Principalization of ideals in abelian extensions of number fields

Sebastien Bosca

Principalization of ideals in abelian extensions of number fields

Sébastien Bosca

Université de Bordeaux I, Laboratoire A2X, 351 cours de la Libération, 33405 TALENCE Cedex, France

Abstract

For a given extension K/k of number fields in which at least one infinite place is totally split, we show that any ideal I of K is principal in $K.k^{ab}$, where k^{ab} is the maximal abelian extension of k.

In fact for a given I, we build an extension f of k, finite, abelian and in which all infinite places are totally split, such that I is principal in $K.f$.

INTRODUCTION

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

When F/K is cyclic, we still have no general answer but the problem is easier. The kernel of the natural map $j : \mathrm{Cl}_K \to \mathrm{Cl}_F$ is partly known by this way, as explained below: at first, cohomology of cyclic groups says that this kernel is a part of $\hat{H}^1(\mathcal{G}, E_F)$, where $\mathcal{G} = \mathrm{Gal}(F/K)$ and E_F is the unit group of F; $\hat{H}^1(\mathcal{G}, E_F)$ itself is not well known but its order can be deduced from the order of $\hat{H}^0(\mathcal{G}, E_F)$ using the Herbrand quotient; after that, the order of $\hat{H}^0(\mathcal{G}, E_F)$ depends partly from the natural map $E_K \to U_S$, where U_S is the subgroup of the ideles of K which is the product of the local units at the places ramified in F/K (S is the set of such ramified places); finally, the map $E_K \to U_S$ depends on the Frobenius of the ramified primes of F/K in the extension $K[\mu_n][E_K^{1/n}]/K$ (μ_n is the group of n-th roots of unity, and $n = [F : K]$). Obviously, this makes sense only if the primes ramified in F/K are prime to the degree n of the extension.

However, even in this cyclic case, $\mathrm{Ker}(j)$ is not completely given by this 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 F/K is ramified at only one finite place $\mathcal{Q}$ prime with $[F : K]$, when the ramification index $e_{\mathcal{Q}}$ is large enough (precisely, when $|\mathrm{Cl}_K|/e_{\mathcal{Q}}$), $\mathrm{Ker}j$ contains at least the class of $\mathcal{Q}$ in Cl_K. This can be easily established by studying $\hat{H}^1(\mathcal{G}, E_F)$ and can be seen as a particular case of the result proved here (with $k = K$ in the theorem below).

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

Note finally that the hypothesis "at least one infinite place is totally split in K/k" in the theorem below is necessary: in [1], Gras gives examples of extensions K/k with ideals which are not principal in $K.k^{ab}$ (k^{ab} is the maximal abelian extension of k).

THEOREM AND COROLLARIES

Theorem: Let K/k be a finite extension of number fields in which at least one infinite place totally splits. There is an extension f of k, abelian, finite and totally split at all infinite places, such that all ideals of K are principal in the compositum $F = K.f$.

Corollary 1 ($k = \mathbb{Q}$): If K is a totally real number field, any ideal of K is principal in a real cyclotomic extension of K.

Corollary 1 was proved by Masato Kurihara in [2]. In the following, k^{ab} is the maximal abelian extension of k and k^{ab+} its maximal totally real subextension. Moreover,with a little abuse, we say that a field is principal when any of its fractional ideal of finite type is principal.

Corollary 2: Let k be a number field with at least one complex place. Any field containing k^{ab} is principal.
Let k be a totally real number field. Any field containing k^{ab+} whose Galois closure has at least one real place is principal.

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

Corollary 3, for $\mathbb{Q}(i)$ or any imaginary quadratic field in the second assertion,

was proved by Kurihara (see [2], theorem 1.1 p35 and theorem A.1 p46).

Corollary 4: Let k be a number field with at least one complex place. Then, k^{ab} is principal.
Let k be a totally real number field. Any field containing k^{ab+} and 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].

PROOFS

1. About cohomology of cyclic groups

Let F/K be a cyclic extension of number fields with Galois group $\mathcal{G}$, generated by σ; the following notations are used:

E_K the unit group of K;

P_K the group of principal fractional ideals of K;

$P_F^{\mathcal{G}}$ the group of principal fractional ideal of F which are invariant over $\mathcal{G}$;

$\hat{H}^0(\mathcal{G}, E_F) = E_K/N_{F:K}(E_F)$;

$\hat{H}^1(\mathcal{G}, E_F) = \{x \in E_F/N_{F:K}(x) = 1\}/E_F^{1-\sigma}$;

the two quotients above are finite and the quotient of their order is

$q(\mathcal{G}, E_F) = |\hat{H}^0(\mathcal{G}, E_F)|/|\hat{H}^1(\mathcal{G}, E_F)|$ the Herbrand quotient of the units of F.

See [4], chapter IX, §1, for elementary properties of the Herbrand quotient. So, we have the following formula allowing its calculation in a cyclic extension of number fields (see [4], chapter IX, §4 for a proof):

$$q(\mathcal{G}, E_F) = \frac{\prod_{v/\infty} d_v(F/K)}{[F:K]}$$

On the other hand, one has the canonical isomorphism

$$\begin{array}{ccc} \hat{H}^1(\mathcal{G}, E_F) & \simeq & P_F^{\mathcal{G}}/P_K \\ u \in E_K, N(u) = 1, u = z^{1-\sigma} & \longleftrightarrow & (z) \end{array}$$

2. Proof of the theorem

To prove the theorem, one fixes an ideal I of K, and will build an extension f of k, finite, abelian, totally split at all infinite places, cyclic most of the time, such that I is principal in the compositum $K.f$. Obviously, any ideal J of K with the same class in Cl_K will be principal in $K.f$ as well, so that's enough to fix the class c of I in Cl_K. Now, if a generating system of Cl_K is (c_i), we will have a corresponding set (f_i) of extensions, and all ideals of K are principal in $K.f$ where f is the compositum of the (f_i); this will prove the theorem.

So, in the following, one fixes c in Cl_K, and must find f. As the class group of K is direct sum of its p-parts for all prime numbers p, one can suppose that the order of c in Cl_K is a power of a prime p. This changes only few things but is a little bit clearer. So, c and p are fixed; Cl_K is now the p-part of the class group of K, and H_K the maximal p-extension contained in the Hilbert field of K.

(1) one can suppose that $\mathbf{c \in \mathrm{Cl}_K^{p^a}}$ for a fixed integer a:

At first, let's call *abelian compositum* of the extension K/k any extension $F = K.f$ where f is a finite, abelian, totally split at all infinite places, extension of k.

One fixes an integer a; if $c \notin \mathrm{Cl}_K^{p^a}$, one will build an abelian compositum K' of K/k, such that $c \in \mathrm{Cl}_{K'}^{p^a}$; so, if F' is an abelian compositum of K'/k in which c is principal, it's as well an abelian compositum of K/k, so that one can legitimately replace K with K', in which one has $c \in \mathrm{Cl}_{K'}^{p^a}$.

Let's build such a $K' = K.f_0$, as follows: let $\mathcal{Q}$ be a prime of K satisfying the three following conditions:

- $\mathcal{Q}$ totally splits in $K/\mathbb{Q}$;
- $\mathrm{Frob}(\mathcal{Q}, K[\mu_{2p^a}]/K) = \mathrm{id}$;
- $\mathrm{Frob}(\mathcal{Q}, H_K/K) = c$.

If such a $\mathcal{Q}$ exists with $\mathcal{Q}/q$, the two first conditions imply the existence of a subfield f_0' of $\mathbb{Q}(\mu_q)$, cyclic, whose degree is p^a over $\mathbb{Q}$, q being totally split in $f_0'/\mathbb{Q}$; the first condition implies that $f_0 = k.f_0'$ and $K' = K.f_0$ have again a degree p^a over k and K respectively. K'/K is totally ramified at $\mathcal{Q}$, say $\mathcal{Q}'/\mathcal{Q}$ in K'/K, and according to the third condition:

$$c = \overline{\mathcal{Q}} = \overline{\mathcal{Q}}'^{p^a} \in \mathrm{Cl}_{K'}^{p^a} ,$$

as wished.

Now we only have to verify the existence of such a prime $\mathcal{Q}$. The three conditions defining $\mathcal{Q}$ all depends on $\mathrm{Frob}(q, \tilde{H}_K[\mu_{2p^a}]/\mathbb{Q})$, where $\tilde{H}_K$ is the Galois closure of H_K; the two first conditions are equivalent to the fact that this Frobenius is in the subgroup $\mathrm{Gal}(\tilde{H}_K[\mu_{2p^a}]/K[\mu_{2p^a}])$, and then are compatible with the last condition for any c in Cl_K, if and only if $K[\mu_{2p^a}] \cap H_K = K$; if this is right, the Čebotarev theorem states there are infinitely many $\mathcal{Q}$ satisfying the conditions. When this is wrong, we replace K with $K'' = K[\mu_{2p^a}] \cap H_K$ which verifies $K''[\mu_{2p^a}] \cap H_{K''} = K''$.

This last replacement is legitimate as seen above, when $K'' = K[\mu_{2p^a}] \cap H_K$ is an abelian compositum of K/k. In fact, $K'' = K.f$ where f is contained in the maximal p-subfield of $k[\mu_{2p^a}]$, which is abelian and finite but in which infinite places are maybe not totally split if $p = 2$. When $p = 2$ we shall complete the proof, and we take in this particular case $K'' = K.k[\mu_{2^c}]^+$, where the symbol $+$ denotes the maximal ∞-split subextension over k, and where c is an integer, large enough so that K'' contains $H_K \cap K.k[\mu_{2^{a+1}}]^+$, and so that K''/K has degree at least 2. Suppose we have found a prime $\mathcal{Q}''$ of K'' such that:

- $\mathcal{Q}''$ totally splits in $K''/\mathbb{Q}$;
- $\mathrm{Frob}(\mathcal{Q}'', K''[\mu_{2^{a+1}}]/K'') = \mathrm{id}$;
- $\mathrm{Frob}(\mathcal{Q}'', H_{K''}/K'') = c$,

so, f_0' being the totally real subfield of $\mathbb{Q}[\mu_q]$ of degree 2^a over $\mathbb{Q}$, if $f_0 = k[\mu_{2^c}]^+.f_0'$, one has in $K.f_0 = K''.f_0'$ (which is an abelian compositum of K/k), where $\mathcal{Q}'''$ denotes the unique prime of $K''.f_0'$ above $\mathcal{Q}''$:

$$c = \overline{\mathcal{Q}}'' = \overline{\mathcal{Q}}'''^{p^a} \in \mathrm{Cl}_{K.f_0}^{p^a} \ ,$$

as expected.

Now we only have to prove the existence of such a prime $\mathcal{Q}''$ verifying our conditions; the Čebotarev theorem affirms it since the image of $c \in \mathrm{Gal}(H_{K''}/K'')$ in $\mathrm{Gal}(H_{K''} \cap K''[\mu_{2^{a+1}}]/K'')$ is trivial. But K'' contains $H_K \cap K.k[\mu_{2^{a+1}}]^+$, so $H_{K''} \cap K''[\mu_{2^{a+1}}] = K'''$ is either K'' or $K''[i]$, and the image of $j_{K'':K}(c)$ in $\mathrm{Gal}(K'''/K'')$ is trivial, using that $\mathrm{Ver}_{B:A \to B':A'}(\sigma) = \sigma^{[A':A]}$ when B'/A is abelian: $\mathrm{Res}_{K'''}(\mathrm{Ver}_{H_K:K \to H_{K''}:K''}(c)) = \mathrm{Ver}_{H_K:K \to K''':K''}(c) = c^{[K'':K]} = \mathrm{id}$.

(2) one can suppose that K/k is Galois:

$\tilde{K}$ denotes the Galois closure of K over k. Imagine the theorem is proved for $\tilde{K}/k$ (in which at least one infinite place totally splits as in K/k). Hence, there exists an abelian compositum $\tilde{K}.f$ of $\tilde{K}/k$ such that all ideals of $\tilde{K}$ are principal in $\tilde{K}.f$; so, c is principal in $\tilde{K}.f$ but maybe not in $K.f$ and we have to study this.

a) When c is norm in $\tilde{K}/K$, say $c = N_{\tilde{K}:K}(c')$, with $c' \in \mathrm{Cl}_{\tilde{K}}$, c' is princi-

pal in $\tilde{K}.f$, say generated by α, then $N_{\tilde{K}.f:K.f}(c') = c''$ is principal in $K.f$, generated by $N(\alpha)$. On the other hand, $c'' = N_{\tilde{K}:\tilde{K}\cap K.f}(c') \in \mathrm{Cl}_{\tilde{K}\cap K.f}$ so that $N_{\tilde{K}\cap K.f:K}(c'') = N_{\tilde{K}\cap K.f:K}(N_{\tilde{K}:\tilde{K}\cap K.f}(c')) = N_{\tilde{K}:K}(c') = c\ .\ c''$ and its conjugates are principal in $K.f$, and so is c.

b) When c is not a norm in $\tilde{K}/K$, maybe c is not principal in $K.f$. But $N_{\tilde{K}:K}(\mathrm{Cl}_{\tilde{K}})$ contains at least $\mathrm{Cl}_K^{[\tilde{K}:K]} = \mathrm{Cl}_K^{p^a}$, where p^a is the largest power of p dividing $[\tilde{K} : K]$. According to (1) we replace K with $K' = K.f_0$ such that $c \in \mathrm{Cl}_{K'}^{p^a}$. Since $[\tilde{K}' : K'] = [\tilde{K}.f_0 : K.f_0]$ divides $[\tilde{K} : K]$, c is norm in $\tilde{K}'/K'$ and a) applies.

(3) building the extension f - the method and a first condition about the prime $\mathfrak{q}$:

By now we suppose K/k Galois. p and c are fixed and we must build an abelian compositum $K.f$ of K/k such that c is principal in $K.f$. For convenience, we choose f/k as a cyclic p-extension, ramified in only one finite place $\mathfrak{q}$ of k, whose the 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 is principal in $K.f$, or in $K'.f$, where K' is a convenient abelian compositum of K/k. At the end of the proof, in **(7)**, we will study the existence of such $\mathfrak{q}$ verifying all conditions.

Now we fix n, a prime $\mathfrak{q}$ of k, and we wonder if c is principal in $F = K.f$, where f is a cyclic p-extension of k with $e_{\mathfrak{q}}(f/k) = p^n$, unramified but in $\mathfrak{q}$ 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, L being the maximal abelian extension of k unramified but in $\mathfrak{q}$ and ∞-split, class field theory identifies the Galois group $\mathrm{Gal}(L/k)$ with the completion of the quotient

$$\mathcal{I}_k \Big/ k^\times . \prod_{v/\infty} k_v^\times . \prod_{\mathfrak{q}'\neq\mathfrak{q}} U_{\mathfrak{q}'}\ ,$$

where $\mathcal{I}_k$ is the idele group of k and $U_{\mathfrak{q}'}$ the subgroup of local units of $k_{\mathfrak{q}'}^\times$ ($k_{\mathfrak{q}'}$ is the completion of k at the place $\mathfrak{q}'$). The inertia subgroup of $\mathfrak{q}$ in L/k is, according to class field theory, the image of $U_{\mathfrak{q}}$ in the completion of this quotient, that is

$$U_{\mathfrak{q}} \Big/ \overline{U_{\mathfrak{q}} \cap (k^\times . \prod_{v/\infty} k_v^\times . \prod_{\mathfrak{q}'\neq\mathfrak{q}} U_{\mathfrak{q}'})} = U_{\mathfrak{q}} \Big/ \overline{E_k}\ ,$$

where E_k is the unit group of k and the overlining means closure in $U_{\mathfrak{q}}$. If f exists it is contained in the maximal p-extension of L, 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 $|(U_{\mathfrak{q}}/\overline{E_k})_p|$, that is, when $\mathfrak{q} \nmid p$:

- $\mu_{p^n} \subset k_{\mathfrak{q}}^{\times}$, and
- $E_k \subset U_{\mathfrak{q}}^{p^n}$.

This necessary conditions are enough to ensure the existence of f, according to an obvious lemma, which states: if M is an abelian finite group and C is a cyclic subgroup of M of which p^n divides the order, then there is a cyclic quotient of M in which the image of C has order p^n. Note that f is unique if and only if $\mathrm{Cl}_k = 0$.

Now we suppose that $\mathfrak{q}$ verifies the two above conditions, so f exists; we also suppose that $\mathfrak{q}$ is unramified in K/k: then all primes $\mathcal{Q}/\mathfrak{q}$ of K/k are ramified in $F = K.f$ with the same index $e_{\mathcal{Q}} = p^n$; and then $[F : K] = p^{n+d}$ for some positive integer d. $\mathcal{G}$ denotes the Galois group $\mathrm{Gal}(F/K)$, cyclic with order p^{n+d}, while $G = \mathrm{Gal}(K/k)$.

(4) obtaining a big $\hat{\mathbf{H}}^{\mathbf{0}}(\mathcal{G}, \mathbf{E_F})$:

At least one infinite place is totally split in the extension K/k with Galois group G, and according the Herbrand theorem, the character of $\mathbb{Q} \otimes_{\mathbb{Z}} E_K$ is

$$\chi(E_K) = \left(\sum_{\substack{v/\infty \\ v \in \mathrm{Pl}_{(K)}}} \mathrm{Ind}_{D_v}^{G} 1 \right) - 1 \ ,$$

where 1 is the trivial character of G; so that the character of $\mathbb{Q} \otimes_{\mathbb{Z}} (E_K/\mu_K.E_k)$ satisfies

$$\chi(E_K/\mu_K.E_k) \geq \chi(\mathbb{Z}[G]) - 1 \ ,$$

and we can deduce from this the existence of a map

$$\varphi : E_K/\mu_K.E_k \longrightarrow \mathbb{Z}$$

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

On the other hand, since $K[\mu_{p^n}, E_K^{1/p^n}]/K[\mu_{p^n}]$ is a Kummer extension, if $\mathcal{Q}_0$ is one of the primes of K dividing $\mathfrak{q}$, $\sigma_0 = \mathrm{Frob}(\mathcal{Q}_0, K[\mu_{p^n}, E_K^{1/p^n}]/K)$ is given by the map $\begin{pmatrix} E_K \longrightarrow \mu_{p^n} \\ u \mapsto \frac{\sigma_0(u^{1/p^n})}{u^{1/p^n}} \end{pmatrix}$ and we suppose now this map is

$$\lambda_n : E_K \longrightarrow E_K/\mu_K.E_k \xrightarrow{\varphi} \mathbb{Z} \longrightarrow \mu_{p^n} \ ,$$

where the left map is the natural one and the right one is surjective (you must choose one primitive p^n-th root of unity for the right map, but this choice

doesn't change the Frobenius defined up to conjugation: changing the choice of the root is the same that changing the choice of a prime $\mathcal{Q}'/\mathcal{Q}$ in $K[\mu_{p^n}/K]$).

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

Let ϕ denote the map $\begin{pmatrix} E_K & \longrightarrow & \{X=\sum_g \alpha_g e_g \in \mathbb{Z}[G]/\sum_g \alpha_g = 0\} = R_G \\ u & \mapsto & \sum_g \varphi(g^{-1}(u))e_g \end{pmatrix}$;
$\mathrm{Im}\phi$ has finite index, say A. So, p^δ being the maximal power of p dividing A, one has:

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

On the arithmetical side, the ramification indexes at all primes $\mathcal{Q}/\mathfrak{q}$ of K are all equal to p^n in F/K, so that, with $\mathcal{Q}'/\mathcal{Q}/\mathfrak{q}$ in $F/K/k$:

$$N_{F:K}(E_F) \subset \prod_{\mathcal{Q}'/\mathfrak{q}} N_{F:K}(U_{\mathcal{Q}'}) = \prod_{\mathcal{Q}/\mathfrak{q}} U_{\mathcal{Q}}^{p^n} \ ,$$

and then,

$$\{u \in E_K/\forall g \in G, \lambda_n(g(u))=1\} = E_K \cap \prod_{\mathcal{Q}/\mathfrak{q}} U_{\mathcal{Q}}^{p^n} \supset N_{F:K}(E_F) \ ,$$

so that

$$|H^0(\mathcal{G},E_F)| = |E_K/N_{F:K}(E_F)| \geq |E_K/\{u \in E_K/\forall g \in G, \lambda_n(g(u))=1\}| \ ,$$

and we finally have from the character theory side

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

(5) study of $\hat{\mathbf{H}}^{\mathbf{1}}(\mathcal{G},\mathbf{E_F})$:

F/K is totally split at all infinite places, so that according to **1.**, one has

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

and then

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

1. also states that there is a canonical isomorphism

$$\hat{H}^1(\mathcal{G},E_F) = P_F^{\mathcal{G}}/P_K \ ,$$

then $|P_F^{\mathcal{G}}/P_K| \geq p^{n|G|+d-\delta}$; on the other hand,

$$|I_F^{\mathcal{G}}/I_K| = \prod_{\mathcal{Q}} e_{\mathcal{Q}} = p^{n.|G|} \ ,$$

where I_K is the group of the fractional ideals of K; then, one has

$$|I_F^{\mathcal{G}}/P_F^{\mathcal{G}}| = \frac{|I_F^{\mathcal{G}}/P_K|}{|P_F^{\mathcal{G}}/P_K|} = \frac{|I_F^{\mathcal{G}}/I_K|.|I_K/P_K|}{|P_F^{\mathcal{G}}/P_K|} = \frac{p^{n|G|}.|\mathrm{Cl}_K|}{|P_F^{\mathcal{G}}/P_K|} \leq \frac{p^{n|G|}.|\mathrm{Cl}_K|}{p^{n|G|+d-\delta}} \ ,$$

that is

$$|I_F^{\mathcal{G}}/P_F^{\mathcal{G}}| \leq |\mathrm{Cl}_K|.p^{\delta-d} \ .$$

Note that the number at the right hand doesn't depend on n.

(6) is c principal in F ?

Here, we also suppose that

$$\mathrm{Frob}(\mathcal{Q}_0, H_K/K) = c \ .$$

F_{td} being the maximal subfield of F/K in which $\mathcal{Q}_0$ totally splits, one has

$$\mathcal{Q}_0 = \prod_{\mathcal{Q}_0'/\mathcal{Q}_0 \text{ in } F_{td}/K} \mathcal{Q}_0'$$

and for all prime $\mathcal{Q}_0'/\mathcal{Q}_0$ of F_{td}/K,

$$\mathcal{Q}_0' = \mathcal{Q}_0''^{p^n} \ ,$$

where $\mathcal{Q}_0''$ is the unique prime of F dividing $\mathcal{Q}_0'$. Finally, in F,

$$\mathcal{Q}_0 = \left(\prod_{\mathcal{Q}_0'/\mathcal{Q}_0} \mathcal{Q}_0'' \right)^{p^n} \ ,$$

with $\prod_{\mathcal{Q}_0'/\mathcal{Q}_0} \mathcal{Q}_0'' \in I_F^{\mathcal{G}}$. According to (5), $|I_F^{\mathcal{G}}/P_F^{\mathcal{G}}| \leq |\mathrm{Cl}_K|.p^{\delta-d}$, then

$$\left(\prod_{\mathcal{Q}_0'/\mathcal{Q}_0} \mathcal{Q}_0'' \right)^{|\mathrm{Cl}_K|.p^{\delta-d}} \in P_F^{\mathcal{G}} \ .$$

Hence, in Cl_F, one has both

$$c = \overline{\mathcal{Q}}_0 = \left(\prod_{\mathcal{Q}_0'/\mathcal{Q}_0} \overline{\mathcal{Q}}_0'' \right)^{p^n} \quad \text{and} \quad \left(\prod_{\mathcal{Q}_0'/\mathcal{Q}_0} \overline{\mathcal{Q}}_0'' \right)^{|\mathrm{Cl}_K|.p^{\delta-d}} = 0 \ .$$

So, w being such that $|\mathrm{Cl}_K| = p^w$, c is principal in F since

$$\boxed{n \geq w + \delta - d}$$

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

We just proved that c is principal in F when n is large enough and when $\mathfrak{q}$ (or $\mathcal{Q}_0/\mathfrak{q}$) satisfies the following six conditions:

- $\mathfrak{q} \nmid p$
- $\mu_{p^n} \subset k_{\mathfrak{q}}^{\times}$
- $E_k \subset U_{\mathfrak{q}}^{p^n}$
- $\mathfrak{q}$ is totally split in K/k
- $\mathrm{Frob}(\mathcal{Q}_0, K[\mu_{p^n}, E_K^{1/p^n}]/K) = \lambda_n$
- $\mathrm{Frob}(\mathcal{Q}_0, H_K/K) = c$

The definition of $\lambda_n \in \mathrm{Gal}(K[\mu_{p^n}, E_K^{1/p^n}]/K)$ shows it is trivial on $K[\mu_{p^n}, E_k^{1/p^n}]$ 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 and λ_n are equal on the extension $H_K \cap K[\mu_{p^n}, E_K^{1/p^n}]$ of K.

Let m be the integer such that $|\mu_K| = p^m$; one has, where the exponent ab means abelian part over K:

$$H_K \cap K[\mu_{p^n}, E_K^{1/p^n}] \subset H_K \cap (K[\mu_{p^n}, E_K^{1/p^n}])^{ab} = H_K \cap K[\mu_{p^{n+m}}, E_K^{1/p^m}] \; ;$$

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

$$H_K \cap K[\mu_{p^n}, E_K^{1/p^n}] = H_K \cap K[\mu_{p^{m'}}, E_K^{1/p^m}] \; .$$

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

About the restriction of λ_n on $H_K \cap K[\mu_{p^n}, E_K^{1/p^n}]$, we can as well suppose it is trivial, by replacing eventually λ_n with $\lambda_n^{p^{m'}}$, and φ with $p^{m'}.\varphi$ which as the same properties.

Up to replacing K with K' and choosing a convenient φ, restrictions of c and of λ_n are both trivial on $H_K \cap K[\mu_{p^n}, E_K^{1/p^n}]$: 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 F in which c is principal. This proves the theorem.

3. 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 K containing k^{ab+} and in which at least one infinite place totally splits over k is principal.

To prove this, Let I be a fractional ideal of finite type of K. I is as well a fractional ideal of an extension K_I with finite dimension over $\mathbb{Q}$, contained in K. We can suppose $K_I \supset k$, then K_I/k is an extension of number fields in which at least one infinite place is totally split; according to the theorem, I is principal in an abelian compositum $K_I.f$ of K_I/k; but $K_I.f \subset K.k^{ab+} = K$ and I is principal in K.

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

Corollary 4 comes from Corollary 2.

References

[1] Georges Gras, *Principalisation d'idéaux par extensions absolument abéliennes*, Journal of Number Theory n°62, 1997, p 403-421.

[2] Masato Kurihara, *On the ideal class group of the maximal real subfields of number fields with all roots of unity*, Journal of the European Mathematical Society n°1, 1999, p 35-49.

[3] Sébastien Bosca, *Capitulations abéliennes*, thèse de l'université Bordeaux I soutenue le 7 novembre 2003.

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