QUESTIONS - REMARQUES

Question 1. Soit K un corps de nombres. Comment préciser les nombres premiers p tels que pO_K soit un idéal de Carmichael de O_K ?

Remarque 0.1. Si p est totalement décomposé dans K, alors pO_K est un idéal de Carmichael dans O_K. En effet, pO_K est sans facteurs carrés et $p-1$ divise $p^{[K:\mathbb{Q}]}-1$. On a $\mathrm{Norm}(\mathfrak{p}) = p$ et $\mathrm{Norm}(p) = p^{[K:\mathbb{Q}]}$, d'où l'assertion. Si d est le degré sur $\mathbb{Q}$ de la clôture galoisenne $\tilde{K}$ de K, il y a une densité $1/d$ de tels nombres premiers. (En fait, p est totalement décomposé dans K si et seulement si p est totalement décomposé dans $\tilde{K}$.)

Remarque 0.2. D'après le th. 2.3, si K est galoisien sur $\mathbb{Q}$, il faut et il suffit que p soit non ramifié (pour qu'il soit sans facteurs carrés) et non inerte dans K (pour qu'il soit composé).

Lemme 1. *Soit $K/\mathbb{Q}$ un corps de nombres de degré un nombre premier. Soit p un nombre premier. Alors, pO_K est un idéal de Carmichael si et seulement si p est totalement décomposé dans K.*

Démonstration. Supposons p non totalement décomposé dans K. Si p est ramifié dans K, pO_K n'est pas un idéal de Carmichael (il n'est pas sans facteurs carrés). Supposons p non ramifié dans K. Il existe alors un idéal premier $\mathfrak{p}$ de O_K divisant p de degré résiduel $f \geq 2$. On a $\mathrm{Norm}(\mathfrak{p}) = p^f$. Par ailleurs, si $p^f - 1$ divise $p^{[K:\mathbb{Q}]} - 1$ alors f divise $[K:\mathbb{Q}]$. Par suite, $f = [K:\mathbb{Q}]$ et p est inerte dans K i.e. pO_K est un idéal premier de O_K, donc n'est pas un idéal de Carmichael, d'où l'assertion avec la première remarque. □

Question 2. Soit $n \geq 1$ un entier composé. Soit K un corps de nombres tel que nO_K soit un idéal de Carmichael. Soit $L \subseteq K$ un sous-corps de K. Est-il vrai que nO_L est un idéal de Carmichael de O_L ? (c'est faux si on ne suppose pas n composé).

Question 3. Que dire sur une réciproque éventuelle du th. 2.7 ? Par exemple : soit $d \geq 1$ un entier. Soit $n \geq 1$ un entier tel que pour toute extension $K/\mathbb{Q}$ de degré d, de discriminant premier avec n, nO_K soit un idéal de Carmichael (auquel cas n est sans facteurs carrés). Est-il vrai que pour tout p premier divisant n et tout i tel que $0 < i \leq d$, on ait $n^d \equiv 1 \pmod{p^i - 1}$? C'est vrai si $d = 1$ (Korselt) et si $d = 2$ (th. 2.5).

Question 4. Soit N un nombre de Carmichael d'ordre 2, par exemple celui donné dans l'article :

$$N = 443372888629441 = 17 \times 31 \times 41 \times 43 \times 89 \times 97 \times 167 \times 331.$$

(29 est un témoin d'Euler pour N). D'après le th. 2.7, pour tout corps quadratique K, de discriminant premier avec N, l'idéal NO_K est de Carmichael. Comment expliciter des extensions cubiques abéliennes $K/\mathbb{Q}$ (une infinité ?), de discriminant premier avec N, telles que NO_K ne soit pas un idéal de Carmichael dans O_K ?

Date: 17 février 2020.

Remarque 0.3. Soit n un nombre de Carmichael. Il est facile d'expliciter tous les corps quadratiques K tels que nO_K ne soit pas un idéal de Carmichael dans O_K, $\mathrm{pgcd}(D_K, n) = 1$, pourvu que l'on connaisse la décomposition de n en facteurs premiers. Par exemple, les corps quadratiques K tels que $561O_K$ soit un idéal de Carmichael sont exactement ceux tels que 3 soit non ramifié dans K et que $11, 17$ soient décomposés dans K (à vérifier).

Question 5. Existe-t-il un nombre de Carmichael n plus petit que 10^{10}, non divisible par 5, qui ne soit pas un produit de nombres premiers congrus à 1 modulo 5, dans lequel (n) soit de Carmichael dans $\mathbb{Q}(\mu_5)$ (il y a des tables de nombres de Carmichael plus petits qu'une borne donnée, sans doute jusqu'à 10^{15} ou 10^{16}) ?

561 n'est pas de Carmichael dans $\mathbb{Q}(\mu_5)$ car 17 est inerte dans $\mathbb{Q}(\mu_5)$ et $17^4 - 1$ ne divise pas $561^4 - 1$. On peut ausi vérifier que

$$(1 - \zeta_5)^{\mathrm{Norm}(561)} \not\equiv 1 - \zeta_5 \pmod{561\mathbb{Z}[\zeta_5]},$$

et que

$$(1 + \zeta_5)^{\mathrm{Norm}(561)} \not\equiv 1 + \zeta_5 \pmod{561\mathbb{Z}[\zeta_5]}.$$

Avec le th. 2.3 cela montre aussi que 561 est composé en utilisant le test de Fermat sur les corps de nombres.

Question 6. Soit n un nombre de Carmichael ayant plusieurs centaines de chiffres décimaux (par exemple ceux de type Chernick ou des analogues). Peut-on démontrer facilement avec le test de Fermat sur les corps quadratiques que n est composé ?

Par exemple, posons

$$p = 296744956686855105501541746429053327307719917998530433509950755312768387531717701995942385964281211880336647542183455624931687828 83.$$

Alors p est premier et l'entier

$$N = p\,(313(p-1)+1)\,(353(p-1)+1)$$

est un nombre de Carmichael, produit de trois nombres premiers, qui possède 397 chifrres décimaux.

D'après le th. 2.5 il y a une infinité de corps quadratiques K tels que NO_K ne soit pas de Carmichael. Quel est celui de plus petit discriminant pour lequel NO_K ne soit pas de Carmichael ? ($K = \mathbb{Q}(\sqrt{-1})$, $K = \mathbb{Q}(\sqrt{2})$ $\cdots$?)

Remarque 0.4. Voici une autre démonstration du th. 2.3 qui n'utilise pas le critère de Korselt. Soit f le degré résiduel des idéaux premiers de O_K au-dessus de p (c'est le même pour tous car $K/\mathbb{Q}$ est galoisenne). Soit $\mathfrak{p}$ un idéal premier de O_K au-dessus de p. Par hypothèse, p est non ramifié dans K, donc le sous-groupe de décomposition $D_\mathfrak{p}$ en $\mathfrak{p}$ de $\mathrm{Gal}(K/\mathbb{Q})$ est isomorphe au groupe de Galois $\mathrm{Gal}(k/\mathbb{F}_p)$ où $k = O_K/\mathfrak{p}$. Le groupe $D_\mathfrak{p}$ est cyclique d'ordre f engendré par l'automorphisme de Frobenius σ, qui est caractérisé par le fait que pour tout a dans O_K on ait $\sigma(a) \equiv a^p \pmod{\mathfrak{p}}$. On a $\sigma^f = 1$. Parce que f divise le degré $[K : \mathbb{Q}]$, on

a donc $\sigma^{[K:\mathbb{Q}]} = 1$, d'où $a^{p^{[K:\mathbb{Q}]}} \equiv a \pmod{\mathfrak{p}}$. D'après le th. chinois on obtient ainsi pour tout $a \in O_K$

$$a^{p^{[K:\mathbb{Q}]}} \equiv a \pmod{pO_K}.$$

On a $\mathrm{Norm}(p) = p^{[K:\mathbb{Q}]}$, d'où $a^{\mathrm{Norm}(p)} \equiv a \pmod{p}$.

Notons que l'on a en fait, pour tout $a \in O_K$

$$a^{p^f} \equiv a \pmod{pO_K}.$$

Remarquons aussi que la conclusion du th. 2.3 est fausse si p est ramifié dans K : avec $K = \mathbb{Q}(\sqrt{2})$, $p = 2$ et $a = \sqrt{2}$, on a $a^4 = 4 \not\equiv \sqrt{2} \pmod{2}$.