SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

PHILIPPE SATGE

Décomposition des nombres premiers dans certaines extensions non abéliennes de Q

Séminaire de théorie des nombres de Grenoble, tome 4 (1974-1975), exp. n° 5, p. 1-10

<http://www.numdam.org/item?id=STNG_1974-1975__4__A5_0>

Séminaire de Théorie des Nombres
6 et 7 novembre 1974
Grenoble

DECOMPOSITION DES NOMBRES PREMIERS DANS CERTAINES EXTENSIONS NON ABELIENNES DE $\mathbb{Q}$

par Philippe SATGE

INTRODUCTION.

Soit A une extension abélienne de $\mathbb{Q}$; on sait (théorie du corps de classe) qu'il existe un entier tel que la décomposition dans A d'un nombre premier ne dépend que de la classe de ce nombre modulo cet entier. Peu de choses sont connues sur la décomposition des nombres premiers dans des extensions non abéliennes de $\mathbb{Q}$. On va étudier le cas des extensions galoisiennes de $\mathbb{Q}$ dont le groupe de Galois G vérifie la condition suivante : G contient un sous-groupe abélien distingué H tel que l'application transfert relative à H soit nulle ; dans le cas où le corps des invariants de H est réel et où l'indice de H dans G est strictement plus grand que 2, nous supposerons en plus que le cardinal de H est impair.

Ce travail comprend deux parties. La première est divisée en quatre paragraphes ; le théorème sur la décomposition des nombres premiers est cité sans démonstration dans le dernier de ces paragraphes ; les trois autres servent d'une part à préciser les objets intervenant dans l'énoncé du théorème et d'autre part à donner une idée de sa démonstration.

La démonstration (dont une première rédaction se trouve dans le séminaire de Théorie des Nombres de Caen) va faire l'objet d'un article.

La deuxième partie contient deux paragraphes ; chacun d'eux est

un exemple d'application du théorème de la première partie.

1ère partie. LE THEOREME PRINCIPAL

1.1. Soit k une extension galoisienne de degré n de $\mathbb{Q}$ et $\mathcal{O}$ un ordre de k. On désigne par $cl(\mathcal{O})$ le quotient du groupe des $\mathcal{O}$ idéaux fractionnaires inversibles par le sous-groupe des $\mathcal{O}$ idéaux principaux engendrés par les éléments de norme positive.

A tout $\mathcal{O}$ idéal fractionnaire et toute base $a_1,\ldots,a_n$ de cet idéal on associe la forme $\overline{\prod_{s\in G(k/\mathbb{Q})}}(s(a_1)X_1+\ldots+s(a_n)X_n)$ où $G(k/\mathbb{Q})$ est le groupe de Galois de $k/\mathbb{Q}$ et où $X_1,\ldots,X_n$ sont des indéterminées ; cette forme homogène de degré n à n variables a ses coefficients dans $\mathbb{Q}$. On montre que le produit de cette forme par l'inverse de la norme de l'idéal (la norme est prise par rapport à $\mathcal{O}$) est une forme à coefficients entiers si de plus l'idéal est $\mathcal{O}$ inversible, la forme ainsi obtenue est primitive (i.e. le p.g.c.d. de ses coefficients est 1). Dans la suite $\mathcal{O}$ sera stable par $G(k/\mathbb{Q})$; ce groupe agira donc sur $cl(\mathcal{O})$. Par "forme associée à une orbite", nous désignerons l'une quelconque des formes primitives attachées à un idéal dont la classe est dans cette orbite.

Remarque : On montre facilement que deux formes primitives attachées à deux idéaux dont les classes sont dans la même orbite se déduisent l'une de l'autre par un changement de variable linéaire dont la matrice est dans $GL_n(\mathbb{Z})$ (i.e. on passe de l'une à l'autre en remplaçant la $i^{\text{ème}}$ variable X_i par une combinaison linéaire $\sum_{j=1}^{n} a_{i,j}X_j$, la matrice $(a_{i,j})_{i,j=1,\ldots,n}$ appartenant à $GL_n(\mathbb{Z})$).

1.2. Soit K une extension galoisienne de $\mathbb{Q}$ dont le groupe de Galois G vérifie les conditions énoncées dans l'introduction, on désigne par k le corps des invariants de H ; l'extension K/k est abélienne, on note $\underline{f}$ le conducteur de cette extension. Il résulte des hypothèses

faites sur G que le sous-groupe du groupe des idéaux de k attaché par la théorie du corps de classe à K/k contient le sous-groupe $N(\underline{f})$ définit de la manière suivante : $N(\underline{f})$ est le plus petit groupe contenant les idéaux principaux étrangers à $\underline{f}$ engendrés par des rationnels et ceux engendrés par les éléments de k^* de norme positive et congrus à 1 modulo $\underline{f}$. Rappelons en terminant ce paragraphe qu'un idéal premier de k qui ne divise pas $\underline{f}$ n'est pas ramifié dans K et que son degré résiduel dans ce corps est l'ordre de sa classe modulo le sous-groupe des idéaux de k qui lui est attaché par la théorie du corps de classe.

1.3. On désigne par $I(\underline{f})$ le groupe des idéaux de k étrangers à $\underline{f}$ et par $\mathcal{O}_{\underline{f}}$ le plus petit ordre de k contenant $\underline{f}$ (on voit facilement que $\mathcal{O}_{\underline{f}} = \mathbb{Z} + \underline{f}$). L'application qui a un idéal entier de $I(\underline{f})$ associe son intersection avec $\mathcal{O}_{\underline{f}}$ se prolonge en un homomorphisme de groupe de $I(\underline{f})$ dans le groupe des $\mathcal{O}_{\underline{f}}$ idéaux fractionnaires inversibles ; on montre que cet homomorphisme induit un isomorphisme du quotient $I(\underline{f})/N(\underline{f})$ sur $cl(\mathcal{O}_{\underline{f}})$. L'extension $K/\mathbb{Q}$ étant galoisienne, $\underline{f}$ est invariant par $G(k/\mathbb{Q})$; ce groupe agit donc sur $I(\underline{f})/N(\underline{f})$ et sur $cl(\mathcal{O}_{\underline{f}})$. L'isomorphisme définit ci-dessus est clairement compatible avec cette action, il induit donc une bijection sur les ensembles d'orbite.

1.4. Soit p un nombre premier étranger à $\underline{f}$ dont le degré résiduel dans $k/\mathbb{Q}$ est r ; les classes des inverses des idéaux premiers de k contenant p appartiennent à une même orbite de $I(\underline{f})/N(\underline{f})$. Leurs images dans $cl(\mathcal{O}_{\underline{f}})$ appartiennent donc à l'image de cette orbite par la bijection définie dans 1.3. On montre que, parmi les formes associées aux orbites de $cl(\mathcal{O}_{\underline{f}})$, celle associée à l'orbite que l'on vient de définir est la seule à représenter p^r (i.e. la seule telle que p^r soit valeur de cette forme pour un n-uple d'entiers). Compte tenu de 1.2, ce résultat s'énonce à nouveau sous la forme du théorème suivant :

THEOREME 1. On désigne par K une extension galoisienne de $\mathbb{Q}$ dont le groupe de galois vérifie les conditions de l'introduction, par k le corps des invariants de H et par n l'indice de H dans G . Il existe un ensemble fini de formes à coefficients entiers (primitives homogènes de degré n à n variables) telles que :

a) Si p est un nombre premier étranger au conducteur de K/k et si r est le degré résiduel de p dans $k/\mathbb{Q}$, une et une seule de ces formes représente p^r .

b) Le degré résiduel de p dans $K/\mathbb{Q}$ ne dépend que de la forme représentant p^r .

Remarque : 1) La forme associée à une orbite a été choisie arbitrairement dans une famille de formes attachée à cette orbite ; la remarque qui achève le paragraphe 1.1 montre que toutes les formes d'une même famille représentent les mêmes entiers ; les formes n'interviennent dans le théorème que par les entiers qu'elles représentent; cela confirme que ce choix n'a pas d'importance.

2) L'application du théorème nécessite le calcul du degré résiduel des nombres premiers dans $k/\mathbb{Q}$; ce calcul est particulièrement simple lorsque k est une extension abélienne de $\mathbb{Q}$; ce sera le cas dans les exemples.

3) Dans le cas $n = [k:\mathbb{Q}] = 2$, les formes sont des formes quadratiques à deux variables ; de plus, dans ce cas, la seule condition à imposer au groupe de Galois de $K/\mathbb{Q}$ est la condition relative au transfert.

4) Le théorème des idéaux principaux ([1] chapitre XIII) montre que la condition relative au transfert est vérifiée lorsque k est la clôture abélienne de $\mathbb{Q}$ dans K . Nous nous servirons de cette remarque dans la deuxième partie.

5) Il résulte du théorème que les formes associées à deux orbites différentes ne représentent pas les mêmes nombres premiers et donc elles sont différentes ; le nombre des formes qui interviennent dans le théorème est donc le nombre des orbites de $I(\underline{f})/N(\underline{f})$ (ou de $cl(\mathcal{O}_{\underline{f}})$).

2e partie. DEUX EXEMPLES.

2.1. Soit m un entier naturel strictement plus grand que 2 et a un entier relatif qui n'est pas une puissance $m^{\text{ième}}$. Nous allons caractériser les nombres premiers ne divisant pas am modulo lesquels la classe de a est une puissance $m^{\text{ième}}$. Remarquons d'abord que, si $d = (p-1, m)$, la classe de a modulo p est une puissance $m^{\text{ième}}$ si et seulement si c'est une puissance $d^{\text{ième}}$; on peut donc se limiter dans notre étude aux $p \equiv 1$ modulo m.

Soit ζ une racine primitive $m^{\text{ième}}$ de l'unité ; posons $k = \mathbb{Q}(\zeta)$ et $K = k(\sqrt[m]{a})$. Il est clair que la classe de a modulo un nombre premier $p \equiv 1 \bmod m$ est une puissance $m^{\text{ième}}$ si et seulement si p est totalement décomposé dans K. Mais l'extension $K/\mathbb{Q}$ est galoisienne et k est un corps imaginaire qui est la clôture abélienne de $\mathbb{Q}$ dans K ; les remarques de la fin de la première partie montrent que l'on peut appliquer le théorème 1 à l'extension $K/\mathbb{Q}$. Les $p \equiv 1 \bmod m$ étant complètement décomposés dans k, ce théorème 1 affirme l'existence d'une famille de formes primitives homogènes de degré $\varphi(m)$ à $\varphi(m)$ variables (φ = indicateur d'Euler) telle que, parmi les $p \equiv 1 \bmod m$, ceux représentés par ces formes soient ceux totalement décomposés dans K. On obtient donc le théorème suivant :

THEOREME 2. *Soit m un entier naturel strictement plus grand que 2 et a un entier naturel qui n'est pas une puissance $m^{\text{ième}}$; il existe un ensemble fini de formes homogènes de degré $\varphi(m)$ à $\varphi(m)$ variables tel que, pour tout nombre premier $p \equiv 1 \bmod m$ ne divisant pas a,*

on ait les équivalences :

a) p est représenté par l'une de ces formes.

b) la classe de a modulo p est une puissance $m^{\text{ième}}$.

Traitons numériquement le cas $a = 2$, $m = 3$; on reprend les notations introduites dans la première partie. Le conducteur de l'extension de Kummer K/k est l'idéal principal $\underline{6}$ engendré par 6 ; le groupe $I(\underline{6})/N(\underline{6})$ est le groupe à trois éléments donc $N(\underline{6})$ est le sous-groupe de $I(\underline{6})$ associé par la théorie du corps de classe à l'extension K/k . Un nombre premier $p \equiv 1 \bmod 3$ est donc totalement décomposé dans $K/\mathbb{Q}$ si et seulement si les idéaux premiers de k qui le contiennent sont dans $N(\underline{6})$, les inverses de ces idéaux sont dans $N(\underline{6})$ donc l'orbite de ces inverses est l'orbite formée de la classe neutre de $I(\underline{6})/N(\underline{6})$; l'image de cette orbite dans $cl(\mathcal{O}_{\underline{6}})$ est formée de la classe neutre de $cl(\mathcal{O}_{\underline{6}})$. L'ordre $\mathcal{O}_{\underline{6}}$ représente cette classe neutre, 1 et $3(1+\sqrt{-3})$ forment une base de $\mathcal{O}_{\underline{6}}$ et la norme de $\mathcal{O}_{\underline{6}}$ par rapport à lui-même est 1 ; la forme $(X_1 + 3(1+\sqrt{-3})X_2)(X_1 + 3(1-\sqrt{-3})X_2) = X_1^2 + 6X_1X_2 + 36X_2^2$ est donc une forme associée à cette orbite ; on peut remarquer que

$$X_1^2 + 6X_1X_2 + 36X_2^2 = (X_1 + 3X_2)^2 + 27X_2^2 ,$$

donc $X_1^2 + 27X_2^2$ est aussi une forme associée à notre orbite. On a obtenu le résultat suivant : soit $p \equiv 1 \bmod 3$ un nombre premier 2 est un cube modulo p si et seulement si $p = x_1^2 + 27x_2^2$ avec x_1 et x_2 dans $\mathbb{Z}$.

Ce résultat peut être obtenu par d'autres méthodes. Une méthode reposant sur la loi de réciprocité cubique est proposé en exercice dans [2] . Une autre due à Gauss est exposé par Emma Lehmer dans [3] ; dans ce même article Emma Lehmer traite les cas $a = 2$ ou 3 et $m = 5$. Martinet et Barrucand ont obtenus des résultats dans le cas $m = 3$ pour certaines valeurs de a . Aucune de ces méthodes ne s'étend au cas général traité ici ; tous les résultats partiels que j'ai trouvé dans la littérature sont tels que l'ensemble des formes qui apparaissent par la méthode exposée ici est réduit à une forme. Il est clair que pour n'importe quelle valeur de

m on peut trouver des valeurs de a telles que le nombre des formes qui interviennent soit plus grand que 1 .

2.2. On désigne par ℓ un nombre premier impair, par k un corps quadratique réel, par ε l'unité fondamentale et par s le $\mathbb{Q}$-automorphisme non trivial de ce corps. Si $\underline{p_1}$ et $\underline{p_2}$ sont deux idéaux premiers de k contenant un même nombre premier, il résulte de l'égalité $\varepsilon.s(\varepsilon) = \pm 1 = (\pm 1)^{\ell}$ que la classe de ε mod $\underline{p_1}$ est une puissance $\ell^{\text{ième}}$ si et seulement si sa classe mod $\underline{p_2}$ en est une ; cela justifie la définition suivante : on dira que ε est une puissance $\ell^{\text{ième}}$ modulo un nombre premier si la classe de ε modulo un idéal premier de k contenant ce nombre est une puissance $\ell^{\text{ième}}$. Nous allons caractériser les nombres premiers modulo lesquels ε est une puissance $\ell^{\text{ième}}$.

Pour cela désignons par $\mathbb{Q}'$ le corps engendré sur $\mathbb{Q}$ par une racine primitive $\ell^{\text{ième}}$ de l'unité et posons $k' = \mathbb{Q}'.k$. Nous supposerons que $k \not\subset \mathbb{Q}'$ mais tout ce qui va suivre s'adapte de manière évidente lorsque $k \subset \mathbb{Q}'$. Nous désignons par $\tilde{k}$ le sous-corps de k' ne contenant ni k ni $\mathbb{Q}'$ tel que $[k':\tilde{k}] = 2$ et par K' le corps engendré sur k' par une racine $\ell^{\text{ième}}$ de ε . On montre que $K'/\tilde{k}$ est abélienne et donc (puisque $[K':\tilde{k}] = 2\ell$) il existe une et une seule extension $\tilde{K}$ de degré ℓ de $\tilde{k}$ contenue dans K' . On montre que $\tilde{K}$ est galoisienne sur $\mathbb{Q}$ et que $\tilde{k}$ est la clôture abélienne de $\mathbb{Q}$ dans $\tilde{K}$ (les démonstrations de ces affirmations peuvent se faire en remarquant que $K'/\mathbb{Q}$ est galoisienne et que son groupe de Galois est simple à décrire ; de toutes manières elles résultent de l'étude générale faite par Liliane BOUVIER dans [4]).

D'autre part, il est clair que la classe de ε modulo un nombre premier différent de ℓ est une puissance $\ell^{\text{ième}}$ si et seulement si le degré résiduel de ce nombre premier dans K' est étranger à ℓ ; cette dernière condition est équivalente au fait que les idéaux premiers de $\tilde{k}$ contenant ce nombre premier sont totalement décomposés dans $\tilde{K}$. Mais ce que l'on a fait ci-dessus montre que l'on peut appliquer le théorème 1 à l'extension $\tilde{K}/\mathbb{Q}$ en prenant $\tilde{k}$ comme corps intermédiaire. Il existe

donc un ensemble fini de formes homogènes de degré $[\tilde{k}:\mathbb{Q}] = \ell-1$ variables tel que la classe de ϵ modulo un nombre premier p de degré $\tilde{f}$ dans $\tilde{k}/\mathbb{Q}$ est une puissance $\ell^{\text{ième}}$ si et seulement si $p^{\tilde{f}}$ est représenté par l'une de ces formes. Remarquons que si le degré résiduel de p dans k est 1 (resp. 2) et si $p \not\equiv 1 \bmod \ell$ (resp. $p \not\equiv \pm 1 \bmod \ell$) la classe de n'importe quel entier de k modulo p est une puissance $\ell^{\text{ième}}$ (et donc $p^{\tilde{f}}$ est représenté par l'une des formes introduites ci-dessus). D'autre part, si $p \equiv 1 \bmod \ell$ le nombre p est totalement décomposé dans $\mathbb{Q}'$ et donc le degré résiduel de p dans $\tilde{k}$ est égal à son degré résiduel dans k. Si $p \equiv -1 \bmod \ell$, le nombre p est totalement décomposé dans le sous-corps réel maximum $\mathbb{Q}^{(o)}$ de $\mathbb{Q}'$ et les idéaux premiers de $\mathbb{Q}^{(o)}$ contenant p sont inertes dans $\mathbb{Q}'$; il en résulte que le degré résiduel de p dans $\tilde{k}$ est égal à 1 si son degré résiduel dans k est 2 (en effet $\tilde{k} \supset \mathbb{Q}^{(o)}$ un idéal premier de $\mathbb{Q}^{(o)}$ non ramifié et de degré résiduel 2 est toujours inerte dans deux des corps quadratiques intermédiaires et décomposé dans le troisième, ce troisième étant le corps des invariants du Frobenius de l'idéal). On obtient donc le théorème suivant :

THEOREME 2. Soit k un corps quadratique réel, ϵ son unité fondamentale et ℓ un nombre premier impair ; on suppose que k n'est pas contenu dans le corps des racines $\ell^{\text{ièmes}}$ de l'unité. Il existe un ensemble fini de formes homogènes de degré $\ell-1$ à $\ell-1$ variables tel que :

a) Si $p \equiv 1 \bmod \ell$ est un nombre premier de degré résiduel r dans $k/\mathbb{Q}$, la classe de ϵ modulo p est une puissance $\ell^{\text{ième}}$ si et seulement si p^r est représenté par l'une de ces formes.

b) Si $p \equiv -1 \bmod \ell$ est un nombre premier inerte dans $k/\mathbb{Q}$, la classe de ϵ modulo p est une puissance $\ell^{\text{ième}}$ si et seulement si p est représenté par l'une de ces formes.

La classe de ϵ modulo n'importe quel autre nombre premier différent de ℓ est une puissance $\ell^{\text{ième}}$.

Traitons le cas $\ell = 3$ et $k = \mathbb{Q}(\sqrt{5})$. On a $\epsilon = \frac{1+\sqrt{5}}{2}$ et

$\mathbb{Q}' = \mathbb{Q}(\sqrt{-3})$ donc $\tilde{k} = \mathbb{Q}(\sqrt{-15})$; le nombre 3 est inerte dans k et ramifié dans $\tilde{k}$ donc il y a un seul idéal premier $\underline{\ell}$ de $\tilde{k}$ contenant 3 et un seul idéal $\underline{\ell}'$ de k' contenant $\underline{\ell}$. Le conducteur de l'extension de Kummer K'/k' est $\underline{\ell}'^2$ donc celui de $\tilde{K}/\tilde{k}$ est $\underline{\ell}^2$ qui est l'idéal principal $\underline{3}$ de $\tilde{k}$ engendré par 3 . L'ordre du quotient $I(\underline{3})/N(\underline{3})$ est 6 ; ce groupe est donc formé de l'élément neutre, d'un élément d'ordre 2 , de deux éléments d'ordre 3 et de deux éléments d'ordre 6 . Le sous-groupe attaché à l'extension $\tilde{K}/\tilde{k}$ est le sous-groupe formé de la classe neutre et des deux classes d'ordre 2 . Posons $\omega = \frac{1+\sqrt{-15}}{2}$; on vérifie facilement que la classe d'ordre 2 est représentée par l'idéal $(\omega-4,8)$ engendré par $\omega-4$ et 8 , que les deux classes d'ordre 3 sont les deux classes conjuguées représentées par les idéaux (ω) et $(\overline{\omega})$ engendrés respectivement par ω et par son conjugué et que les deux classes d'ordre 6 sont les deux classes conjuguées représentées par les idéaux $(2,\omega)$ et $(2,\overline{\omega})$ engendrés par 2 et ω et par 2 et $\overline{\omega}$. Il y a donc quatre orbites pour $I(\underline{3})/N(\underline{3})$ et donc quatre orbites pour $cl(\mathcal{O}_{\underline{3}})$. Les $\mathcal{O}_{\underline{3}}$ idéaux fractionnaires $\mathcal{O}_{\underline{3}}$, $(\omega-4,8)\cap\mathcal{O}_{\underline{3}}$, $(\omega)\cap\mathcal{O}_3$ et $(2,\omega)\cap\mathcal{O}_3$ sont des représentants de ces quatre orbites ; ils admettent respectivement comme base 1 et 3ω , $3\omega-4$ et 8 , 4 et 3ω , 2 et 3ω et donc les formes qui leur sont associées sont donc $F_1 = X_1^2 + 3X_1X_2 + 36X_2^2$, $F_2 = 8X_1^2 - 5X_1X_2 + 5X_2^2$, $F_3 = 4X_1^2 + 3X_1X_2 + 9X_2^2$ et $F_4 = 2X_1^2 + 3X_1X_2 + 18X_2^2$.

La classe de ε modulo p est une puissance cubique pour les p vérifiant :

a) $p \equiv 1 \bmod 3$ et p^r représenté par F_1 ou F_2 (r désigne toujours le degré résiduel de p dans $k/\mathbb{Q}$)

b) $p \equiv -1 \bmod 3$, p inerte dans $k/\mathbb{Q}$ et p représenté par F_1 ou F_2

c) $p \not\equiv \pm 1 \bmod 3$ ou $p \equiv -1 \bmod 3$ et p décomposé ou ramifié dans $k/\mathbb{Q}$.

Dans le cas a) si $r = 2$ il est clair que $F_1(p,0) = p^2$ donc p^r est représenté par F_1 et donc, pour tous ces p, la classe de ε modulo p est une puissance cubique. Cela peut se voir facilement directement. Terminons en donnant la liste des $p \leq 200$ vérifiant $p \equiv 1 \bmod 3$ et p décomposé dans k ou $p \equiv -1 \bmod 3$ et p inerte dans k qui sont représentés par F_1 ou F_2 ; on a :

$47 = F_2(2,3)$, $107 = F_2(2,5)$, $113 = F_2(4,1)$, $139 = F_2(-1,2)$,

$151 = F_1(1,2)$ et $199 = F_1(5,2)$;

les autres $p \leq 200$ vérifiant les mêmes conditions sont représentés par F_3 ou F_4 , ce sont :

$17 = F_4(-1,1)$, $19 = F_3(-2,1)$, $23 = F_4(1,1)$, $31 = F_3(2,1)$,

$53 = F_4(-5,1)$, $61 = F_3(-4,1)$, $79 = F_3(-2,3)$, $83 = F_4(5,1)$,

$109 = F_3(-4,3)$, $137 = F_4(7,1)$, $167 = F_4(-5,3)$, $173 = F_4(1,3)$,

$181 = F_3(4,3)$ et $197 = F_4(-7,3)$.

REFERENCES

[1] - Class Field Theory ; Artin-Tate.

[2] - Algebraic Number Theory ; Cassels Frohlich (Séminaire de Brighton).

[3] - Cubic and Quintic residue ; Duke Math. Jour. 18 (1954).

[4] - Séminaire de théorie des nombres de Grenoble 1971-1972.

-o-o-o-