Ann. Inst. Fourier, Grenoble
27, 4 (1977), 1-8.

DÉCOMPOSITION DES NOMBRES PREMIERS DANS DES EXTENSIONS NON ABÉLIENNES

par Philippe SATGE

Introduction.

Gauss [1] montre que 2 est un cube modulo un nombre premier congru à 1 modulo 3 si et seulement si ce nombre premier peut s'écrire $x^2 + 27y^2$ avec x et y entiers. Ce faisant il montre que les nombres premiers totalement décomposés dans le corps $\mathbf{Q}(j, \sqrt[3]{2})$ où j est une racine cubique de l'unité sont ceux représentés par la forme quadratique $X^2 + 27Y^2$. Nous allons généraliser ce résultat en décrivant une classe de corps dans lesquels la décomposition des nombres premiers dépend de la représentation de ces nombres par certaines formes.

Plus précisément, nous considérons les corps galoisiens dont le groupe de Galois contient un sous-groupe abélien distingué vérifiant les deux conditions suivantes :

(*) le transfert relatif à ce sous-groupe est l'application triviale;

(**) ce sous-groupe est d'ordre impair si son corps des invariants est un corps réel de degré strictement supérieur à 2.

Nous montrons que la décomposition des nombres premiers dans un corps de ce type ne dépend que de la représentation de ces nombres par des formes dont le degré et le nombre des variables est l'indice du sous-groupe distingué vérifiant (*) et (**) :

Ce travail est divisé en quatre parties. Dans la première,

on étudie les formes normes associées aux idéaux des ordres des corps de nombres; cette étude est classique dans le cas quadratique (voir [2] par exemple) mais repose sur des remarques qui ne se généralisent pas au cas non quadratique. Dans la deuxième partie, on introduit l'ordre $\mathfrak{O}_{\mathfrak{F}}$ et on le relie au groupe des classes de rayons $\mathfrak{F}$. Dans la troisième, on énonce et démontre le théorème de décomposition. Enfin, dans la quatrième, on traite quelques exemples; en particulier on retrouve le résultat de Gauss sur les nombres premiers modulo lesquels 2 est un cube.

1. Les formes normes.

Dans cette première partie k est une extension galoisienne de degré n du corps $\mathbf{Q}$ des rationnels, $\mathfrak{O}$ est un ordre de k et $X_1, \ldots, X_n$ sont des indéterminées. On désigne par $N_{\mathfrak{O}}$ la norme par rapport à $\mathfrak{O}$ des $\mathfrak{O}$-idéaux fractionnaires (la norme d'un $\mathfrak{O}$-idéal entier est le cardinal du quotient de $\mathfrak{O}$ par cet idéal) et par $N_{k|\mathbf{Q}}$ la norme dans $k|\mathbf{Q}$.

Soit $\mathfrak{A}$ un $\mathfrak{O}$-idéal et $a_1, \ldots, a_n$ une base du $\mathbf{Z}$ module $\mathfrak{A}$; on définit les $b_k^{i,j} \in \mathbf{Z}$ par $a_i a_j = \sum_{k=1}^{n} b_k^{i,j} a_k$. Le déterminant de la matrice $n \times n$ dont l'élément de la $l^{\text{ième}}$ ligne et de la $m^{\text{ième}}$ colonne est $\sum_{i=1}^{n} b_l^{i,m} X_i$ est une forme de degré n à n variables et à coefficients rationnels. Le produit de cette forme par $N_{\mathfrak{O}}(\mathfrak{A})^{-1}$ est, par définition, la forme norme de $\mathfrak{A}$ pour la base $a_1, \ldots, a_n$. Aux différentes bases d'un même $\mathfrak{O}$-idéal correspondent différentes formes normes qui se déduisent l'une de l'autre par un changement d'indéterminée linéaire dont la matrice est dans $GL_n(\mathbf{Z})$ (i.e. on passe de l'une à l'autre en remplaçant X_i par $\sum_{j=1}^{n} \lambda_{i,j} X_j$, la matrice $(\lambda_{i,j})_{i,j=1,\ldots,n}$ appartenant à $GL_n(\mathbf{Z})$). On appelle forme norme associée à l'idéal l'une quelconque de ces formes.

Remarque 1. — Si α est un élément de k de norme positive et si $\mathfrak{A}$ est un $\mathfrak{O}$-idéal, les formes associées à $\mathfrak{A}$ et à $\alpha\mathfrak{A}$ sont les mêmes.

PROPOSITION 1. — *Les coefficients des formes normes définies ci-dessus sont des entiers rationnels.*

Démonstration. — La remarque 1 permet de se restreindre aux formes associées à des idéaux entiers. Soit $\mathfrak{A}$ un tel idéal; choisissons une base du $\mathbf{Z}$ module $\mathfrak{A}$ du type $c_1e_1, \ldots, c_ne_n$ où les $c_i \in \mathbf{Z}$ et où $e_1, \ldots, e_n$ est une base de $\mathfrak{O}$. Les entiers $b_k^{i,j}$ sont donc définis par

$$(c_ie_i)c_je_j) = \sum_{k=1}^{n} b_k^{i,j}(c_ke_k)$$

et on a $N_{\mathfrak{O}}(\mathfrak{A}) = |c_1 \ldots c_n|$. La forme associée à $\mathfrak{A}$ est donc le produit de $|c_1 \ldots c_n|^{-1}$ par le déterminant de la matrice dont l'élément de la $l^{\text{ième}}$ ligne et de la $m^{\text{ième}}$ colonne est $\sum_{i=1}^{n} b_l^{i,m}X_i$. Mais ce produit est le déterminant de la matrice dont l'élément de la $l^{\text{ième}}$ ligne et de la $m^{\text{ième}}$ colonne est $\sum_{i=1}^{n} \frac{b_l^{i,m}}{c_m} X_i$. D'autre part, de

$$(c_ie_i)(c_me_m) = \sum_{k=1}^{n} b_k^{i,m}(c_ke_k)$$

on tire

$$c_ie_ie_m = \sum_{k=1}^{n} \frac{b_k^{i,m}}{c_m} c_ke_k;$$

l'élément $c_ie_ie_m$ étant dans $\mathfrak{A}$ on en déduit que $\frac{b_k^{i,m}}{c_m} \in \mathbf{Z}$ et donc le déterminant de

$$\left(\sum_{i=1}^{n} \frac{b_l^{i,m}}{c_m} X_i\right)_{\substack{l=1,\ldots,n \\ m=1,\ldots,n}}$$

est une forme à coefficients entiers. C.Q.F.D.

PROPOSITION 2. — *La forme norme associée à un $\mathfrak{O}$-idéal inversible est primitive (i.e. ses coefficients sont premiers entre eux dans leur ensemble).*

Démonstration. — Cette proposition résulte clairement de la suivante :

PROPOSITION 3. — *Un $\mathfrak{O}$-idéal est inversible si et seulement si, pour tout nombre premier, la forme norme associée prend en un*

n-uple d'entiers au moins une valeur étrangère à ce nombre premier.

Démonstration. — La remarque 1 permet de supposer le $\mathfrak{O}$-idéal entier. Soit donc $\mathfrak{A}$ un idéal entier et $a_1, \ldots, a_n$ une base du $\mathbf{Z}$ module $\mathfrak{A}$. La valeur prise par la forme norme associée à cette base en un n-uple d'entiers $(x_1, \ldots, x_n)$ est clairement $N_{\mathfrak{O}}(\mathfrak{A})^{-1} N_{k/\mathbf{Q}}(x)$ où $x = \sum_{i=1}^{n} x_i a_i$, c'est-à-dire, au signe près, $(\mathfrak{O} : \mathfrak{A})^{-1}$ $(\mathfrak{O} : x\mathfrak{O})$ soit $(\mathfrak{A} : x\mathfrak{O})$. Désignons par P l'ensemble des nombres premiers et, pour tout $p \in \mathrm{P}$, par $\mathfrak{A}_p$ et $\mathfrak{O}_p$ les localisés de $\mathfrak{A}$ et $\mathfrak{O}$ par rapport à la partie multiplicative $\{\mathbf{Z} - p\mathbf{Z}\}$. Le quotient $\mathfrak{A}/x\mathfrak{O}$ est isomorphe au produit $\prod_{p \in \mathrm{P}} (\mathfrak{A}_p/x\mathfrak{O}_p)$ et chaque $\mathfrak{A}_p/x\mathfrak{O}_p$, qui est un module fini sur le localisé de $\mathbf{Z}$ en p, a pour cardinal une puissance de p. Notre forme prend donc en un n-uple d'entiers une valeur étrangère à p si et seulement si il existe $x \in \mathfrak{A}$ tel que $\mathfrak{A}_p = x\mathfrak{O}_p$. Mais $\mathfrak{A}$ est inversible si et seulement si tous les $\mathfrak{A}_p$ sont principaux d'où notre résultat.

On désigne maintenant par $cl(\mathfrak{O})$ le quotient du groupe des $\mathfrak{O}$-idéaux inversibles par le sous-groupe des idéaux principaux engendrés par les éléments de k de norme positive. La forme norme d'un idéal inversible ne dépendant que de sa classe dans $cl(\mathfrak{O})$ (voir remarque 1) nous pouvons parler de la forme norme d'une classe. Enfin nous dirons qu'une forme représente un entier si cet entier est une valeur de cette forme en un n-uple d'entiers rationnels. Avec ces notations on a :

Proposition 4. — *La forme norme d'une classe représente un entier positif m si et seulement si l'inverse de cette classe contient un idéal entier de norme m.*

Démonstration. — Cette proposition est démontrée dans le cas quadratique dans [2], chap. II, § 5, n° 6. Une démonstration analogue donne le résultat dans le cas général.

Remarque 2. — Si $\mathfrak{O}$ est stable par $\mathrm{Gal}(k|\mathbf{Q})$ alors ce groupe agit sur $cl(\mathfrak{O})$. Les formes normes associées à deux classes d'une même orbite sont identiques, nous parlerons donc de la classe attachée à une orbite.

2. L'ordre $\mathfrak{O}_\mathfrak{F}$ et le quotient $\mathbf{I}(\mathfrak{F})/\mathbf{N}(\mathfrak{F})$.

Soit $\mathfrak{F}$ un idéal entier du corps k stable par $\mathrm{Gal}(k|\mathbf{Q})$. On désigne par $\mathfrak{O}_\mathfrak{F}$ l'ordre $\mathbf{Z}+\mathfrak{F}$ de k, par $\mathrm{I}(\mathfrak{F})$ le groupe des idéaux de k premiers à $\mathfrak{F}$ et par $\mathrm{N}(\mathfrak{F})$ le plus petit sous-groupe de $\mathrm{I}(\mathfrak{F})$ contenant les idéaux principaux engendrés par les éléments de $\mathfrak{O}_\mathfrak{F}$ de norme positive et étrangers à $\mathfrak{F}$. On a alors la proposition suivante :

PROPOSITION 5. — *L'application qui a un idéal entier de* $\mathrm{I}(\mathfrak{F})$ *associe son intersection avec* $\mathfrak{O}_\mathfrak{F}$ *induit un isomorphisme du quotient* $\mathrm{I}(\mathfrak{F})|\mathrm{N}(\mathfrak{F})$ *sur* $cl(\mathfrak{O}_\mathfrak{F})$.

Démonstration. — Désignons par A l'anneau des entiers de k. L'idéal $\mathfrak{F}$ est un multiple du conducteur de $\mathfrak{O}_\mathfrak{F}$ et donc, pour tout $\mathfrak{O}_\mathfrak{F}$-idéal $\mathfrak{A}$ premier à $\mathfrak{F}$, on a $(\mathfrak{A}\mathrm{A}) \cap \mathfrak{O}_\mathfrak{F} = \mathfrak{A}$. En particulier, si $x \in \mathfrak{O}_\mathfrak{F}$ est un élément de norme positive et étranger à $\mathfrak{F}$, on a $x\mathrm{A} \cap \mathfrak{O}_\mathfrak{F} = x\mathfrak{O}_\mathfrak{F}$ et donc l'application qui a un idéal entier de $\mathrm{I}(\mathfrak{F})$ associe son intersection avec $\mathfrak{O}_\mathfrak{F}$ induit une application de $\mathrm{I}(\mathfrak{F})/\mathrm{N}(\mathfrak{F})$ dans $cl(\mathfrak{O}_\mathfrak{F})$. Cette application est clairement un homomorphisme de groupe. Elle est surjective (puisque dans toute classe de $cl(\mathfrak{O}_\mathfrak{F})$ il y a des idéaux étrangers à $\mathfrak{F}$), il reste à voir qu'elle est injective. Pour cela considérons une classe de $\mathrm{I}(\mathfrak{F})|\mathrm{N}(\mathfrak{F})$ dont l'image est triviale et choisissons un idéal entier $\mathfrak{U}$ de $\mathrm{I}(\mathfrak{F})$ représentant cette classe (toute classe modulo $\mathrm{N}(\mathfrak{F})$ contient des idéaux entiers). On a $\mathfrak{U} \cap \mathfrak{O}_\mathfrak{F} = x\mathfrak{O}_\mathfrak{F}$ pour un $x \in \mathfrak{O}_\mathfrak{F}$ de norme positive. Mais $\mathfrak{F}$ étant un multiple du conducteur de $\mathfrak{O}_\mathfrak{F}$ on a $(\mathfrak{U} \cap \mathfrak{O}_\mathfrak{F})\mathrm{A} = \mathfrak{U}$ et donc $\mathfrak{U} = x\mathrm{A}$. La classe de $\mathfrak{U}$ est donc triviale, cela achève la démonstration.

L'idéal $\mathfrak{F}$ étant supposé stable par $\mathrm{Gal}(k/\mathbf{Q})$, ce groupe agit de façon naturelle sur les deux quotients $\mathrm{I}(\mathfrak{F})/\mathrm{N}(\mathfrak{F})$ et $cl(\mathfrak{O}_\mathfrak{F})$. Il est clair que l'isomorphisme décrit dans la proposition précédente est compatible avec cette action et donc définit une bijection entre les ensembles d'orbites.

3. Le théorème de décomposition.

On désigne par K une extension galoisienne de $\mathbf{Q}$ dont le groupe de Galois G contient un sous-groupe abélien dis-

tingué H vérifiant les conditions (*) et (**) de l'introduction. On note k le corps des invariants de H, $\mathfrak{F}$ le conducteur de l'extension abélienne K/k et n le degré de $k/\mathbf{Q}$.

PROPOSITION 6. — *Le sous-groupe de* $I(\mathfrak{F})$ *attaché par la théorie du corps de classe à l'extension* K/k *contient* $N(\mathfrak{F})$.

Démonstration. — Par définition du conducteur, le sous-groupe de $I(\mathfrak{F})$ attaché à K/k contient tous les idéaux principaux engendrés par les éléments de k totalement positifs et congrus à 1 modulo $\mathfrak{F}$. D'autre part, désignons par G' le plus grand quotient abélien de G. Si x est un rationnel étranger au discriminant de K, on note $F(x)$ le Frobenius de x dans G'. On sait que l'image de $F(x)$ par le transfert relatif à H est le Frobenius dans K/k de l'idéal de k engendré par x. Ce transfert étant nul, il en résulte que l'idéal principal engendré par x dans k est dans le sous-groupe de $I(\mathfrak{F})$ attaché à K/k. On en déduit facilement que ce sous-groupe contient tous les idéaux principaux engendrés par les éléments de $\mathfrak{O}_{\mathfrak{F}}$ premiers à $\mathfrak{F}$ et totalement positifs. Si k est un corps quadratique ou un corps imaginaire les éléments totalement positifs coïncident avec ceux de normes positives et la démonstration est achevée. Sinon ils sont d'indice une puissance de 2 et on achève la démonstration grâce à l'hypothèse $[K : k]$ impair.

Le corps K étant galoisien sur $\mathbf{Q}$, le conducteur $\mathfrak{F}$ de K/k est stable par $\mathrm{Gal}\,(k/\mathbf{Q})$. Ce groupe agit donc sur $cl(\mathfrak{O}_{\mathfrak{F}})$. On est maintenant en mesure de démontrer le théorème sur la décomposition des nombres premiers dans K :

THÉORÈME. — *Soit* p *un nombre premier étranger à* $\mathfrak{F}$ *et* r *son degré résiduel dans* k. *Une et une seule des formes normes associées aux orbites de* $cl(\mathfrak{O}_{\mathfrak{F}})$ *représente* p^r *et le degré résiduel de* p *dans* $K/\mathbf{Q}$ *ne dépend que de cette forme.*

Démonstration. — Soit $\mathfrak{p}$ un idéal premier de k au-dessus de p. L'idéal $\mathfrak{p}$ étant étranger au conducteur de $\mathfrak{O}_{\mathfrak{F}}$, on sait que $N_{\mathfrak{O}_{\mathfrak{F}}}(\mathfrak{p} \cap \mathfrak{O}_{\mathfrak{F}})$ est égal à la norme de $\mathfrak{p}$ i.e. à p^r. Il résulte donc de la proposition 4 que p^r est représenté par la forme norme associée à l'orbite de la classe de l'inverse de $\mathfrak{p} \cap \mathfrak{O}_{\mathfrak{F}}$. Réciproquement, si p^r est représenté par la forme

norme associée à une orbite de $cl(\mathfrak{O}_\mathfrak{F})$, les inverses des classes formant cette orbite contiennent tous les $\mathfrak{O}_\mathfrak{F}$-idéaux entiers de norme p^r. Mais ces $\mathfrak{O}_\mathfrak{F}$-idéaux sont les $\mathfrak{q} \cap \mathfrak{O}_\mathfrak{F}$ ou $\mathfrak{q}$ décrit les idéaux premiers de k au-dessus de p. Il résulte donc de la remarque 2 que les classes de ces $\mathfrak{q}$ modulo $N(\mathfrak{F})$ sont dans une orbite qui ne dépend que de la forme représentant p^r. Enfin, la proposition 6 montre que la classe de $\mathfrak{q}$ modulo $N(\mathfrak{F})$ détermine le degré résiduel de $\mathfrak{q}$ dans K/k donc de p dans $K|\mathbf{Q}$ ce qui achève la démonstration.

Remarque 3. — L'application du théorème nécessite le calcul du degré résiduel de p dans $k/\mathbf{Q}$; ce calcul est particulièrement simple lorsque $k/\mathbf{Q}$ est abélienne, ce sera le cas dans les applications.

Remarque 4. — Il résulte du théorème de Furtwängler ([3], chap XIII) que la condition relative au transfert est vérifiée lorsque k est la clôture abélienne de $\mathbf{Q}$ dans K.

4. Exemples.

Retrouvons tout d'abord le résultat de Gauss. Pour cela posons $k = \mathbf{Q}(j)$ où j est une racine cubique de l'unité et $K = \mathbf{Q}(j, \sqrt[3]{2})$. Le conducteur de K/k est l'idéal principal de k engendré par 6; notons le 6. On a

$$cl(\mathfrak{O}_6) \simeq I(6)/N(6) \simeq \mathbf{Z}/3$$

et il y a deux orbites. La forme associée à l'orbite du $\mathfrak{O}_6$-idéal $\mathfrak{O}_6$ est $X_1^2 + 27X_2^2$. Les nombres premiers $p \equiv 1 \bmod 3$ sont décomposés dans $k = \mathbf{Q}(j)$; il résulte donc du théorème qu'ils sont complètement décomposés dans K si et seulement si ils s'écrivent $x^2 + 27y^2$ avec x et y dans $\mathbf{Z}$. Mais les p totalement décomposés dans K sont ceux tels que 2 est un cube modulo p, on a donc retrouvé le résultat de Gauss.

On peut dans l'exemple précédent remplacer 2 par un autre entier a. Notre théorème permet d'affirmer qu'il existe un ensemble fini de formes quadratiques tel que les $p \equiv 1 \bmod 3$ représentés par l'une de ces formes sont ceux modulo lesquels a

est un cube. Le nombre des formes intervenant est en général plus grand que 1. Si l'on prend $a=5$, alors $\mathfrak{F}$ est l'idéal principal engendré par 15; on le note 15. On a

$$I(15)/N(15) \simeq cl(\mathfrak{O}_{15}) \simeq \mathbf{Z}/6$$

et il y a 4 orbites. Les 4 formes correspondantes sont

$$X_1^2 + X_1X_2 + 169X_2^2, \qquad 343X_1^2 - 131X_1X_2 + 13X_2^2,$$
$$7X_1^2 - 5X_1X_2 + 25X_2^2 \quad \text{et} \quad 49X_1^2 + 33X_1X_2 + 9X_2^2.$$

Les $p \equiv 1 \bmod 3$ représentés par l'une des deux premières de ces formes sont ceux modulo lesquels 5 est un cube (par exemple $343 - 131 \times 5 + 13 \times 25 = 13$ et

$$5 \equiv 7^3 \bmod. 13; \qquad 343 - 131 \times 8 + 13 \times 8^2 = 127$$

et

$$5 \equiv 55^3 \bmod. 127; \qquad 36 + 6 + 169 = 211$$

et

$$5 \equiv 6^3 \bmod. 211).$$

La même méthode permet de chercher les nombres premiers modulo lesquels un entier a est une puissance $m^{\text{ième}}$. Les formes intervenant sont alors de degré $\varphi(m)$ et ont $\varphi(m)$ variables. Emma Lehmer [4] a regardé le cas $a = 2,3$ et $m = 5$.

BIBLIOGRAPHIE

[1] Gauss, Arithmetishe Untersuchungen, Werke Bd (traduction française : Blanchard; traduction anglaise : Yale Univ. Press).
[2] Borevich, Shafarevich, Théorie des nombres, *Monographie internationale de Math. Moderne* n° 8, Gauthier-Villard.
[3] Artin, Tate, Class Field Theory, Harvard (1961).
[4] Emma Lehmer, Cubic and Quintic residue, *Duke Math. Journal*, 18 (1951).

Manuscrit reçu le 10 septembre 1976
Proposé par J. Martinet.
Philippe Satge,
U.E.R. de Mathématiques
Faculté de Caen
Esplanade de la Paix
14000 Caen.