Principalization of ideals in abelian extensions of number fields

Sebastien Bosca, Georges Gras, Jean-François Jaulent

Principalization of ideals in abelian extensions of number fields

Sébastien Bosca

Université de Bordeaux, Institut de Mathématiques de Bordeaux, 351 cours de la Libération, 33405 TALENCE Cedex, France

With an Appendix by Georges Gras [1] and Jean-François Jaulent [2]

Abstract

We give a self-contained proof of a general conjecture of G. Gras on principalization of ideals in abelian extensions of a given field L, yet solved by M. Kurihara in the case of totally real extensions L of the rational field $\mathbb{Q}$.

More precisely, for any given extension L/K of number fields, in which at least one infinite place of K is totally split, and for any ideal class c_L of L, we build a finite abelian extension F/K, in which all infinite places are totally split, such that c_L principalizes in the compositum $M = LF$.

A – INTRODUCTION

When M/L is an abelian extension of number fields, the problem of knowing which ideals of L are principal in M is difficult, even if M/L is cyclic. Class field theory gives partial answers. For instance, the Artin-Furtwängler theorem states that when $M = H_L$ is the Hilbert class field of L, all ideals of L are principal in M; but the other cases are more mysterious.

When M/L is cyclic, we still have no general answer but the problem is easier. The kernel of the natural map $j : \mathrm{Cl}_L \to \mathrm{Cl}_M$ is partly known by this way, as explained below: at first, cohomology of cyclic groups says that this kernel is a part of $\hat{H}^1(\mathcal{G}, E_M)$, where $\mathcal{G} = \mathrm{Gal}(M/L)$ and E_M is the group of units of M; $\hat{H}^1(\mathcal{G}, E_M)$ itself is not well known but its order can be deduced from the order of $\hat{H}^0(\mathcal{G}, E_M)$ using the Herbrand quotient; after that, the order of $\hat{H}^0(\mathcal{G}, E_M)$ depends partly from the natural map $E_L \to U_S$, where U_S is the

[1] *Villa la Gardette, Chemin Château Gagnière, 38520 Le Bourg d'Oisans, France*

[2] *Université de Bordeaux, Institut de Mathématiques de Bordeaux, 351 cours de la Libération, 33405 TALENCE Cedex, France.*

subgroup of the unit idèles of L which is the product of the groups of local units at the places ramified in M/L (S is the set of such ramified places); finally, the map $E_L \to U_S$ depends on the Frobenius' of the primes of S in the extension $L[\mu_h,\, E_L^{1/h}]/L$ (where $h = [M : L]$ and where μ_h is the group of hth roots of unity). Obviously, this makes sense only if the primes of S are prime to the degree of the extension.

However, even in this cyclic case, $\mathrm{Ker}(j)$ is not completely given by these Frobenius', so that knowing such Frobenius', we cannot get really more than a minoration of the order of $\mathrm{Ker}(j)$.

This article deals with such minoration techniques, which allow to prove, for instance, this easy fact: if a cyclic extension M/L is ramified at only one finite place $\mathfrak{q}$ prime to $[M : L]$, then, as soon as the ramification index $e_\mathfrak{q}$ is large enough (precisely, when $|\mathrm{Cl}_L|$ divides $e_\mathfrak{q}$), the capitulation kernel $\mathrm{Ker}j$ contains at least the class of $\mathfrak{q}$ in Cl_L. This can be easily established by studying $\hat{H}^1(\mathcal{G}, E_M)$ and may be seen as a particular case of our main theorem.

On the other hand, this article states a result which proves a conjecture of Georges Gras and generalizes a result of Masato Kurihara (see [1] and [2]), so that the theorem exposed here is not only an abstract minoration of $\mathrm{Ker}j$, using cohomology of cyclic groups, Minkowski–Herbrand theorem on units of number fields, class field theory, and Kummer duality. Note also that here, we use new asymptotic methods ("take n large enough", where n is related to the degree $[F : K]$ in a suitable manner).

Note finally that in the theorem below the hypothesis "at least one infinite place of K is totally split in L/K" is necessary: in [1], Georges Gras gives examples of extensions L/K with ideals which do not principalize in the compositum LK^{ab}, where K^{ab} is the maximal abelian extension of K.

B – MAIN THEOREM AND COROLLARIES

Main Theorem. *Let L/K be a finite extension of number fields in which at least one infinite place of K totally splits. There exists a finite abelian extension F/K, which is totally split at all infinite places, such that every ideal of K principalizes in the compositum $M = LF$.*

Corollary 1 ($K = \mathbb{Q}$). *If L is a totally real number field, any ideal of L principalizes in a real cyclotomic extension of L (i.e., in the compositum of L with a real subfield of a suitable cyclotomic extension of $\mathbb{Q}$).*

Corollary 1 was proved by Masato Kurihara in [2].

Notation: In the following, K^{ab} denotes the maximal abelian extension of K and K_+^{ab} its maximal totally real subextension (i.e., the subextension of K^{ab}/K

fixed under the decomposition groups of the infinite places of K).

Definition: Let us say that a number field N is principal when Cl_N is trivial. Then:

Corollary 2. *(i) Let K be a number field with at least one complex place. Then any field containing K^{ab} is principal.*
(ii) Let K be a totally real number field. Any field containing K_+^{ab} and whose Galois closure has at least one real place is principal.

Corollary 3. *(i) Any totally real field containing $\mathbb{Q}_+^{ab}$ is principal.*
(ii) Any field containing $\mathbb{Q}(i)^{ab}$ is principal.

Corollary 3, for $\mathbb{Q}(i)$ or any imaginary quadratic field in (ii), was proved by Masato Kurihara (see [2], theorem 1.1 p. 35 and theorem A.1 p. 46).

Corollary 4. *(i) Let K be a number field with at least one complex place. Then K^{ab} is principal.*
(ii) Let K be a totally real number field. Any field containing K_+^{ab} which is contained in one of the subfields of K^{ab} fixed by a complex conjugation is principal.

Corollary 4 proves a conjecture of Georges Gras, Conjecture (0.5) p. 405 of [1].

C – PROOFS

I. Proof of the main theorem : preliminaries

To prove the theorem, we fix an ideal $\mathfrak{a}_L$ of L, and we shall build a finite abelian extension F of K, which is totally split at all infinite places, cyclic in most cases, such that $\mathfrak{a}_L$ principalizes in the compositum LF. Obviously, any ideal $\mathfrak{b}_L$ of L with the same class in Cl_L will become principal in LF as well, so that it is enough to fix the class c_L of $\mathfrak{a}_L$ in Cl_L. Now, if $(c_i)_i$ is a finite generating system of Cl_L, we will obtain a corresponding set $(F_i)_i$ of extensions, and every ideal of L will principalize in LF, where F is the compositum of the $(F_i)_i$; this will prove the theorem.

So, in the following, we fixe c_L in Cl_L, and must find F. As the class group of L is the direct sum of its p-parts, for all prime numbers p, one can suppose that the order of c_L in Cl_L is a power of a prime p. So, c_L and p are fixed; Cl_L is now the p-part of the class group of K, and H_L the maximal p-extension contained in the Hilbert class field of L.

(1) One can suppose $c_L \in \mathrm{Cl}_L^{p^a}$ for an arbitrary given integer a:

Definition: Let us call *abelian compositum* of the extension L/K any extension

$N = LF$, where F is a finite abelian extension of K, totally split at all infinite places of K.

One fixes an integer a; in case $c_L \notin \mathrm{Cl}_L^{p^a}$, one will build an abelian compositum L' of L/K, such that the extended class $c_{L'} = j(c_L)$ satisfies $c_{L'} \in \mathrm{Cl}_{L'}^{p^a}$; so, if N' is an abelian compositum of L'/K in which $c_{L'}$ is principal, it is as well an abelian compositum of L/K, so that one can legitimately replace L by L', in which case one has $c_{L'} \in \mathrm{Cl}_{L'}^{p^a}$.

Let's build such a $L' = LF_0$ as follows: let $\mathfrak{q}$ be a prime of L satisfying the three following conditions:

(i) $\mathfrak{q}$ totally splits in $L/\mathbb{Q}$;

(ii) $\mathrm{Frob}(\mathfrak{q}, L[\mu_{2p^a}]/L) = \mathrm{id}$;

(iii) $\mathrm{Frob}(\mathfrak{q}, H_L/L) = c_L$.

If such a $\mathfrak{q}$ exists with say $\mathfrak{q}|q$, the first two conditions imply the existence of a (cyclic) subfield F_0' of $\mathbb{Q}(\mu_q)$, with degree $[F_0' : \mathbb{Q}] = p^a$, which is totally ramified at the prime q; the first condition implies that the compositums $F_0 = KF_0'$ and $L' = LF_0$ have again a degree p^a over K and L, respectively. Now L'/L is totally ramified at $\mathfrak{q}$, say $\mathfrak{q} = \mathfrak{q}'^{\,p^a}$, for a prime $\mathfrak{q}'$ in L'; so, according to the third condition, the extended class $c_{L'} = j(c_L)$ satisfies:

$$c_{L'} = \overline{\mathfrak{q}} = \overline{\mathfrak{q}'}^{\,p^a} \in \mathrm{Cl}_{L'}^{p^a}$$

as expected.

Now we only have to verify the existence of such a prime $\mathfrak{q}$. The three conditions defining $\mathfrak{q}$ all depend on $\mathrm{Frob}(q, \tilde{H}_L[\mu_{2p^a}]/\mathbb{Q})$, where $\tilde{H}_L$ is the Galois closure of H_L over $\mathbb{Q}$; the first two conditions are equivalent to the fact that this Frobenius is in the subgroup $\mathrm{Gal}(\tilde{H}_L[\mu_{2p^a}]/L[\mu_{2p^a}])$; so they are compatible with the last condition for any c_L in Cl_L, if and only if one has: $L[\mu_{2p^a}] \cap H_L = L$; if this is right, the Čebotarev theorem states there are infinitely many $\mathfrak{q}$ satisfying the conditions. When this is wrong, we replace L by $L'' = L[\mu_{2p^a}] \cap H_L$ which verifies $L''[\mu_{2p^a}] \cap H_{L''} = L''$.

As explained above, this last replacement is legitimate in case $L'' = L[\mu_{2p^a}] \cap H_L$ is an abelian compositum of L/K. In fact, one has $L'' = LF$ where F is contained in the maximal p-subfield of $K[\mu_{2p^a}]$, which is clearly abelian and finite but in which infinite places are maybe not totally split for $p = 2$.

So, for $p = 2$, we shall complete the proof, and we take in this particular case $L'' = LK[\mu_{2^b}]_+$, where the symbol $+$ denotes the maximal ∞-split subextension over K, and where b is an integer, which is choosen large enough so that L'' contains $H_L \cap LK[\mu_{2^{a+1}}]_+$ and L''/L has degree at least 2.

Suppose we have found a prime $\mathfrak{q}''$ of L'' satisfying the following conditions:

(i) $\mathfrak{q}''$ totally splits in $L''/\mathbb{Q}$;

(ii) $\mathrm{Frob}(\mathfrak{q}'', L''[\mu_{2^{a+1}}]/L'') = \mathrm{id}$;

(iii) $\mathrm{Frob}(\mathfrak{q}'', H_{L''}/L'') = c_{L''}$,

where $c_{L''}$ is extended from c_L. So, let F_0' be the totally real subfield of $\mathbb{Q}[\mu_q]$ of degree 2^a over $\mathbb{Q}$, thus $F_0 = K[\mu_{2^b}]_+ F_0'$ and $L''' = LF_0 = L''F_0'$ (which is an abelian compositum of L/K). If $\mathfrak{q}'''$ denotes the unique prime of L''' above $\mathfrak{q}''$, the extended class $c'''_{L'''}$ in $\mathrm{Cl}_{L'''}$ satisfies the expected condition:

$$c_{L'''} = \overline{\mathfrak{q}''} = \overline{\mathfrak{q}'''}^{\,2^a} \in \mathrm{Cl}_{L'''}^{2^a}.$$

So to conclude we only have to prove the existence of such a prime $\mathfrak{q}''$ verifying the threee conditions above. But this existence follows from the Čebotarev theorem as soon as the image of $c_L \in \mathrm{Gal}(H_{L''}/L'')$ in $\mathrm{Gal}(H_{L''} \cap L''[\mu_{2^{a+1}}]/L'')$ is trivial. To check this last point, let us observe that in the class field description the extension of ideal classes j corresponds to the transfert map Ver. Here L'' contains $H_L \cap LK[\mu_{2^{a+1}}]_+$, so $H_{L''} \cap L''[\mu_{2^{a+1}}] = L'''$ is either L'' or $L''[i]$, and the image of $j_{L''/L}(c_L)$ in $\mathrm{Gal}(L'''/L'')$ is trivial, since one has:

$$\mathrm{Ver}_{B/A \to B'/A'}(\sigma) = \sigma^{[A':A]}$$

when B'/A is abelian, so:

$$\mathrm{Res}_{L'''}(\mathrm{Ver}_{H_L/L \to H_{L''}/L''}(c_L)) = \mathrm{Ver}_{H_L/L \to L'''/L''}(c_L) = c_L^{[L'':L]} = \mathrm{id}.$$

(2) One can suppose that L/K is Galois:

Let $\tilde{L}$ denotes the Galois closure of L over K. Imagine the theorem is proved for $\tilde{L}/K$ (in which at least one infinite place totally splits as in L/K). Hence, there exists an abelian compositum $\tilde{L}F$ of $\tilde{L}/K$ such that every ideal of $\tilde{L}$ principalize in $\tilde{L}F$; so, c_L principalizes in $\tilde{L}F$ but maybe does not in LF and we have to study this case.

(a) When c_L is norm in $\tilde{L}/L$, say $c_L = \mathrm{N}_{\tilde{L}/L}(\tilde{c}_{\tilde{L}})$, the class $\tilde{c}_{\tilde{L}} \in \mathrm{Cl}_{\tilde{L}}$ principalizes in $\tilde{L}F$, say $j_{\tilde{L}F/\tilde{L}}(\tilde{c}_{\tilde{L}}) = 1$ in $\mathrm{Cl}_{\tilde{L}F}$; so we obtain: $c_L = \mathrm{N}_{\tilde{L}\cap LF/L}(c'_{\tilde{L}\cap LF})$ with $c'_{\tilde{L}\cap LF} = (\mathrm{N}_{\tilde{L}/(\tilde{L}\cap LF)}(\tilde{c}_{\tilde{L}}))$ and the class $c'_{\tilde{L}\cap LF}$, which satisfies $j_{LF/\tilde{L}\cap LF} \circ \mathrm{N}_{\tilde{L}/(\tilde{L}\cap LF)}(\tilde{c}_{\tilde{L}}) = \mathrm{N}_{\tilde{L}F/LF} \circ j_{\tilde{L}F/\tilde{L}}(\tilde{c}_{\tilde{L}}) = 1$, principalizes in FL; and so is c_L.

(b) When c_L is not a norm in $\tilde{L}/L$, maybe c_L is not principal in LF. But $\mathrm{N}_{\tilde{L}/L}(\mathrm{Cl}_{\tilde{L}})$ contains $\mathrm{Cl}_L^{[\tilde{L}:L]} = \mathrm{Cl}_L^{p^a}$, where p^a is the largest power of p dividing $[\tilde{L} : L]$. According to Section **(1)** we replace L by $L' = LF_0$ such that $c_L \in \mathrm{Cl}_{L'}^{p^a}$. Since $[\tilde{L}' : L'] = [\tilde{L}F_0 : LF_0]$ divides $[\tilde{L} : L]$, c_L is norm in $\tilde{L}'/L'$ and (a) applies.

II. Proof of the theorem : building the extension F

(3) The method and a first condition about the prime $\mathfrak{q}$:

By now we suppose L/K Galois. The prime p and the class c_L are fixed and we must build an abelian compositum LF of L/K such that c_L principalizes in LF. For convenience, we choose F/K as a cyclic p-extension, ramified at only one finite place $\mathfrak{q}$ of K, and whose ramification index is $e_{\mathfrak{q}}(F/K) = p^n$ for a given integer n. We will see that with many conditions about $\mathfrak{q}$, when n is large enough, c_L is principal in LF, or in $L'F$, where L' is a convenient abelian compositum of L/K. At the end of the proof, in Section **(6)**, we will study the existence of such $\mathfrak{q}$ verifying all conditions.

Now for a given integer n and a given prime $\mathfrak{q}$ of K, we wonder if c_L is principal in $M = LF$, where F is a cyclic p-extension of K with $e_{\mathfrak{q}}(F/K) = p^n$, unramified but at $\mathfrak{q}$ and in which all infinite places are totally split. The first question is the existence of such an extension F/K and class field theory gives the answer as follows.

Indeed, N being the maximal abelian extension of K unramified but at $\mathfrak{q}$ and ∞-split, class field theory describes the Galois group $\mathrm{Gal}(N/K)$ from the quotient

$$J_K \Big/ K^{\times}.\prod_{v|\infty} K_v^{\times}.\prod_{\mathfrak{q}'\neq\mathfrak{q}} U_{\mathfrak{q}'} \ ,$$

where J_K is the idèle group of K and $U_{\mathfrak{q}'}$ the subgroup of local units of the completion $K_{\mathfrak{q}'}$ of K at the place $\mathfrak{q}'$. The inertia subgroup of $\mathfrak{q}$ in N/K is, according to class field theory, isomorphic to the quotient

$$U_{\mathfrak{q}} \Big/ \overline{U_{\mathfrak{q}} \cap (K^{\times}.\prod_{v|\infty} K_v^{\times}.\prod_{\mathfrak{q}'\neq\mathfrak{q}} U_{\mathfrak{q}'})} = U_{\mathfrak{q}} \Big/ \overline{E_K} \ ,$$

where E_K is the group of global units in K and the overlining means closure in $U_{\mathfrak{q}}$ of the diagonal embedding. Of course if F exists, it is contained in the maximal p-extension of N, whose ramification subgroup is the p-part of $U_{\mathfrak{q}} \Big/ \overline{E_K}$, denoted $(U_{\mathfrak{q}} \Big/ \overline{E_K})_p$.

We suppose now:

- $\mathfrak{q} \nmid p$.

So, if F exists, p^n divides $|(U_{\mathfrak{q}} \Big/ \overline{E_K})_p|$, that is, under the assumption $\mathfrak{q} \nmid p$:

- $\mu_{p^n} \subset K_{\mathfrak{q}}^{\times}$,

and

- $E_K \subset U_{\mathfrak{q}}^{p^n}$.[3]

[3] The canonical embedding of E_K in $K_{\mathfrak{q}}^{\times}$ must be contained in $U_{\mathfrak{q}}^{p^n}$ since $(U_{\mathfrak{q}})_p$ is here a cyclic group.

These necessary conditions are enough to ensure the existence of F, according to an obvious lemma, which states: if A is an abelian finite group and C is a cyclic subgroup of A of which p^n divides the order, then there exists a cyclic quotient of A in which the image of C has order p^n.

Now we suppose that $\mathfrak{q} \nmid p$ verifies the two above conditions and the additional assumption:

- $\mathfrak{q}$ is unramified in L/K. [4]

So F exists; all primes $\mathfrak{q}_L \mid \mathfrak{q}$ are ramified in $M/L = LF/L$ with the same index $e_{\mathfrak{q}} = p^n$; and we have $[M : L] = p^{n+d}$ for some positive integer d.

(4) Obtaining a big cohomology group $\hat{H}^0(\mathcal{G}, E_M)$:

Let $\mathcal{G}$ denotes the Galois group $\mathrm{Gal}(M/L)$, which is cyclic with order p^{n+d}, and $G = \mathrm{Gal}(L/K)$.

According to the Minkowski–Herbrand theorem, the character of the representation $\mathbb{Q} \otimes_{\mathbb{Z}} E_L$ of $G = \mathrm{Gal}(L/K)$, given by the group of global units E_L, is:

$$\chi(E_L) = \sum_{v|\infty} \mathrm{Ind}_{D_v}^G 1_{D_v} - 1_G \ ,$$

where 1_G is the trivial character of G and 1_{D_v} the trivial character of the decomposition subgroup D_v.

Since at least one infinite place is totally split in the extension L/K, the character of $\mathbb{Q} \otimes_{\mathbb{Z}} (E_L/\mu_L E_K)$ satisfies

$$\chi(E_L/\mu_L E_K) \geq \chi(\mathbb{Z}[G]) - 1 \ ,$$

and we can deduce from this the existence of a map: [5]

$$\varphi : E_L/\mu_L.E_K \longrightarrow \mathbb{Z}$$

such that, in $\mathrm{Hom}(E_L/\mu_L.E_K, \mathbb{Z})$, φ generates a $\mathbb{Z}[G]$-submodule whose character is $\chi(\mathbb{Z}[G]) - 1$.

On the other hand, since $L[\mu_{p^n}, E_L^{1/p^n}]/L[\mu_{p^n}]$ is a Kummer extension, if $\mathfrak{q}_L$ is one of the primes of L dividing $\mathfrak{q}$, the Frobenius automorphism

$$\sigma = \mathrm{Frob}(\mathfrak{q}_L, L[\mu_{p^n}, E_L^{1/p^n}]/L)$$

[4] In fact, in the sequel Bosca will suppose that $\mathfrak{q}$ is totally split in L/K.
[5] See the details in the Appendix.

corresponds, in the Kummer duality, to the map:

$$u \mapsto (u^{1/p^n})^{(\sigma-1)} \in \mu_{p^n}, \quad \text{for all } u \in E_L,$$

and we impose the new condition:

- this map σ coincides with $\lambda_n : E_L \longrightarrow E_L/\mu_L.E_K \xrightarrow{\varphi} \mathbb{Z} \longrightarrow \mu_{p^n}$,

where the left map is the natural one and the right one is surjective (we must choose a primitive p^nth root of unity for the right map, but this choice does not change the Frobenius defined up to conjugation: changing the choice of the root of unity is the same that changing the choice of a prime $\mathfrak{q}' \mid \mathfrak{q}$ in $L[\mu_{p^n}]$).

So, the property of φ leads to the following facts:

Let ϕ denotes the map (see the Appendix):

$$\begin{aligned} E_L \ &\longrightarrow R_G := \{\sum_g \alpha_g\, g \in \mathbb{Z}[G] \ \mid \sum_g \alpha_g = 0\} \\ u \ &\longmapsto \ \sum_g \varphi(g^{-1}(u))\, g \ ; \end{aligned}$$

$\mathrm{Im}(\phi)$ has finite index, say r. So, p^δ being the maximal power of p dividing r, one has:

$$|\{E_L/\{u \in E_L \mid \forall g \in G, \lambda_n(g(u)) = 1\}| \geq |R_G/R_G^{p^n}|/p^\delta = p^{n(|G|-1)-\delta} \ .$$

On the arithmetical side, the ramification indices in M/L of all primes $\mathfrak{q}_L \mid \mathfrak{q}$ of L are all equal to p^n; so, with $\mathfrak{q}_M|\mathfrak{q}_L|\mathfrak{q}$ in $M/L/K$, one has [6] :

$$\mathrm{N}_{M/L}(E_M) \subset \mathrm{N}_{M/L}\Big(\prod_{\mathfrak{q}_M|\mathfrak{q}} U_{\mathfrak{q}_M}\Big) = \prod_{\mathfrak{q}_L|\mathfrak{q}} U_{\mathfrak{q}_L}^{p^n} \ ,$$

and then,

$$\{u \in E_L \mid \forall g \in G, \lambda_n(g(u)) = 1\} = E_L \cap \prod_{\mathfrak{q}_L|\mathfrak{q}} U_{\mathfrak{q}_L}^{p^n} \supset \mathrm{N}_{M/L}(E_M) \ ,$$

so that

$$|H^0(\mathcal{G}, E_M)| = |E_L/\mathrm{N}_{M/L}(E_M)| \geq |E_L/\{u \in E_L \,|\, \forall g \in G, \lambda_n(g(u)) = 1\}| \ ,$$

and we finally have from the character theory side:

$$|H^0(\mathcal{G}, E_M)| \geq p^{n(|G|-1)-\delta} \ .$$

[6] Using the fact that the global norm is the product of the corresponding local norms.

(5) Study of $\hat{H}^1(\mathcal{G}, E_M)$ and majoration of $|I_M^{\mathcal{G}}/P_M^{\mathcal{G}}|$:

Recal that $M := FL$. According to [4], chapter IX, §1, since the cyclic extension M/L is totally split at all infinite places, the Herbrand quotient $q(\mathcal{G}, E_M)$ of the units is given by:

$$q(\mathcal{G}, E_M) := \frac{|\hat{H}^0(\mathcal{G}, E_M)|}{|\hat{H}^1(\mathcal{G}, E_M)|} = \frac{1}{[M:L]} = \frac{1}{p^{n+d}} \ ,$$

and this gives:

$$|\hat{H}^1(\mathcal{G}, E_M)| = p^{n+d} \, . \, |\hat{H}^0(\mathcal{G}, E_M)| \geq p^{n+d} \, . \, p^{n(|G|-1)-\delta} = p^{n|G|+d-\delta} \ .$$

On the other hand, one has the canonical isomorphism:

$$\hat{H}^1(\mathcal{G}, E_M) \simeq P_M^{\mathcal{G}}/P_L$$

where $P_M^{\mathcal{G}}$ is the group of principal ideals of M which are invariant under $\mathcal{G}$.

So one obtains:

$$|P_M^{\mathcal{G}}/P_L| \geq p^{n|G|+d-\delta}.$$

Thus, from the formula: [7]

$$|I_M^{\mathcal{G}}/I_L| = \prod_{\mathfrak{q}_L|\mathfrak{q}} e_{\mathfrak{q}_L} = p^{n|G|} \ ,$$

where I_M is the group of fractional ideals of M, one deduces:

$$|I_M^{\mathcal{G}}/P_M^{\mathcal{G}}| = \frac{|I_M^{\mathcal{G}}/P_L|}{|P_M^{\mathcal{G}}/P_L|} = \frac{|I_M^{\mathcal{G}}/I_L| \, . \, |I_L/P_L|}{|P_M^{\mathcal{G}}/P_L|} = \frac{p^{n|G|} \, . \, |\mathrm{Cl}_L|}{|P_M^{\mathcal{G}}/P_L|} \leq \frac{p^{n|G|} \, . \, |\mathrm{Cl}_L|}{p^{n|G|+d-\delta}} \ ,$$

that is:

$$|I_M^{\mathcal{G}}/P_M^{\mathcal{G}}| \leq |\mathrm{Cl}_L| \, . \, p^{\delta-d} \ .$$

Note that the number at the right hand side does not depend on n.

(6) Does the class c_L principalize in M ?

Here, we also suppose:

• $\mathrm{Frob}(\mathfrak{q}_L, H_L/L) = c_L$.

M' being the maximal subfield of M/L in which $\mathfrak{q}_L$ totally splits, one has:

$$\mathfrak{q}_L = \prod_{\mathfrak{q}'_M|\mathfrak{q}_L \text{ in } M'/L} \mathfrak{q}'_M;$$

[7] Since we have supposed that $\mathfrak{q}$ is totally split in L/K.

and for all prime $\mathfrak{q}'_M|\mathfrak{q}_L$ of M'/L, we have $\mathfrak{q}'_M = \mathfrak{q}_M^{p^n}$, where $\mathfrak{q}_M$ is the unique prime of M dividing $\mathfrak{q}'_M$.

Finally in M,

$$\mathfrak{q}_L = \left(\prod_{\mathfrak{q}'_M|\mathfrak{q}_L} \mathfrak{q}_M \right)^{p^n} ,$$

with $\prod_{\mathfrak{q}'_M|\mathfrak{q}_L} \mathfrak{q}_M \in I_M^{\mathcal{G}}$. According to Section **(5)**, one has:

$$|I_M^{\mathcal{G}}/P_M^{\mathcal{G}}| \leq |\mathrm{Cl}_L| \,.\, p^{\delta-d},$$

then:

$$\left(\prod_{\mathfrak{q}'_M|\mathfrak{q}_L} \mathfrak{q}_M \right)^{|\mathrm{Cl}_L| \,.\, p^{\delta-d}} \in P_M^{\mathcal{G}} \ .$$

Hence, in Cl_M, the extended class c_M of c_L satisfies both:

$$c_M = \overline{\mathfrak{q}}_L = \left(\prod_{\mathfrak{q}'_M|\mathfrak{q}_L} \overline{\mathfrak{q}}_M \right)^{p^n} \quad \text{and} \quad \left(\prod_{\mathfrak{q}'_M|\mathfrak{q}_L} \overline{\mathfrak{q}}_M \right)^{|\mathrm{Cl}_L| \,.\, p^{\delta-d}} = 1 \ .$$

So, w being such that $|\mathrm{Cl}_L| = p^w$, c_L is principal in M under the assumption:

$$n \geq w + \delta - d.$$

(7) Existence of $\mathfrak{q}$:

We just proved that c_L principalizes in M when n is large enough and when $\mathfrak{q}$ (or $\mathfrak{q}_L|\mathfrak{q}$) satisfies the following six conditions:

(1) $\mathfrak{q} \nmid p$,

(2) $\mu_{p^n} \subset K_{\mathfrak{q}}^{\times}$,

(3) $E_K \subset U_{\mathfrak{q}}^{p^n}$,

(4) $\mathfrak{q}$ is totally split in L/K,

(5) $\mathrm{Frob}(\mathfrak{q}_L, L[\mu_{p^n}, E_L^{1/p^n}]/L) = \lambda_n$,

(6) $\mathrm{Frob}(\mathfrak{q}_L, H_L/L) = c_L$.

The definition of $\lambda_n \in \mathrm{Gal}(L[\mu_{p^n}, E_L^{1/p^n}]/L)$ shows it is trivial on $L[\mu_{p^n}, E_K^{1/p^n}]$ then conditions (4) and (5) imply (2) and (3), so we only study compatibility between conditions (1), (4), (5), (6). This compatibility is possible if and only if c_L and λ_n are equal on the extension $H_L \cap L[\mu_{p^n}, E_L^{1/p^n}]$ of L.

Let m be the integer such that $|(\mu_L)_p| = p^m$; one has, where the exponent ab means abelian subextension over L:

$$H_L \cap L[\mu_{p^n}, E_L^{1/p^n}] \subset H_L \cap (L[\mu_{p^n}, E_L^{1/p^n}])^{ab} = H_L \cap L[\mu_{p^{n+m}}, E_L^{1/p^m}] \ ;$$

let m' be the integer such that $H_L \cap L[\mu_{p^\infty}] = L[\mu_{p^{m'}}]$, so $m' \geq m$ and

$$H_L \cap L[\mu_{p^n}, E_L^{1/p^n}] = H_L \cap L[\mu_{p^{m'}}, E_L^{1/p^m}] \ .$$

The exponent of the Galois group $\mathrm{Gal}(L[\mu_{p^{m'}}, E_L^{1/p^m}]/L)$ is less than $p^{m'}$, so is this of $\mathrm{Gal}(H_L \cap L[\mu_{p^n}, E_L^{1/p^n}]/L)$. According to Section **(1)**, taking $a = m'$, one can suppose that $c_L \in \mathrm{Cl}_L^{p^{m'}}$ (replacing L by L' as in Section**(1)**; note that $m'(L') = m'(L)$ because L'/L is unramified at all places dividing p, so that $c_L \in \mathrm{Cl}_L^{p^{m'(L')}}$ as expected); in that case, the restriction of c_L is trivial on $H_L \cap L[\mu_{p^n}, E_L^{1/p^n}]$.

About the restriction of λ_n on $H_L \cap L[\mu_{p^n}, E_L^{1/p^n}]$, we can as well suppose it is trivial, by replacing eventually λ_n by $\lambda_n^{p^{m'}}$ (*i.e.* φ by $p^{m'}\varphi$) which has the same properties. [8]

Up to replacing L by L' and choosing a convenient φ, the restrictions of c_L and of λ_n are both trivial on $H_L \cap L[\mu_{p^n}, E_L^{1/p^n}]$: Čebotarev theorem then ensures the existence of infinitely many convenient primes $\mathfrak{q}$ of K satisfying all conditions, and each one gives us an abelian compositum M in which L principalizes. This proves the Main Theorem.

III. Proofs of corollaries

Corollary 1 is just the case $K = \mathbb{Q}$, and the Kronecker-Weber theorem which states that abelian extensions of $\mathbb{Q}$ are cyclotomic.

Corollary 2 is equivalent to the following fact: Let K be a number field and K_+^{ab} its maximal ∞-split abelian extension. Any field L containing K_+^{ab} and in which at least one infinite place totally splits over K is principal.

To prove this, Let $\mathfrak{a}$ be a fractional ideal of finite type of L. Of course $\mathfrak{a}$ is as well a fractional ideal of a subfield $L_\mathfrak{a}$ of L with finite dimension over $\mathbb{Q}$. We can suppose $L_\mathfrak{a} \supset K$, then $L_\mathfrak{a}/K$ is an extension of number fields in which at least one infinite place is totally split. According to the main theorem, $\mathfrak{a}$ principalizes in an abelian compositum $L_\mathfrak{a}F$ of $L_\mathfrak{a}/K$; but $L_\mathfrak{a}F$ is contained in $L_\mathfrak{a}K_+^{ab} \subseteq L$ and so $\mathfrak{a}$ is principal in L.

Corollary 3 comes from corollary 2, by taking $K = \mathbb{Q}$ and $K = \mathbb{Q}(i)$, respectively.

Corollary 4 comes from Corollary 2.

[8] See the Appendix.

D – APPENDIX [9]

The original project of publication of S. Bosca was first written in french from his thesis and a provisional text, in english, was given to us before his departure from the University. Thus, due to the interest of the ideas of this work, it has been decided to publish it, with suitable corrections in the text and with a complement which is given below in this Appendix.

Definition of φ. For a group of global units E we denote by $\overline{E}$ the quotient of E by its torsion subgroup μ.

Let N be the norm in L/K and let ${}_{\mathrm{N}}E$ be the kernel of N in E. From the exact sequence:

$$1 \longrightarrow {}_{\mathrm{N}}\overline{E}_L \longrightarrow \overline{E}_L \longrightarrow \mathrm{N}(\overline{E}_L) \subseteq \overline{E}_K \longrightarrow 1 \quad \text{(finite index)}$$

we get:

$$\mathbb{Q} \otimes_{\mathbb{Z}} (\overline{E}_L) = \mathbb{Q} \otimes_{\mathbb{Z}} ({}_{\mathrm{N}}\overline{E}_L) \oplus \mathbb{Q} \otimes_{\mathbb{Z}} (\overline{E}_K) \ \textit{i.e.} \ \ \mathbb{Q} \otimes_{\mathbb{Z}} (\overline{E}_L/\overline{E}_K) = \mathbb{Q} \otimes_{\mathbb{Z}} ({}_{\mathrm{N}}\overline{E}_L).$$

Since at least one infinite place of K is totally split in the extension L/K, the Dirichlet–Herbrand theorem implies that the character of $\mathbb{Q} \otimes_{\mathbb{Z}} ({}_{\mathrm{N}}\overline{E}_L)$ contains $\chi(\mathbb{Q}[G]) - 1$ and the representation $\mathbb{Q} \oplus \mathbb{Q} \otimes_{\mathbb{Z}} ({}_{\mathrm{N}}\overline{E}_L)$ contains at least a representation R isomorphic to $\mathbb{Q}[G]$.

We can put $R = \mathbb{Q} \otimes_{\mathbb{Z}} \langle\, \theta \,\rangle$ with $\theta = \rho \,.\, \varepsilon_*$ where $\rho \in \mathbb{Q}^\times$, $\rho \neq \pm 1$, and where $\varepsilon_* \in {}_{\mathrm{N}}\overline{E}_L$ may be seen as a " relative Minkowski unit ".

Thus any element $u \in R$ is written, in a unique manner, $u = \theta^\omega$ with $\omega = \sum_{g \in G} \alpha_g \, g \in \mathbb{Q}[G]$. It follows that u is a unit (in $\langle\, \varepsilon_* \,\rangle_{\mathbb{Z}[G]}$) if and only if $\sum_{g \in G} \alpha_g = 0$. We note that in this case the α_g can be taken in $\frac{1}{m}\mathbb{Z}[G]$ for a suitable $m \in \mathbb{Z}$ (for instance $m = |\, G \,|$, but if necessary we can adjust the value of m large enough; at the end of the reasoning, Bosca uses this possibility); in any case m depends only on L/K and not on n.

For the same reasons, the choice of ε_* is not crucial and $\langle\, \varepsilon_* \,\rangle_{\mathbb{Z}[G]}$ is not necessarily a direct summand in ${}_{\mathrm{N}}\overline{E}_L$.

The map φ is then defined as follows: noting that

$$\overline{E}_L/{}_{\mathrm{N}}\overline{E}_L \,.\, \overline{E}_K = \overline{E}_L/{}_{\mathrm{N}}\overline{E}_L \oplus \overline{E}_K$$

is killed by $|\, G \,|$, for $\varepsilon \in \overline{E}_L$, we have $\varepsilon^{|G|} = \eta_* \,.\, \varepsilon_0$, $\eta_* \in {}_{\mathrm{N}}\overline{E}_L$, $\varepsilon_0 \in \overline{E}_K$.

[9] Written by G. Gras and J.-F. Jaulent.

Working in $\mathbb{Q}\oplus\mathbb{Q}\otimes_{\mathbb{Z}}({}_{\mathrm{N}}\overline{E}_L)$, in which R is a direct summand, we associate with $\varepsilon\in\overline{E}_L$ the component of ε^m on R, of the form θ^ω, with $\omega=\sum_{g\in G}\alpha_g\,g\in\mathbb{Z}[G]$, where $\sum_{g\in G}\alpha_g=0$, then we put:

$$\varphi(\varepsilon)=\alpha_1\in\mathbb{Z}.$$

This map is trivial on $\overline{E}_K$ and defines an element of $\mathrm{Hom}(E_L/\mu_L\,.\,E_K,\mathbb{Z})$ with the G-module action defined as usual by:

$$\psi^h(x):=\psi(x^{h^{-1}}),\quad\text{for all }\psi\in\mathrm{Hom}(E_L/\mu_L\,.\,E_K,\mathbb{Z})\ \text{ and all } h\in G.$$

It is clear that φ generates a $\mathbb{Z}[G]$-submodule whose character is $\chi(\mathbb{Z}[G])-1$. More precisely, a straightforward computation gives $\varphi^g(\varepsilon)=\alpha_g$ for any $g\in G$, thus $\omega=\sum_{g\in G}\alpha_g\,g=\sum_{g\in G}\varphi(\varepsilon^{g^{-1}})\,g$.

In the sequel of the main text we will put $\omega:=\phi(\varepsilon)$.

At this step, Bosca introduces the map λ_n:

$$\lambda_n:\ E_L\longrightarrow E_L/\mu_L\,.\,E_K\xrightarrow{\ \varphi\ }\mathbb{Z}\longrightarrow\mu_{p^n}\longrightarrow 1$$

by a choice of a primitive p^nth root of unity.

This yields an element of $\mathrm{Hom}(E_L,\mu_{p^n})$ which will be, by abuse of notation, identified, via the Kummer duality between radicals and Galois groups, to the corresponding element σ' of the Galois group of $L[\mu_{p^n},E_L^{1/p^n}]/L[\mu_{p^n}]$; then one creates a new condition by saying that σ' coincide with a suitable Frobenius σ, which is the key idea for the proof of the conjecture involving the necessary and sufficient condition about the splitting of at least an infinite place.

References

[1] Georges Gras, *Principalisation d'idéaux par extensions absolument abéliennes*, J. Number Th. **62** (1997), 403–421.

[2] Masato Kurihara, *On the ideal class group of the maximal real subfields of number fields with all roots of unity*, J. European Math. Society **1** (1999), 35–49.

[3] Sébastien Bosca, *Capitulations abéliennes*, thèse de l'Université Bordeaux 1 (2003).

[4] Serge Lang, *Algebraic Number Theory*, second edition, Graduate Texts in Mathematics **110** (1994).