Antoine Hugounet

placeholder Titre

travail encadré de recherche
encadré par Alain Kraus[1] (IMJ-PRG)
de janvier à juin 2020

Sorbonne Université

Trop Long ; Pas Lu

placeholder

Mots-clés : ***placeholder***

1. https://webusers.imj-prg.fr/~alain.kraus/

1 Un nombre de Carmichael dans un anneau d'entiers ne l'est pas forcément dans un anneau plus petit trouver plus court

Question : soient $\mathbb{Q} \subset K \subset L$ une tour de corps de nombres et $n \in \mathbb{Z}$ un entier, si n est de Carmichael dans $\mathcal{O}_L$, l'est-il dans $\mathcal{O}_K$? Nous affirmons que cette assertion est fausse en exhibant un contre exemple à l'aide du critère de Korselt généralisé ([1], théorème 2.2). Ce critère impose une condition sur les facteurs de $n\mathcal{O}_K$ ($n\mathcal{O}_K$ doit être sans facteurs carrés) et une condition sur les normes des diviseurs premiers de $n\mathcal{O}_K$ ($\mathrm{N}(\mathfrak{p})$ doit diviser $\mathrm{N}(n\mathcal{O}_K)$ pour tout idéal premier de $\mathcal{O}_L$ divisant $n\mathcal{O}_K$). L'enjeu est de comprendre si ces propriétés vraies dans $\mathcal{O}_L$ sont transmises à $n\mathcal{O}_K$.

Remarque 1. Si n est premier, il peut très bien être de Carmichael dans un anneau d'entiers, mais ne le sera jamais dans l'anneau $\mathbb{Z}$, car un nombre de Carmichael est composé. Nous pouvons donc supposer n composé.

1.1 Étude des facteurs carrés

Nous voyons ici que si $n\mathcal{O}_L$ est sans facteur carré, $n\mathcal{O}_K$ l'est également.

Lemme 2. *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. Par contraposée. Soit $\mathfrak{p}$ un idéal premier de A tel que $\mathfrak{p}^n$ divise I. On a

$$I \subset \mathfrak{p}^n.$$

Comme $(JJ')B = (JB)(J'B)$ pour tout couple J, J' d'idéaux de A, on a

$$IB \subset (\mathfrak{p}B)^n = \mathfrak{p}^n B \subset \mathfrak{P}^n,$$

pour tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ divisant $\mathfrak{p}B$, d'où la division $\mathfrak{P}^n \mid IB$ et la conclusion. □

En reprenant les notations du préambule, si $n\mathcal{O}_L$ est de Carmichael dans $\mathcal{O}_L$, il est sans facteurs carrés. En appliquant le lemme précédent à $A = \mathcal{O}_K$, $B = \mathcal{O}_L$ et $I = n\mathcal{O}_K$, on voit que $n\mathcal{O}_K$ demeure lui aussi dans facteur carré. Il faut donc étudier la norme pour conclure.

1.2 Protoétude de la norme

Reprenons les notations du préambule et supposons que n est de Carmichael dans $\mathcal{O}_L$. On a en particulier

$$\mathrm{N}_{\mathcal{O}_L}(\mathfrak{P}) - 1 \mid \mathrm{N}_{\mathcal{O}_K}(n\mathcal{O}_L) - 1$$

pour tout idéal premier $\mathfrak{P} \in \mathrm{Spec}(\mathcal{O}_L)$ divisant $n\mathcal{O}_K$. Écrivons $n\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ la factorisation de n en produit d'idéaux premiers de $\mathcal{O}_K$ distincts ($n\mathcal{O}_K$ est sans facteurs carrés d'après la sous-section précédente). Pour tout $i \in [\![1, r]\!]$ on voudrait $\mathrm{N}_{\mathcal{O}_K}(\pi) - 1 \mid \mathrm{N}_{\mathcal{O}_K}(n) - 1$. On a bien[2]

$$\mathrm{N}_{\mathcal{O}_K}(n\mathcal{O}_K) = n^{[K:\mathbb{Q}]} \mid \mathrm{N}_{\mathcal{O}_L}(n\mathcal{O}_L) = n^{[L:\mathbb{Q}]}$$

et

$$\mathrm{N}_{\mathcal{O}_L}(\mathfrak{p}_i\mathcal{O}_L) \mid \mathrm{N}_{\mathcal{O}_L}(\mathfrak{P})$$

pour tout idéal premier $\mathfrak{P}$ de $\mathcal{O}_L$ au dessus de $\mathfrak{p}_i$, mais a priori pas recoller les morceaux pour avoir les divisions désirées. C'est ce constat qui nous amène à chercher un contre exemple.

1.3 Synthèse et contre-exemple

Après avoir cherché sans succès un contre-exemple « malin », nous décidons d'écrire un algorithme naïf pour chercher ledit contre-exemple dans des corps quadratiques. L'idée est simple : passer en revue une liste d'entiers d sans facteur carré qui engendrent ces corps et pour chaque tel d, tester parmi une liste arbitraire d'entiers naturels, lesquels engendrent un idéal de Carmichael sans être un nombre de Carmichael.

Il est facile avec un outil de calcul formel de déterminer si un entier n est de Carmichael dans un corps quadratique $\mathbb{Q}(\sqrt{d})$, d étant sans facteurs carrés. Posons $K = \mathbb{Q}(\sqrt{d})$ et $I = \mathcal{O}_K$. Le logiciel SageMath[3] est capable de donner la décomposition de I en produit d'idéaux premiers de $\mathcal{O}_K$ et calculer des normes d'idéaux. Pour tester si I est de Carmichael, on demande à SageMath sa décomposition, on regarde s'il est sans facteurs carrés et si c'est le cas on teste si $\mathrm{N}_{\mathcal{O}_K}(\mathfrak{p}) - 1$ divise $\mathrm{N}_{\mathcal{O}_K}(I) - 1$ pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant I. Comme l'extension considérée est quadratique, I a au plus deux facteurs premiers. La norme $\mathrm{N}_{\mathcal{O}_K}(I)$ est quant à elle donnée par n^2.

Il reste à déterminer si n est un entier de Carmichael. Comme nous n'allons pas chercher bien loin[4] — plutôt que d'effectuer des calculs couteux et inutiles avec le critère

2. Si $[K : \mathbb{Q}] \mid [L : \mathbb{Q}]$ on a même $\mathrm{N}_{\mathcal{O}_K}(n\mathcal{O}_K) - 1 \mid \mathrm{N}_{\mathcal{O}_L}(n\mathcal{O}_L) - 1$. C'est trivialement le cas lorsque l'on considère $K = \mathbb{Q}$ mais cela ne change rien.

3. Voir `https://www.sagemath.org` et plus particulièrement `http://doc.sagemath.org/html/en/reference/number_fields/sage/rings/number_field/number_field.html`.

4. Nous nous sommes limités à $d \in [\![-100, 100]\!]$ et $n \in [\![2, 10000]\!]$.

de Korselt — il est préférable de regarder si n est dans la (maigre) liste des entiers de Carmichael[5] inférieurs à 10000 :

$$\{561, 1105, 1729, 2465, 2821, 6601, 8911\}.$$

Pour l'implémentation, nous écrivons séparément une fonction testant si I est de Carmichael et l'invoquons pour tout couple (d, n). L'algorithme est donc le suivant ; son implémentation est disponible sur le compte GitHub de l'auteur (`https://github.com/kryzar/TER-Carmichael/blob/master/Script/Script.sage`).

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

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 $8029 = 7 \cdot 31 \cdot 37$ est le produit de trois nombres premiers (on rappelle qu'un nombre de Carmichael a au moins trois facteurs premiers). De même, 8029 n'est pas un entier de Carmichael, mais il engendre un idéal de Carmichael dans $\mathbb{Q}(\sqrt{95})$.

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`.

5. La liste complète des entiers de Carmichael, à l'exception d'une infinité d'entre eux, est disponible ici : `https://oeis.org/A002997`.

[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.