Journal de Théorie des Nombres
de Bordeaux **17** (2005), 467–473

Comparing orders of Selmer groups

par SÉBASTIEN BOSCA

RÉSUMÉ. En utilisant la théorie du corps de classes et la théorie de Kummer, nous calculons l'ordre de deux groupes de Selmer, et nous les comparons: le quotient des deux ordres ne dépend que de conditions locales.

ABSTRACT. Using both class field and Kummer theories, we propose calculations of orders of two Selmer groups, and compare them: the quotient of the orders only depends on local criteria.

Notations

- K is a number field.
- E_K is the unit group of K.
- $\mu_{K,n}$ is the set of n^{th} roots of unity in K.
- $\mathrm{Pl}(K)$ is the set of places of K.
- r_1 is the number of real places of K.
- r_2 is the number of complex places of K.
- (x) the principal fractionnal ideal genberated by x, with $x \in K^\times$.
- $\mathcal{I}_K$ is the group of fractionnal ideals of K.
- $\mathcal{I}'_K \subset \mathcal{I}_K$ is the subgroup of fractionnal ideals of K prime to some set S of prime ideals (to be named after).
- $P_K \subset \mathcal{I}_K$ is the group of principal fractionnal ideals of K.
- $\mathcal{P}'_K \subset \mathcal{P}_K$ is the group of principal fractionnal ideals of K prime to S.
- $\mathrm{Cl}_K = \mathcal{I}_K/P_K$ is the class group of K.
- $K^{\times\prime} \subset K^\times$ is the subgroup of elements prime to S.
- $\mathcal{J}_K$ is the idele group of K.
- $U_v \subset K_v^\times$ is the subgroup of v-units for a given finite place v of K. When v is an infinite place of K, our convention is to note U_v for the whole group $K_v^\times$.
- e_v is the ramification index of v in F/K for a given finite place v of K. When v is an infinite place of K, our convention is: $e_v = 1$ when v totally splits at v and $e_v = 2$ in the other case; with this convention, we see v as a ramified place if $e_v = 2$.

Manuscrit reçu le 30 mai 2005.

- $\mathfrak{U}_K = \prod_{v|\infty} K_v^\times \prod_{v\nmid\infty} U_v$ is the subgroup of "units" of $\mathfrak{I}_K$.
- $\mathfrak{M} \subset \mathfrak{U}_K$ is an open subgroup of the unit idele group of K; more precisely, $\mathfrak{M} = \prod_v \mathfrak{M}_v$ is a product of open subgroups of the multiplicative groups $K_v^\times$, and $\mathfrak{M}_v = U_v$ if v is a finite place which is not in S.
- $P_{\mathfrak{M}} \subset P_K'$ is the subgroup of principal ideals generated by an element x of $K^\times$ whose image in $\mathfrak{I}_K$ is in $\mathfrak{M}_v$ for all v in S or dividing the infinite place of $\mathbb{Q}$.
- $N = N_{F:K}$ is the norm map.

Finally, for a given finite abelian group G and a given integer n, we note

$$G^{(n)} = \{g \in G / g^n = 1\}$$

and

$$G_{(n)} = G/G^n.$$

$G^{(n)}$ and $G_{(n)}$ are respectively the maximal subgroup and quotient of G with n as an exponant. They have the same order.

Introduction

For a given cyclic extension of number fields F/K with degree n, to answer a question by Henri Cohen (asked in the particular case $F = K(i)$), we propose to calculate the orders of

$$S(F/K) = \{x \in K^\times / (x) \in \mathcal{I}_K^n, x \in N(F^\times)\}/K^{\times n}$$

and

$$G(F/K) = \{I \in \mathcal{I}_K / \exists J \in \mathcal{I}_F, N(J) = I\}/\mathcal{I}_K^n N(P_F)\ .$$

In fact, calculations of the orders of these groups are not very usefull because we cannot express them only with local criteria (however we express them with only classical things manipulated in class field theory). But the point is that the quotient of these two orders only depends on local criteria, and that was enough to solve the problem of H. Cohen. So, the main result is the following:

Theorem. *If F/K is a cyclic extension of number fields with degree n, one has:*

$$\frac{|S(F/K)|}{|G(F/K)|} = \frac{|\mu_{K,n}| n^{r_1+r_2}}{\prod_{v \in \mathrm{Pl}(K)} e_v}\ .$$

Two ways are given to prove this result: the first one uses class field theory and interpretations of some groups as Galois groups or Kummer radicals of some extensions; the second one is faster and only uses the ambigous classes formula from Chevalley; it was proposed by Georges Gras, who referred the first version of this article. I thank him for his work. So, the second way is more acheived, while the first one shows more how to find the result. Note also that in section 1 (the first way), we suppose that K contains all n^{th} roots of unity, while in section 2 (the second way), this hypothesis is useless; that's a pity, but the question was initially asked for $n = 2$ (see [1]), and all number fields contains 1 and -1; moreover, the calculus made in section 1 can be adapted when K doesn't contain all n^{th} roots of unity, replacing K with $K[\mu_n]$ and things like this, but that seem complications for nothing since the second way prove the result in all cases. An interested reader may examine that.

1. Using Class Field theory

1.1. Calculation of the order of $S(F/K)$ as a Galois group.

Here, we see $S(F/K)$ as a ray class group, according to class field theory. One has a natural map

$$\phi \begin{pmatrix} S(F/K) & \longrightarrow & \mathrm{Cl}_K^{(n)} \\ x & \mapsto & \overline{I}/(x) = I^n \end{pmatrix}$$

whose kernel is

$$\mathrm{Ker}\ \phi = \frac{E_K \cap N(F^\times)}{E_K^n} .$$

To study Im ϕ, let's note, for each place v of K with w/v in F/K, $N_v = U_v \cap N(F_w^\times)$, and

$$\mathfrak{M} = \prod_{v \in \mathrm{Pl}(K)} U_v \ ;$$

we also note S the set of ramified places in the extension F/K. The Hasse principle applied in the cyclic extension F/K, leads to

$$\mathrm{Im}\ \phi = \{I \in \mathcal{I}'_K / I^n \in P_{\mathfrak{M}}\}/P'_K \ ,$$

so that

$$\begin{aligned} |\mathrm{Im}\ \phi| &= |\{I \in \mathcal{I}'_K/I^n \in P_{\mathfrak{M}}\}/P_{\mathfrak{M}}||P'_K/P_{\mathfrak{M}}|^{-1} \\ &= |(\mathcal{I}'_K/P_{\mathfrak{M}})^{(n)}||P'_K/P_{\mathfrak{M}}|^{-1} \ . \end{aligned}$$

On the other hand, $K^\times \cap \mathfrak{M}$ denoting the group of elements of $K^\times$ whose image in $\mathcal{I}_K$ is in $\mathfrak{M}$, one has the exact sequence

$$1 \longrightarrow E_K/E_K \cap \mathfrak{M} \longrightarrow K^{\times'}/K^{\times'} \cap \mathfrak{M} \longrightarrow P'_K/P_{\mathfrak{M}} \longrightarrow 1 \ ,$$

so that

$$|P'_K/P_{\mathfrak{M}}| = |K^{\times'}/K^{\times'} \cap \mathfrak{M}|/|E_K/E_K \cap \mathfrak{M}|$$
$$= \prod_v e_v/|E_K/E_K \cap \mathfrak{M}| \ .$$

Using the facts that $|S(F/K)| = |\mathrm{Ker}\ \phi||\mathrm{Im}\ \phi|$ and that $E_K \cap \mathfrak{M} = E_K \cap N(F^\times)$; $|E_K/E_K^n| = n^{r_1+r_2-1}|\mu_{K,n}|$, one has

$$|S(F/K)| = \frac{|(\mathcal{I}'_K/P_{\mathfrak{M}})^{(n)}|n^{r_1+r_2-1}|\mu_{K,n}|}{\prod_v e_v} \ .$$

1.2. Calculation of the order of $S(F/K)$ as a radical.

In subsections 1.2 and 1.3 we suppose $|\mu_{K,n}| = n$.

$S(F/K)$ is a subgroup of $K^\times/K^{\times n}$, so that it is the radical of some Kummer extension L of K, with exponant n. We should study the local norm group $N_{L:K}(\mathfrak{I}_L)$ to calculate the degree of L/K.

Let $x \in K^\times/K^{\times n}$; according to the Hasse principle, $x \in S(F/K)$ if and only if:

- $n/v_{\mathfrak{P}}(x)$ is for each prime $\mathfrak{P}$;
- $x \in N_v$ for all $v \in S$.

For any prime ideal $\mathfrak{P}$, we note $\eta_{\mathfrak{P}}$ the unique element of $U_{\mathfrak{P}}/U_{\mathfrak{P}}^n$ such that $K_{\mathfrak{P}}[\eta_{\mathfrak{P}}^{1/n}]$ is the unique non ramified extension of $K_{\mathfrak{P}}$ with degree n. The first condition about the elements of the radical of L/K is equivalent to the fact that $N_{L:K}(\mathfrak{I}_L) \ni \eta_{\mathfrak{P}}$ (use the symetry of the local n^{th} Hilbert symbol to see this: for a local Kummer extension with exponant n L_w/K_v, $\mathrm{Rad}(L_w/K_v) \subset X \iff < \mathrm{Rad}(L_w/K_v), X^\perp > = 1 \iff N(L_w^\times) \supset X^\perp$). The last condition is equivalent to the fact that $N_{L:K}(\mathfrak{I}_L)$ contains both η_v and x_0 for each v in S.

Finally, L is then defined by the fact that

$$N_{L:K}(\mathfrak{I}_L) \supset \mathfrak{M}^*\mathfrak{I}_K^n \ ,$$

where

$$\mathfrak{M}^* = \prod_{v \in \mathrm{Pl}(K)} N_v^\perp = \prod_{v \text{ real}} N_v^\perp \prod_{v \text{ complex}} K_v^\times \prod_{\mathfrak{P} \text{ prime}} x_0^{\mathbb{Z}} \eta_{\mathfrak{P}}^{\mathbb{Z}} U_{\mathfrak{P}}^n \ .$$

Note that $\mathfrak{M}^* \subset \mathfrak{U}_K$. So, one has:

$$|S(F/K)| = |\mathrm{Rad}(L/K)| = |\mathrm{Gal}(L/K)|$$
$$= |\mathfrak{I}_K/K^\times \mathfrak{M}^* \mathfrak{I}_K^n| = |(\mathcal{I}'_K/P_{\mathfrak{M}^*})_{(n)}| \ ,$$

the last equality coming from $\mathfrak{I}_K/K^\times\mathfrak{M}^* = \mathcal{I}'_K/P_{\mathfrak{M}^*}$ is a well known Galois group with ray $\mathfrak{M}^*$.

1.3. Calculation of the order of $G(F/K)$.

One has:

$$|G(F/K)| = |\{I \in \mathcal{I}_K / \exists J \in \mathcal{I}_F, N(J) = I\}/\mathcal{I}_K^n N(P_F)|$$
$$= |N(I_F)/I_K^n N(P_F)| \ ;$$

note now that $I_M = \mathfrak{I}_M/\mathfrak{U}_M$ for $M = F$ and $M = K$, so that

$$|G(F/K)| = |N(\mathfrak{I}_F/N(\mathfrak{U}_F)\mathfrak{I}_K^n N(F^\times)| \ .$$

On the other hand, the Hasse principle leads to

$$N(\mathfrak{U}_F)N(F^\times) = N(\mathfrak{I}_F) \cap K^\times N(\mathfrak{U}_F) \ ,$$

so that

$$|G(F/K)| = |N(\mathfrak{I}_F)/[N(\mathfrak{I}_F) \cap K^\times N(\mathfrak{U}_F)]\mathfrak{I}_K^n| \ .$$

We now interprete this formula: at first,

$$\mathfrak{I}_K/K^\times N(\mathfrak{U}_F)$$

is, according to class field theory, the Galois group of the maximal abelian extension of K which is not more ramified than F (note also that $N(\mathfrak{U}_F$ is equal to $\mathfrak{M}$ defined in subsection 1.1). Call T this extension. After this,

$$\mathfrak{I}_K/K^\times N(\mathfrak{U}_F)\mathfrak{I}_K^n$$

is just $(\mathrm{Gal}(T/K))_{(n)} = \mathrm{Gal}(T'/K)$, where $T' \subset T$ is the maximal subextension with exponant n. So, $N(\mathfrak{I}_F)/[N(\mathfrak{I}_F) \cap K^\times N(\mathfrak{U}_F)]\mathfrak{I}_K^n$ is the subgroup of $\mathfrak{I}_K/K^\times N(\mathfrak{U}_F)\mathfrak{I}_K^n$ whose elements are norms from $\mathfrak{I}_F$ (since $\mathfrak{I}_K^n \subset N(\mathfrak{I}_F)$). But the subgroup of norms from F on the idele side corresponds with the subgroup obtained by restriction from F on the Galois side, so that

$$G(F/K) = \mathrm{Gal}(T'/F) = \frac{[T' : K]}{n} \ .$$

Now, $[T' : K] = |\mathrm{Gal}(T'/K)| = |\mathrm{Gal}(T/K)_{(n)}| = |(\mathfrak{I}'_K/P_{\mathfrak{M}})_{(n)}|$, so that

$$|G(F/K)| = |(\mathfrak{I}'_K/P_{\mathfrak{M}})_{(n)}|/n \ .$$

The subsections 1.1 and 1.3 prove the theorem.

2. Using Ambigous classes formula

One has the following 4 short exact sequences, for any cyclic extension F/K with degree n and σ as a generator of $\mathrm{Gal}(F/K)$ (j denotes natural maps):

$$1 \to E_K \cap N(F^\times)/E_K^n \to S(F/K) \to \{c \in \mathrm{Cl}_K, j(c) \in \mathrm{Cl}_F^{\sigma-1}\} \to 1 \ ,$$

$$1 \to \mathcal{I}_F^{\sigma-1} j(\mathcal{I}_K)P_F/j(\mathcal{I}_K)P_F \to \mathcal{I}_F/j(\mathcal{I}_K)P_F \to$$
$$N(\mathcal{I}_F)/\mathcal{I}_K^n N(P_F) = G(K) \to 1 \ ,$$

$$1 \to j(\mathcal{I}_K)P_F/P_F \to \mathcal{I}_F^{\sigma-1}j(\mathcal{I}_K)P_F/P_F \to \mathcal{I}_F^{\sigma-1}j(\mathcal{I}_K)P_F/j(\mathcal{I}_K)P_F \to 1 \ ,$$
$$1 \to \{c \in \mathrm{Cl}_K, j(c) \in \mathrm{Cl}_F^{\sigma-1}\} \to \mathrm{Cl}_K \to \mathrm{Cl}_F^{\sigma-1}j(\mathrm{Cl}_K)/\mathrm{Cl}_F^{\sigma-1} \to 1 \ .$$

So, one has

$$\begin{aligned} |S(F/K)| &= |E_K \cap N(F^\times)/E_K^n||\{c \in \mathrm{Cl}_K, j(c) \in \mathrm{Cl}_F^{\sigma-1}\}| \\ &= |E_K \cap N(F^\times)/E_K^n|\frac{|\mathrm{Cl}_K|}{|\mathrm{Cl}_F^{\sigma-1}j(\mathrm{Cl}_K)/\mathrm{Cl}_F^{\sigma-1}|} \end{aligned}$$

and

$$\begin{aligned} |G(F/K)| &= \frac{|\mathcal{I}_F/j(\mathcal{I}_K)P_F|}{|\mathcal{I}_F^{\sigma-1}j(\mathcal{I}_K)P_F/j(\mathcal{I}_K)P_F|} \\ &= |\mathcal{I}_F/j(\mathcal{I}_K)P_F|.\frac{|j(\mathcal{I}_K)P_F/P_F|}{|\mathcal{I}_F^{\sigma-1}j(\mathcal{I}_K)P_F/P_F|} \\ &= |\mathrm{Cl}_F/j(\mathrm{Cl}_K)|.\frac{|j(\mathrm{Cl}_K)|}{|\mathrm{Cl}_F^{\sigma-1}j(\mathrm{Cl}_K)|} \ , \end{aligned}$$

so that

$$\begin{aligned} \frac{S(F/K)}{G(F/K)} &= \frac{|E_K \cap N(F^\times)/E_K^n|\frac{|\mathrm{Cl}_K|}{|\mathrm{Cl}_F^{\sigma-1}j(\mathrm{Cl}_K)/\mathrm{Cl}_F^{\sigma-1}|}}{|\mathrm{Cl}_F/j(\mathrm{Cl}_K)|.\frac{|j(\mathrm{Cl}_K)|}{|\mathrm{Cl}_F^{\sigma-1}j(\mathrm{Cl}_K)|}} \\ &= \frac{|E_K \cap N(F^\times)/E_K^n|.|\mathrm{Cl}_K|.|\mathrm{Cl}_F^{\sigma-1}|}{|\mathrm{Cl}_F|} \ . \end{aligned}$$

Remember now the well known ambigous classes formula from Chevalley (see [2]): for any cyclic extension F/K with degree n, one has:

$$|\mathrm{Cl}_F^G| = |\mathrm{Cl}_F/\mathrm{Cl}_F^{\sigma-1}| = \frac{|\mathrm{Cl}_K|\prod_{v\in\mathrm{Pl}(K)} e_v}{n.|E_K/E_K \cap N(F^\times)|} \ ;$$

Then, it comes

$$\begin{aligned} \frac{S(F/K)}{G(F/K)} &= \frac{|E_K \cap N(F^\times)/E_K^n|.|\mathrm{Cl}_K|}{|\mathrm{Cl}_F/\mathrm{Cl}_F^{\sigma-1}|} \\ &= \frac{|E_K \cap N(F^\times)/E_K^n|.n.|E_K/E_K \cap N(F^\times)|}{\prod_{v\in\mathrm{Pl}(K)} e_v} \\ &= \frac{n.|E_K/E_K^n|}{\prod_{v\in\mathrm{Pl}(K)} e_v} = \frac{n^{r_1+r_2}|\mu_{K,n}|}{\prod_{v\in\mathrm{Pl}(K)} e_v} \ , \end{aligned}$$

as wished.

References

[1] Henri Cohen, Francisco Diaz y Diaz, Michel Olivier, *Counting Cyclic Quartic Extensions of a Number Field.* Journal de Théorie des Nombres de Bordeaux **17** (2005), 475–510.

[2] Georges Gras, *Class Field Theory, from theory to practice.* Springer Monographs in Mathematics, second edition 2005.

Sébastien Bosca
Université de Bordeaux I
Laboratoire A2X
351, cours de la libération
33405 TALENCE Cedex, France
E-mail : Sebastien.Bosca@math.u-bordeaux1.fr