Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
C. R. Acad. Sci. Paris, Ser. I 336 (2003) 7–10
COMPTES RENDUS MATHEMATIQUE

Algèbre/Théorie des nombres

La classe invariante d'une forme binaire

The invariant class of a binary form

Denis Simon

LMNO-UMR 6139, Université de Caen–France, Campus II, boulevard Mal Juin, BP 5186, 14032 Caen cedex, France

Reçu le 27 mars 2002 ; accepté après révision 19 novembre 2002

Présenté par Jean-Pierre Serre

Résumé

Nous montrons comment on peut associer à chaque forme binaire irréductible un élément du groupe de classes de l'anneau associé. Cette classe ne dépend pas du choix du représentant de la forme modulo l'action de SL_2. Il s'agit d'une généralisation de la théorie classique pour les formes quadratiques. ***Pour citer cet article : D. Simon, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

Abstract

We explain how to associate to any irreducible binary form an element of the class group in the corresponding ring. This class does not depend on the choice of the form modulo the action of SL_2. The question is to generalize the classical theory of quadratic forms. ***To cite this article: D. Simon, C. R. Acad. Sci. Paris, Ser. I 336 (2003).***

1. Introduction

Soit R un anneau commutatif intègre, et K son corps des fractions. Soit P un polynôme homogène en x et y de degré n à coefficients dans R. Le groupe $\mathrm{SL}_2(R)$ agit sur de tels polynômes par $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) P(x,y) = P(ax+by, cx+dy)$. Il est bien connu que le discriminant de P est un invariant pour cette action.

Dans [6], nous avons vu comment associer à la forme P un ordre dans $L = K[x]/P(x,1)$ de discriminant $\mathrm{Disc}\, P$. Nous avons prouvé que cet ordre est invariant par l'action de $\mathrm{SL}_2(R)$ sur P.

Notre objectif dans cette Note est de décrire un nouvel invariant pour P quand P est primitive. A une forme P fixée, nous pouvons associer un idéal entier dans son ordre invariant : on décrira cet idéal comme le numérateur ou le dénominateur d'une racine de P. Cet idéal est inversible (en tant qu'idéal fractionnaire), et son image dans le groupe de classes ne change pas lorsque $\mathrm{SL}_2(R)$ agit sur P.

Adresse e-mail : simon@math.unicaen.fr (D. Simon).

1631-073X/03/$ – see front matter
doi:10.1016/S1631-073X(02)00021-3

Cet invariant, donné par la classe d'un idéal entier dans un certain groupe de classes est défini classiquement pour les formes quadratiques sur $\mathbb{Z}$ (voir par exemple [2, §7]). On peut donc voir les résultats de cette Note comme une généralisation de cette belle théorie classique aux degrés supérieurs. Mais nous verrons sur quelques exemples que les résultats ne sont pas aussi remarquables que dans le cas quadratique. En effet, les classes des formes binaires ne permettent pas d'atteindre tout le groupe de classes, et il peut aussi arriver que deux formes non équivalentes aient la même classe.

2. Notations et hypothèses générales

Soit R un anneau commutatif intègre, et K son corps des fractions. Soit $R_n[x, y]$ le R-module des formes binaires homogènes de degré n en les variables x et y à coefficients dans R, et soit $R_n[x]$ le R-module des polynômes de degré $d \leqslant n$ en x. Nous identifions $R_n[x, y]$ et $R_n[x]$ par $P(x, y) \to P(x, 1)$.

Le groupe $\mathrm{SL}_2(R)$ des matrices 2×2 de déterminant 1 et à coefficients dans R agit sur $R_n[x, y]$ par $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) P(x, y) = P(ax + by, cx + dy)$. Il est bien connu que cette action ne change pas le discriminant Disc P de la forme $P(x, y)$.

Hypothèses. *Nous supposerons désormais que toutes les formes P qui interviennent sont primitives, ce qui signifie que les coefficients a_i de P sont premiers entre eux* (*dans le sens précis que la somme des idéaux principaux $a_i R$ est exactement R*). *Cette propriété est préservée par l'action de* $\mathrm{SL}_2(R)$. *Nous supposerons aussi que les formes sont irréductibles* (*en tant que formes à coefficients dans le corps K*). *Avec cette hypothèse, les résultats sont plus faciles à énoncer, mais resteraient essentiellement vrais, à condition que le discriminant et le coefficient dominant des formes P ne s'annulent pas* (*on parlera alors d'algèbres étales au lieu de corps*).

Notations. Soit θ l'image de x dans la projection canonique $K[x] \to L = K[x]/P(x)$. L'élément θ doit être vu comme une racine de P. Le corps $L = K(\theta)$ ne change pas lorsque $\mathrm{SL}_2(R)$ agit sur P. Notons $P = a_0x^n + a_1x^{n-1} + \cdots + a_n$. Puisque $P(x, y)$ est irréductible, on a $a_0 \neq 0$. Pour $0 \leqslant i < n$, posons

$$P_i(x) = a_0x^i + a_1x^{i-1} + \cdots + a_i.$$

Ces polynômes satisfont la formule de récurrence $xP_i + a_{i+1} = P_{i+1}$. Par exemple, on a $P_0 = a_0$, et $\theta P_{n-1}(\theta) = -a_n$. L'anneau invariant de P est défini par

$$R_P = R \oplus P_1(\theta)R \oplus \cdots \oplus P_{n-1}(\theta)R.$$

On a montré dans [6] que ce R-module est un ordre de L qui ne change pas lorsque $\mathrm{SL}_2(R)$ agit sur P. Comme c'est un ordre, ses éléments sont entiers sur R. Le discriminant de cet anneau est exactement Disc P. Remarquons que $P_i(\theta) \in R_P$ et $\theta P_i(\theta) \in R_P$.

On rappelle qu'un idéal fractionnaire I dans un anneau commutatif intègre R est *inversible* s'il existe un autre idéal fractionnaire I^{-1} tel que $I \cdot I^{-1} = R$. Un idéal principal est toujours inversible. Le groupe de classes $\mathrm{Cl}(R)$ est le quotient du groupe des idéaux inversibles de R par le sous-groupe des idéaux principaux.

Dans l'extension R_P/R, le *groupe de classes relatif* $\mathrm{Cl}(R_P/R)$ est par définition le noyau de la norme de $\mathrm{Cl}(R_P)$ vers $\mathrm{Cl}(R)$. Lorsque $\mathrm{Cl}(R) = 1$, on a $\mathrm{Cl}(R_P/R) = \mathrm{Cl}(R_P)$.

3. Resultats

Nous commençons par considérer plusieurs idéaux de R_P associés à une forme primitive irréductible P. Le premier est

$$\mathfrak{b} = P_0R_P + P_1(\theta)R_P + \cdots + P_{n-1}(\theta)R_P.$$

C'est un idéal entier puisque $P_j(\theta) \in R_P$. Nous verrons qu'il s'agit du *dénominateur de* θ. Considérons aussi l'idéal $\mathfrak{a} = \theta\mathfrak{b}$. Ce second idéal est encore entier puisque

$$\mathfrak{a} = \theta P_0 R_P + \theta P_1(\theta) R_P + \cdots + \theta P_{n-1}(\theta) R_P$$

et que $\theta P_j(\theta) \in R_P$. L'idéal $\mathfrak{a}$ est le *numérateur de* θ. Enfin, pour $0 \leqslant j < n$, considérons les idéaux entiers

$$\mathfrak{I}_j = P_j(\theta) R_P + \theta P_j(\theta) R_P.$$

Lemme 3.1. *On a* $\mathfrak{a} + \mathfrak{b} = \sum_{j=0}^{n-1} \mathfrak{I}j = R_P$.

Démonstration. Soit $\mathfrak{J} = \mathfrak{a} + \mathfrak{b}$. D'après la définition, il est clair que $\mathfrak{J} = \sum_{j=0}^{n-1} \mathfrak{I}j$, et que $\mathfrak{J}$ est un idéal entier de R_P. Cet idéal contient $P_j(\theta) \in \mathfrak{b}$ et $\theta P_{j-1}(\theta) \in \mathfrak{a}$ pour $0 < j < n$, donc il contient $P_j(\theta) - \theta P_{j-1}(\theta) = a_j$. Mais il contient aussi $a_0 = P_0(\theta) \in \mathfrak{b}$ et $a_n = -\theta P_{n-1}(\theta) \in \mathfrak{a}$. Comme P est primitive, on déduit que $\mathfrak{J} = R_P$. □

Proposition 3.2. *Les idéaux* $\mathfrak{a}$, $\mathfrak{b}$ *et* $\mathfrak{I}_j$ (*pour* $0 \leqslant j < n$) *sont inversibles* (*comme idéaux fractionnaires de* R_P). *Leurs images dans* $\mathrm{Cl}(R_P)$ *satisfont la relation*

$$\mathrm{Cl}(\mathfrak{a})^{-1} = \mathrm{Cl}(\mathfrak{b})^{-1} = \mathrm{Cl}(\mathfrak{I}_j).$$

Démonstration. On a $\mathfrak{I}_0 \cdot \mathfrak{b} = a_0\mathfrak{b} + a_0\theta\mathfrak{b} = a_0(\mathfrak{b} + \mathfrak{a}) = a_0 R_P$. On déduit de cette relation que $\mathfrak{b}$ et $\mathfrak{I}_0$ sont inversibles. Mais on sait que $\mathfrak{a} = \theta\mathfrak{b}$ et que $\mathfrak{I}_j = \frac{1}{a_0} P_j(\theta)\mathfrak{I}_0$, donc les autres idéaux sont aussi inversibles. La relation entre leurs images dans le groupe de classes $\mathrm{Cl}(R_P)$ est claire. □

Nous savons maintenant que $\theta = \mathfrak{a}/\mathfrak{b}$ où $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux entiers premiers entre eux. Ceci signifie que $\mathfrak{a}$ et $\mathfrak{b}$ sont le numérateur et le dénominateur de θ. La proposition suivante donne une R-base pour ces idéaux, ainsi que leur norme.

Proposition 3.3. *On a* $\mathfrak{b} = \bigoplus_{j=0}^{n-1} P_j(\theta) R$ *et* $\mathfrak{a} = \bigoplus_{j=0}^{n-1} \theta P_j(\theta) R$. *En particulier,* $R_P/\mathfrak{b} = R/a_0 R$ *et* $R_P/\mathfrak{a} = R/a_n R$. *On a aussi* $\mathcal{N}_{R_P/R}(\mathfrak{a}) = a_n R$ *et* $\mathcal{N}_{R_P/R}(\mathfrak{b}) = a_0 R$.

Démonstration. C'est une application de la formule $P_j(\theta)\theta + a_{j+1} = P_{j+1}(\theta)$. La norme de $\mathfrak{a}$ vient de la relation $\theta P_{n-1}(\theta) = -a_n$. □

Théorème 3.4. *Soit* $P \in R_n[x, y]$ *une forme primitive irréductible de degré* n. *La classe de l'idéal* $\mathfrak{I}_0$ *dans le groupe de classes* $\mathrm{Cl}(R_P)$ *est dans* $\mathrm{Cl}(R_P/R)$ *et est invariante lorsque* $\mathrm{SL}_2(R)$ *agit sur* P.

Démonstration. D'après les résultats précédents, on sait que la norme de $\mathfrak{b}$ est un idéal principal de R, et que les classes de $\mathfrak{b}$ et $\mathfrak{I}_0$ sont inverses l'une de l'autre dans $\mathrm{Cl}(R_P)$. Ceci prouve que la classe de $\mathfrak{I}_0$ est dans $\mathrm{Cl}(R_P/R)$. Soit $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(R)$. On a $M \cdot P(x, y) = P(ax + by, cx + dy) = P(a, c)x^n + \cdots$. La racine générique de $M \cdot P$ est $\theta' = (d\theta - b)/(-c\theta + a)$ où θ est définie comme précédemment. D'après [6], on sait que $R_P = R_{M\cdot P}$, ce qui donne

$$\mathfrak{I}'_0 = P(a, c) R_P + P(a, c)\theta' R_P = P(a, c)(-c\theta + a)^{-1}\big((-c\theta + a) R_P + (d\theta - b) R_P\big).$$

Il est clair que $(-c\theta + a) R_P + (d\theta - b) R_P \subset R_P + \theta R_P$. L'inclusion inverse est aussi vraie puisque $ad - bc = 1$. On a donc prouvé que $\mathfrak{I}'_0 = P(a, c)(-c\theta + a)^{-1} a_0^{-1} \mathfrak{I}_0$, ce qui nous donne le résultat. □

Nous avons énoncé le Théorème 3.4 avec l'idéal $\mathfrak{I}_0$, car c'est sous cette forme qu'on l'énonce habituellement dans le cas quadratique. Le même résultat est encore valable avec $\mathfrak{a}$ ou bien $\mathfrak{b}$, qui sont peut-être plus concrets.

On remarquera qu'un polynôme P unitaire donne toujours la classe principale de $\mathrm{Cl}(R_P)$, puisque dans ce cas, le dénominateur de θ est simplement 1.

4. Exemples

Nous donnons tous nos exemples dans le cas où $R = \mathbb{Z}$.

Il est bien connu que l'application qui associe un élément du groupe de classes à une classe d'équivalence de formes quadratiques primitives irréductibles de discriminant fixé est une application bijective (voir par exemple [2, §7]).

Les classes d'équivalence des formes cubiques (modulo $\mathrm{GL}_2(\mathbb{Z})$, et pas seulement $\mathrm{SL}_2(\mathbb{Z})$) sont en correspondance bijective avec les ordres (non nécessairement maximaux) des corps cubiques : voir [4]. Cette correspondance est donnée de la manière suivante : à chaque P, on associe son anneau invariant $\mathbb{Z}_P$. Inversement, pour un ordre cubique $\mathcal{O}$, soit $1,\ \alpha,\ \beta$ une $\mathbb{Z}$-base de $\mathcal{O}$. L'indice $I(x, y)$ de $\alpha x + \beta y$ est la forme cubique associée à $\mathcal{O}$. Nous voyons donc dans ce cas que deux formes cubiques sont équivalentes si et seulement si elles ont le même anneau invariant. En particulier, il y a exactement une classe dans le groupe de classes qui est l'image d'une forme cubique.

L'exemple suivant montre que ce n'est pas toujours la classe principale. Cet exemple a été calculé à l'aide de PARI/GP (voir [1]). Soit L le corps cubique cyclique de discriminant 63^2. Son ordre maximal est l'anneau invariant de $P = 2x^3 + 9x^2 + 3x - 2$. Le dénominateur (ou le numérateur) d'une racine θ de P est de norme 2. Dans ce corps, il y a trois idéaux conjugués de norme 2, qui sont tous non principaux (d'ordre 3 dans le groupe de classes). Nous voyons donc que l'image de P est un élément d'ordre 3 de $\mathrm{Cl}(L)$.

Nous finissons en donnant un exemple de deux formes quartiques non équivalentes ayant le même anneau invariant et la même image dans le groupe de classes. Considérons l'unique corps quartique L totalement complexe de discriminant 189 (voir [5]). Ce corps est engendré par une racine de $p_1 = x^4 - x^3 + 3x^2 - x + 1$ ou alors par une racine de $p_2 = -x^4 + 2x^3 - x - 1$. Ces deux polynômes ont le même anneau invariant (dans ce cas, c'est l'ordre maximal de L puisque l'indice est 1). Ils sont tous les deux associés à la classe principale puisqu'ils sont unitaires. Ils ont les mêmes invariants I et J ($I = 18$ et $J = 135$). Pourtant ils ne sont pas équivalents puisque p_1 ne prend que des valeurs positives sur $\mathbb{R}$, alors que p_2 ne prend que des valeurs négatives. On voit aussi que p_1 et $-p_2$ ne peuvent pas être équivalents puisqu'ils n'ont pas le même J invariant. On trouvera dans [3] un algorithme général pour tester l'équivalence de deux polynômes quartiques ayant les mêmes invariants I et J.

5. Le cas des formes non primitives

Lorsque l'anneau R est principal, on peut facilement se ramener au cas des formes primitives. Lorsque R n'est plus principal, ce n'est pas toujours possible. Nous proposons donc des nouvelles formules dans ce cas. Nous disons que la forme P est *quasi-primitive* si l'idéal fractionnaire $D = \sum a_i R$ est inversible (c'est toujours le cas si R est un anneau de Dedekind). Cet idéal est stable par l'action de $\mathrm{SL}_2(R)$ sur P. Lorsque P est quasi-primitive, on définit l'anneau invariant de P par $R_P = R \oplus P_1(\theta)D^{-1} \oplus \cdots \oplus P_{n-1}(\theta)D^{-1}$, et le dénominateur de θ par $\mathfrak{b} = P_0 D^{-1} R_P + P_1(\theta)D^{-1}R_P + \cdots + P_{n-1}(\theta)D^{-1}R_P$. Les idéaux $\mathfrak{a}$ et $\mathfrak{I}_j$ sont définis de manière semblable. En tenant compte de l'idéal D, on peut généraliser tous les résultats de cette Note.

Références

[1] H. Cohen, A Course in Computational Algebraic Number Theory, in: Graduate Texts in Math., Vol. 138, Springer-Verlag, 1996. Third corrected printing.
[2] D.A. Cox, Primes of the Form $x^2 + ny^2$, Wiley, New York, 1989.
[3] J.E. Cremona, Classical invariants and 2-descent on elliptic curves, J. Symbolic Comput. 31 (1–2) 71–87.
[4] B.N. Delone, D.K. Faddeev, Theory of irrationalities of third degree, Trudy Mat. Inst. Steklov 11 (1940).
[5] ftp://megrez.math.u-bordeaux.fr/pub/numberfields/.
[6] D. Simon, The index of nonmonic polynomials, Indag. Math. (N.S) 12 (4) (2001) 505–517.