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

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 $n\mathcal{O}_K$.

1.1 Remarque. 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

1.1 Lemme. *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 :

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

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. $\square$

Nous en déduisons le très utile résultat suivant.

1.2 Lemme. *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. $\square$

1.1 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 $I = n\mathcal{O}_K$. $\square$

En reprenant les notations du préambule, si $n\mathcal{O}_L$ est de Carmichael dans $\mathcal{O}_L$, il est sans facteurs carrés. Le corollaire précédent assure que $n\mathcal{O}_K$ sera aussi sans facteurs carrés et il nous 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 il ne semble pas évident de 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 $\mathfrak{n} = \mathcal{O}_K$. Le logiciel SageMath[3] est capable de donner la décomposition de $\mathfrak{n}$ en produit d'idéaux premiers de $\mathcal{O}_K$ et calculer des normes d'idéaux. Pour tester si $\mathfrak{n}$ 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 $\mathrm{N}_{\mathcal{O}_K}(\mathfrak{p}) - 1$ă $\mid \mathrm{N}_{\mathcal{O}_K}(\mathfrak{n}) - 1$ pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant $\mathfrak{n}$. Comme l'extension considérée est quadratique, $\mathfrak{n}$ a au plus deux facteurs premiers. La norme $\mathrm{N}_{\mathcal{O}_K}(\mathfrak{n})$ 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 de Korselt — il est préférable de regarder si n est dans la (maigre) liste des entiers de Carmichael[5] inférieurs à 10000 :

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

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 $n \in [\![2, 10000]\!]$.

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

Pour l'implémentation, nous écrivons séparément une fonction testant si $\mathfrak{n}$ est de Carmichael et qui est invoquée pour tout couple (d, n). L'algorithme est donc le suivant ; son implémentation est disponible sur GitHub (**lien**).

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 $\mathbb{Q}(\sqrt{95})$.

Addenda

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. □

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

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

En appelant f la composée des deux flèches, on obtient $\mathrm{Ker}\, f = I \cap \mathcal{O}_K$ 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. □

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, $\mathrm{N}_{\mathbb{Q}/\mathbb{Q}}(\mathfrak{P} \cap \mathbb{Z}) \mid \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P})$. 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.