Stickelberger's congruences for absolute norms of relative discriminants

Georges Gras

Journal de Théorie des Nombres
de Bordeaux 00 (XXXX), 000–000

Stickelberger's congruences for absolute norms of relative discriminants

par Georges GRAS

Résumé. Nous généralisons un résultat de J. Martinet sur les congruences de Stickelberger pour les normes absolues des discriminants relatifs des corps de nombres, en utilisant des arguments classiques du corps de classes.

Abstract. We give an improvement of a result of J. Martinet on Stickelberger′s congruences for the absolute norms of relative discriminants of number fields, by using classical arguments of class field theory.

1. Introduction

Let L/K be a finite extension of number fields. Denote by $\mathfrak{d}_{L/K}$ the relative discriminant of L/K and by c the number of complex infinite places of L which lie above a real place of K.

The absolute norm of an ideal $\mathfrak{a}$ of K is a positive rational denoted $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{a})$; it is the positive generator of $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$, where $\mathrm{N}_{K/\mathbb{Q}}$ is the arithmetic norm. If $\alpha \in K^\times$, we define the *absolute norm of* α (or (α)) by $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\alpha) := |\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)\,|$ (this has some importance in class field theory).

In [Ma], J. Martinet proved the following result about $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})$:

Proposition 1. *If K contains a primitive 2^{m+1}th root of unity ($m \geq 0$) and if L/K is not ramified at 2, then $(-1)^c\,\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) \equiv 1 \bmod (4 \cdot 2^m)$.*

In [Pi], S. Pisolkar proved, in connection with the previous result:

Proposition 2. *Let $p \geq 2$ be any prime number. Let K_v be the completion of K at a place $v \,|\, p$ (or any finite extension of $\mathbb{Q}_p$); we suppose that K_v contains a primitive p^{h+1}th root of unity, $h \geq 0$. Let $K_v(\sqrt[p]{\alpha})$, $\alpha \in K_v^\times$, be an unramified Kummer extension of K_v. Then $\mathrm{N}_{K_v/\mathbb{Q}_p}(\alpha) \equiv 1 \bmod (p^{h+2})$.*

Manuscrit reçu le 27 mars 2010, révisé le 8 avril 2010.
1991 *Mathematics Subject Classification.* 11R29, 11R37.
Mots clefs. Number fields, Discriminants, Stickelberger congruences, Class field theory, Kummer theory.

In this paper we give a synthetic proof of these results with some generalization of the hypothesis (especially for the case $p = 2$); see Theorem 2.

2. Prerequisites on discriminants

Classical proofs of Stickelberger's congruences make use of the fact that any odd discriminant ideal $\mathfrak{d}_{L/K}$ is canonically associated with the discriminant of a quadratic extension of K, unramified at 2. This essential reduction is summarized in the following proposition (see [Ma, § 3]).

Proposition 3. *Let L/K be a finite extension of number fields and let $\alpha\, K^{\times 2}$, in $K^\times/K^{\times 2}$, be the image of the discriminant α of a K-base of L. Then:*

(i) The class $\alpha\, K^{\times 2}$ does not depend on the choice of the K-base.

(ii) Let $K' := K(\sqrt{\alpha})$; then there exists an integral ideal $\mathfrak{a}$ of K such that $\mathfrak{d}_{L/K} = \mathfrak{d}_{K'/K}\, \mathfrak{a}^2$.

(iii) If 2 is unramified in L/K it is unramified in K'/K and we have $\mathfrak{d}_{K'/K} = (\alpha)\, \mathfrak{b}^2$, hence $\mathfrak{d}_{L/K} = (\alpha)\, \mathfrak{c}^2$, where $\mathfrak{b}$ and $\mathfrak{c}$ are ideals of K.

We suppose in the sequel that $\mathfrak{d}_{L/K}$ is odd; thus we can choose, modulo $K^{\times 2}$, an odd α, which implies that $\mathfrak{c}$ is odd. We then have to compute $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{c})^2$ and $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\alpha)$.

3. Computation of $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{c})^2$.

From class field theory over $\mathbb{Q}$ we get $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{c}) \in A_K$, the Artin group of K which is that of K^{ab}, where K^{ab} is the maximal abelian subextension of K.

So we see that to obtain nontrivial congruences modulo a power of 2 we must suppose that this Artin group is roughly a ray group mudulo a power of 2 in the following way.

Let $\mathbb{Q}(\mu_{2^\infty})$ be the field generated by all roots of unity of order a power of 2. The best hypothesis is that K does contain a subfield k of $\mathbb{Q}(\mu_{2^\infty})$ of degree 2^m, $m \geq 0$.

For $m = 0$ we get $k = \mathbb{Q}$ (which is also $\mathbb{Q}^{(0)}$ in the description below) and for any $m \geq 1$, the field k is equal to one of the following three fields, for which we indicate its Artin group as a subgroup of $A_{\mathbb{Q}} := \{u\,\mathbb{Z},\ u \in \mathbb{Q}^\times,\ u \text{ odd}\}$ (see e.g. [Gr, II.5.5.2]):

- $k = \mathbb{Q}^{(m)}$ is the subfield, of degree 2^m, of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$; its Artin group is:

$$A_{\mathbb{Q}^{(m)}} = \{u\,\mathbb{Z},\ u \in \mathbb{Q}^\times,\ u > 0,\ u \equiv \pm 1 \bmod (4 \cdot 2^m)\}\,;$$

- $k = \mathbb{Q}'^{(m)}$, $m \geq 1$, is the subfield of $\mathbb{Q}(\mu_{4\cdot 2^m})$ of relative degree 2, distinct from $\mathbb{Q}(\mu_{4\cdot 2^{m-1}})$ and from $\mathbb{Q}^{(m)}$; its Artin group is

$$A_{\mathbb{Q}'^{(m)}} = \{u\,\mathbb{Z},\ u \in \mathbb{Q}^\times,\ u > 0,\ u \equiv 1 \text{ or } -1 + 4\cdot 2^{m-1} \bmod (4\cdot 2^m)\}\,;$$

- $k = \mathbb{Q}(\mu_{4\cdot 2^{m-1}})$, $m \geq 1$; its Artin group is

$$A_{\mathbb{Q}(\mu_{4\cdot 2^{m-1}})} = \{u\,\mathbb{Z},\ u \in \mathbb{Q}^\times,\ u > 0,\ u \equiv 1 \bmod (4\cdot 2^{m-1})\}\,.$$

So this yields

$$\mathrm{N}_{K/\mathbb{Q}}\,(\mathfrak{c})^2 \in \{u\,\mathbb{Z},\ u \in \mathbb{Q}^\times,\ u > 0,\ u \equiv 1 \bmod (4\cdot 2^m)\}\,,$$

except if $k = \mathbb{Q}^{(m)}$, in which case

$$\mathrm{N}_{K/\mathbb{Q}}\,(\mathfrak{c})^2 \in \{u\,\mathbb{Z},\ u \in \mathbb{Q}^\times,\ u > 0,\ u \equiv 1 \bmod (4\cdot 2^{m+1})\}\,;$$

in other words, taking absolute norms:

$$\begin{aligned}
\overline{\mathrm{N}}_{K/\mathbb{Q}}\,(\mathfrak{c})^2 &\equiv 1 \bmod (4\cdot 2^m), \quad \text{if } k = \mathbb{Q}'^{(m)} \text{ or } \mathbb{Q}(\mu_{4\cdot 2^{m-1}}),\ m \geq 1,\\
\overline{\mathrm{N}}_{K/\mathbb{Q}}\,(\mathfrak{c})^2 &\equiv 1 \bmod (4\cdot 2^{m+1}), \quad \text{if } k = \mathbb{Q}^{(m)},\ m \geq 0.
\end{aligned}$$

4. Computation of $\overline{\mathrm{N}}_{K/\mathbb{Q}}\,(\alpha)$.

The best way is to use local class field theory by computing $\mathrm{N}_{K/\mathbb{Q}}\,(\alpha) = \prod_{v\mid 2} \mathrm{N}_{K_v/\mathbb{Q}_2}\,(\alpha)$, where K_v is the completion of K at the place $v \mid 2$ of K and $\mathrm{N}_{K_v/\mathbb{Q}_2}$ the local norm.

The result is given by the following generalization of the result of [Pi].

Let $p \geq 2$ be a prime number, let K_v be the completion of the number field K at $v \mid p$ (or any finite extension of $\mathbb{Q}_p$); we suppose that K_v contains μ_p and a subfield $k_{(v)}$ of $\mathbb{Q}_p(\mu_{p^\infty})$ of degree p^m over $\mathbb{Q}_p(\mu_p)$, $m \geq 0$ (if $p = 2$, the context is that of the previous section for which the hypothesis are satisfied for all $v \mid 2$, with $k_{(v)} = k_v := \mathbb{Q}_2\,k$ and $[k_{(v)} : \mathbb{Q}_2] = [k : \mathbb{Q}] = 2^m$, independently of $v \mid 2$, since $k/\mathbb{Q}$ is totally ramified at 2).[1]

The local norm group of $k_{(v)}$, restricted to the norms of units, is the following subgroup of $\mathbb{Z}_p^\times = \mu_{p-1} \oplus (1 + p\,\mathbb{Z}_p)$ for $p \neq 2$ or of $\mathbb{Z}_2^\times = \langle -1 \rangle \oplus (1 + 4\,\mathbb{Z}_2)$ for $p = 2$:

- $p \neq 2$, $k_{(v)} = \mathbb{Q}_p(\mu_{p^{m+1}})$, $m \geq 0$; the norm group is $1 + p^{m+1}\,\mathbb{Z}_p$;
- $p = 2$, $k_{(v)} = \mathbb{Q}_2^{(m)}$, $m \geq 0$; the norm group is $\langle -1 \rangle \oplus (1 + 4\cdot 2^m\,\mathbb{Z}_2)$;
- $p = 2$, $k_{(v)} = \mathbb{Q}_2'^{(m)}$, $m \geq 1$; the norm group is $\langle -1 + 4\cdot 2^{m-1} \rangle_{\mathbb{Z}_2}$;
- $p = 2$, $k_{(v)} = \mathbb{Q}_2(\mu_{4\cdot 2^{m-1}})$, $m \geq 1$; the norm group is $1 + 4\cdot 2^{m-1}\,\mathbb{Z}_2$.

[1] Take care that if $k = K \cap \mathbb{Q}(\mu_{2^\infty})$, k_v may not be equal to $K_v \cap \mathbb{Q}_2(\mu_{2^\infty})$ (for instance $K = \mathbb{Q}(\sqrt{-17})$ for which $k = \mathbb{Q}$, $k_v = \mathbb{Q}_2$, $m = 0$); but Theorem 1 applies to $k_{(v)} = K_v \cap \mathbb{Q}_2(\mu_{2^\infty}) = \mathbb{Q}_2(\sqrt{-1})$ with $m = 1$.

We then have:

Theorem 1. *Let K_v be the completion of a number field K at $v \,|\, p$; suppose that K_v contains μ_p and a subfield $k_{(v)}$ of $\mathbb{Q}_p(\mu_{p^\infty})$ of degree p^m over $\mathbb{Q}_p(\mu_p)$, $m \geq 0$. Let $K_v(\sqrt[p]{\alpha})$, $\alpha \in K_v^\times$, be an unramified Kummer extension of K_v (modulo $K_v^{\times p}$ we can suppose that α is a local unit).*

Then we have $\mathrm{N}_{K_v/\mathbb{Q}_p}(\alpha) \equiv 1 \bmod (p^{m+2})$.

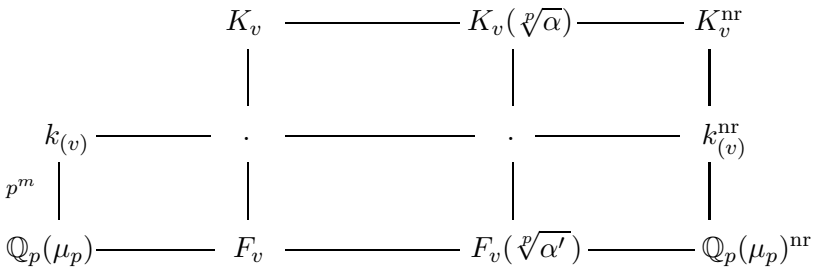
Moreover, if $p = 2$ and $k_{(v)} = \mathbb{Q}_2^{(m)}$, $m \geq 0$, and if at least one of the following two conditions holds:

(i) $\alpha \in K_v^{\times 2}$,

(ii) the index of ramification $e_v(K_v/k_{(v)})$ of $K_v/k_{(v)}$ is even,

we then have $\mathrm{N}_{K_v/\mathbb{Q}_2}(\alpha) \equiv 1 \bmod (4 \cdot 2^{m+1})$.

Proof. We consider the following diagram:



where for any field L, L^{nr} is the maximal unramified pro-extension of L; we know that we have for instance $L^{\mathrm{nr}} = L\,\mathbb{Q}_p^{\mathrm{nr}}$ (see e.g. [Gr, II.1.1.5]). Put $F_v := K_v \cap \mathbb{Q}_p(\mu_p)^{\mathrm{nr}}$. All horizontal extensions are unramified and all vertical extensions are totally ramified.

Consider the intersection $K_v(\sqrt[p]{\alpha}) \cap \mathbb{Q}_p(\mu_p)^{\mathrm{nr}}$ as a Kummer extension of F_v; thus there exists a suitable local unit $\alpha' \in F_v^\times$ such that $\alpha = \alpha'\, x^p$ with $x \in K_v^\times$.

Then $\mathrm{N}_{K_v/\mathbb{Q}_p}(\alpha) = \mathrm{N}_{K_v/\mathbb{Q}_p}(\alpha') \cdot \mathrm{N}_{K_v/\mathbb{Q}_p}(x)^p$; since $F_v(\sqrt[p]{\alpha'})/F_v$ is unramified we have (see e.g. [Gr, I.6.3, (ii)]):

$$\alpha' = x'^p\,(1 + p\,(1-\zeta)\,y')\,,$$

$x', y' \in F_v^\times$, $v(y') \geq 0$, where ζ is a primitive pth root of unity (for $p = 2$ we have $p\,(1-\zeta) = 4$). Then:

$$\mathrm{N}_{K_v/\mathbb{Q}_p}(\alpha) = \mathrm{N}_{K_v/\mathbb{Q}_p}(1 + p\,(1-\zeta)\,y') \cdot \mathrm{N}_{K_v/\mathbb{Q}_p}(x\,x')^p\,;$$

but (see the above list of norm groups of $k_{(v)}$), we have

$$\mathrm{N}_{K_v/\mathbb{Q}_p}(x\,x')^p \equiv 1 \bmod (p^{m+2})\,,$$

and in the particular case when $p = 2$ and $k_{(v)} = \mathbb{Q}_2^{(m)}$,

$$\mathrm{N}_{K_v/\mathbb{Q}_2}(x\,x')^2 \equiv 1 \bmod (4 \cdot 2^{m+1}),$$

and

$$\mathrm{N}_{K_v/\mathbb{Q}_p}(1 + p\,(1-\zeta)\,y') = \mathrm{N}_{F_v/\mathbb{Q}_p}(1 + p\,(1-\zeta)\,y')^{[K_v:F_v]} \equiv 1 \bmod (p^{m+2})$$

since $[K_v : F_v]$ is a multiple of p^m, which implies first that

$$(1 + p\,(1-\zeta)\,y')^{[K_v:F_v]} = 1 + p^{m+1}\,(1-\zeta)\,y'',$$

and then that

$$\mathrm{N}_{F_v/\mathbb{Q}_p}(1 + p^{m+1}\,(1-\zeta)\,y'') \in 1 + p^{m+2}\,\mathbb{Z}_p\,;$$

hence we have the congruence

$$\mathrm{N}_{K_v/\mathbb{Q}_p}(\alpha) \equiv 1 \bmod (p^{m+2}).$$

(i) If $p = 2$, $k_{(v)} = \mathbb{Q}_2^{(m)}$, $m \geq 0$, and $\alpha \in K_v^{\times 2}$, then we obtain $\mathrm{N}_{K_v/\mathbb{Q}_2}(\alpha) \equiv 1 \bmod (4 \cdot 2^{m+1})$.

(ii) If $p = 2$, $e_v(K_v/k_{(v)})$ is even, the above computation yields $\mathrm{N}_{F_v/\mathbb{Q}_2}(1 + 4\,y')^{[K_v:F_v]} \equiv 1 \bmod (4 \cdot 2^{m+1})$; if moreover $k_{(v)} = \mathbb{Q}_2^{(m)}$, since $\mathrm{N}_{K_v/\mathbb{Q}_2}(x\,x')^2 \equiv 1 \bmod (4 \cdot 2^{m+1})$ in that case, we obtain

$$\mathrm{N}_{K_v/\mathbb{Q}_2}(\alpha) \equiv 1 \bmod (4 \cdot 2^{m+1}).$$

This completes the proof of the theorem. □

5. Statement of the main result

We return to the case $p = 2$. In Sections 3 and 4, we have computed $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})$, making use of $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{c})^2$ (absolute norm) and of $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ (arithmetic norm) from the $\mathrm{N}_{K_v/\mathbb{Q}_2}(\alpha)$, taking into account that the congruence $\mathrm{N}_{K_v/\mathbb{Q}_2}(\alpha) \equiv 1 \bmod (4 \cdot 2^m)$ is independent of v with the choice of $k_{(v)} := k_v = \mathbb{Q}_2\,k$ for all $v \mid 2$.

To determine $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\alpha)$ we note that $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\alpha) = (-1)^\rho\,\mathrm{N}_{K/\mathbb{Q}}(\alpha)$, where ρ is the number of conjugates of α which are negative in the real embeddings of K; from [Ma, § 3], the numbers ρ and c have same parity.

Thus we have obtained in general:

Theorem 2. *Let L/K be a finite extension of number fields, unramified at 2. Denote by $\mathfrak{d}_{L/K}$ the discriminant of L/K, by c the number of complex places of L which lie above a real place of K, and by $\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K})$ the absolute norm of $\mathfrak{d}_{L/K}$. Let k be the maximal subfield of $\mathbb{Q}(\mu_{2^\infty})$ contained in K and put $[k : \mathbb{Q}] =: 2^m$, $m \geq 0$.*

Then we have the congruence $(-1)^c\,\overline{\mathrm{N}}_{K/\mathbb{Q}}(\mathfrak{d}_{L/K}) \equiv 1 \bmod (4 \cdot 2^m)$.

Remark 1. *We have the following improvement in two particular circumstances: if* $k = \mathbb{Q}^{(m)}$, $m \geq 0$, *then under at least one of the following two conditions:*

(i) 2 *splits totally in* $K(\sqrt{\alpha})/K$, [2]

(ii) the indices of ramification of $v \,|\, 2$ *in* K/k *are all even,*

we obtain the congruence $(-1)^c \cdot \overline{\mathrm{N}}_{K/\mathbb{Q}}\,(\mathfrak{d}_{L/K}) \equiv 1 \bmod (4 \cdot 2^{m+1})$. [3]

References

[Gr] G. Gras, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag, 2003; second corrected printing: 2005.

[Ma] J. Martinet, *Les discriminants quadratiques et la congruence de Stickelberger*, Sém. Théorie des Nombres, Bordeaux **1** (1989), 197–204.

[Pi] S. Pisolkar, *Absolute norms of p-primary units*, Jour. de Théorie des Nombres de Bordeaux **21** (2009), 733–740.

Georges Gras
Villa la Gardette, chemin Château Gagnière,
F-38520 Le Bourg d'Oisans
E-mail : g.mn.gras@wanadoo.fr
URL: http://monsite.orange.fr/maths.g.mn.gras/

[2] If $\alpha = x^2\,(1+4\,y)$, $y \in K^\times$, y 2-integer, this condition is equivalent to $\mathrm{Tr}_{\mathbb{F}_v/\mathbb{F}_2}(y) = 0$ for all $v \,|\, 2$, where $\mathrm{Tr}_{\mathbb{F}_v/\mathbb{F}_2}$ is the absolute trace from the residue field $\mathbb{F}_v$ of K (see [Gr, I.6.3, Lemma]).

[3] Use the computation of $\overline{\mathrm{N}}_{K/\mathbb{Q}}\,(\mathfrak{c})^2$ at the end of Sections 3, then Theorem 1 for the computation of $\mathrm{N}_{K_v/\mathbb{Q}_2}\,(\alpha)$ for $v \,|\, 2$ in these particular cases.