

ALAIN FAISANT

Interprétation factorielle du nombre de classes dans les ordres des corps quadratiques

Annales mathématiques Blaise Pascal, tome 7, n° 2 (2000), p. 13-18

http://www.numdam.org/item?id=AMBP_2000__7_2_13_0

© Annales mathématiques Blaise Pascal, 2000, tous droits réservés.

L'accès aux archives de la revue « Annales mathématiques Blaise Pascal » (<http://math.univ-bpclermont.fr/ambp/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

Interprétation factorielle du nombre de classes dans les ordres des corps quadratiques

Alain FAISANT

Résumé : Soit \mathcal{O} un ordre d'un corps quadratique, de conducteur f et de nombre de classes h ; l'anneau \mathcal{O} n'est pas en général factoriel ; on définit une notion d'élément h -premier qui donne une « sorte de factorialité » à une certaine partie A_f de \mathcal{O} .

1. Notations et rappels

1.1. $K = \mathbb{Q}(\sqrt{d})$ ($d \in \mathbb{Z}$ sans facteur carré) étant donné, on définit \mathcal{O}_K comme étant l'anneau des entiers de K : $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$ où $\omega = \frac{1+\sqrt{d}}{2}$ si $d \equiv 1 \pmod{4}$ et $\omega = \sqrt{d}$ si $d \equiv 2, 3 \pmod{4}$.

1.2. Soit \mathcal{O} un ordre de K (i.e. un sous-anneau unitaire de rang 2 de K) ; \mathcal{O} est de la forme $\mathcal{O} = \mathcal{O}_f = \mathbb{Z} + \mathbb{Z}f\omega$, où $f \in \mathbb{N}$, $f \geq 1$: \mathcal{O} est caractérisé par son conducteur f ; pour alléger les notations on ne précise pas toujours f ; \mathcal{O} est un anneau noethérien et $\mathcal{O}_f \subset \mathcal{O}_1 = \mathcal{O}_K$.

1.3. M_f désigne le groupe des modules de K associés à \mathcal{O}_f , c'est-à-dire : $M \in M_f$ si et seulement si M est un sous-groupe additif de K dont l'anneau de stabilisateurs $\{x \in K ; xM \subset M\}$ est exactement \mathcal{O}_f .

Si $P_f = \{M \in M_f ; M = \alpha\mathcal{O}_f, \alpha \in K\}$, alors le groupe $Cl_f = M_f/P_f$ des classes de l'ordre \mathcal{O}_f est un groupe fini ; son ordre est noté h_f .

1.4. Pour $M \in M_f$ on note $\mathcal{N}(M)$ la norme de M ($0 \leq \mathcal{N}(M) \in \mathbb{Q}$, et $\mathcal{N}(M) \in \mathbb{N}$ si et seulement si $M \subset \mathcal{O}_f$) ; si $\alpha \in K$ et $M = \alpha\mathcal{O}_f$, alors $\mathcal{N}(M) = |\mathcal{N}(\alpha)|$.

1.5. Si $M \in M_f$ et $M \subset \mathcal{O}_f$ on dit que M est un \mathcal{O}_f -idéal : M est en particulier un idéal de l'anneau \mathcal{O}_f ; un idéal I de \mathcal{O}_f n'est pas forcément un \mathcal{O}_f -idéal ; néanmoins si I est premier avec $f\mathcal{O}_f$, on montre que I est un \mathcal{O}_f -idéal : cf [3] (lemme IV.5, p.163) ou [2] (Exercice 8, p.169).

1.6. Un \mathcal{O} -idéal I de l'ordre \mathcal{O} est dit \mathcal{O} -irréductible si : $I \neq \mathcal{O}$ et $I = I_1.I_2$, où I_1 et I_2 sont des \mathcal{O} -idéaux entraîne $I_1 = \mathcal{O}$ ou $I_2 = \mathcal{O}$.

• Tout \mathcal{O}_f -idéal (non nul si $f = 1$) est produit de \mathcal{O}_f -idéaux \mathcal{O}_f -irréductibles (ceci est dû au fait que \mathcal{O}_f est noethérien).

1.7. Un \mathcal{O} -idéal I est dit \mathcal{O} -premier si : I divise $I_1.I_2$ implique I divise I_1 ou I_2 (où I divise I_1 signifie qu'il existe un \mathcal{O} -idéal L tel que $I_1 = I.L$). Il est clair que \mathcal{O} -premier implique \mathcal{O} -irréductible (la réciproque est fautive : cf [3], exercice IV.15) ; pour remédier à cela on introduit :

1.8. $J_f = \{I; I \text{ } \mathcal{O}_f\text{-idéal et } I + f\mathcal{O}_f = \mathcal{O}_f\}$: c'est donc l'ensemble des \mathcal{O}_f -idéaux premiers avec l'idéal $f\mathcal{O}_f$ de \mathcal{O}_f .

Lemme 1. *Soit I un idéal de \mathcal{O}_f .*

Pour que $I \in J_f$ il faut et suffit que $\text{PGCD}(\mathcal{N}(I), f) = 1$.

Preuve. cf [3], p.163.

Théorème 1.

- 1) *Si $I \in J_f$ on a : I est \mathcal{O}_f -irréductible si et seulement si I est \mathcal{O}_f -premier*
- 2) *Tout \mathcal{O}_f -idéal, non nul lorsque $f = 1$, de J_f est, de façon unique, produit de \mathcal{O}_f -idéaux \mathcal{O}_f -irréductibles*

Preuve. 1) provient essentiellement du lemme 1 ; 2) est alors évident.

2. Éléments k-premiers ; k-factorialité

\mathcal{O}_f étant noethérien, on sait que tout $x \in \mathcal{O}_f \setminus \{0\}$ admet une décomposition en produit de facteurs irréductibles ; comme en général « irréductible $\not\Rightarrow$ premier » on n'a pas unicité de la décomposition. L'idée consiste à introduire le nombre de classes h_f , ou mieux k_f , pour retrouver cette unicité ; à cet effet on définit

$$A_f = \{x \in \mathcal{O}_f; \text{PGCD}(\mathcal{N}(x), f) = 1\},$$

analogue de J_f pour les éléments.

Lemme 2.

- i) $\mathcal{O}_f^\times \subset A_f$ (\mathcal{O}_f^\times est le groupe des unités de \mathcal{O}_f)
- ii) *Si $f = 1$ on a $A_f = \mathcal{O}_K$*

iii) Si $f > 1$, alors A_f est un sous-demi-groupe multiplicatif de \mathcal{O}_f ; de plus A_f est consistant : si x et $y \in \mathcal{O}_f$ et $xy \in A_f$, alors x et $y \in A_f$.

iv) Si $x \in \mathcal{O}_f$ et $x \neq 0$ on a : $x \in A_f \Leftrightarrow x\mathcal{O}_f \in J_f$.

Preuve.

i) et ii) sont clairs.

iii) Si $\text{PGCD}(\mathcal{N}(xy), f) = 1$ alors $\text{PGCD}(\mathcal{N}(x), f) = \text{PGCD}(\mathcal{N}(y), f) = 1$.

iv) $I = x\mathcal{O}_f$ est un idéal de l'anneau \mathcal{O}_f ; d'après le lemme 1 on a $I \in J_f$ si et seulement si $\mathcal{N}(I)$ est premier à f , mais $\mathcal{N}(I) = |\mathcal{N}(x)|$, d'où le résultat.

On désigne par k_f l'exposant du groupe Cl_f (k_f est le maximum des ordres des éléments de Cl_f ; on sait que k_f divise l'ordre h_f de Cl_f); on dira que $\pi \in A_f$ est k_f – premier s'il vérifie :

$$(\pi \text{ divise } xy \text{ dans } A_f) \Rightarrow (\pi \text{ divise } x^{k_f} \text{ ou } \pi \text{ divise } y^{k_f} \text{ dans } A_f).$$

Lemme 3.

Soient P un élément \mathcal{O}_f – irréductible de J_f , $\alpha \geq 1$ l'ordre de $\text{cl}(P)$ dans Cl_f et $\pi \in \mathcal{O}_f$ tel que $P^\alpha = \pi\mathcal{O}_f$. Alors :

i) $\pi \in A_f$

ii) π est irréductible dans A_f : si $\pi = xy$, où x et $y \in A_f$, on a $x \in \mathcal{O}_f^\times$ ou $y \in \mathcal{O}_f^\times$

iii) π est k_f – premier.

Preuve.

i) car $\pi \in \mathcal{O}_f$ et $|\mathcal{N}(\pi)| = \mathcal{N}(P)^\alpha$ est premier à f .

ii) Si $\pi = xy$, alors $P^\alpha = x\mathcal{O}_f.y\mathcal{O}_f$ et $x\mathcal{O}_f, y\mathcal{O}_f \in J_f$; le théorème 1 donne $x\mathcal{O}_f = P^u$ et $y\mathcal{O}_f = P^v$, où $u + v = \alpha$; alors P^u est principal donc α divise u ; de même α divise v : si $u = \alpha u'$ et $v = \alpha v'$ on a $\alpha = u + v = \alpha(u' + v')$ qui impose $u' + v' = 1$, d'où par exemple $u' = 0, v' = 1$, auquel cas $u = 0, v = \alpha$, alors $y\mathcal{O}_f = P^\alpha = \pi\mathcal{O}_f$: il existe $\varepsilon \in \mathcal{O}_f^\times$ tel que $y = \varepsilon\pi$, et enfin $x = \varepsilon^{-1} \in \mathcal{O}_f^\times$.

iii) Si π divise xy alors $\pi\mathcal{O}_f = P^\alpha$ divise $x\mathcal{O}_f.y\mathcal{O}_f$, donc par exemple P divise $x\mathcal{O}_f$: si $x\mathcal{O}_f = P.J$, alors $x^\alpha\mathcal{O}_f = P^\alpha.J^\alpha = \pi J^\alpha$, donc $x^\alpha \in \pi J^\alpha$ et π divise x^α ; comme α divise k_f , a fortiori π divise x^{k_f} .

Il n'y a pas d'autres irréductibles k_f – premiers que ceux du lemme 3 :

Lemme 4.

Soit $\pi \in \mathbf{A}_f$ irréductible et k_f - premier ; alors il existe un élément \mathcal{O}_f - irréductible P de \mathbf{J}_f tel que $\pi\mathcal{O}_f = P^\alpha$ (où α est l'ordre de $cl(P)$ dans Cl_f).

Preuve.

On note \mathcal{O} pour \mathcal{O}_f et k pour k_f . Le théorème 1 donne $\pi\mathcal{O} = P_1 \dots P_n$, où les P_i sont \mathcal{O} - irréductibles ; alors si α_i est l'ordre de $cl(P_i)$ dans Cl_f il existe $p_i \in \mathcal{O}$ tel que $P_i^{\alpha_i} = p_i\mathcal{O}$; soit $s_i = k/\alpha_i$ de sorte que $\pi^k\mathcal{O} = (p_1\mathcal{O})^{s_1} \dots (p_n\mathcal{O})^{s_n} = p_1^{s_1} \dots p_n^{s_n}\mathcal{O}$, donc $\pi^k = \varepsilon p_1^{s_1} \dots p_n^{s_n}$ où $\varepsilon \in \mathcal{O}^\times$; comme π est k - premier il existe i tel que π divise $p_i^{s_i k}$; si $p_i^{s_i k} = \pi x$ on a $p_i^{s_i k}\mathcal{O} = \pi\mathcal{O}.x\mathcal{O} = P_i^{s_i \alpha_i k}$ et l'unicité (théorème 1) donne $\pi\mathcal{O} = P_i^{r_i}$, donc α_i divise r_i ; si $r_i = \alpha_i t$ on a $\pi = u p_i^t$, où $u \in \mathcal{O}^\times$; comme π est irréductible on a $p_i \notin \mathcal{O}^\times$ et on en déduit que $t = 1$ donc $\pi\mathcal{O} = P_i^{\alpha_i}$.

Théorème 2.

Soit $x \in \mathbf{A}_f$ tel que $x \notin \mathcal{O}_f^\times$ et $x \neq 0$, alors

- i) il existe π_1, \dots, π_r irréductibles, k_f - premiers et non associés deux à deux tels que $x^{k_f} = \pi_1^{s_1} \dots \pi_r^{s_r}$, où les nombres entiers s_i sont ≥ 1 ;
- ii) cette décomposition est unique à l'ordre près des facteurs et à unité près.

On dit que \mathbf{A}_f est k_f - factoriel.

Preuve. On note encore \mathcal{O} pour \mathcal{O}_f et k pour k_f .

- i) On a $x\mathcal{O} = P_1 \dots P_n$ et l'ordre α_i de $cl(P_i)$ divise k : si $k = \alpha_i \sigma_i$ et $P_i^{\alpha_i} = \pi_i\mathcal{O}$, où $\pi_i \in \mathcal{O}$, on a $x^k\mathcal{O} = \pi_1^{\sigma_1}\mathcal{O} \dots \pi_n^{\sigma_n}\mathcal{O}$ donc $x^k = \varepsilon \pi_1^{\sigma_1} \dots \pi_n^{\sigma_n}$, où $\varepsilon \in \mathcal{O}^\times$; les π_i sont irréductibles et k - premiers (lemme 3) ; après regroupement on obtient $x^k = \varepsilon \pi_1^{s_1} \dots \pi_r^{s_r}$.
- ii) Si $x^k = \rho_1^{t_1} \dots \rho_n^{t_n}$ est une décomposition du même type, alors ρ_1 divise $\pi_1^{s_1} \dots \pi_r^{s_r}$, donc, quitte à renuméroter, ρ_1 divise $\pi_1^{s_1 k}$ (car ρ_1 est k - premier) : si $\pi_1^{s_1 k} = a\rho_1$, comme $\pi_1\mathcal{O} = P_1^{\alpha_1}$ (lemme 4), on a $P_1^{\alpha_1 s_1 k} = \rho_1\mathcal{O}.a\mathcal{O}$; l'unicité de la décomposition des \mathcal{O} - idéaux et le fait que ρ_1 et $a \in \mathbf{A}_f$ montrent que $\rho_1\mathcal{O} = P_1^\psi$. Ainsi α_1 divise w : si $w = \alpha_1 v_1$, on a $\rho_1\mathcal{O} = \pi_1^{v_1}\mathcal{O}$, donc $\rho_1 = u\pi_1^{v_1}$, où $u \in \mathcal{O}^\times$; comme ρ_1 est irréductible on a $v_1 = 1$ donc ρ_1 et π_1 sont associés.

On montre maintenant que $s_1 = t_1$:

- a) Si $t_1 > s_1$ on écrit $t_1 = s_1 + \sigma$, où $\sigma > 0$, d'où, après simplification :

$$\pi_2^{s_2} \dots \pi_r^{s_r} = u \pi_1^\sigma \rho_2^{t_2} \dots \rho_n^{t_n}$$

donc π_1 divise $\pi_2^{s_2} \dots \pi_r^{s_r}$; comme π_1 est k - premier, π_1 divise, par exemple, π_2^k : si $\pi_2^k = \pi_1 y$ on a $P_2^{\alpha_2 k} = P_1^{\alpha_1} . y \mathcal{O}$; l'unicité de la décomposition des \mathcal{O} - idéaux impose $P_1 = P_2$ et π_2 serait associé à π_1 , ce qui n'est pas.

b) On a donc $s_1 \geq t_1$ donc $s_1 = t_1 + \sigma$, où $\sigma \geq 0$, d'où $\pi_1^\sigma \pi_2^{s_2} \dots \pi_r^{s_r} = u \rho_2^{t_2} \dots \rho_n^{t_n}$. Si on avait $\sigma > 0$ on en déduirait que π_1 divise, par exemple, ρ_2^k , donc que ρ_1 diviserait ρ_2^k ; en raisonnant comme en a), on conclurait que ρ_1 et ρ_2 sont associés, ce qui n'est pas. Ainsi $\sigma = 0$ et $s_1 = t_1$.

On conclut par itération.

Corollaire.

Si $h_f = 1$ le demi-groupe A_f est factoriel en ce sens que tout $x \in A_f \setminus \mathcal{O}_f^\times$ et non nul s'écrit $x = \pi_1^{s_1} \dots \pi_r^{s_r}$, où les π_i sont irréductibles et premiers dans A_f non associés deux à deux, et cette écriture est unique à l'ordre près des facteurs et à unité près.

Exemples 1

Les ordres $\mathbf{Z} + \mathbf{Z}\sqrt{-3}$, $\mathbf{Z} + \mathbf{Z}\sqrt{-7}$, $\mathbf{Z} + \mathbf{Z}2i$ des corps $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-7})$, $\mathbf{Q}(i)$ ont pour conducteur $f = 2$ et nombre de classes $h_2 = 1$: le demi-groupe correspondant A_2 est factoriel ; il en est de même pour l'ordre \mathcal{O}_3 de $\mathbf{Q}(\sqrt{-3})$: $f = 3$, $h_3 = 1$; ces quatre ordres sont les seuls ordres de corps quadratiques imaginaires de conducteur $f \geq 2$ pour lesquels le nombre de classes h_f vaut 1. Par contre le demi-groupe A_2 de $\mathbf{Z} + \mathbf{Z}\sqrt{-11}$ est « 3-factoriel » : on a $x^3 = \pi_1^{s_1} \dots \pi_r^{s_r}$ pour tout $x \in A_2 \setminus \mathcal{O}_2^\times$, où les π_i sont des éléments irréductibles et 3-premiers de A_2 . C'est la factorialité du A_2 de $\mathbf{Z} + \mathbf{Z}2i$ qui est utilisée dans [1].

Exemple 2

L'anneau des entiers de $K = \mathbf{Q}(\sqrt{-5})$ est $\mathcal{O}_K = \mathbf{Z}[\omega]$, où $\omega^2 = -5$; le nombre de classes est $h = 2$; l'exemple classique (cf [4]) est

$$x = 6 = 2 \times 3 = (1 + \omega)(1 - \omega).$$

Pour avoir la décomposition de x^2 selon le théorème 2 (ici $f = 1$) on calcule

$$(1 \pm \omega)^2 = 2(-2 \pm \omega), \text{ d'où}$$

$$x^2 = 2^2 (-2 + \omega)(-2 - \omega).$$

C'est la décomposition recherchée :

- 2 est irréductible et 2-premier puisque $2\mathcal{O}_K = P^2$ (2 est ramifié car $\text{Disc } K = -20$) et d'après le lemme 3

• 3 est décomposé (car $\text{Disc } K$ est un résidu quadratique modulo 3) donc $3\mathcal{O}_K = Q \cdot Q'$. On a $Q^2 = (2 + \omega)\mathcal{O}_K$ et $Q'^2 = (2 - \omega)\mathcal{O}_K$, donc $-2 \pm \omega$ sont 2-premiers, et irréductibles car de norme 9 et, dans \mathcal{O}_K il n'y a pas d'élément de norme 3 ($a^2 + 5b^2 = 3$ n'a pas de solution dans \mathbf{Z}^2).

La décomposition $x^2 = 2^2 \times 3^2$ est à rejeter car le nombre $\pi = 3$ est irréductible, mais n'est pas 2-premier : 3 divise $(1 + \omega)(1 - \omega) = 6$ mais ne divise pas $(1 \pm \omega)^2 = -4 \pm 2\omega$ (car 3 ne divise pas 4 dans \mathbf{Z}); de même $x^2 = (1 + \omega)^2(1 - \omega)^2$ est à rejeter puisque l'irréductible $\pi = 1 + \omega$ divise 2×3 mais ne divise ni 2^2 ni 3^2 ($\mathcal{N}(\pi) = 6$, $\mathcal{N}(2^2) = 16$, $\mathcal{N}(3^2) = 81$).

Remarque : Il est facile de voir que, si le nombre premier p est ramifié ou inerte dans K , alors p est irréductible et k -premier dans \mathcal{O}_K ($f = 1$); alors que si p est décomposé, il n'est pas k -premier.

Bibliographie

- [1] L. BAPOUNGUÉ. – *Sur la résolubilité de l'équation diophantienne $ax^2 + 2bxy - kay^2 = \pm 1$* ; C. R. Acad. Sci. Paris, série I, t.309 (1989), 235-238.
- [2] Z. BOREVITCH et I. CHAFAREVITCH. – *Théorie des nombres*; Gauthier-Villars, Paris, 1967.
- [3] A. FAISANT. – *L'équation diophantienne du second degré*; Hermann, Paris, 1991.
- [4] P. SAMUEL. – *Théorie algébrique des nombres*; Hermann, Paris, 1967.

Alain FAISANT
 Équipe de Théorie des Nombres
 Faculté des Sciences
 23, rue du Docteur Paul Michelon
 42023 ST ETIENNE CEDEX 2