}_7^{\mathrm{v}(b)}\mathfrak{b}$) whose Artin symbol we must compute is thus the unit ideal, hence b is indeed a local norm at $\mathfrak{p}_7$.

The product formula tells us that b is also a local norm at $\mathfrak{p}_2$. To double-check this, we want to compute the symbol:

$$\left(\frac{b,\, L/K}{\mathfrak{p}_2}\right) = \left(\frac{-15(1+\sqrt{2}),\, L/K}{\mathfrak{p}_2}\right),$$

which does not have any simple formula. We proceed as above, and we check that $9 + 5\sqrt{2}$ is a $\mathfrak{p}_2$-associate which yields $\mathfrak{b} = \mathfrak{p}_{31}$ split in L/K since the residual image of a is a square.

Thus, the given quadratic form represents 0 in K.

(v) The norm conditions on b at the unramified odd places $v = (\ell)$ (i.e., such that $\mathrm{v}(a) \equiv 0 \bmod (2)$) are therefore (by (iii)) $\left(\frac{a\ell^{-\mathrm{v}(a)}}{v}\right)^{\mathrm{v}(b)} = 1$, including for $v = \infty$; we thus indeed obtain $\left(\frac{u}{v}\right) = 1$ in this case.

There remain the odd places $v = (\ell)$ such that $\mathrm{v}(a) \equiv 1 \bmod (2)$ (i.e., the ramified finite odd places) for which we must check that b is in the norm group of $\mathbb{Q}_\ell(\sqrt{a}\,)/\mathbb{Q}_\ell$. Set $a' := a\ell^{-\mathrm{v}(a)}$ and $b' := b\ell^{-\mathrm{v}(b)}$. We use Exercise 1.6.5 which shows that b is a local norm at ℓ if and only if $b \in N_2$ (resp. N_3) when $\left(\frac{-a'}{\ell}\right) = 1$ (resp. -1) (we see whether $\mathbb{Q}_\ell(\sqrt{a}\,) = \mathbb{Q}_\ell(\sqrt{-\ell}\,)$ or $\mathbb{Q}_\ell(\sqrt{-\ell\zeta}\,)$). But $b \in N_2$ (resp. N_3) is equivalent to $\left(\frac{b'}{\ell}\right) = 1$ (resp. $(-1)^{\mathrm{v}(b)}$). It follows that b is a local norm at ℓ if and only if:

$$\left(\frac{-a'}{\ell}\right)^{\mathrm{v}(b)} = \left(\frac{b'}{\ell}\right),$$

hence $\left(\frac{u}{\ell}\right) = 1$ with the given formula for u since $\mathrm{v}(a)$ is odd.

The case of the place $v = 2$ can be obtained in analogous way by noting that the Hilbert symbol and the explicit formulas that we must prove are $\mathbb{F}_2$-bilinear and symmetrical in a and b, and thus we are reduced to the computation of the six symbols:

$$\left(\frac{2\,,\,2}{v}\right),\ \left(\frac{2\,,\,q}{v}\right),\ \left(\frac{2\,,\,-1}{v}\right),\ \left(\frac{q\,,\,q}{v}\right),\ \left(\frac{q\,,\,-1}{v}\right),\ \left(\frac{-1\,,\,-1}{v}\right),$$

where q is an odd prime. The computation of these symbols is immediate from the results of 1.6.5. In fact, the general properties of symbols (see 7.1.1 below) show that it is sufficient to compute:

$$\left(\frac{2\,,\,q}{v}\right),\ \left(\frac{q\,,\,-1}{v}\right),\ \left(\frac{-1\,,\,-1}{v}\right).$$ □

6.4.1 Remark. If the quadratic form $X^2 - a\,Y^2 - b\,Z^2$ does not represent 0 in K, it does not represent 0 in a nonzero even number of completions of K (consider for instance $X^2 + Y^2 + Z^2$ in $\mathbb{Q}$). □

§7 Symbols Over Number Fields — Hilbert and Regular Kernels

The notion of symbol, which can be set in the very general context of Milnor's K-theory, where the letter $\mathrm{K} \neq K$ does not denote a field but a functor (see [Mil], [Sil]), is directly inspired from the Hilbert symbols that we have already encountered in 1.6.7, 1.6.8, 6.4; hence we will start by giving more completely their properties, obtain from this the general definition of symbols over a field, and ask whether or not we know all the symbols over a number field.

Thanks to this, we will see that class field theory is only an (essential) prelude to a larger theory which involves many invariants which we have not met up to now; as already said, the only unified point of view on these questions is of a cohomological nature (see [Schn], [Ta2]), and we refer to the enormous bibliography devoted to higher K-theory.

7.1 Definitions (local Hilbert symbol). Let K be a number field. Then for any place v of K we define the local Hilbert symbol at v:

$$(\bullet\,,\,\bullet)_v\ :\ K_v^\times \times K_v^\times \longrightarrow \mu(K_v),$$

by:

$$(x\,,\,y)_v := \frac{(y\,,\,K_v(\sqrt[m_v]{x})/K_v)\ \sqrt[m_v]{x}}{\sqrt[m_v]{x}}$$

for all $x,\ y \in K_v^\times$, where $m_v := |\mu(K_v)|$ and where $(\bullet\,,\,K_v(\sqrt[m_v]{x})/K_v)$ is the norm residue symbol for the cyclic extension $K_v(\sqrt[m_v]{x})/K_v$ (see 1.4). □

Note, once and for all, that if v is a complex place at infinity, then $(\bullet\,,\,\bullet)_v = 1$.

7.1.1 Proposition. *The local Hilbert symbol* $(\bullet\,,\,\bullet)_v$ *has the following properties:*

(i) it is $\mathbb{Z}$-bilinear, nondegenerate as a bilinear map on $K_v^\times/K_v^{\times m_v} \times K_v^\times/K_v^{\times m_v}$, and continuous as a map on $K_v^\times \times K_v^\times$;

(ii) it satisfies:

$$(x\,,\,1-x)_v = 1 \text{ for all } x \in K_v^\times \setminus \{1\},$$
$$(x\,,\,-x)_v = 1 \text{ for all } x \in K_v^\times,$$
$$(x\,,\,y)_v = (y\,,\,x)_v^{-1} \text{ for all } x,\ y \in K_v^\times \text{ (antisymmetry)};$$

(iii) we have $(x\,,\,y)_v = 1$ if and only if y is a norm in $K_v(\sqrt[m_v]{x})/K_v$ (or x is a norm in $K_v(\sqrt[m_v]{y})/K_v$);

(iv) in an extension L/K, for any $w|v$ in L we have, with evident notations:

$$\left(x^{\frac{m_w}{m_v}}\,,\,y'\right)_w = \left(x\,,\,\mathrm{N}_{L_w/K_v}(y')\right)_v$$

for all $x \in K_v^\times$ and $y' \in L_w^\times$;

(v) for any isomorphism τ of K, we have $(\tau x\,,\,\tau y)_{\tau v} = \tau(x\,,\,y)_v$ for all $x,\ y \in K_v^\times$;

(vi) if v is unramified in $K_v(\sqrt[m_v]{x})/K_v$, we have:

$$(x\,,\,y)_v = \left(\frac{\mathrm{Frob}\left(K_v(\sqrt[m_v]{x})/K_v\right)\sqrt[m_v]{x}}{\sqrt[m_v]{x}}\right)^{\mathrm{v}(y)}$$

for all $y \in K_v^\times$.

Note. In (v), τv is the place of τK for which $|\tau a|_{\tau v} = |a|_v$ for all $a \in K$; afterwards, by abuse of notation, τ also denotes the isomorphism $\tau : K_v \longrightarrow (\tau K)_{\tau v}$ coming from $K \subset \bigoplus_{v'|\ell} K_{v'} \longrightarrow \tau K \subset \bigoplus_{v'|\ell} (\tau K)_{\tau v'}$, by density (the generalization of the situation of 2.3.1), the embeddings $\bigoplus_{v'|\ell} i_{v'}$ on K and $\bigoplus_{v'|\ell} i_{\tau v'}$ on τK being understood (here, ℓ denotes a prime number or ∞); then it is also the extension by continuity of $i_{\tau v} \circ \tau \circ i_v^{-1}$ on $i_v(K)$. Thanks to this, the expressions τx, τy, and $\tau(x\,,\,y)_v$ make sense.

Proof of the proposition. (i) We have $(x\,,\,yz)_v = (x\,,\,y)_v(x\,,\,z)_v$ because of the multiplicativity of the norm residue symbol and of the isomorphism of Kummer duality (see I.6.1).

We have $(xy\,,\,z)_v = \dfrac{\tau(\sqrt[m_v]{xy})}{\sqrt[m_v]{xy}}$, where $\tau := (z\,,\,K_v(\sqrt[m_v]{xy})/K_v)$; but τ is the restriction to $K_v(\sqrt[m_v]{xy})$ of $\sigma := (z\,,\,K_v(\sqrt[m_v]{x},\ \sqrt[m_v]{y})/K_v)$ by 1.4, (ii), and we have:

$$\frac{\sigma(\sqrt[m_v]{xy})}{\sqrt[m_v]{xy}} = \frac{\sigma(\sqrt[m_v]{x})}{\sqrt[m_v]{x}} \times \frac{\sigma(\sqrt[m_v]{y})}{\sqrt[m_v]{y}},$$

thus giving the result since the restrictions of σ to $K_v(\sqrt[m_v]{x})$ and to $K_v(\sqrt[m_v]{y})$ are the corresponding norm residue symbols of z.

Assume that $(x\,,\,y)_v = 1$ for all $y \in K_v^\times$; the surjectivity of the norm residue symbol implies that $K_v(\sqrt[m_v]{x}) = K_v$, so that $x \in K_v^{\times m_v}$.

If $(x\,,\,y)_v = 1$ for all $x \in K_v^\times$, we have $\big(y,\, K_v(\sqrt[m_v]{K_v^\times})/K_v\big) = 1$ hence y is a norm in $K_v(\sqrt[m_v]{K_v^\times})$, hence $y \in K_v^{\times m_v}$ (see 1.6.6).

Continuity comes from the fact that, if u and u' are sufficiently close to 1 in U_v, then u and u' are m_vth powers in $K_v^\times$, and we have trivially $(xu\,,\,yu')_v = (x\,,\,y)_v$.

To prove some of the above properties, we may use the antisymmetry that we will prove in full generality in 7.2.1.

(ii) Let us show that $1-x$ is the norm of an element of $M := K_v(\sqrt[m_v]{x})$. If $d|m_v$ is the degree of M/K_v, Kummer theory shows that there exists $t \in K_v^\times$ such that $x = t^{\frac{m_v}{d}}$, and we have $M = K_v(\sqrt[d]{t})$. Since for all $\xi \in \mu(K_v)$ we have:

$$\mathrm{N}_{M/K_v}(1 - \xi\sqrt[d]{t}) = 1 - \xi^d t,$$

then denoting by ζ_v a generator of $\mu(K_v)$, it follows that:

$$\mathrm{N}_{M/K_v}\Big(\prod_{i=1}^{\frac{m_v}{d}}(1-\zeta_v^i\sqrt[d]{t})\Big) = \prod_{i=1}^{\frac{m_v}{d}}(1-\zeta_v^{di}t) = 1 - t^{\frac{m_v}{d}} = 1 - x.$$

The relation $(x\,,\,-x)_v = 1$ as well as antisymmetry then follow from this (see 7.2.1).

Facts (iii), (iv), (v), and (vi) follow trivially from the corresponding properties 1.4 of the norm residue symbol. □

7.1.2 Remark. If m is a divisor of m_v, the symbol $(\bullet\,,\,\bullet)_v^{(m)}$ defined by:

$$(x\,,\,y) \in K_v^\times \times K_v^\times \longmapsto \frac{(y\,,\,K_v(\sqrt[m]{x})/K_v)\ \sqrt[m]{x}}{\sqrt[m]{x}}$$

for all $x,\ y \in K_v^\times$, is equal to $\big(\bullet\,,\,\bullet\big)_v^{\frac{m_v}{m}}$ since $\sqrt[m_v]{x^{\frac{m_v}{m}}} = \sqrt[m]{x}$. By abuse of language, it is called the local Hilbert symbol of order m. In common usage, we write simply $(x\,,\,y)_v$ instead of $(x\,,\,y)_v^{(m)}$, the context being in general sufficient to give the order of the symbols under study (for example $m = 2$ for the usual quadratic Hilbert symbol). The Hilbert symbol defined in 7.1 has maximal order with an evident meaning. □

Before going any further, it is necessary to introduce the regular Hilbert symbol (which has the advantage of being explicit), and for this we give some notations and definitions.

7.1.3 Notations. (i) Let $v \in Pl_0$ and let ℓ be the residue characteristic of v. We know (see I.3.1.1) that we have the decomposition:

$$\mu(K_v) = \mu_{q_v-1} \oplus \mu_\ell(K_v),$$

where $q_v := |F_v|$ is a power of ℓ and where $\mu_\ell(K_v) = \mathrm{tor}_{\mathbb{Z}}(U_v^1)$ is also of order a power of ℓ, which we will write here in the more descriptive form:

$$\mu(K_v) =: \mu(K_v)^{\mathrm{reg}} \oplus \mu(K_v)^1.$$

(ii) For $v \in Pl_\infty^{\mathrm{r}}$, we have $\mu(K_v) = \mu_2$ and we set, in accordance with the fact that $U_v^1 = \mathbb{R}^{\times +}$:

$$\mu(K_v)^{\mathrm{reg}} := \mu_2, \quad \mu(K_v)^1 := 1.$$

(iii) As is easily checked, $\mu(K_v)^1 = 1$ for almost all places of K (indeed, $\mu(K_v)^1 \neq 1$ implies that K_v contains μ_ℓ, hence $\mathbb{Q}_\ell(\mu_\ell)$, which implies that $\ell - 1 \leq [K : \mathbb{Q}]$). The places v for which $\mu(K_v)^1 \neq 1$ will be called the irregular places of K. □

7.1.4 Definitions (regular Hilbert symbol). We define the regular or tame Hilbert symbol at a noncomplex place v as the Hilbert symbol of order $|\mu(K_v)^{\mathrm{reg}}|$, in other words as the symbol $(\bullet\,,\,\bullet)_v^{\mathrm{reg}} := (\bullet\,,\,\bullet)_v^{m_v^1}$, where $m_v^1 := |\mu(K_v)^1|$ (equal to $\dfrac{m_v}{q_v - 1}$ in the finite case). □

7.1.5 Proposition (regular Hilbert symbol formula). *For any $x,\ y \in K_v^\times$, $(x\,,\,y)_v^{\mathrm{reg}}$ is the component on $\mu(K_v)^{\mathrm{reg}}$ of:*

$$(-1)^{\mathrm{v}(x)\mathrm{v}(y)} x^{\mathrm{v}(y)} y^{-\mathrm{v}(x)}.$$

Note. For computations and when v is finite, it is equivalent to take the residual image of the above expression since $\mu(K_v)^{\mathrm{reg}} = \mu_{q_v - 1} \simeq F_v^\times$ (canonically), and for a real infinite place v, it is the sign of this same expression, equal to $(-1)^{\mathrm{v}(x)\mathrm{v}(y)}$.

Proof of the proposition. The case of an infinite place v being trivial directly, we assume that v is a finite place. We have:

$$(x\,,\,y)_v^{m_v^1} = (x^{m_v^1}\,,\,y)_v = \frac{(y\,,\,K_v(\sqrt[q_v-1]{x})/K_v)\ \sqrt[q_v-1]{x}}{\sqrt[q_v-1]{x}}.$$

To identify this Hilbert symbol, it is sufficient to compute (using bilinearity and antisymmetry):

$$(u\,,\,u')_v^{m_v^1}, \quad (u\,,\,\pi)_v^{m_v^1}, \quad (\pi\,,\,\pi)_v^{m_v^1},$$

for $u,\ u' \in U_v$ and for a uniformizer π of K_v:

- by 7.1.1, (vi), we have $(u\,,\,u')_v^{m_v^1} = 1$ since $K_v(\sqrt[q_v-1]{u})/K_v$ is unramified;
- in the same way, $(u\,,\,\pi)_v^{m_v^1} = \dfrac{\sigma(\sqrt[q_v-1]{u})}{\sqrt[q_v-1]{u}}$, where $\sigma := \mathrm{Frob}(K_v(\sqrt[q_v-1]{u})/K_v)$;

it follows that we have:

$$\frac{\sigma(\sqrt[q_v-1]{u})}{\sqrt[q_v-1]{u}} \equiv \frac{(\sqrt[q_v-1]{u})^{q_v}}{\sqrt[q_v-1]{u}} \equiv u \bmod (\pi),$$

which shows that $(u\,,\,\pi)_v^{m_v^1}$ is the component of u on μ_{q_v-1};

• by 7.1.1, (ii), we have $(\pi\,,\,-\pi)_v = 1$, hence $(\pi\,,\,\pi)_v^{m_v^1} = (-1\,,\,\pi)_v^{m_v^1}$, so that we are reduced to the preceding situation with $u = -1$.

By "gluing the pieces together", we obtain the desired formula. □

Note. It is also possible to use symbols having an order dividing $q_v - 1$ (v finite); this is for instance the case for quadratic Hilbert symbols which are given, for any odd place v, by the residual image of $\big((-1)^{\mathrm{v}(a)\mathrm{v}(b)}\, a^{\mathrm{v}(b)}\, b^{-\mathrm{v}(a)}\big)^{\frac{q_v-1}{2}}$. By abuse of language, we will also say that they are regular symbols.

Note that the basic symbols $(\bullet\,,\,\bullet)_v^{\mathrm{reg}}$ and $(\bullet\,,\,\bullet)_v$ coincide for almost every place (the regular places).

We will see in 7.5 how to compute in practice the irregular Hilbert symbols, which are finite in number; the numerical computations done in 6.4 for some quadratic symbols are illustrations of this.

The above study motivates the general definition of a symbol on a field k, with values in an abelian group A.

7.2 Definition (symbols on a field). Let k be a field, and let A be an abelian group. A symbol (on k, with values in A) is a $\mathbb{Z}$-bilinear map:

$$(\bullet\,,\,\bullet)\ :\ k^\times \times k^\times \longrightarrow A,$$

such that $(x\,,\,y) = 1$ for all $x,\ y \in k^\times \setminus \{1\}$ such that $x + y = 1$. □

If we consider the quotient group:

$$\mathrm{K}_2(k) := k^\times \otimes_{\mathbb{Z}} k^\times / \langle\, x \otimes y\,;\ x,\ y \in k^\times \setminus \{1\},\ x + y = 1 \,\rangle$$

(second Milnor's K-group of the field k), it is immediate to check that this object satisfies the following universal property. For any symbol:

$$(\bullet\,,\,\bullet)\ :\ k^\times \times k^\times \longrightarrow A,$$

there exists a unique group homomorphism $h : \mathrm{K}_2(k) \longrightarrow A$, such that the following diagram commutes:

$$\begin{array}{ccc} k^\times \times k^\times & \xrightarrow{\ (\bullet\,,\,\bullet)\ } & A \\ {\scriptstyle \{\bullet\,,\,\bullet\}}\big\downarrow & \nearrow_{h} & \\ \mathrm{K}_2(k) & & \end{array}$$

the vertical arrow being the canonical map sending the pair $(x,\ y)$ to the image of $x \otimes y$; this map is not necessarily surjective, but its image generates $\mathrm{K}_2(k)$.

We have denoted $\{x\,,\,y\}$ the canonical image of $x \otimes y$ in $\mathrm{K}_2(k)$; by construction, it is clear that $\{\,\bullet\,,\ \bullet\,\}$ is itself a symbol with values in $\mathrm{K}_2(k)$.

7.2.1 Exercise. Show that any symbol $(\,\bullet\,,\ \bullet\,) \ :\ k^\times \times k^\times \longrightarrow A$ satisfies $(x\,,\,-x) = 1$ for all $x \in k^\times$. Deduce that any symbol is antisymmetric.

Answer. If $x = 1$, we have $(1\,,\,-1) = 1$ by linearity on the first component. Thus we may assume that $x \neq 1$. We then have the equalities:

$$\begin{aligned} 1 = \Big(\frac{1}{x}\ ,\ 1-\frac{1}{x}\Big) = \Big(x\ ,\ 1-\frac{1}{x}\Big)^{-1} &= \Big(x\ ,\ \frac{1-x}{-x}\Big)^{-1} \\ &= \Big(x\ ,\ 1-x\Big)^{-1}\Big(x\ ,\ \frac{1}{-x}\Big)^{-1} = (x\,,\,-x). \end{aligned}$$

We then apply this property to the product xy, and we obtain:

$$\begin{aligned} 1 = (xy\,,\,-xy) &= (x\,,\,-xy)(y\,,\,-xy) \\ &= (x\,,\,-x)(x\,,\,y)(y\,,\,x)(y\,,\,-y) = (x\,,\,y)(y\,,\,x), \end{aligned}$$

so the antisymmetry follows. □

7.2.2 Examples. (i) If $k = K_v$ (the completion of the number field K at a finite place v), the local Hilbert symbol $(\,\bullet\,,\ \bullet\,)_v$ defines the group homomorphism:

$$h_v : \mathrm{K}_2(K_v) \longrightarrow \mu(K_v),$$

which is in fact an isomorphism, a result of Moore (see [e, Ko3, Ch. 2, § 6.6]).

(ii) If $k = K$, we can consider the symbol obtained by globalizing the family of local Hilbert symbols in the following way:

$$\begin{array}{rccl} (\,\bullet\,,\ \bullet\,) \ :\ K^\times \times K^\times & \longrightarrow & \displaystyle\bigoplus_{v \in Pl^{\mathrm{nc}}} \mu(K_v), \\ (x\,,\,y) & \longmapsto & \big((i_v(x)\,,\,i_v(y))_v\big)_{v \in Pl^{\mathrm{nc}}} \end{array}$$

where $Pl^{\mathrm{nc}} := Pl \setminus Pl_\infty^{\mathrm{c}}$ is the set of noncomplex places of K. This symbol indeed takes its values in the direct sum since for any place v such that $\mathrm{v}(x) = \mathrm{v}(y) = 0$, $i_v(y)$ is a unit and the extension $K_v(\sqrt[m_v]{i_v(x)})/K_v$ is unramified except perhaps if the residue characteristic ℓ of v divides m_v, which happens only for a finite number of places (the irregular places, i.e., those for which K_v contains μ_ℓ; see 7.1.3, (iii)). For convenience, this symbol will be called the global Hilbert symbol. It defines the homomorphism:

$$h : \mathrm{K}_2(K) \longrightarrow \bigoplus_{v \in Pl^{\mathrm{nc}}} \mu(K_v).$$

(iii) We can also define the global regular Hilbert symbol, from the local regular Hilbert symbols (see 7.1.4, 7.1.5):

$$(\bullet\,,\,\bullet)^{\mathrm{reg}}\ :\ K^\times\times K^\times\longrightarrow\bigoplus_{v\in Pl^{\mathrm{nc}}}\mu(K_v)^{\mathrm{reg}}$$

which sends any pair $(x,\ y)$ to $\big((i_v(x)\,,\,i_v(y))_v^{\mathrm{reg}}\big)_{v\in Pl^{\mathrm{nc}}}$. Recall that for $v\in Pl_0$:

$$(\bullet\,,\,\bullet)_v^{\mathrm{reg}}:=(\bullet\,,\,\bullet)_v^{m_v^1},\quad\text{where } m_v^1:=|\mu(K_v)^1|=\frac{m_v}{q_v-1}\cdot$$

The resulting homomorphism $\mathrm{K}_2(K)\longrightarrow\bigoplus_{v\in Pl^{\mathrm{nc}}}\mu(K_v)^{\mathrm{reg}}$ is denoted h^{reg}. □

7.3 Theorem. *For all $x,\ y\in K^\times$, we have in $\mu(K)$ the product formula:*

$$\prod_{v\in Pl^{\mathrm{nc}}}i_v^{-1}\Big(\big(i_v(x)\,,\,i_v(y)\big)_v^{\frac{m_v}{m}}\Big)=1,$$

where $m:=|\mu(K)|$, $m_v:=|\mu(K_v)|$.

Proof. We have $\big(i_v(x)\,,\,i_v(y)\big)_v^{\frac{m_v}{m}}=\big(i_v(x^{\frac{m_v}{m}})\,,\,i_v(y)\big)_v$, and the norm residue symbol:

$$\Big(i_v(y)\,,\,K_v\Big(\sqrt[m_v]{i_v(x^{\frac{m_v}{m}})}\Big)\Big/K_v\Big)=\Big(i_v(y)\,,\,K_v\Big(\sqrt[m]{i_v(x)}\Big)\Big/K_v\Big)$$

being the norm residue symbol in L_v/K_v for $L:=K(\sqrt[m]{x}\,)$, which is abelian over K, in terms of Hasse symbols 3.1.2 we obtain:

$$i_v^{-1}\Big(\big(i_v(x)\,,\,i_v(y)\big)_v^{\frac{m_v}{m}}\Big)=\left(\frac{y\,,\,K(\sqrt[m]{x}\,)/K}{v}\right)\sqrt[m]{x}\Big/\sqrt[m]{x}\in\mu(K)\ ;$$

hence, by the isomorphism of Kummer duality I.6.1, the product formula (in $G:=\mathrm{Gal}(K(\sqrt[m]{x}\,)/K)$):

$$\prod_v\left(\frac{y\,,\,K(\sqrt[m]{x}\,)/K}{v}\right)=1$$

is transformed into the analogous formula on the $i_v^{-1}\Big(\big(i_v(x)\,,\,i_v(y)\big)_v^{\frac{m_v}{m}}\Big)$ (in $\mu(K)$). □

7.3.1 Definitions (Hilbert symbols of K — product formula). If we set:

$$\left(\frac{x\,,\,y}{v}\right):=i_v^{-1}\Big(\big(i_v(x)\,,\,i_v(y)\big)_v^{\frac{m_v}{m}}\Big)=\left(\frac{y\,,\,K(\sqrt[m]{x}\,)/K}{v}\right)\sqrt[m]{x}\Big/\sqrt[m]{x}\in\mu(K)$$

for all $x,\ y \in K^\times$, then this defines $\left(\frac{\bullet\,,\,\bullet}{v}\right)$, which we call the v-Hilbert symbol of K (defined on $K^\times \times K^\times$); its order m is maximal. We then have the simpler expression:

$$\prod_{v \in Pl^{\rm nc}} \left(\frac{x\,,\,y}{v}\right) = 1, \text{ for all } x,\ y \in K^\times,$$

which is called the product formula for Hilbert symbols on K. □

Note. Do not confuse the symbol $(\bullet,\ \bullet)_v$ defined on K_v with values in $\mu(K_v)$, with the symbol $\left(\frac{\bullet\,,\,\bullet}{v}\right)$ defined on K with values in $\mu(K)$. We have:

$$i_v \circ \left(\frac{\bullet\,,\,\bullet}{v}\right) = (\bullet,\ \bullet)_v^{\frac{m_v}{m}} \circ i_v \ \text{ on } \ K^\times \times K^\times.$$

7.3.2 Exercise (prescribed Hilbert symbols). Let K be a number field and let $m := |\mu(K)|$.

(i) For $i = 1, \dots, r$, let a_i be fixed elements of $K^\times$, and let $(\zeta_{i,v})_v$ with $\zeta_{i,v} \in \mu(K)$ be r families with finite support in $Pl^{\rm nc}$; assume that for each $v \in Pl^{\rm nc}$ there exists $x(v) \in K^\times$ such that:

$$\left(\frac{a_i\,,\,x(v)}{v}\right) = \zeta_{i,v}, \quad i = 1, \dots, r,$$ [46]

and assume (product formula!) that:

$$\prod_v \zeta_{i,v} = 1, \quad i = 1, \dots, r.$$

Show that there exists $x \in K^\times$ such that for all $v \in Pl^{\rm nc}$:

$$\left(\frac{a_i\,,\,x}{v}\right) = \zeta_{i,v}, \quad i = 1, \dots, r.$$

(ii) Deduce the Hasse–Minkowski theorem for quadratic forms in four variables over K (hint: let $a\,Y^2 + b\,Z^2 - (c\,T^2 + d\,U^2)$, a, b, c, $d \in K^\times$, be such a quadratic form; check that there exists $x \in K^\times$ for which $x\,X^2 - a\,Y^2 - b\,Z^2$ and $x\,X^2 - c\,T^2 - d\,U^2$ represent 0 in K).

Answer. (i) Let $A := \langle a_1, \dots, a_r \rangle$, $L := K(\sqrt[m]{A})$, and $G := \mathrm{Gal}(L/K)$. Denote by $s_v \in G$ the Hasse symbol $\left(\frac{x(v)\,,\,L/K}{v}\right)$; we thus have $s_v \in D_v := D_v(L/K)$. We have:

$$s_v(\sqrt[m]{a_i}) = \left(\frac{x(v)\,,\,K(\sqrt[m]{a_i})/K}{v}\right)\sqrt[m]{a_i} = \zeta_{i,v}\,\sqrt[m]{a_i}$$

[46] A necessary condition is that the order of $\zeta_{i,v}$ must be a divisor of that of the decomposition group of v in $K(\sqrt[m]{a_i})/K$ since this decomposition group is an image under the Hasse symbol and that $K(\sqrt[m]{a_i})/K$ is cyclic; it is sufficient only for $r = 1$: for $K = \mathbb{Q}(\sqrt{-1})$, $v|2$, $a_1 = 2$, $a_2 = -2$, $\zeta_{1,v} = -1$, $\zeta_{2,v} = 1$, $x(v)$ does not exist.

for all v and $i = 1, \dots, r$, so that $(s_v)_v$ has finite support. Set $s := \prod_v s_v$; we easily obtain $s(\sqrt[m]{a_i}) = \left(\prod_v \zeta_{i,v}\right)\sqrt[m]{a_i} = \sqrt[m]{a_i}$, $i = 1, \dots, r$, hence $s = 1$. We can thus apply Theorem 3.4.4 on the converse of the product formula, and so there exists $x \in K^\times$ such that:

$$\left(\frac{x\,,\, L/K}{v}\right) = s_v$$

for all $v \in Pl^{\mathrm{nc}}$. By construction we immediately have:

$$\left(\frac{a_i\,,\, x}{v}\right) = s_v(\sqrt[m]{a_i})/\sqrt[m]{a_i} = \zeta_{i,v}, \quad i = 1, \dots, r$$

for all $v \in Pl^{\mathrm{nc}}$.

(ii) Consider the quadratic form:

$$(q) \qquad aY^2 + bZ^2 - (cT^2 + dU^2), \quad a,\ b,\ c,\ d \in K^\times,$$

and assume that it represents 0 in all the K_v. For all v there exist y_v, z_v, t_v, $u_v \in K_v$ (not all zero) such that:

$$x_v := ay_v^2 + bz_v^2 = ct_v^2 + du_v^2,$$

in K_v (we have omitted the embeddings i_v).

If $x_v = 0$, it is easy to see that the forms $aY^2 + bZ^2$ and $cT^2 + dU^2$ represent any element of K_v, so we can find a solution $y'_v,\ z'_v,\ t'_v,\ u'_v$ which yields $x_v = 1$, which we will now assume (for instance, since y_v and t_v cannot be equal to zero, we take $y'_v := (a^{-1} + 1)/2$, $t'_v := (c^{-1} + 1)/2$, $z'_v := z_v(a^{-1} - 1)/2y_v$, and $u'_v := u_v(c^{-1} - 1)/2t_v$).

Since $ax_v = (ay_v)^2 + abz_v^2$, we have (see 6.4):

$$1 = (ax_v,\, -ab)_v = (a,\, -a)_v(a,\, b)_v(x_v,\, -ab)_v,$$

so that we obtain:

$$(-ab,\, x_v)_v = (a,\, b)_v =: \left(\frac{a,\, b}{v}\right)$$

for all v, and similarly:

$$(-cd,\, x_v)_v = (c,\, d)_v =: \left(\frac{c,\, d}{v}\right).$$

For all v set:

$$\zeta_{1,v} := (-ab,\, x_v)_v, \quad \zeta_{2,v} := (-cd,\, x_v)_v,$$

which satisfies the first assumption of (i) with $a_1 = -ab$, $a_2 = -cd$, for the $\zeta_{i,v}$, $i = 1, 2$ (the fact that $x_v \in K_v^\times$ does not matter since there also exists $x(v) \in K^\times$ by approximation at v). Since for all v:

$$(-ab,\, x_v)_v = \Big(\frac{a,\, b}{v}\Big),\quad (-cd,\, x_v)_v = \Big(\frac{c,\, d}{v}\Big),$$

by the product formula we have:

$$\prod_v \zeta_{1,v} = \prod_v \Big(\frac{a,\, b}{v}\Big) = 1,\quad \prod_v \zeta_{2,v} = \prod_v \Big(\frac{c,\, d}{v}\Big) = 1.$$

It follows that there exists $x \in K^\times$ such that:

$$\Big(\frac{-ab,\, x}{v}\Big) = \Big(\frac{a,\, b}{v}\Big) = \Big(\frac{-ab,\, a}{v}\Big)^{-1},\quad \Big(\frac{-cd,\, x}{v}\Big) = \Big(\frac{c,\, d}{v}\Big) = \Big(\frac{-cd,\, c}{v}\Big)^{-1}$$

for all v, which can also be written:

$$\Big(\frac{-ab,\, ax}{v}\Big) = 1,\quad \Big(\frac{-cd,\, cx}{v}\Big) = 1$$

for all v. The forms $xX^2 - aY^2 - bZ^2$ and $xX^2 - cT^2 - dU^2$ thus represent 0 in all the K_v and hence in K. The result follows by equality of the two expressions for x which one obtains from this.

Beware that we are not allowed to exclude a place in the statement; for example, for $K = \mathbb{Q}$:

$$Y^2 + Z^2 + 3T^2 + 5U^2$$

represents 0 in all the completions of $\mathbb{Q}$ except in $\mathbb{R}$. Indeed, for $\ell \neq 2$ the given form represents 0 in $\mathbb{Q}_\ell$ (in each case, we put a suitable variable T or U equal to zero, and write that -5 or -3 is a norm in $\mathbb{Q}_\ell(\sqrt{-1}\,)/\mathbb{Q}_\ell$ since it is then a unit in an unramified local extension). For $\ell = 2$, we check that -3 is a norm in $\mathbb{Q}_2(\sqrt{-1}\,)/\mathbb{Q}_2$ (the norm group is $\langle\, 2\,\rangle \oplus \langle\, 5\,\rangle_{\mathbb{Z}_2}$ and $-3 = 5^u$ for $u \equiv -1 \bmod (4)$). □

7.4 Power Residue Symbol, nth Power Reciprocity Law. Let K be a number field, m the order of $\mu(K)$ and n a divisor of m. We have just defined the v-Hilbert symbol of K:

$$\begin{array}{rccc} \Big(\frac{\bullet,\, \bullet}{v}\Big) \;:\; K^\times \times K^\times & \longrightarrow & \mu(K) \\ (x\,,\, y) & \longmapsto & i_v^{-1}\Big(\big(i_v(x)\,,\, i_v(y)\big)_v^{\frac{m_v}{m}}\Big) \end{array}$$

which is essentially the same as the local Hilbert symbol of order m restricted to $i_v(K)$, and which is also given by the action of the Hasse symbol $\Big(\frac{y\,,\, K(\sqrt[m]{x}\,)/K}{v}\Big)$ on $\sqrt[m]{x}$. We will be using the Hilbert symbol of order n:

$$\Big(\frac{\bullet,\, \bullet}{v}\Big)_n := \Big(\frac{\bullet,\, \bullet}{v}\Big)^{\frac{m}{n}}.$$

7.4.1 Definition. For $x \in K^\times$, we denote by R_x the set of finite places of K which are ramified in $K(\sqrt[n]{x}\,)/K$ (R_x, which depends on n, is contained

in the set of places v such that $\mathrm{v}(x) \not\equiv 0 \bmod (n)$, or dividing n). For $v \notin R_x$ we define via the Frobenius symbol:

$$\Big(\frac{x}{v}\Big)_n := \Big(\frac{K(\sqrt[n]{x})/K}{v}\Big)\sqrt[n]{x}\Big/\sqrt[n]{x}. \qquad \square$$

This defines an nth power residue symbol (including when $v \in Pl^{\mathrm{r}}_\infty$) since, if $v \notin R_x$, we have:

$$\Big(\frac{x}{v}\Big)_n = 1 \text{ if and only if } i_v(x) \in K_v^{\times n}.$$

7.4.2 Remarks. (i) If $v \notin R_x$ is a finite place, we also set $\Big(\frac{x}{v}\Big)_n =: \Big(\frac{x}{\mathfrak{p}_v}\Big)_n$, so that we can define by multiplicativity:

$$\Big(\frac{x}{\mathfrak{b}}\Big)_n := \prod_{v \in Pl_0} \Big(\frac{x}{v}\Big)_n^{\mathrm{v}(\mathfrak{b})} \text{ for all } \mathfrak{b} \in I_{R_x}.$$

Hence, in terms of Artin symbols, we have (since $\mu_n \subset K$):

$$\Big(\frac{x}{\mathfrak{b}}\Big)_n = \Big(\frac{K(\sqrt[n]{x})/K}{\mathfrak{b}}\Big)\sqrt[n]{x}\Big/\sqrt[n]{x}.$$

(ii) We can also define an idelic version $\Big(\frac{x}{(y_v)_v}\Big)_n$, in a completely clear and analogous way, so that, for all $y \in K^\times$ prime to R_x (identifying $i(y)$ with y) we get:

$$\Big(\frac{x}{y}\Big)_n := \prod_{v \in Pl^{\mathrm{nc}}} \Big(\frac{x}{v}\Big)_n^{\mathrm{v}(y)},$$

which thus involves the real infinite places. Note that in the literature, $\Big(\frac{x}{y}\Big)_n$ usually means $\Big(\frac{x}{(y)}\Big)_n$. $\square$

Note. If $n > 2$, $Pl^{\mathrm{r}}_\infty = \emptyset$ and the infinite places do not enter in the definition. If $n = 2$, $(\frac{x}{v}) = (-1)^{\mathrm{v}(x)}$, and the properties of the more general symbol may be easily deduced from the following.

7.4.3 Proposition. *We have the following functorial properties of the nth power residue symbol for $n|m := |\mu(K)|$, where x, y, are elements of $K^\times$:*

(i) $\Big(\frac{x}{\mathfrak{b}}\Big)_n\Big(\frac{y}{\mathfrak{b}}\Big)_n = \Big(\frac{x\,y}{\mathfrak{b}}\Big)_n$, *if* $\mathfrak{b} \in I_{R_x} \cap I_{R_y}$;

(ii) $\Big(\frac{x}{\mathfrak{b}}\Big)_n\Big(\frac{x}{\mathfrak{c}}\Big)_n = \Big(\frac{x}{\mathfrak{b}\,\mathfrak{c}}\Big)_n$, *if* $\mathfrak{b},\ \mathfrak{c} \in I_{R_x}$;

(iii) for any isomorphism τ of K we have $\Big(\frac{\tau(x)}{\tau(\mathfrak{b})}\Big)_n = \tau\Big(\frac{x}{\mathfrak{b}}\Big)_n$, *if* $\mathfrak{b} \in I_{R_x}$;

(iv) for any divisor d of n we have $\left(\frac{x}{\mathfrak{b}}\right)_n^d = \left(\frac{x}{\mathfrak{b}}\right)_{\frac{n}{d}}$, *if* $\mathfrak{b} \in I_{R_x}$;

(v) let L be a finite extension of K; we have $\left(\frac{x}{\mathfrak{b}'}\right)_{L,n} = \left(\frac{x}{\mathrm{N}_{L/K}(\mathfrak{b}')}\right)_n$, *if* $\mathfrak{b}' \in I_{L,R_x}$;

(vi) for any prime ideal $\mathfrak{p}$, prime to x and n, we have $\left(\frac{x}{\mathfrak{p}}\right)_n \equiv x^{\frac{\mathrm{N}\mathfrak{p}-1}{n}} \bmod \mathfrak{p}$;

(vii) let $N_x \subset I_{R_x}$ be the norm group corresponding to $K(\sqrt[n]{x})/K$; then, for $\mathfrak{b},\ \mathfrak{c} \in I_{R_x}$, *we have* $\left(\frac{x}{\mathfrak{b}}\right)_n = \left(\frac{x}{\mathfrak{c}}\right)_n$ *if and only if* $\mathfrak{b}\,\mathfrak{c}^{-1} \in N_x$;

(viii) for $v \notin R_x$, we have $\left(\frac{x\,,\,y}{v}\right)_n = \left(\frac{x}{v}\right)_n^{\mathrm{v}(y)}$ *for all* $y \in K^\times$.

Proof. Use properties 4.5 of the Artin map and/or properties 7.1.1 of the local Hilbert symbol, noting that $i_v\Big(\left(\frac{x}{v}\right)_n\Big) = \big(i_v(x)^{\frac{m_v}{n}},\, \pi_v\big)_v$ if $v \notin R_x$. □

Then we can state:

7.4.4 Theorem. *The nth power reciprocity law (n dividing $|\mu(K)|$) is given by the relation:*

$$\left(\frac{y}{x}\right)_n \left(\frac{x}{y}\right)_n^{-1} = \prod_{v|n} \left(\frac{x\,,\,y}{v}\right)_n$$

for all $x,\ y \in K^\times$, x and y coprime (i.e., for any place v, we have $\mathrm{v}(x) = 0$ or $\mathrm{v}(y) = 0$, including the case $v|\infty$ if $n = 2$) and prime to n.

Proof. We compute the left hand side by using the definition of the symbols $\left(\frac{\bullet}{\bullet}\right)_n$ and by noting that the products can be restricted to the places not dividing n (because of the relations $\mathrm{v}(x) = \mathrm{v}(y) = 0$ for $v|n$):

$$\left(\frac{y}{x}\right)_n \left(\frac{x}{y}\right)_n^{-1} = \prod_{v\nmid n} \left(\frac{y}{v}\right)_n^{\mathrm{v}(x)} \prod_{v\nmid n} \left(\frac{x}{v}\right)_n^{-\mathrm{v}(y)};$$

then, treating the cases $\mathrm{v}(x) \neq 0$ and $\mathrm{v}(y) \neq 0$ for $v \nmid n$ separately [47] and coming back to Hilbert symbols because of 7.4.3, (viii), this yields:

$$\left(\frac{y}{x}\right)_n \left(\frac{x}{y}\right)_n^{-1} = \prod_{\substack{v\nmid n \\ \mathrm{v}(x)\neq 0}} \left(\frac{y\,,\,x}{v}\right)_n \prod_{\substack{v\nmid n \\ \mathrm{v}(y)\neq 0}} \left(\frac{x\,,\,y}{v}\right)_n^{-1} = \prod_{\substack{v\nmid n \\ \mathrm{v}(xy)\neq 0}} \left(\frac{y\,,\,x}{v}\right)_n = \prod_{v\nmid n} \left(\frac{y\,,\,x}{v}\right)_n$$

since $\left(\frac{y\,,\,x}{v}\right)_n = 1$ if $\mathrm{v}(xy) = 0$, $v \nmid n$; the theorem follows by using the product formula. □

[47] The case $\mathrm{v}(x) \neq 0$ implies $\mathrm{v}(y) = 0$ and, since $v \nmid n$, this yields $v \notin R_y$; the case $\mathrm{v}(y) \neq 0$ is symmetrical.

The nth power reciprocity law for the number field K is thus explicit as soon as the right hand side is computed. Because of 7.5 below and the continuity of the Hilbert symbols, using suitable representatives $x,\ y \in K^\times$ of the finite groups $U_v/(U_v)^n$, $v|n$, we only need a *finite number* of numerical computations (once for all). We thus obtain in particular the quadratic reciprocity law of Jacobi ($K = \mathbb{Q}$, $n = 2$; the signed form that we have obtained being a slight generalization) by checking that:

$$\Big(\frac{y}{x}\Big)\Big(\frac{x}{y}\Big) = \Big(\frac{x\,,\,y}{2}\Big)_2 = \Big(-1\Big)^{\frac{x-1}{2}\frac{y-1}{2}}$$

for all rational $x,\ y$, coprime, odd, not both negative (see 6.4, (v)).

7.4.5 Remark. The above formula is false when the rationals x and y are both negative; for example we have:

$$\Big(\frac{-3}{-5}\Big)\Big(\frac{-5}{-3}\Big) = \Big(\frac{-3}{\infty}\Big)\Big(\frac{-3}{5}\Big)\Big(\frac{-5}{\infty}\Big)\Big(\frac{-5}{3}\Big) = \Big(\frac{15}{\infty}\Big)\Big(\frac{-3}{5}\Big)\Big(\frac{-5}{3}\Big) = -1,$$

although $\frac{x-1}{2}\frac{y-1}{2} = 6$ which would give the value $+1$; in the general case for $K = \mathbb{Q}$, we must multiply the right hand side of the formula by $(-1)^{\mathrm{v}(x)\mathrm{v}(y)} = \big(-1\big)^{\frac{\mathrm{sgn}(x)-1}{2}\frac{\mathrm{sgn}(y)-1}{2}}$, where v is the valuation corresponding to $v = \infty$. □

7.4.6 Proposition. *If $z \in K^\times$ is such that $\mathrm{v}(z) = 0$ for any place v not dividing n, and if $x \in K^\times$ is prime to n, we have the supplementary formula:*

$$\Big(\frac{z}{x}\Big)_n = \prod_{v|n}\Big(\frac{x\,,\,z}{v}\Big)_n.$$

Proof. We have:

$$\Big(\frac{z}{x}\Big)_n = \prod_v \Big(\frac{z}{v}\Big)_n^{\mathrm{v}(x)} = \prod_{v\nmid n} \Big(\frac{z}{v}\Big)_n^{\mathrm{v}(x)} = \prod_{v\nmid n}\Big(\frac{z\,,\,x}{v}\Big)_n = \prod_{v|n}\Big(\frac{x\,,\,z}{v}\Big)_n. \qquad \square$$

This can be applied to $K = \mathbb{Q}$ and the quadratic case to prove that:

$$\Big(\frac{2}{x}\Big)_2 = \Big(\frac{x\,,\,2}{2}\Big)_2 = \Big(-1\Big)^{\frac{x^2-1}{8}},$$

for any odd rational x.

For additional material on these reciprocity laws aspects, see [a, Ko1], [f, Lem1], [Kub2], [KubO], [Wy].

7.5 Computation of a Hilbert Symbol by Global Means. As already mentioned in 1.6.8, assume that we want to compute a local Hilbert symbol

$(x\,,\,y)$ of order n, with $x,\ y \in k^\times$, where k is a finite extension of $\mathbb{Q}_\ell$ containing the group μ_n of nth roots of unity. The method consists in looking for a number field K containing μ_n, and such that $K_v = k$ for some place $v|\ell$ of K.

In general it is an irregular symbol (i.e., $\ell|n$), and by localizing the problem, we are reduced to the case where $n = \ell^h$ for $h \geq 1$. Then, if $(K,\, v|\ell)$ is a solution, we consider here K as a subfield of k and, by density, we are reduced to the case where $x,\ y \in K^\times$ (this only involves the properties of $k^\times$ deduced from the knowledge of $k^\times/k^{\times \ell^h}$); we then have $(x\,,\,y) = \left(\frac{x\,,\,y}{v}\right)$ which reduces to the computation of the Hasse symbol $\left(\frac{y\,,\,K(\sqrt[\ell^h]{x})/K}{v}\right)$.

We can even construct K containing μ_{ℓ^h} and having a *unique* ℓ-adic place v, in which case the Hilbert symbol $\left(\frac{x\,,\,y}{v}\right)$ can be computed, because of the product formula, by using only regular symbols: if $k =: \mathbb{Q}_\ell(\mu_{\ell^h})(\alpha)$, $\alpha \in \overline{\mathbb{Q}}_\ell$, of degree d over $\mathbb{Q}_\ell(\mu_{\ell^h})$, we may assume that $\alpha \in \overline{\mathbb{Q}}$ and that it has degree d over $\mathbb{Q}(\mu_{\ell^h})$ (Krasner's lemma proven and illustrated in [b, Rob, Ch. 3, § 1.5]), hence $K := \mathbb{Q}(\mu_{\ell^h})(\alpha)$ is a suitable field since $v|\ell$ is split neither in $K/\mathbb{Q}(\mu_{\ell^h})$ (by our choice of α) nor in $\mathbb{Q}(\mu_{\ell^h})/\mathbb{Q}$ (totally ramified). However, if this construction is numerically too delicate, it is still very much possible to compute the Hasse symbol $\left(\frac{y\,,\,L/K}{v}\right)$, with $L = K(\sqrt[\ell^h]{x}\,)$ for K containing μ_{ℓ^h}, if necessary by brutally adjoining these roots of unity, by the usual method explained in 4.4.3; in this case, we do not need to assume that $v|\ell$ is unique (and in general we cannot). We then obtain an Artin symbol of the form $\left(\frac{L/K}{\mathfrak{b}}\right)^{-1}$, for some ideal $\mathfrak{b}$ of K prime to a modulus $\mathfrak{m}$, multiple of the conductor of L/K, $\mathfrak{m}$ divisible by all the prime ideals dividing (x) and (ℓ), from which we obtain:

$$(x\,,\,y) = \left(\frac{L/K}{\mathfrak{b}}\right)^{-1} \sqrt[\ell^h]{x} \Big/ \sqrt[\ell^h]{x} = \left(\frac{x}{\mathfrak{b}}\right)_{\ell^h}^{-1},$$

in L/K. If $\mathfrak{p}$ is a prime ideal of K dividing $\mathfrak{b}$, by definition of a Frobenius, and since x and ℓ^h are prime to $\mathfrak{p}$, we know that:

$$\left(\frac{x}{\mathfrak{p}}\right)_{\ell^h} \equiv x^{\frac{q-1}{\ell^h}} \bmod \mathfrak{p},$$

where $q := \mathrm{N}\mathfrak{p}$, which identifies $\left(\frac{x}{\mathfrak{p}}\right)_{\ell^h}$ in μ_{ℓ^h} (global). We thus obtain $\left(\frac{x}{\mathfrak{b}}\right)_{\ell^h}$ by multiplicativity.

If we are *a priori* in a given (global) field K containing μ_{ℓ^h}, and that we want to compute $\left(\frac{x\,,\,y}{v}\right)$, $x,\, y \in K^\times$, where $v|\ell$ is not unique, we can either use the Hasse symbol, or change the global field K (note that x and y must be reinterpreted in the new field by means of the common completion!). The reader can practice on the field $K := \mathbb{Q}\Big(\sqrt{-3+\sqrt{2}},\, \sqrt{-3-\sqrt{2}},\, \mu_8\Big)$.

Let us give an example in the nonsplit case so as to apply both points of view.

7.5.1 Example. Take $k = \mathbb{Q}_2(i)$, where $i = \sqrt{-1}$ and let us compute the symbol of order 4:

$$(6\,,\,3+i).$$

We will choose $K = \mathbb{Q}(i)$, $L = K(\sqrt[4]{6}\,)$ and begin by computing the Hasse symbol $\left(\frac{3+i\,,\,L/K}{v}\right)$, where v is the place of K above 2.

Since $6 = -3i(1+i)^2$, $K(\sqrt{6}\,) = K(\sqrt{-3i}\,)$, and by Kummer theory ($-3i \equiv i \bmod (4)$, which is not congruent to a square modulo (4)) we see that v is ramified in $K(\sqrt{6}\,)/K$, hence totally ramified in L/K. We then check that:

$$\pi = \frac{1+\sqrt{-3i}}{\sqrt[4]{6}} - 1$$

is a uniformizer of L_v. Using the higher ramification groups we find (by computing the valuations of $\pi^{\sigma-1}$ and π^{σ^2-1} for a generator σ of $\mathrm{Gal}(L/K)$) that the conductor of L/K is equal to (24) (see 1.6.2). We then look for $y' \in K$ such that:

$$\frac{y'}{3+i} \equiv 1 \bmod (8)$$
$$y' \equiv 1 \bmod (3),$$

and we obtain for instance $y' = -5 + 9i = (1+i)(2+7i)$ which yields $\mathfrak{b} = (2+7i)$ (a prime ideal above 53). Thus, we have $\left(\frac{6}{\mathfrak{b}}\right)_4 \equiv 6^{13} \equiv -1$ modulo $\mathfrak{b}$; hence:

$$(6\,,\,3+i) = (-1)^{-1} = -1.$$

Beware that if $\mathfrak{b}$ is not a prime ideal, we must come back to the $\left(\frac{x}{\mathfrak{p}}\right)_4$ for $\mathfrak{p}|\mathfrak{b}$, and conclude by multiplicativity.

The product formula is here reduced to (using prime ideals instead of places):

$$\left(\frac{3+i,\,L/K}{\mathfrak{p}_2}\right)\left(\frac{3+i,\,L/K}{\mathfrak{p}_5}\right)\left(\frac{3+i,\,L/K}{(3)}\right) = 1,$$

where $\mathfrak{p}_2 = (1+i)$, $\mathfrak{p}_5 = (2-i)$, which can be written:

$$\left(\frac{6,\,3+i}{\mathfrak{p}_2}\right)\left(\frac{6,\,3+i}{\mathfrak{p}_5}\right)\left(\frac{6,\,3+i}{(3)}\right) = 1,$$

in terms of Hilbert symbols of order 4. But the computation of regular symbols yields:

$$\left(\frac{6,\,3+i}{\mathfrak{p}_5}\right) \equiv 6^1 \equiv 1 \bmod \mathfrak{p}_5,$$
$$\left(\frac{6,\,3+i}{(3)}\right) \equiv ((3+i)^{-1})^2 \equiv -1 \bmod (3),$$

giving once again the result in a nicer way.

However the first method is useful when x $(= 6)$ is fixed and y varies: setting $y =: (1+i)^m z$, $m \in \mathbb{Z}$, z prime to $\mathfrak{p}_2$, and using the chinese remainder theorem, we obtain the general solution:

$$\mathfrak{b} =: (z'), \quad z' := 9z - 8(i-1)^m,$$

where z' is defined modulo (24). The solution is then given by the Artin symbol:

$$\left(\frac{L/K}{(z')}\right)^{-1}.$$

Thus, let $A \subset I_T$ for $T = \{\mathfrak{p}_2, (3)\}$ be the Artin group of $K(\sqrt[4]{6}\,)$; we check that $I_T = \langle\, \mathfrak{p}_{13} \,\rangle\, A$, for $\mathfrak{p}_{13} := (3+2i)$, whose Frobenius sends $\sqrt[4]{6}$ to $-i\,\sqrt[4]{6}$, so that $(6,\, y) = 1,\ -1,\ i,\ -i$, according to whether:

$$(z') \in A,\ (3+2i)^2\, A,\ (3+2i)\, A,\ (3+2i)^3\, A = (3-2i)\, A.$$

If $y = 9 + 32i$, we find $z' \equiv 1 \bmod (24)$, hence $(6,\, y) = 1$, although method using the product formula needs the computation of four regular symbols. The generalized class group $I_T/P_{T,(24)}$ has order 64, so that $A/P_{T,(24)}$ has order 16 and can easily be computed.

Finally, since any class modulo $P_{T,(24)}$ contains an infinity of prime ideals, we can look for $\mathfrak{b} =: \mathfrak{q}$ prime, and then $(6,\, y)$ is given by the residual image of $\left(6^{\frac{\mathrm{N}\mathfrak{q}-1}{4}}\right)^{-1} \bmod \mathfrak{q}$. For example, if $y = 3 + 2i$ then $z' = 19 + 18i$ which is composite, but $z' - 24(1+i) = -5 - 6i$ yields $\mathfrak{p}_{61}$, and $(6^{15})^{-1} \equiv 11 \bmod \mathfrak{p}_{61}$ implies that $(6,\, 3+2i) = -i$. □

Note that the case $n = 2$ is particularly simple since K is easier to find and that all the computations lead to quadratic residue symbols.

Let us come back to the general theory of symbols for a number field K. The homomorphism:

$$h : \mathrm{K}_2(K) \longrightarrow \bigoplus_{v \in Pl^{\mathrm{nc}}} \mu(K_v)$$

which comes from the global Hilbert symbol (see 7.2.2, (ii)) is therefore the most precise possible for identifying $\mathrm{K}_2(K)$ as a function of known symbols. The two main questions which can be asked about h are what are its kernel and image. One is deep (Garland's theorem given in 1971 in [Ga], for the

finiteness of the kernel, which we will assume), the other is a nontrivial application of the techniques of class field theory that we have developed. This is Moore's theorem on the characterization of the image, which we are going to prove by following a paper of Jaulent written in [Ja1] from the paper [ChaW] of Chase–Waterhouse; see also [Mil, Th. 16.1]. With the above notations and definitions 7.1.3, 7.2.2, we can then state:

7.6 Theorem (fundamental diagram of the K_2 (1971/1972)). *We have, for any number field K, the following commutative diagram:*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{WK}_2(K) & \longrightarrow & \mathrm{K}_2(K) & \xrightarrow{h} & \bigoplus_{v\in Pl^{\mathrm{nc}}} \mu(K_v) & \xrightarrow{\pi} & \mu(K) \longrightarrow 1 \\ & & \big\downarrow & & \big\| & & \big\downarrow{\scriptstyle \oplus m_v^1} & & \big\downarrow{\scriptstyle m} \\ 1 & \longrightarrow & \mathrm{R}_2^{\mathrm{ord}}(K) & \longrightarrow & \mathrm{K}_2(K) & \xrightarrow{h^{\mathrm{reg}}} & \bigoplus_{v\in Pl^{\mathrm{nc}}} \mu(K_v)^{\mathrm{reg}} & \longrightarrow & 1 \end{array}$$

where $\pi((\xi_v)_v) := \prod_v i_v^{-1}\big(\xi_v^{\frac{m_v}{m}}\big)$ *for all* $(\xi_v)_v \in \bigoplus_{v\in Pl^{\mathrm{nc}}} \mu(K_v)$, $m := |\mu(K)|$, $m_v := |\mu(K_v)|$, $m_v^1 := |\mu(K_v)^1| = \dfrac{m_v}{q_v - 1}$ *for v finite, and where* $\mathrm{WK}_2(K)$ *(resp.* $\mathrm{R}_2^{\mathrm{ord}}(K)$*) denotes the kernel of the global Hilbert symbol h (resp. of the global regular Hilbert symbol h^{reg}).*

Proof. The crucial point is to show that the set of families:

$$(\xi_v)_v \in \bigoplus_{v\in Pl^{\mathrm{nc}}} \mu(K_v),$$

such that $\prod_v i_v^{-1}\big(\xi_v^{\frac{m_v}{m}}\big) = 1$, is contained in the image of h. By localizing the problem, we can fix a prime number p and reduce to families in $\bigoplus_{v\in Pl^{\mathrm{nc}}} \mu_p(K_v)$ satisfying the product formula. Denote by Σ the set formed by the places of K dividing p, the real infinite places, and the irregular places (i.e., the places v such that $m_v^1 \neq 1$) (Σ is finite).

Thus, let $(\xi_v)_v \in \bigoplus_{v\in Pl^{\mathrm{nc}}} \mu_p(K_v)$ such that $\prod_v i_v^{-1}\big(\xi_v^{\frac{m_v}{m}}\big) = 1$. The first step consists in reducing to a situation where the (bad) places of Σ do not occur. For each $v \in \Sigma$, there exist $x_v,\ y_v \in K_v^\times$ such that $(x_v\,,\, y_v)_v = \xi_v$ (we choose x_v such that $K_v(\sqrt[m_v]{x_v})/K_v$ has degree m_v, and we use the surjectivity of the norm residue symbol to find y_v). By approximation on Σ, we can find $x,\ y \in K^\times$ such that:

$$(i_v(x)\,,\, i_v(y))_v = (x_v\,,\, y_v)_v = \xi_v \text{ for all } v \in \Sigma.$$

Since $h(\{x\,,\, y\})$ belongs to a direct sum, replacing if necessary x (for example) by a suitable power (prime to p), we may assume that $h(\{x\,,\, y\}) \in$

$\bigoplus_{v\in Pl^{\rm nc}}\mu_p(K_v)$ and that, on Σ, we still have $(i_v(x)\,,\,i_v(y))_v=\xi_v$. If we consider:

$$(\xi'_v)_v:=\frac{(\xi_v)_v}{h(\{x\,,\,y\})},$$

it is an element of $\bigoplus_{v\in Pl^{\rm nc}}\mu_p(K_v)$ satisfying the product formula, and it is such that $\xi'_v=1$ for all $v\in\Sigma$. Hence, for the support Σ' of $(\xi'_v)_v$ the Hilbert symbols are regular, and we are going to obtain the equality $h(\{x'\,,\,y'\})=(\xi'_v)_v$ for suitable x' and y' in $K^\times$.

For $e:={\rm v}_p(m)\geq 0$, consider now the cyclotomic field $K_{e+1}:=K(\zeta_{e+1})$, where as usual ζ_{e+1} is a primitive p^{e+1}th root of unity; it is a nontrivial cyclic extension of K (of degree p if $e\geq 1$, of degree dividing $p-1$ if $e=0$). Let:

$$\mathfrak{a}':=\prod_{v\in\Sigma'}\mathfrak{p}_v,$$

which is an ideal of K prime to p (since $\xi'_v\neq 1$ implies that $v\notin\Sigma$), hence prime to the ramified places of K_{e+1}/K. By the Čebotarev Theorem 4.6, there exists a prime ideal $\mathfrak{q}$ of K, prime to $\Sigma\cup\Sigma'$, such that the Artin symbol $\left(\frac{K_{e+1}/K}{\mathfrak{a}'\mathfrak{q}}\right)$ generates ${\rm Gal}(K_{e+1}/K)$. Since on Σ' we have regular symbols, we have:

$$(\xi'_v\,,\,\pi_v)_v=\xi'_v \text{ for all } v\in\Sigma',$$

the result being independent of the choice of a uniformizer π_v of K_v (see 7.1.5). By approximation on $\Sigma'\cup\{\mathfrak{q}\}$, we can find $x'\in K^\times$ such that:

$$x'\equiv 1 \bmod \mathfrak{q},$$

$$i_v(x')\,\xi'^{-1}_v\in U^1_v \text{ for all } v\in\Sigma'.$$

We then have (again by 7.1.5):

$$(i_v(x')\,,\,\pi_v)_v=(\xi'_v\,,\,\pi_v)_v=\xi'_v \text{ for all } v\in\Sigma'.$$

Let T be the union of $\Sigma_0:=\Sigma\cap Pl_0$ with the set of finite places dividing x' (T is prime to $\mathfrak{q}$ and to Σ'). Consider the modulus $\mathfrak{n}=\prod_{v\in T}\mathfrak{p}_v^n$, for a sufficiently large integer n (in particular, we can assume that $\mathfrak{n}$ is a multiple of the conductor of K_{e+1}/K). By the Čebotarev theorem, there exists a prime ideal $\mathfrak{l}$ prime to $T\cup\Sigma'$ and such that $cl^{\rm res}_{\mathfrak{n}}(\mathfrak{l})=cl^{\rm res}_{\mathfrak{n}}(\mathfrak{a}'\mathfrak{q})$, in $\mathcal{C}l^{\rm res}_{\mathfrak{n}}$, so that we can write:

$$\mathfrak{a}'\mathfrak{q}=\mathfrak{l}\,(y'),\quad y'\in K^\times_{T,\mathfrak{n},{\rm pos}}.$$

Now consider $h(\{x'\,,\,y'\})=\big((i_v(x')\,,\,i_v(y'))_v\big)_v$:

- if v is an infinite place, we have $(i_v(x')\,,\,i_v(y'))_v=1$ since $i_v(y')>0$;
- if $v\in\Sigma'$, because of the congruences imposed on x', we have:

$$(i_v(x')\,,\,i_v(y'))_v=(\xi'_v\,,\,i_v(y'))_v,$$

but $i_v(y')$ is a uniformizer of K_v since $\mathrm{v}(y') = \mathrm{v}(\mathfrak{a}') = 1$, and by what we have seen above:

$$(i_v(x')\,,\, i_v(y'))_v = \xi'_v\ ;$$

- if v corresponds to $\mathfrak{q}$, we obtain $(i_v(x')\,,\, i_v(y'))_v = 1$ since we have chosen $x' \equiv 1 \bmod \mathfrak{q}$;
- if $v \in T$ (the symbol is then not necessarily regular), we have $(i_v(x')\,,\, i_v(y'))_v = 1$ since $i_v(y') \in U_v^n$ (a local norm for n sufficiently large);
- if v is none of the above and if v does not correspond to $\mathfrak{l}$, we have $(i_v(x')\,,\, i_v(y'))_v = 1$ since $i_v(x')$ and $i_v(y')$ are local units by definition of T and y', and the symbol is regular;
- finally, assume that v is the place corresponding to $\mathfrak{l}$; we have:

$$\left(\frac{K_{e+1}/K}{\mathfrak{a}'\mathfrak{q}}\right) = \left(\frac{K_{e+1}/K}{\mathfrak{l}}\right)\left(\frac{K_{e+1}/K}{(y')}\right) = \left(\frac{K_{e+1}/K}{\mathfrak{l}}\right)$$

since by assumption $y' \equiv 1 \bmod \mathfrak{n}$, and $\mathfrak{n}$ is a multiple of the conductor of K_{e+1}/K. Hence, $\left(\frac{K_{e+1}/K}{\mathfrak{l}}\right) = \left(\frac{K_{e+1}/K}{\mathfrak{a}'\mathfrak{q}}\right)$ is by assumption a generator of $\mathrm{Gal}(K_{e+1}/K)$, which shows that $\mathfrak{l}$ is not split in K_{e+1}/K, hence that K_v does not contain ζ_{e+1}, or, equivalently that $\mathrm{v}_p(\frac{m_v}{m}) = 0$. Since $\frac{m_v}{m}$ is a p-adic unit, we deduce from this and the product formula that $(i_v(x')\,,\, i_v(y'))_v = 1$.

We have thus proved the first exact sequence of the diagram.

The surjectivity of h^{reg} is equivalent to the fact that any element of $\bigoplus_{v\in Pl^{\mathrm{nc}}} \mu(K_v)^{\mathrm{reg}}$ (which can be written $\left((\zeta_v^{\mathrm{reg}})^{m_v^1}\right)_v$ since m_v^1 is prime to the order of ζ_v^{reg}) is the image under the surjection $\oplus m_v^1$ of an element $(\zeta_v)_v =: (\zeta_v^{\mathrm{reg}}\,.\,\zeta_v^1)_v$ of $\bigoplus_{v\in Pl^{\mathrm{nc}}} \mu(K_v)$ satisfying the product formula. Since the component $(\zeta_v^1)_v$ belongs to the kernel of $\oplus m_v^1$, it is sufficient to check that it is possible to find it so that $(\zeta_v)_v \in \mathrm{Ker}(\pi)$, and this is equivalent to be able to solve, for any $\zeta \in \mu(K)$:

$$\prod_v i_v^{-1}(\zeta_v^1)^{\frac{m_v}{m}} = \zeta, \quad \text{with } (\zeta_v^1)_v \in \bigoplus_{v\in Pl^{\mathrm{nc}}} \mu(K_v)^1.$$

Let us localize at a prime divisor p of m (the case $p \nmid m$ being trivial), take $\zeta \in \mu_p(K)$, and consider $v_0|p$; the inclusion $i_{v_0}(\mu_p(K)) \subseteq \mu(K_{v_0})^1$ shows that, taking the p-parts:

$$\left(\frac{m_{v_0}}{m}\right)_p = \frac{m_{v_0}^1}{m_p},$$

and implies the existence of $\zeta_{v_0}^1$ such that $(\zeta_{v_0}^1)^{\frac{m_{v_0}}{m}} = i_{v_0}(\zeta)$; we then set $\zeta_v^1 = 1$ for all $v \neq v_0$.

This proves the two exact sequences of the diagram. □

The snake lemma applied to the fundamental diagram yields:

7.6.1 Corollary. *We have the exact sequence:*

$$1 \longrightarrow \mathrm{R}_2^{\mathrm{ord}}(K)/\mathrm{WK}_2(K) \xrightarrow{\alpha} \bigoplus_v \mu(K_v)^1 \xrightarrow{\beta} \mu(K) \longrightarrow 1,$$

in which α is obtained from the restriction of h to $\mathrm{R}_2^{\mathrm{ord}}(K)$ and β is the restriction of π to $\bigoplus_v \mu(K_v)^1$. Thus $(\mathrm{R}_2^{\mathrm{ord}}(K) : \mathrm{WK}_2(K)) = \frac{1}{m} \prod_v m_v^1$. □

This result indicates that everything can be reduced to the fundamental invariant $\mathrm{WK}_2(K)$, even though $\mathrm{R}_2^{\mathrm{ord}}$ can be more easily interpreted arithmetically (see below).

We note that $\mathrm{WK}_2(K) = \mathrm{R}_2^{\mathrm{ord}}(K)$ if and only if for all prime number p:

$$\mu_p(K) \simeq \bigoplus_{v|p} \mu_p(K_v) \ ;$$

for applying this, it is sufficient to check the primes p for which there exists an irregular place $v|p$. We will often encounter this condition (see for example III.4.2.5).

7.6.2 Definitions (Hilbert and regular kernels). The kernel of h (denoted $\mathrm{H}_2(K)$ or $\mathrm{WK}_2(K)$) is called the Hilbert or wild kernel (in $\mathrm{K}_2(K)$) [48], and the kernel of h^{reg} (denoted $\mathrm{R}_2^{\mathrm{ord}}(K)$), is called the regular or tame kernel. □

Recall that $\mathrm{R}_2^{\mathrm{ord}}(K)$ is also equal to $\mathrm{K}_2^{\mathrm{ord}}(Z_K)$ and that this interpretation of "$\mathrm{R}_2(K)$" as the K_2 of the ring of integers Z_K of K is due to Quillen (1973) and must be understood with the language of the general K-theory of rings (see an arithmetic study of the regular and Hilbert kernels in [Keu1], as a prelude to numerous developments on this subject).

7.6.3 Remarks. (i) The notation $\mathrm{R}_2^{\mathrm{ord}}(K) = \mathrm{K}_2^{\mathrm{ord}}(Z_K)$ represents the modification (introduced in 1986 in [Gr6]) coming from the consideration of the real places at infinity in the definition of h^{reg}; in other words, the classical kernel $\mathrm{R}_2(K) = \mathrm{K}_2(Z_K)$ must be understood as $\mathrm{R}_2^{\mathrm{res}}(K) = \mathrm{K}_2^{\mathrm{res}}(Z_K)$, which fortunately is compatible with the general system of notations that we have adopted here. The difference between these two definitions is given precisely by the following trivial exact sequence:

$$1 \longrightarrow \mathrm{K}_2^{\mathrm{ord}}(Z_K) \longrightarrow \mathrm{K}_2(Z_K) \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{r_1} \longrightarrow 1,$$

but the existence of $\mathrm{K}_2^{\mathrm{ord}}(Z_K)$ (and also probably the existence of more general groups of the form $\mathrm{K}_2^S(Z_{K,T})$ for our usual sets of places T and S, $Z_{K,T}$ being the ring of T-integers of K) is essential.

(ii) The equality $\pi \circ h = 1$ follows of course from the product formula 7.3 for Hilbert symbols, but the exactness that is obtained (Moore's theorem)

[48] The notation WK_2 is to be preferred, instead of H_2, to avoid confusion with homology groups, but we will continue to speak of the Hilbert kernel.

says that this product formula is the unique relation between Hilbert symbols. This property is called "uniqueness of reciprocity laws".

(iii) The existence of $\mathrm{WK}_2(K)$ (a finite group which is in general nontrivial) means that there can exist symbols on K which do not come from Hilbert symbols (and called exotic symbols because of this) [49]; but, although class field theory gives quite good information on these kernels (see below), up to now it has not been possible to exhibit (numerically) a single exotic symbol!

It is easy to find fields for which $\mathrm{WK}_2(K) \neq 1$; for instance, we have $\{-1,-1\} \neq 1$ in $\mathrm{WK}_2(K)$ if $K = \mathbb{Q}(\sqrt{d}\,)$, $d<0$, $d \equiv 2 \bmod (16)$ (see [Keu2]). On the contrary, it is more difficult to characterize the cases where, for a given p, the p-Sylow subgroup of this kernel is trivial. See for example the results of Kolster–Movahhedi in [KM1] dealing (after a few particular cases of Thomas) with the case of biquadratic fields for $p=2$, the case of quadratic fields having been treated before by Browkin–Schinzel, then revisited by Jaulent–Soriano. Many other papers are concerned with the case $p=2$ (Conner–Hurrelbrink, Candiotti–Kramer, Berger, Hettling, Hutchinson, ...).

In [KM2] is given a characterization of the p-extensions of $\mathbb{Q}$ such that the p-Sylow subgroup of the Hilbert kernel is trivial ($p \neq 2$).

In [Sor] is given an approach of the structure of the Hilbert kernel in a Kummer situation. □

Thus many new questions related to the K-theory of number fields can be asked, which are not the subject of this book. However, we will mention some of the most classical results, since as mentioned in the introduction to this section, they involve invariants which are directly linked with class field theory (in particular through the reflection theorem).

7.7 Links Between Class Field Theory and $\mathrm{K}_2(K)$. The relationships which exist between these K-theory kernels and class field theory are the following.

7.7.1 Logarithmic Class Group. Concerning $\mathrm{WK}_2(K)$, under the fundamental assumption $\mu_{2p} \subset K$, the results of Jaulent can be summarized by the relation:

$$\mathrm{WK}_2(K)/\mathrm{WK}_2(K)^p \simeq \mu_p \otimes \widetilde{\mathcal{C}\ell}_K,$$

where the p-group $\widetilde{\mathcal{C}\ell}_K$ (of logarithmic classes) is an invariant of class field theory, related to Gross's conjecture which we will state in III.4.13, which can be defined from the usual arithmetic of the number field K. [50] This represents the best practical approach to the Hilbert kernel since we have at our disposal

[49] Such an exotic symbol is given by $f \circ \{\bullet, \bullet\}$ for any group homomorphism $f : \mathrm{K}_2(K) \longrightarrow \bigoplus_v \mu(K_v)$, nontrivial on $\mathrm{WK}_2(K)$.

[50] [Ja4; Ja5; Ja6], [JaSor1], [JaSor2], [Sor], [JaMi], [JaMai].

the corresponding formalism, which is completely parallel with the (better-known) one for class groups "$\mathcal{C}\ell$" or (a little less known) for the torsion groups "$\mathcal{T}$". It is therefore possible to perform numerical computations (as in [DS]). See (Ch. III, § 7) for a direct approach of the definition of the logarithmic class group and the proof of the above property.

7.7.2 Tate's Results. For $\mathrm{R}_2^{\mathrm{ord}}(K)$, still when $\mu_p \subset K$, we have a Kummer interpretation coming from the results of Tate published in 1976 in [Ta2], which is given by the exact sequence:

$$1 \longrightarrow \mu_p \otimes \mathrm{N}_2(K) \longrightarrow \mu_p \otimes W_{K,Pl_p,\mathrm{pos}} \xrightarrow{f} {}_p\mathrm{R}_2^{\mathrm{ord}}(K) \longrightarrow 1,$$

where $W_{K,Pl_p,\mathrm{pos}} := \mathrm{Rad}(H^{\mathrm{ord}}_{Pl_p[p]}/K)$ is the radical of the maximal abelian p-ramified noncomplexified elementary p-extension of K, f being defined by:

$$f(\zeta \otimes x) := \{\zeta\,,\, x\}$$

for all $\zeta \in \mu_p$, $x \in W_{K,Pl_p,\mathrm{pos}}$, and where:

$$\mathrm{N}_2(K) := \{x \in K^\times,\ \{\zeta_1\,,\, x\} = 1\}/K^{\times p}$$

(Tate's kernel, where ζ_1 is a generator of μ_p) is such that:

$$\mu_p \otimes \mathrm{N}_2(K) \simeq (\mu_p \otimes \mu_p) \oplus \mu_p^{r_2}.$$

Note. When the number field K is given together with an automorphism group g, the fact that in these statements we write $\mu_p \otimes X$ (instead of ${}_pX$ or X/X^p) allows us to have canonical isomorphisms of g-modules.

Tate's exact sequence already yields:

7.7.2.1 Proposition. *When K contains μ_p we have:*

$$\mathrm{rk}_p(\mathrm{R}_2^{\mathrm{ord}}(K)) = \mathrm{rk}_p(\mathcal{C}\ell^{\mathrm{ord}}_{Pl_p}) - (r_2 + 1). \qquad \square$$

Note. Recall that $H^{\mathrm{ord}}_{Pl_p[p]}$ has a conductor which divides $\mathfrak{m} = \prod_{v|p} \mathfrak{p}_v^{pe_v+1}$, where e_v is the ramification index of v in $K/\mathbb{Q}(\mu_p)$. Therefore, $\mathrm{rk}_p(\mathcal{C}\ell^{\mathrm{ord}}_{Pl_p}) = \mathrm{rk}_p(\mathcal{C}\ell^{\mathrm{ord}}_{\mathfrak{m}})$. Moreover, the radical of $H^{\mathrm{ord}}_{Pl_p(p)}$ is $\{xK^{\times p},\ x \in K^\times_{\mathrm{pos}},\ (x) \in I^p\langle\, Pl_p\,\rangle\}$.

Assuming the Leopoldt conjecture for p, the p-rank of $\mathrm{R}_2^{\mathrm{ord}}(K)$ is also equal to the p-rank of the torsion group of $\mathrm{Gal}(H^{\mathrm{ord}}_{Pl_p(p)}/K)$ (see III.2.1.1 for $S = Pl^{\mathrm{r}}_\infty$, $T = Pl_p$, and III.4.2.2).

The reflection theorem I.4.6, (ii), applied to $\mathcal{C}\ell^{\mathrm{ord}}_{Pl_p}$, implies:

7.7.2.2 Corollary. *In the Kummer case we have:*

$$\mathrm{rk}_p(\mathrm{R}_2^{\mathrm{ord}}(K)) = \mathrm{rk}_p\big(\mathcal{C}\ell^{Pl_p\,\mathrm{res}}\big) + |Pl_p| - 1. \qquad \square$$

7.7.3 Tate's Results in the Non-Kummer Case. In the general case, we must introduce $K' := K(\mu_p)$, use formulas with characters and the reflection principle. More precisely, starting from Tate's exact sequence, the reflection theorem allows us to prove the following general formula.

7.7.3.1 Theorem. *For any number field K, we have:*

$$\mathrm{rk}_p(\mathrm{R}_2^{\mathrm{ord}}(K)) = \mathrm{rk}_{\omega^{-1}}\Big(\mathcal{C}\ell_{K'}^{Pl'_p\,\mathrm{res}}\Big) + \big|\{v|p,\ d_v = 1\}\big| - \delta,$$

where ω is the Teichmüller character, d_v is the decomposition group of v in K'/K, and $\delta = 1$ or 0 according as $\mu_p \subset K$ or not. $\square$

7.8 p-Regular Fields. We have introduced in 1989, in [GrJ], the following definition.

7.8.1 Definition. Number fields for which $(\mathrm{R}_2^{\mathrm{ord}}(K))_p = 1$ are called p-regular. $\square$

These fields have a much simpler arithmetic since deep invariants vanish, and for these fields we can even compute higher K-groups (as in [RØ] and a few others). We will see in III.4.1.10, III.4.2.6, (i), and especially in (Ch. IV; § 3, (b)), the similar notion of p-rational fields and what class field theory says about them. The above general formula shows that the p-regularity depends on the ω^{-1}-component of the Pl'_p-class group (in the restricted sense) of $K' := K(\mu_p)$. We will see that the ω-component is concerned with the p-rationality and that the two notions coincide if and only if $\omega^2 = 1$. Then, if K contains the maximal real subfield of $\mathbb{Q}(\mu_p)$, p-regularity and p-rationality will be equivalent notions (this condition is always satisfied for $p = 2$ and $p = 3$).

7.8.1.1 Example. The number field $K \supset \mu_p$ is p-regular (or p-rational) if and only if p does not split in $K/\mathbb{Q}$ and $(\mathcal{C}\ell^{\mathrm{res}})_p$ is generated by means of the single prime ideal of K above p (use 7.7.2.2). $\square$

We will now prove that $\mathbb{Q}$ is p-regular for all p. Thus for $K = \mathbb{Q}$, we will have:

$$\mathrm{WK}_2(\mathbb{Q}) = \mathrm{R}_2^{\mathrm{ord}}(\mathbb{Q}) = 1, \quad \mathrm{R}_2^{\mathrm{res}}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

The proof given below is a direct one and does not use the class field theory results we have seen up to now; but it is also possible to check that the rank formula above gives the result by analytical means.

7.8.1.2 Theorem (Gauss's first proof of the quadratic reciprocity law, revisited by Tate). *The global regular Hilbert symbol induces the isomorphism:*

$$\mathrm{K}_2(\mathbb{Q}) \simeq \mu(\mathbb{R}) \bigoplus_{\substack{\ell \text{ prime} \\ \ell \neq 2}} \mu(\mathbb{Q}_\ell) \simeq \{\pm 1\} \bigoplus_{\substack{\ell \text{ prime} \\ \ell \neq 2}} \mathbb{F}_\ell^\times.$$

Proof. [51] The letters ℓ, p, q denote prime numbers, a, b, c denote nonzero elements of $\mathbb{Z}$, and $\{a, b\}$ is the image of (a, b) in $\mathrm{K}_2(\mathbb{Q})$. We use the regular Hilbert's symbol $h^{\mathrm{reg}} : \mathrm{K}_2(\mathbb{Q}) \longrightarrow \{\pm 1\} \bigoplus_\ell \mu(\mathbb{Q}_\ell)^{\mathrm{reg}}$, where we replace $\mu(\mathbb{Q}_\ell)^{\mathrm{reg}}$ by $\mathbb{F}_\ell^\times$ (note that $\mu(\mathbb{Q}_2)^{\mathrm{reg}} = \mathbb{F}_2^\times = 1$ and $\mu(\mathbb{Q}_2)^1 = \langle -1 \rangle$); the first factor corresponds to the place ∞. Put:

$$\begin{aligned} t_\infty &= \langle \{-1, -1\} \rangle, \\ t_0 &= \langle \{a, b\},\ a, b \in [1, \infty[\rangle, \\ t_\ell &= \langle \{a, b\},\ a, b \in [1, \ell] \rangle,\ \ \ell \text{ prime}. \end{aligned}$$

Note that $\mathrm{K}_2(\mathbb{Q})$ is generated by the $\{u, v\}$, $u,\ v \in \mathbb{Z} \setminus \{0\}$.

Lemma 1. *We have* $\mathrm{K}_2(\mathbb{Q}) = t_\infty \oplus t_0$.

Proof. The bilinearity gives $\{a, b\} = \{|a|, |b|\} . s$, where s is an element of $\langle \{-1, -1\};\ \{c, -1\},\ c > 0 \rangle$. But $\{c, -c\} = 1$, which yields $\{c, -1\} = \{c, c\} \in t_0$. The sum is direct since we have $\left(\frac{-1, -1}{\infty}\right) = -1$ and $\left(\frac{|a|, |b|}{\infty}\right) = 1$, proving the result. □

Since by 7.1.5, $h^{\mathrm{reg}}(t_\infty) = \{\pm 1\}$ and $h^{\mathrm{reg}}(t_0) \subseteq \bigoplus_\ell \mathbb{F}_\ell^\times$, it is equivalent to prove that the restriction of h^{reg} to t_0 yields $t_0 \simeq \bigoplus_\ell \mathbb{F}_\ell^\times$.

Lemma 2. *Let p be fixed. Then the restriction of h^{reg} to t_p yields an isomorphism of t_p onto $\bigoplus_{\ell \leq p} \mathbb{F}_\ell^\times$.*

Proof. We note that $t_2 \simeq \mathbb{F}_2^\times$ (indeed, $\{2, 2\} = \{2, -2\}\{2, 1 - 2\} = 1$). For $p \neq 2$, let q be the greatest prime number such that $q < p$; we suppose, by induction, that $t_q \simeq \bigoplus_{\ell \leq q} \mathbb{F}_\ell^\times$. Thus it is sufficient to prove that $t_p / t_q \simeq \mathbb{F}_p^\times$ under h^{reg}.

Consider the following two maps:

$$\varphi : t_p / t_q \longrightarrow \mathbb{F}_p^\times, \quad \theta : \mathbb{F}_p^\times \longrightarrow t_p / t_q,$$

[51] Inspired by a conference of Tate (Grenoble 1968): "Sur la première démonstration par Gauss de la loi de réciprocité". See also [Ta1, § 3, (17)], [Mil, Th. 11.6], [f, Lem1, Th. 2.30].

for which:

$$\varphi(\{a,\,b\}) := \Big(\frac{a,\,b}{p}\Big)^{\mathrm{reg}} \in \mathbb{F}_p^\times, \quad \theta(\overline{c}) = \{c,\,p\} \bmod t_q,$$

where c is the representative of $\overline{c} \in \mathbb{F}_p^\times$ in $[1,\,p[$. Since:

$$\Big(\frac{a,\,b}{p}\Big)^{\mathrm{reg}} = (-1)^{\mathrm{v}_p(a)\mathrm{v}_p(b)}\ a^{\mathrm{v}_p(b)}\,b^{-\mathrm{v}_p(a)} \mod (p),$$

φ is trivial on t_q since $\mathrm{v}_p(a) = \mathrm{v}_p(b) = 0$ for such a, b.

We will prove that $\varphi \circ \theta$ and $\theta \circ \varphi$ are the corresponding identity maps (it is not a priori evident that θ is a group homomorphism).

We have $\varphi \circ \theta(\overline{c}) = \varphi(\{c,\,p\}) = \Big(\frac{c,\,p}{p}\Big)^{\mathrm{reg}} = \overline{c}$ since $\mathrm{v}_p(c) = 0$. Then $\theta \circ \varphi(\{a,\,b\}) = \theta\Big(\Big(\frac{a,\,b}{p}\Big)^{\mathrm{reg}}\Big) = \theta(\overline{c})$, where $\overline{c} = (-\overline{1})^{\mathrm{v}_p(a)\mathrm{v}_p(b)}\ \overline{a}^{\mathrm{v}_p(b)}\,\overline{b}^{\,-\mathrm{v}_p(a)}$. The case where $a,\,b \in [1,\,p[$ is immediate since $\{a,\,b\} \in t_q$. If $a < p$ and $b = p$, then $c = a$, thus $\theta(\overline{c}) \equiv \{a,\,p\} \bmod t_q$. If $a = p$ and $b < p$, then $\overline{c} = \overline{b}^{\,-1}$, and we have to verify that $\{p,\,b\}\{c,\,p\}^{-1} = \{p,\,b\,c\} \in t_q$. Put $b\,c = 1 + d\,p$; the case $b = 1$ being trivial, suppose $b > 1$, thus $0 < d < p$. Then we have $1 = \{-d\,p,\,1 + d\,p\} = \{-d\,p,\,b\,c\} = \{-d,\,b\}\{-d,\,c\}\{p,\,b\,c\}$ giving the result since $\{-1,\,u\} = \{u,\,u\}$. If $a = b = p$, then $\overline{c} = -\overline{1}$, $c = p - 1$, but we have $\{p-1,\,p\} = \{-1,\,p\} = \{p,\,p\}$. This finishes the proof of the lemma. □

Taking the direct limit (i.e., the union $t_0 = \bigcup\limits_{\ell} t_\ell$), the theorem follows. □

We now consider the Hilbert symbol $\big(\frac{\bullet,\,\bullet}{2}\big)$ for the place 2; it takes its values in $\langle -1 \rangle$. Since this Hilbert symbol is of order 2, we can write $\big(\frac{\bullet,\,\bullet}{2}\big) =: g \circ \{\bullet,\ \bullet\}$, where $g : \{\pm 1\} \bigoplus\limits_{\ell \neq 2} \mathbb{F}_\ell^\times / \mathbb{F}_\ell^{\times 2} \longrightarrow \langle -1 \rangle$, is such that:

$$g((u_v)_{v \neq 2}) = g_\infty(u_\infty) \prod_{\ell \neq 2} g_\ell(u_\ell),$$

with $g_\infty := g_{|_{\{\pm 1\}}}$, $g_\ell := g_{|_{\mathbb{F}_\ell^\times / \mathbb{F}_\ell^{\times 2}}}$. We then have $g_v(\bullet) = (\bullet)^{\delta_v}$, $\delta_v = 0$ or 1 depending only on v. Let $a,\,b \in \mathbb{Z} \setminus \{0\}$. Taking $u_\infty = \Big(\frac{a,\,b}{\infty}\Big)$ and, $u_\ell = \Big(\frac{a,\,b}{\ell}\Big) \bmod \mathbb{F}_\ell^{\times 2}$ for all $\ell \neq 2$, which implies that $\Big(\frac{a,\,b}{\ell}\Big) \bmod \mathbb{F}_\ell^{\times 2}$ is the quadratic Hilbert symbol $\Big(\frac{a,\,b}{\ell}\Big)_2 := \Big(\frac{a,\,b}{\ell}\Big)^{\frac{\ell-1}{2}} = \pm 1$, we get:

$$\Big(\frac{a,\,b}{2}\Big) = \Big(\frac{a,\,b}{\infty}\Big)^{\delta_\infty} \prod_{\ell \neq 2} \Big(\frac{a,\,b}{\ell}\Big)_2^{\delta_\ell} \quad \text{for all } a,\,b \in \mathbb{Z} \setminus \{0\}.$$

The uniqueness of the product formula readily gives $\delta_v = 1$ for all $v \neq 2$, but of course, the point of view of Gauss was to *prove* the product formula, giving easily the reciprocity law as we know it. For this, the computation

of $\left(\frac{-1,\,-1}{2}\right)$ gives $\delta_\infty = 1$; if $\ell \equiv 3 \bmod (4)$, the computation of $\left(\frac{\ell,\,-1}{2}\right)$ gives $\delta_\ell = 1$; if $\ell \equiv 5 \bmod (8)$, the computation of $\left(\frac{\ell,\,2}{2}\right)$ gives $\delta_\ell = 1$; for $\ell \equiv 1 \bmod (8)$, the computation is not easy since $\left(\frac{\ell,\,b}{2}\right) = 1$ for any b. In this case, let p be the least prime $\ell \equiv 1 \bmod (8)$ such that $\delta_\ell = 0$. Gauss proved the existence of a prime $q < p$ such that $\left(\frac{p}{q}\right) = -1$ (see [f, Lem1, Th. 2.30]), yielding a contradiction to the computation of $\left(\frac{p,\,q}{2}\right) = \prod_{\ell \neq 2} \left(\frac{p,\,q}{\ell}\right)_2^{\delta_\ell} = \left(\frac{p,\,q}{q}\right)_2 \left(\frac{p,\,q}{p}\right)_2^0 = \left(\frac{p}{q}\right)$ since $\left(\frac{p,\,q}{2}\right) = 1$.

Note. The isomorphism of Theorem 7.8.1.2 is not canonical, the image of h being $\{(\zeta_v)_v \in \bigoplus_{v \in Pl_{\mathbb{Q}}} \mu(\mathbb{Q}_v),\ \prod_v \zeta_v^{\frac{m_v}{2}} = 1\}$. Since $\frac{m_\infty}{2} = \frac{m_2}{2} = \frac{m_3}{2} = 1$, we can express ζ_∞, ζ_2, or ζ_3 by means of the other ζ_v. Here, we "eliminate" the wild place.

7.8.2 Remark. Recall that the main theorem of Mazur–Wiles–Kolyvagin on abelian extensions K of $\mathbb{Q}$ yields, in the real case, the following analytical expression for $|\mathrm{R}_2^{\mathrm{ord}}(K)|$ which had been conjectured by Birch–Tate (on this subject, see [Grt1]):

$$|\mathrm{R}_2^{\mathrm{ord}}(K)| = \frac{w_2}{2^{[K:\mathbb{Q}]}}\,|\zeta_K(-1)| =: w_2\,|\zeta_K^{\mathrm{ord}}(-1)|,$$

where ζ_K is the Dedekind zeta function of K, which must be interpreted as the restricted zeta function ζ_K^{res} (see III.2.6.5, (ii)), and w_2 is the largest integer n such that $\mathrm{Gal}(K(\mu_n)/K)$ is killed by 2.

For $K = \mathbb{Q}$, we have $w_2 = 24$, $\zeta_{\mathbb{Q}}^{\mathrm{ord}}(-1) = \frac{1}{2}\zeta_{\mathbb{Q}}^{\mathrm{res}}(-1) = -\frac{1}{24}$, thus giving $\mathrm{R}_2^{\mathrm{ord}}(\mathbb{Q}) = 1$. □

http://www.springer.com/978-3-540-44133-5

Class Field Theory
From Theory to Practice
Gras, G.
2003, XIII, 491 p., Hardcover
ISBN: 978-3-540-44133-5