REMARQUES

1. Théorème 3.1

Soit n un entier naturel.

Lemme 1. *Soit p un nombre premier. Notons $G = (\mathbb{Z}/p\mathbb{Z})^*$. Supposons que p ne divise pas n. Soit d l'ordre de n modulo p. Supposons de plus*

$$\mathrm{pgcd}\Big(\frac{p-1}{d}, d\Big) = 1.$$

Soit H le sous-groupe de G d'ordre $(p-1)/d$. Alors, nH est un générateur de G/H.

Démonstration. Soit g un générateur de G. L'élément g^d est d'ordre $(p-1)/\mathrm{pgcd}(d, p-1) = (p-1)/d$. Par suite, on a $H =< g^d >$. Par ailleurs, G possède $\varphi(d)$ eléments d'ordre d. Ce sont les éléments (au nombre de $\varphi(d)$)

$$g^{a(p-1)/d} \quad \text{avec} \quad 1 \le a \le d, \quad \mathrm{pgcd}(a, d) = 1.$$

En effet, $g^{(p-1)/d}$ est d'ordre d, donc engendre l'unique sous-groupe de G d'ordre d et les générateurs de ce sous-groupe sont exactement les éléments ci-dessus. Parce que n est d'ordre d, il existe donc a tel que $1 \le a \le d$, $\mathrm{pgcd}(a, d) = 1$ et que l'on ait dans G

$$n = g^{a(p-1)/d}.$$

Le groupe G/H est d'ordre d. Il s'agit donc de montrer que d est le plus petit entier $k \ge 1$ tel que n^k appartienne à H. Soit k l'ordre de n dans G/H. On a

$$n^k = g^{ak(p-1)/d} \in H.$$

On a $H =< g^d >$, donc il existe un entier s tel que l'on ait

$$g^{ak(p-1)/d} = (g^d)^s = g^{ds}.$$

On obtient la congruence

$$ak(p-1)/d \equiv ds \pmod{p-1}.$$

L'entier d divise $p-1$ donc d divise $ak(p-1)/d$. Par ailleurs, a est premier avec d et $\mathrm{pgcd}\big(\frac{p-1}{d}, d\big) = 1$, donc d divise k. On a $n^d \in H$, d'où $k = d$ et le résultat. □

Lemme 2. *Soit $m \in \mathbb{N}$ un entier divisible par au moins deux nombres premiers distincts, p et q. Il existe d_0 tel que pour tout $d > d_0$, $p^d - 1$ ne divise pas $m^d - 1$.*

Démonstration. Voir la référence [2]. □

Lemme 3. *Il existe une infinité de nombres premiers p tels que $p-1$ soit sans facteurs carrés.*

Démonstration. Voir la référence [5]. □

Date: 7 mai 2020.

Remarque 1.1. Soit H un sous-groupe de $G = (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre n. Notons $d = |G/H|$. Il existe un unique sous-groupe H' de $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ d'ordre n (avec $\zeta = \zeta_p$). Soit K le corps laissé fixe par ce sous-groupe. On a $[K : \mathbb{Q}] = d$. Vérifions que l'application

$$f : G/H \to \mathrm{Gal}(K/\mathbb{Q})$$

définie par

$$f(aH) = \sigma_a|_K \quad \text{où} \quad \sigma_a(\zeta) = \zeta^a,$$

est un isomorphisme. D'abord si on a $aH = bH$, alors $\sigma_{ab^{-1}}$ appartient à H' donc la restriction de $\sigma_{ab^{-1}}$ à K est l'identité, et on a donc $\sigma_a|_K = \sigma_b|_K$. Par ailleurs, si $\sigma_a|K = 1$, cela signifie que $a \in H$, donc f est injective, d'où l'assertion. (En fait, a est dans H si et seulement si σ_a est dans H' car $a \mapsto \sigma_a$ est un isomorphisme de G sur $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ et G (donc aussi $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$)possède un unique sous-groupe d'ordre d.) Ainsi, pour tout nombre premier $q \neq p$, le Frobenius en q restreint à K est l'image de qH. Le Frobenius en q restreint à K étant le Frobenius en q de l'extension $K/\mathbb{Q}$, on en déduit que si qH est un générateur de G/H, alors le Frobenius en q de l'extension $K/\mathbb{Q}$ est un générateur de $\mathrm{Gal}(K/\mathbb{Q})$, autrement dit q est inerte dans K.

1.1. **Preuve du théorème 3.1.** On suppose n composé. Soit p un diviseur premier de n. Si n est une puissance d'un nombre premier, pour tout K l'idéal nO_K n'est pas de Carmichael. On peut donc supposer que n n'est pas la puissance d'un nombre premier. Parce que n est composé, n est donc divisible par au moins deux nombres premiers distincts. D'après le lemme ci-dessus, il existe d_0 tel que pour tout $d > d_0$, $p^d - 1$ ne divise pas $n^d - 1$.

Remarque 1.2. Soit K un corps de nombres tel que $[K : \mathbb{Q}] = d > d_0$. Supposons p inerte dans K. On a

$$\mathrm{Norm}(p) - 1 = p^d - 1,$$

qui ne divise pas $n^d - 1 = \mathrm{Norm}(nO_K) - 1$. Dans ce cas, nO_K n'est donc pas un idéal de Carmichael dans K.

Il y a une infinité de nombres premiers q tels que $q - 1$ soit sans facteurs carrés. Choisissons un tel nombre premier q tel que

$$q > p^{d_0} - 1.$$

Soit d l'ordre de p modulo q. On a

$$d > d_0.$$

Par ailleurs, d divise $q - 1$. Parce que $q - 1$ est sans facteurs carrés, on a

$$\mathrm{pgcd}\Big(\frac{q-1}{d}, d\Big) = 1.$$

Posons

$$E = \mathbb{Q}(\zeta_q).$$

Le groupe $\mathrm{Gal}(E/\mathbb{Q})$ est isomorphe à $G = (\mathbb{Z}/q\mathbb{Z})^*$. Soit H le sous-groupe de G d'ordre $(q-1)/d$. Soit K le sous-corps de E laissé fixe par H. On utilise le lemme 2 avec le nombre premier q et $n = p$ (ce sont les notations du lemme 2). On en déduit que p est un générateur de G/H donc que p est inerte dans K. On a $[K : \mathbb{Q}] = d > d_0$, donc nO_K n'est pas un idéal Carmichael dans O_K (d'après la remarque ci-dessus), d'où le résultat.

Résumé de la preuve : Soit p un diviseur premier fixé de n. Soit d_0 tel que pour tout $d > d_0$, $p^d - 1$ ne divise pas $n^d - 1$. Soit S l'ensemble des nombres premiers q tels que $q - 1$ soit sans facteurs carrés et que $q > p^{d_0} - 1$. L'ensemble S est infini. Pour chaque $q \in S$, soit d_q l'ordre de p modulo q. Il existe un unique sous-corps K_q de $\mathbb{Q}(\zeta_q)$ de degré d_q sur $\mathbb{Q}$. Dans chacun des corps K_q, q est inerte donc nO_K n'est pas un idéal Carmichael dans O_{K_q}. Il y a une infinité de tels corps K_q. Le discriminant de K_q est une puissance q, donc si q ne divise pas n, la condition $\mathrm{pgcd}(D_{K_q}, n) = 1$ est remplie. Cela prouve le résultat.