Antoine Hugounet

Petits résultats sur les idéaux de Carmichael

travail encadré de recherche
encadré par Alain Kraus (IMJ-PRG)
soutenu le **date**

Sorbonne Université

Trop Long ; Pas Lu

placeholder

Mots-clés : ***placeholder***

1 Question 2

Soit $n \in \mathbb{Z}$ un entier. Peut on trouver une tour de corps de nombres $\mathbb{Q} \subset K \subset L$ telle que n engendre un idéal de Carmichael dans $\mathcal{O}_L$ et non dans $\mathcal{O}_K$? Ce problème revient à se demander si le fait que $n\mathcal{O}_L$ vérifie le critère de Korselt implique que $n\mathcal{O}_K$ le vérifie. Nous affirmons que cette assertion est fausse en exhibant un contre exemple.

1.1 Étude des facteurs carrés

Commençons par ce résultat simple.

1.2 Fait. *Soient A un anneau commutatif, B une A-algèbre commutative et I, J deux idéaux de A. Alors*

$$(IJ)B = (IB)(JB).$$

Démonstration. Par double inclusion. L'inclusion

$$(IJ)B \subset (IB)(JB)$$

est triviale, car $(IB)(JB)$ est un idéal contenant IB. Réciproquement, $(IB)(JB)$ est l'idéal de B engendré par les produits $\alpha\beta$, où $\alpha \in IB$ et $\beta \in JB$. Montrons qu'un tel générateur $\alpha\beta$ est forcément dans $(IJ)B$. Nous savons que α et β sont de la forme suivante :

$$\begin{cases} \alpha = \sum_{i=1}^{n} x_i a_i, & x_i \in B, a_i \in I \\ \beta = \sum_{j=1}^{m} y_j b_j, & y_j \in B, b_j \in J. \end{cases}$$

Quitte à rajouter des termes nuls dans l'une des deux sommes, nous pouvons supposer $m = n$. Cela permet d'écrire le produit

$$\alpha\beta = \sum_{i,j=1}^{n} (x_i y_j)(a_i b_j).$$

Pour tout couple $(i, j) \in [\![1, n]\!]^2$, $x_i y_j \in B$, $a_i b_j \in IJ$, d'où

$$(x_i y_j)(a_i b_j) \in (IB)J.$$

La somme de ces éléments reste dans $(IB)J$ et donc $\alpha\beta \in (IJ)B$, d'où l'inclusion

$$(IB)(JB) \subset (IJ)B,$$

et le résultat désiré. □

Nous en déduisons le très utile résultat suivant.

1.3 Fait. *Soient A un anneau de Dedekind, B une A-algèbre qui soit elle aussi un anneau de Dedekind, I un idéal de A et $n \in \mathbb{N}^*$ un entier. Si IB n'est pas divisé par un idéal premier à la puissance n, alors I non plus.*

Démonstration. Supposons par l'absurde que $\mathfrak{p}$ est un idéal premier de A et que $\mathfrak{p}^n$ divise I, autrement dit que I d'écrit

$$I = \mathfrak{p}^n J$$

pour un certain idéal J de A. D'après le résultat précédent, on peut écrire

$$IB = (\mathfrak{p}B)^n J.$$

Soit $\mathfrak{P}$ un idéal premier de B au dessus de $\mathfrak{p}$. On constate alors que $\mathfrak{P}^n$ divise IB, contradiction. Il n'existe donc aucun idéal premier $\mathfrak{p}$ de A tel que $\mathfrak{p}^n$ divise I. □

1.4 Corollaire. *Soient $n \in \mathbb{Z}$ un entier et $\mathbb{Q} \subset K \subset L$ une tour de corps de nombres. Si $n\mathcal{O}_L$ est sans facteurs carrés, alors $n\mathcal{O}_K$ l'est également.*

Démonstration. Il suffit d'appliquer le fait précédent avec $A = \mathcal{O}_K$, $B = \mathcal{O}_L$ et $I = n\mathcal{O}_K$. □

Reprenons les notations du préambule et supposons que $n\mathcal{O}_L$ soit de Carmichael. Il vérifie alors le critère de Korselt et est sans facteurs carrés. Le corollaire précédent montre que $n\mathcal{O}_K$ l'est aussi : il vérifie donc cette condition du critère de Korselt. Il faut donc étudier la norme de $n\mathcal{O}_K$ et ses propriétés par rapport à celle de $n\mathcal{O}_L$ pour répondre à notre question.

1.5 Étude de la norme

Puisque la norme des éléments se comporte très bien avec les sous-extensions[1], il est raisonnable de penser que cela sera aussi le cas des normes d'idéaux. Nous avons alors ce premier résultat.

1.6 Fait. *Soient $\mathbb{Q} \subset K \subset L$ une tour de corps de nombres et I un idéal non trivial de $\mathcal{O}_L$. Si l'idéal restreint $I \cap \mathcal{O}_K$ est non trivial, alors*

$$\mathrm{N}_{\mathcal{O}_K}(I \cap \mathcal{O}_K) \mid \mathrm{N}_{\mathcal{O}_L}(I).$$

Démonstration. C'est un résultat de théorie des groupes à peine déguisé. On a une suite de morphismes de groupes

$$\mathcal{O}_K \to \mathcal{O}_L \to \mathcal{O}_L/I.$$

1. Si l'on se donne x un élément de $\mathcal{O}_K$, alors $\mathrm{N}_{\mathcal{O}_L}(x) = \mathrm{N}_{\mathcal{O}_K}(x)^{[L:K]}$.

En appelant f la composée des deux flèches, on obtient $\operatorname{Ker} f = I \cap \mathcal{O}_K$ et l'on en déduit l'existence d'un morphisme de groupes injectif

$$\mathcal{O}_K/I \cap \mathcal{O}_K \hookrightarrow \mathcal{O}_L/I.$$

Ainsi, $\mathcal{O}_K/I \cap \mathcal{O}_K$ s'identifie à un sous-groupe de $\mathcal{O}_L/I$. D'après le théorème de Lagrange, son cardinal divise donc celui de $\mathcal{O}_L/I$. Or, comme nos idéaux sont non triviaux, nous pouvons en prendre les normes, qui sont exactement les cardinaux de ces quotients, par définition. D'où le résultat. □

1.7 Synthèse et contre-exemple

Intuitivement, la condition imposée sur les normes par le critère de Korselt semble trop forte pour être transmise du grand anneau d'entiers au moyen anneau d'entiers. Reprenons les notations du premier paragraphe, supposons que $n\mathcal{O}_L$ est de Carmichael, et admettons que $n\mathcal{O}_K$ demeure sans facteur carré. Soit $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ divisant $n\mathcal{O}_K$. Alors $p = \mathfrak{P} \cap \mathcal{O}_K$, où $\mathfrak{P}$ est un idéal premier de $\mathcal{O}_L$ divisant $n\mathcal{O}_L$. On sait d'après le fait 1.6 que

$$\mathrm{N}_K(\mathfrak{p}) \mid \mathrm{N}_L(\mathfrak{P}),$$

et même en cherchant longtemps, cette condition ne permet en aucun cas de conclure que $\mathrm{N}_K(\mathfrak{p}) - 1 \mid \mathrm{N}_K(n\mathcal{O}_K) - 1$ en ayant pour seule hypothèse (critère de Korselt) que $\mathrm{N}_L(\mathfrak{P}) - 1 \mid \mathrm{N}_L(n\mathcal{O}_L) - 1$.

Après avoir cherché sans succès un contre-exemple «malin», nous décidons d'écrire un algorithme naïf pour chercher ledit contre-exemple. L'idée est simple : se restreindre aux corps quadratiques, passer en revue une liste d'entiers d sans facteur carré qui engendrent ces corps, et pour chaque tel d, tester parmi un nombre arbitraire d'entiers naturels n, lesquels engendrent un idéal de Carmichael dans $\mathbb{Q}(\sqrt{d})$ sans être un nombre de Carmichael. Voici l'algorithme en pseudo code.

Entrées : a, b, c
pour chaque $d \in [\![a, b]\!]$ *et d est sans facteur carré* **faire**
  $K = \mathbb{Q}(\sqrt{d})$;
  pour chaque $n \in [\![2, c]\!]$ **faire**
    si *n n'est pas de Carmichael et* $n\mathcal{O}_K$ *est un idéal de Carmichael* **alors**
      exporter (d, n) dans un fichier texte ;
    fin
  fin
fin

La version implémentée dans Sage de cet algorithme est disponible sur GitHub (**lien**). Nous avons pu exhiber de nombreux contre-exemples, comme le couple

$$(d, n) = (11, 35).$$

L'entier 35 n'est pas de Carmichael, mais il engendre un idéal de Carmichael dans $\mathbb{Q}(\sqrt{11})$. Le couple

$$(d, n) = (95, 8029)$$

est un autre contre-exemple, avec la particularité que 8029 soit le produit de trois nombres premiers distincts (7, 31 et 37). De même, 8029 n'est pas un entier de Carmichael, mais il engendre un idéal de Carmichael dans $\mathbb{Q}(\sqrt{95})$.

2 Addenda

2.1 Fait. *Soient n un entier qui soit une puissance non triviale d'un nombre premier et K un corps de nombres. Alors $n\mathcal{O}_K$ n'est pas un idéal premier.*

Démonstration. Écrivons $n = p^r, r > 1$ et supposons que $n\mathcal{O}_K$ soit un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. Alors $\mathrm{N}_K(n\mathcal{O}_K)$ est une puissance de la caractéristique $\mathrm{Car}(\mathcal{O}_K/\mathfrak{p})$, disons

$$\mathrm{N}_K(n\mathcal{O}_K) = \mathrm{Car}(\mathcal{O}_K/\mathfrak{p})^f,$$

où $f \leqslant [K : \mathbb{Q}]$. Mais on a aussi que

$$\mathrm{N}_K(n\mathcal{O}_K) = \mathrm{N}_K(n) = (p^r)^{[K:\mathbb{Q}]}.$$

La caractéristique $\mathrm{Car}(\mathcal{O}_K/\mathfrak{p})$ étant un nombre premier, il vient $p^f = p^{r[K:\mathbb{Q}]}$. Comme par ailleurs

$$f \leqslant [K : \mathbb{Q}] < r[K : \mathbb{Q}],$$

l'égalité est impossible, et nous avons une contradiction. $n\mathcal{O}_K$ n'est donc pas un idéal premier. □

2.2 Fait. *Soient K un corps de nombres et $\mathfrak{P}$ un idéal premier de son anneau d'entiers. Alors*

$$\mathfrak{P} \cap \mathbb{Z} = \mathrm{Car}(\mathcal{O}_K/\mathfrak{P})\mathbb{Z}.$$

Démonstration. D'après 1.6, $\mathrm{N}_{\mathbb{Q}/\mathbb{Q}}(\mathfrak{P} \cap \mathbb{Z}) \mid \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P})$. Or, $\mathbb{N}_{K/\mathbb{Q}}(\mathfrak{P})$ est la puissance d'un nombre premier, et ce nombre premier n'est autre que la caractéristique du *corps* $\mathcal{O}_K/\mathfrak{P}$. Or $\mathfrak{P} \cap \mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, et $\mathbb{Z}$ étant principal, $\mathfrak{P} \cap \mathbb{Z}$ est engendré par un nombre premier $p \in \mathbb{Z}$. Ainsi,

$$\mathrm{N}_{\mathbb{Q}/\mathbb{Q}}(\mathfrak{P} \cap \mathbb{Z}) = |\mathbb{Z}/p\mathbb{Z}| = p,$$

et donc

$$p \mid \mathrm{Car}(O_K/\mathfrak{P}).$$

Comme ces deux nombres sont premiers, on a $p = \mathrm{Car}(O_K/\mathfrak{P})$. □

Références

[1] G. Ander Seele. « Carmichael numbers in number rings ». In : *Journal of Number Theory* 128 (2008), p. 910-917. URL : https://core.ac.uk/download/pdf/82709152.pdf.

[2] Alain Kraus. *Corps locaux et applications. Cours accéléré de DEA, Université Pierre et Marie Curie*. Sept. 2000.

[3] Pierre Samuel. *Théorie algébrique des nombres*. 2e éd. Hermann Paris, oct. 1971.