

Démonstration du théorème de Kummer

Correction des exercices

1. Exercices préliminaires

Exercice 1

1) L'application $\mathbb{Z} \rightarrow A/\mathfrak{P}$ qui à un entier a associe sa classe modulo \mathfrak{P} est surjective : on a $\zeta \equiv 1 \pmod{\mathfrak{P}}$ de sorte que tout élément de A est congru à un entier modulo \mathfrak{P} . Il existe donc $m \in \mathbb{Z}$ tel que $x \equiv m \pmod{\mathfrak{P}}$. On écrit que $x = m + \lambda y$ où $y \in A$. Si n est un entier tel que $y \equiv n \pmod{\mathfrak{P}}$, on obtient alors la congruence $x \equiv m + n\lambda \pmod{\mathfrak{P}^2}$. Par ailleurs, x n'étant pas dans \mathfrak{P} , m n'est pas divisible par p . Soit r un entier naturel tel que $rm \equiv n \pmod{p}$. Vérifions que $\zeta^r x$ est semi-primaire. Cet élément n'est pas dans \mathfrak{P} car tel est le cas de x (et ζ est une unité) et l'on a

$$\zeta^r x = (1 - \lambda)^r x \equiv (1 - r\lambda)x \pmod{\mathfrak{P}^2},$$

d'où l'on déduit que $\zeta^r x \equiv m \pmod{\mathfrak{P}^2}$ et le résultat.

L'entier r est unique modulo p : soient r et r' tels que $\zeta^r x$ et $\zeta^{r'} x$ soient semi-primaires. Il existe des entiers relatifs m et m' tels que $\zeta^r x \equiv m \pmod{\mathfrak{P}^2}$ et $\zeta^{r'} x \equiv m' \pmod{\mathfrak{P}^2}$. On a $x(\zeta^r - \zeta^{r'}) \equiv m - m' \pmod{\mathfrak{P}^2}$. Si p ne divise pas $r - r'$, on en déduit que l'on a $\lambda x u \equiv m - m' \pmod{\mathfrak{P}^2}$, où u est une unité de A . Par suite, λ divise $m - m'$ et donc p divise $m - m'$, en particulier $m - m' \equiv 0 \pmod{\mathfrak{P}^2}$. Cela entraîne que x est dans \mathfrak{P} d'où une contradiction.

2) Puisque x et y ne sont pas dans \mathfrak{P} il en est de même de xy . Il existe des entiers r et s tels que $x \equiv r \pmod{\mathfrak{P}^2}$ et $y \equiv s \pmod{\mathfrak{P}^2}$. Par suite, on a $xy \equiv rs \pmod{\mathfrak{P}^2}$, donc xy est semi-primaire. Soit $m \in \mathbb{Z}$ tel que $ms \equiv r \pmod{p}$. On a alors $my \equiv x \pmod{\mathfrak{P}^2}$ (car p est associé à λ^{p-1} et p est impair).

Exercice 2

1) On a l'égalité

$$(1) \quad z^p = x^p + y^p = \prod_{k=0}^{p-1} (x + \zeta^k y).$$

Considérons alors deux indices j et k tels que $0 \leq j < k \leq p-1$. Soit I' le pgcd des idéaux $(x + \zeta^j y)A$ et $(x + \zeta^k y)A$. D'abord, I est un diviseur de ces deux idéaux, donc I divise I' , autrement dit, I' est contenu dans I . Inversement, montrons que I est contenu dans I' . On considère pour cela un entier k' compris entre 0 et $p-1$. Vérifions que $x + \zeta^{k'} y$ appartient

à I' . En écrivant que $x + \zeta^j y$ et $x + \zeta^k y$ sont dans I' , on déduit que λy est aussi dans I' . Par ailleurs, on a

$$x + \zeta^{k'} y = (x + \zeta^j y) + (\zeta^{k'-j} - 1)\zeta^j y.$$

Si $k' = j$, on a l'assertion ; si $k' \neq j$, on a $\zeta^{k'-j} - 1 = \lambda u$ où u est une unité de A , ce qui entraîne le résultat. Puisque I est l'idéal engendré par les $x + \zeta^i y$ où $i = 0, \dots, p-1$, on obtient notre assertion. D'où $I = I'$.

2) Posons

$$J'_k = \frac{(x + \zeta^k y)A}{I} \quad \text{pour } k = 0, \dots, p-1.$$

D'après la question 1, les idéaux J'_k sont premiers entre eux deux à deux. Par ailleurs, d'après (1), on a l'égalité

$$\left(\frac{zA}{I}\right)^p = \prod_{k=0}^{p-1} J'_k.$$

L'idéal I divise zA : s'il existait un idéal premier \mathfrak{q} tel que $v_{\mathfrak{q}}(zA/I) < 0$, la valuation en \mathfrak{q} de l'un des idéaux J'_k serait < 0 , ce qui n'est pas. L'unicité de la décomposition d'un idéal de A en produit d'idéaux premiers, entraîne alors que J'_k est la puissance p -ième d'un idéal J_k de A . D'où le résultat.

Exercice 3

Puisque xy n'est pas dans \mathfrak{P} , quitte à multiplier x et y par des puissances convenables de ζ , on peut supposer que x et y sont semi-primaires. Il existe alors des entiers relatifs a et b tels que $x \equiv a \pmod{\mathfrak{P}^2}$ et $y \equiv b \pmod{\mathfrak{P}^2}$. L'égalité $pA = \mathfrak{P}^{p-1}$ entraîne

$$x^p \equiv a^p \pmod{\mathfrak{P}^{p+1}} \quad \text{et} \quad y^p \equiv b^p \pmod{\mathfrak{P}^{p+1}}.$$

Il existe ainsi $t \in A$ tel que

$$x^p + y^p = a^p + b^p + t\lambda^{p+1}.$$

Supposons que z ne soit pas dans \mathfrak{P}^2 . Il existe alors $\delta \in A$ qui n'est pas dans \mathfrak{P} tel que $z = \lambda\delta$. On obtient l'égalité

$$(1) \quad a^p + b^p = \lambda^p(u\delta^p - t\lambda).$$

Posons $e = v_p(a^p + b^p)$ ($e \geq 0$). On a $v_{\mathfrak{P}}(a^p + b^p) = e(p-1)$. Puisque $u\delta$ n'est pas dans \mathfrak{P} , on a $v_{\mathfrak{P}}(u\delta^p - t\lambda) = 0$, d'où $v_{\mathfrak{P}}(a^p + b^p) = p$ (formule (1)), ce qui conduit à $p = e(p-1)$ puis $p = 2$, d'où une contradiction et l'assertion.

Exercice 4

1) On écrit que l'on a

$$(1) \quad uz^p = x^p + y^p = \prod_{j=0}^{p-1} (x + \zeta^j y) \in \mathfrak{P}.$$

Il existe un indice j tel que $x + \zeta^j y$ soit dans \mathfrak{P} . Soit k un indice distinct de j compris entre 0 et $p-1$. On a

$$x + \zeta^k y = (x + \zeta^j y) + (\zeta^{k-j} - 1)\zeta^j y,$$

ce qui entraîne l'assertion car $\zeta^{k-j} - 1$ est dans \mathfrak{P} .

2) D'après la question 1, les éléments

$$\frac{x+y}{\lambda}, \frac{x+\zeta y}{\lambda}, \dots, \frac{x+\zeta^{p-1}y}{\lambda}$$

sont dans A . Ils sont mutuellement non congrus modulo \mathfrak{P} . En effet, supposons qu'il existe deux indices j et k avec $0 \leq j < k \leq p-1$ tels que

$$x + \zeta^j y \equiv x + \zeta^k y \pmod{\mathfrak{P}^2}.$$

Dans ce cas, on obtient $\zeta^j(1 - \zeta^{k-j})y \equiv 0 \pmod{\mathfrak{P}^2}$. Compte tenu du fait que $1 - \zeta^{k-j}$ est associé à λ , cela entraîne que y est dans \mathfrak{P} , contrairement à l'hypothèse faite. Puisque le cardinal de A/\mathfrak{P} est p , il existe donc un indice j_0 tel que l'on ait

$$\frac{x + \zeta^{j_0} y}{\lambda} \equiv 0 \pmod{\mathfrak{P}} \quad \text{et} \quad \frac{x + \zeta^j y}{\lambda} \not\equiv 0 \pmod{\mathfrak{P}} \quad \text{si } j \neq j_0.$$

Il résulte alors de l'égalité (1) que l'on a

$$v_{\mathfrak{P}}\left(\frac{x + \zeta^{j_0} y}{\lambda}\right) = p(m-1) \quad \text{et} \quad v_{\mathfrak{P}}(x + \zeta^j y) = 1 \quad \text{si } j \neq j_0,$$

d'où l'assertion.

3) Pour tout $j = 0, \dots, p-1$, l'idéal I' divise $(x + \zeta^j y)A$ et \mathfrak{P} ne divise pas I' car xy n'est pas dans \mathfrak{P} . On en déduit l'existence d'idéaux I'_j de A tels que l'on ait

$$(x + \zeta^{j_0} y)A = \mathfrak{P}^{p(m-1)+1} I' I'_{j_0},$$

$$(x + \zeta^j y)A = \mathfrak{P} I' I'_j \quad \text{si } j \neq j_0.$$

D'après la question 2, les idéaux I'_j ne sont pas divisibles par \mathfrak{P} . Vérifions qu'ils sont premiers entre eux deux à deux. Supposons pour cela qu'il existe un idéal premier \mathfrak{q} de A qui divise I'_j et I'_k avec $j < k$. D'après les égalités ci-dessus, les idéaux $(x + \zeta^k y)A$ et $(x + \zeta^j y)A$ sont alors divisibles par $\mathfrak{P}\mathfrak{q}I'$. On en déduit que $\mathfrak{q}I'$ divise yA puis xA , ce qui conduit à une contradiction par définition de I' [$x + \zeta^j y$ et $x + \zeta^k y \in \mathfrak{P}I'\mathfrak{q}$ d'où $(\zeta^k - \zeta^j)y \in \mathfrak{P}\mathfrak{q}I'$ puis $\lambda y \in \mathfrak{P}\mathfrak{q}I'$. Par suite, $\mathfrak{P}yA \subseteq \mathfrak{P}\mathfrak{q}I'$ puis $yA \subseteq \mathfrak{q}I'$ et y appartient à

$\mathfrak{q}I'$. On en déduit que x est aussi dans $\mathfrak{q}I'$ car $\mathfrak{P}\mathfrak{q}I'$ est contenu dans $\mathfrak{q}I'$. Posons $z = \lambda^m \delta$ où $\delta \in A$ (et δ non dans \mathfrak{P}). Puisque u est une unité, on déduit alors de (1) l'égalité

$$(\delta A)^p = I'^p \prod_{k=0}^{p-1} I'_k,$$

ce qui entraîne le résultat.

2. Lemmes de Kummer sur les unités

Exercice 5

1) Par hypothèse, on a $u \equiv m \pmod{pA}$. On a donc $u^{p-1} \equiv m^{p-1} \pmod{pA}$. Puisque p ne divise pas m , on en déduit que $u^{p-1} \equiv 1 \pmod{pA}$. Par ailleurs, u^{p-1} est une puissance p -ième dans K si et seulement si tel est le cas de u . En remplaçant u par u^{p-1} , on constate ainsi que la condition (1) de l'énoncé n'est pas restrictive pour prouver la proposition.

2) Il existe $b \in \mathbb{Z}$ et $y \in A$ tels que l'on ait

$$(1) \quad u = 1 + pb + p\lambda y.$$

En effet, il existe $t \in A$ tel que $u = 1 + pt$. Le corps résiduel $A/(\lambda)$ étant isomorphe à $\mathbb{Z}/p\mathbb{Z}$, il existe $b \in \mathbb{Z}$ (compris entre 0 et $p-1$) tel que $t \equiv b \pmod{\lambda A}$. On a donc $t = b + \lambda y$ où $y \in A$ et l'égalité (1). D'après (1), en notant G le groupe de Galois de K sur \mathbb{Q} , on a

$$N_{K/\mathbb{Q}}(u) = \prod_{\sigma \in G} (1 + pb + p\sigma(\lambda y)),$$

d'où il résulte que

$$N_{K/\mathbb{Q}}(u) \equiv (1 + pb)^{p-1} \pmod{p\lambda},$$

car λ et $\sigma(\lambda)$ sont associés pour tout $\sigma \in G$. On a donc

$$N_{K/\mathbb{Q}}(u) \equiv 1 + (p-1)bp \equiv 1 - bp \pmod{p\lambda},$$

On en déduit que $N_{K/\mathbb{Q}}(u) = 1$ (sinon $N_{K/\mathbb{Q}}(u) = -1$ et $p = 2$). Par suite, λ divise b . L'égalité (1) entraîne alors le résultat (p et λ^{p-1} sont associés).

3) Il résulte de l'hypothèse faite que le polynôme minimal de $u^{1/p}$ sur K est $g := X^p - u$. L'extension L/K est donc de degré p et elle est galoisienne car les racines p -ièmes de l'unité sont dans K . C'est donc une extension abélienne de groupe de Galois isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Puisque K est une extension totalement imaginaire de \mathbb{Q} les places à l'infini de K sont nécessairement non ramifiées dans L . Vérifions que L/K est non ramifiée en dehors de \mathfrak{P} . Indiquons deux démonstrations.

a) Soit \mathfrak{q} un idéal premier non nul de A autre que \mathfrak{P} . Le polynôme g est séparable modulo \mathfrak{q} , car g et $g' = pX^{p-1}$ réduits modulo \mathfrak{q} sont premiers entre eux dans $A/\mathfrak{q}[X]$; on peut aussi évoquer le fait que le discriminant de g est :

$$\Delta(g) = (-1)^{\frac{p(p-1)}{2}} p^p u^{p-1},$$

de sorte que $\Delta(g)$ est non nul modulo \mathfrak{q} . L'extension L/K étant galoisienne, le théorème 2 du chapitre I entraîne que \mathfrak{q} est non ramifié dans L .

b) On peut aussi considérer la différentielle $\mathfrak{D}_{L/K}$ de l'extension L/K . Notons C l'anneau d'entiers de L et posons $\theta = u^{1/p}$. La différentielle $\mathfrak{D}_{L/K}$, qui est un idéal de C , divise l'idéal de C engendré par $g'(\theta)$ [θ est dans C et est un élément primitif de L/K]. On a $g'(\theta) = p\theta^{p-1}$. Puisque θ^{p-1} est une unité de C , on a donc $g'(\theta)C = pC$, par suite $\mathfrak{D}_{L/K}$ n'est divisible que par des idéaux premiers de C au-dessus de p . D'où l'assertion. [θ est une unité de C car $\theta^p = u$ et pour tout idéal premier \mathfrak{p} de C , on a $0 = v_{\mathfrak{p}}(u) = pv_{\mathfrak{p}}(\theta)$.]

4.1) Le polynôme f est clairement unitaire, son terme constant est dans A car on a $u \equiv 1 \pmod{\lambda^p}$ et les coefficients binomiaux C_p^j pour $1 \leq j \leq p-1$ sont divisibles par p , donc f appartient à $A[X]$.

4.2) Les racines de f , qui ne sont pas dans K car u n'est pas dans K^p , appartiennent à L . Le degré de α sur K est donc p , d'où l'assertion.

5) On déduit de la question 4 que $\mathfrak{D}_{L/K}$ divise l'idéal principal $f'(\alpha)C$. Soit \mathfrak{P}' un idéal de C au-dessus de \mathfrak{P} . L'élément p/λ^{p-1} est une unité de A , et parce que $\lambda \in \mathfrak{P}'$, on a la congruence

$$f'(\alpha) = \frac{p(\lambda\alpha - 1)^{p-1}}{\lambda^{p-1}} \equiv \frac{p}{\lambda^{p-1}} \pmod{\mathfrak{P}'}.$$

Il en résulte que $f'(\alpha)$ n'appartient pas à \mathfrak{P}' , autrement dit, que \mathfrak{P}' ne divise pas $f'(\alpha)C$. En particulier, \mathfrak{P}' ne divise pas $\mathfrak{D}_{L/K}$, ce qui prouve le résultat.

6) L'extension L/K étant abélienne de degré p et non ramifiée, le nombre de classes de K doit être divisible par p (théorème de réciprocité), ce qui contredit l'hypothèse faite sur p . D'où la proposition 1.

Exercice 6

1) Soit $n \geq 1$ un entier. Posons $\beta = \alpha^n$. Le degré t de β sur \mathbb{Q} est inférieur ou égal au degré d de α sur \mathbb{Q} . Soient $\beta_1 = \beta, \dots, \beta_t$ les conjugués de β sur \mathbb{Q} . Puisque β est entier, le polynôme minimal $P \in \mathbb{Z}[X]$ de β sur \mathbb{Q} est unitaire. On en déduit que l'on a

$$P = X^t + \sum_{k=1}^t (-1)^k \sigma_k X^{t-k},$$

où σ_k est la k -ième fonction symétrique élémentaire des β_i . Il résulte de l'hypothèse faite que les coefficients de P sont bornés par une constante qui ne dépend que de d (par exemple

2^d). Il n'y a donc qu'un nombre fini de polynômes irréductibles de $\mathbb{Z}[X]$ dont une puissance de α soit racine. On en déduit que l'ensemble des puissances de α est fini, ce qui entraîne le résultat.

L'hypothèse que α soit entier est essentielle comme le montre l'exemple où $\alpha = \frac{3}{5} + i\frac{4}{5}$.

2) Les racines $2p$ -ièmes de l'unité sont les éléments $\pm\zeta^k$ pour $k = 0, \dots, p-1$, et ils appartiennent à K . Inversement, soit μ l'ensemble des racines de l'unité contenues dans K . En utilisant le fait que la fonction indicateur d'Euler $n \mapsto \varphi(n)$ tend vers l'infini avec n (*), on déduit que μ est un groupe fini. De plus μ est cyclique (rappelons que si L est un corps, les sous-groupes multiplicatifs finis de L^* sont cycliques). Soient m l'ordre de μ et η un générateur de μ i.e. une racine primitive d'ordre m de l'unité. Vérifions que l'on a $m = 2p$, ce qui prouvera le résultat. Le degré de $\mathbb{Q}(\eta)/\mathbb{Q}$ est $\varphi(m)$. Posons $m = p^r m_0$ où p ne divise pas m_0 et où $r \geq 1$. On a $\varphi(m) = p^{r-1}(p-1)\varphi(m_0)$. Puisque $\mathbb{Q}(\eta)$ est contenu dans K , on a

$$p^{r-1}(p-1)\varphi(m_0) \leq p-1.$$

Cela entraîne $r = 1$ et $\varphi(m_0) = 1$, d'où $m_0 = 2$ puis $m = 2p$.

3) Tout élément de K s'écrit sous la forme $a_0 + a_1\zeta + \dots + a_{p-2}\zeta^{p-2}$ où les a_i sont dans \mathbb{Q} . Le conjugué complexe de cet élément appartient à K car l'image de ζ par la conjugaison complexe est ζ^{-1} . D'où l'assertion et l'on a $\tau(\zeta) = \zeta^{-1}$.

4) Les conjugués sur \mathbb{Q} de $\alpha \in A$ sont de module 1. En effet, pour tout plongement $\sigma : K \rightarrow \mathbb{C}$ i.e. pour tout élément σ du groupe de Galois de K sur \mathbb{Q} , qui est abélien, on a

$$\sigma(\alpha) = \frac{\sigma(u)}{\sigma\tau(u)} = \frac{\sigma(u)}{\tau\sigma(u)},$$

d'où $|\sigma(\alpha)| = 1$. D'après la question 1, α est donc une racine de l'unité. La question 2 entraîne alors le résultat.

5) Supposons que l'on ait $\alpha = -\zeta^a$. Il existe des entiers $b_i \in \mathbb{Z}$ tels que l'on ait $u = b_0 + b_1\zeta + \dots + b_{p-2}\zeta^{p-2}$. On a les congruences

$$u \equiv b_0 + b_1 + \dots + b_{p-2} \pmod{\mathfrak{P}} \quad \text{et} \quad \tau(u) \equiv b_0 + b_1 + \dots + b_{p-2} \pmod{\mathfrak{P}},$$

d'où $\tau(u) \equiv u \pmod{\mathfrak{P}}$. D'après l'hypothèse faite, on a donc

$$-\zeta^a \tau(u) \equiv \tau(u) \pmod{\mathfrak{P}}.$$

On a $\zeta \equiv 1 \pmod{\mathfrak{P}}$, d'où $2\tau(u) \equiv 0 \pmod{\mathfrak{P}}$. On obtient ainsi une contradiction car p est impair et $\tau(u)$ est une unité de A . D'où l'assertion.

6) On considère alors un entier r tel que $2r \equiv a \pmod{p}$. Posons

$$u_1 = \zeta^{-r} u.$$

On déduit de la question 5 que l'on a $\tau(u_1) = u_1$ [En effet, on a $\tau(u_1) = \zeta^r \tau(u) = u \zeta^{r-a}$, d'où $\tau(u_1) = u_1 \zeta^{2r-a} = u_1$]. Par ailleurs, le sous-corps de $\mathbb{Q}(\zeta)$ laissé fixe par la conjugaison complexe est K^+ . Il en résulte que u_1 appartient à B . D'où le lemme.

(*) Il s'agit de montrer que pour tout $A > 0$ il existe n_0 tel que dès que $n \geq n_0$ on a $\varphi(n) \geq A$. On considère l'ensemble F des entiers naturels dont les diviseurs premiers sont tous $\leq A$. Il existe $n_1 \in F$ tels pour tout $n \in F$ et $n \geq n_1$, on ait $\varphi(n) > A$. En effet, soient p_1, \dots, p_s l'ensemble des nombres premiers $\leq A$. Pour tout i il existe e_i tel que $\varphi(p_i^{e_i}) \geq A$. On prend pour n_1 :

$$n_1 = \prod_{i=1}^s p_i^{e_i}.$$

En effet, pour tout $n \in F$ et $n \geq n_1$, il existe un nombre premier p_i tel que $v_{p_i}(n) \geq e_i$. Puisque $\varphi(p_i^{e_i}) \geq A$, on a en particulier $\varphi(n) \geq A$. D'où l'assertion. Alors, l'entier $n_0 = n_1$ convient; on a deux cas à considérer. Si $n \geq n_0$, si n est dans F on a l'inégalité souhaitée et si n n'est pas dans F , il existe un diviseur premier p de n avec $p \geq A + 1$. On a $\varphi(p) = p - 1 \geq A$, d'où encore $\varphi(n) \geq A$ et le résultat.

Remarque. On a $B = \mathbb{Z}[\zeta + \zeta^{-1}]$ et

$$(1 - \zeta)(1 - \zeta^{-1}) = 2 - (\zeta + \zeta^{-1}).$$

Par suite, tout élément de B est congru modulo λ^2 à un entier relatif. En particulier, les unités de B sont semi-primaires.

Considérons alors une unité u de A semi-primaire. Montrons que u est dans B . D'après l'exercice 6, il existe $u_1 \in B$ et $a \in \mathbb{N}$ tels que $u = u_1 \zeta^a$. Il existe $N \in \mathbb{Z}$ tel que $u_1 \equiv N \pmod{\lambda^2}$. On a

$$\zeta^a = (1 - \lambda)^a \equiv 1 - a\lambda \pmod{\lambda^2}.$$

On obtient

$$u_1 \zeta^a \equiv u_1 - u_1 a \lambda \equiv N - Na \lambda \pmod{\lambda^2}.$$

D'après l'hypothèse faite, on a $u \equiv m \pmod{\lambda^2}$. Cela entraîne

$$N - m \equiv aNa \pmod{\lambda^2}.$$

On en déduit que λ divise $m - N$, donc p divise $m - N$ (cf. la norme sur \mathbb{Q} de $N - m$ i.e. $(N - m)^{p-1}$ qui est divisible par la norme de λ i.e. p), d'où λ divise aNa puis p divise aNa . Puisque u_1 est une unité, p ne divise pas N , donc p divise a , d'où $u = u_1$ et notre assertion.

3. Démonstration du premier cas

Exercice 7

1) Supposons $p = 3$. On a $x, y, z \equiv \pm 1 \pmod{\mathfrak{P}}$, d'où $x^3, y^3, z^3 \equiv \pm 1 \pmod{\mathfrak{P}^3}$. On en déduit que ± 1 est congru à 0 ou ± 2 modulo \mathfrak{P}^3 , puis que 3 appartient à \mathfrak{P}^3 , ce qui conduit à une contradiction, car 3 est associé à λ^2 .

Supposons $p = 5$. On a dans ce cas, $x, y, z \equiv \pm 1, \pm 2 \pmod{\mathfrak{P}}$, et l'on obtient les congruences $x^5, y^5, z^5 \equiv \pm 1, \pm 32 \pmod{\mathfrak{P}^5}$. On en déduit que l'on a

$$\pm 1, \pm 32 \equiv 0, \pm 2, \pm 31, \pm 33, \pm 64 \pmod{\mathfrak{P}^5},$$

autrement dit,

$$0 \equiv \pm 1, \pm 3, \pm 30, \pm 32, \pm 34, \pm 63, \pm 65, \pm 96 \pmod{\mathfrak{P}^5}.$$

On obtient de nouveau une contradiction car $v_{\mathfrak{P}}(30) = v_{\mathfrak{P}}(65) = 4$. D'où le résultat.

Exercice 8

D'après l'exercice 2, il existe des idéaux J_j pour $j = 0, \dots, p-1$ premiers entre eux deux à deux, non divisibles par \mathfrak{P} , tels que

$$(x + \zeta^j y)A = J_j^p I,$$

où I est le pgcd des idéaux $(x + \zeta^j y)A$. On a l'égalité

$$(1) \quad \left(\frac{x + \zeta^j y}{x + \zeta^{p-1} y} \right) A = \left(\frac{J_j}{J_{p-1}} \right)^p \quad \text{pour } j = 0, \dots, p-1.$$

Puisque p est **régulier**, on en déduit que l'idéal fractionnaire

$$\frac{J_j}{J_{p-1}} \text{ est principal.}$$

Il existe donc μ_j et $\nu_j \in A$, $\nu_j \neq 0$, tels que l'on ait

$$(2) \quad \frac{J_j}{J_{p-1}} = \left(\frac{\mu_j}{\nu_j} \right) A.$$

On a ainsi l'égalité $J_j \cdot (\nu_j A) = J_{p-1}(\mu_j A)$. On peut supposer que

$$\mu_j \nu_j \not\equiv 0 \pmod{\lambda}.$$

En effet, puisque \mathfrak{P} ne divise pas $J_j J_{p-1}$, on a $v_{\mathfrak{P}}(\mu_j) = v_{\mathfrak{P}}(\nu_j) := e$, d'où l'assertion quitte à remplacer μ_j et ν_j par μ_j/λ^e et ν_j/λ^e . Les égalités (1) et (2) entraînent alors le résultat.

Exercice 9

Soit j un entier tel que $0 \leq j \leq p-1$. D'après l'exercice 8 et l'égalité (2) de l'énoncé, on a l'égalité

$$\nu_j^p(x + \zeta^j y) = \zeta^{c_j} \varepsilon_j \zeta^h(x + \zeta^{p-1} y) \mu_j^p.$$

On en déduit que

$$\nu_j^p(x' + \zeta^j y') = \varepsilon_j \zeta^{c_j} \mu_j^p.$$

Il existe des entiers m_j et $n_j \in \mathbb{Z}$ tels que $\mu_j \equiv m_j \pmod{\mathfrak{P}}$ et $\nu_j \equiv n_j \pmod{\mathfrak{P}}$. On a $\mu_j^p \equiv m_j^p \pmod{\lambda^p}$ et $\nu_j^p \equiv n_j^p \pmod{\lambda^p}$. On a ainsi

$$(1) \quad n_j^p(x' + \zeta^j y') \equiv \varepsilon_j \zeta^{c_j} m_j^p \pmod{\lambda^p A_{\mathfrak{P}}}.$$

En appliquant la conjugaison complexe à la congruence (1), on obtient ($\varepsilon_j \in \mathbb{R}$)

$$(2) \quad n_j^p(\tau(x') + \zeta^{-j} \tau(y')) \equiv \varepsilon_j \zeta^{-c_j} m_j^p \pmod{\lambda^p A_{\mathfrak{P}}}.$$

[On a $\tau(\lambda) = 1 - \zeta^{-1}$, qui est associé à λ et τ laisse stable $A_{\mathfrak{P}}$ car \mathfrak{P} est l'unique idéal premier de A au-dessus de p]. D'après (1) et (2) on a donc

$$\zeta^{2c_j} n_j^p(\tau(x') + \zeta^{-j} \tau(y')) \equiv n_j^p(x' + \zeta^j y') \pmod{\lambda^p A_{\mathfrak{P}}}.$$

Puisque λ ne divise pas ν_j , il en est de même de n_j , de sorte que $1/n_j^p \in A_{\mathfrak{P}}$. D'où le résultat.

Exercice 10

1) D'après la condition (3) de la feuille d'énoncés, on a

$$x + \zeta^{p-1} y \equiv a \zeta^h(x + \zeta^{p-1} y) + \zeta^{p-1} b \zeta^h(x + \zeta^{p-1} y) \pmod{\lambda^2 A}.$$

On en déduit (en divisant par $x + \zeta^{p-1} y$) que $1 - \zeta^h(a + \zeta^{p-1} b)$ appartient à \mathfrak{P}^2 (donc à \mathfrak{P}), et ainsi $1 - \zeta^h(a + \zeta^{p-1} b)$ est dans \mathfrak{P} . Compte tenu du fait que ζ^{p-1} et ζ^h sont congrus à 1 modulo \mathfrak{P} , on a donc $1 \equiv a + b \pmod{\mathfrak{P}}$, d'où l'assertion (car $1 - (a + b) \in \mathbb{Z}$).

2) On déduit de l'exercice 9 et de la condition (4) de la feuille d'énoncés la congruence

$$a + \zeta^j b \equiv \zeta^{2c_j} (a + \zeta^{-j} b) \pmod{\lambda^2 A_{\mathfrak{P}}}.$$

Les deux membres de cette congruence étant dans A , on a donc

$$a + \zeta^j b \equiv \zeta^{2c_j} (a + \zeta^{-j} b) \pmod{\lambda^2 A}.$$

[Si $r = \lambda^2 u/t \in A$, $t \not\equiv 0 \pmod{\mathfrak{P}}$, on a $rt = \lambda^2 u$, d'où $v_{\mathfrak{P}}(r) \geq 2$ i.e. $r \in \mathfrak{P}^2$]. Par ailleurs, pour tout $N \in \mathbb{Z}$ on a $\zeta^N = (1 - \lambda)^N \equiv 1 - N\lambda \pmod{\lambda^2 A}$. Il en résulte que $jb - c_j(a + b)$ appartient à \mathfrak{P} . Par suite, on a

$$c_j(a + b) \equiv jb \pmod{p},$$

ce qui, d'après la question 1, entraîne le résultat.

Exercice 11

En multipliant la troisième et la quatrième colonne de M par -1 , on obtient un déterminant de Vandermonde. On vérifie que l'on a

$$\det(M) = (1 - \zeta)(1 - \zeta^{2b})(1 - \zeta^{2b-1})(\zeta - \zeta^{2b})(\zeta - \zeta^{2b-1})(\zeta^{2b} - \zeta^{2b-1}).$$

On peut supposer $\det(M) \neq 0$. Dans ce cas, en posant

$$M_1 = \begin{pmatrix} \rho_0 \lambda^p & 1 & -1 & -1 \\ \rho_1 \lambda^p & \zeta & -\zeta^{2b} & -\zeta^{2b-1} \\ \rho_2 \lambda^p & \zeta^2 & -\zeta^{4b} & -\zeta^{4b-2} \\ \rho_3 \lambda^p & \zeta^3 & -\zeta^{6b} & -\zeta^{6b-3} \end{pmatrix},$$

on a

$$x' = \frac{\det(M_1)}{\det(M)}.$$

Puisque les ρ_i sont dans $A_{\mathfrak{P}}$, le déterminant de M_1 appartient à $\lambda^p A_{\mathfrak{P}}$ (on développe par rapport à la première colonne). On a ainsi

$$v_{\mathfrak{P}}(\det(M_1)) \geq p.$$

Par ailleurs, on a $v_{\mathfrak{P}}(x') = 0$ (car x et $x + \zeta^{p-1}y$ ne sont pas dans \mathfrak{P}). On en déduit que

$$v_{\mathfrak{P}}(\det(M)) \geq p,$$

autrement dit, puisque $\det(M)$ est dans A , que l'on a $\det(M) \equiv 0 \pmod{\lambda^p A}$. D'où l'exercice.

Exercice 12

Rappelons que l'on a $p \geq 7$. On est amené à distinguer plusieurs cas selon la congruence de b modulo p .

1) Supposons $b \equiv 0 \pmod{p}$. D'après la condition (3) de la feuille d'énoncés, on a alors $y \equiv 0 \pmod{\lambda^2}$, ce qui n'est pas (car y n'est pas dans \mathfrak{P}).

2) Supposons $b \equiv 1 \pmod{p}$. On a alors $y \equiv \zeta^h(x + \zeta^{p-1}y) \pmod{\lambda^2 A}$ d'où l'on déduit que $y \equiv x + y \pmod{\lambda A}$. Par suite, x est divisible par λ , d'où de nouveau une contradiction.

3) Supposons $b \not\equiv 0, 1 \pmod{p}$ et $2b \not\equiv 1 \pmod{p}$. L'égalité

$$\det(M) = (1 - \zeta)(1 - \zeta^{2b})(1 - \zeta^{2b-1})(\zeta - \zeta^{2b})(\zeta - \zeta^{2b-1})(\zeta^{2b} - \zeta^{2b-1})$$

entraîne alors $v_{\mathfrak{P}}(\det(M)) = 6$. Or $\det(M)$ étant divisible par λ^p on en déduit que $p \leq 5$, d'où une contradiction.

4) Il en résulte que l'on a $b \not\equiv 0, 1 \pmod{p}$ et $2b \equiv 1 \pmod{p}$. On a $a + b \equiv 1 \pmod{p}$ (exercice 10), ce qui conduit à la congruence $a \equiv b \pmod{p}$. Par suite, on a (condition (3) de la feuille d'énoncés)

$$x \equiv y \pmod{\mathfrak{P}}.$$

Par symétrie de x , y et $-z$, on en déduit que l'on a aussi $x \equiv -z \pmod{\mathfrak{P}}$. On a donc

$$0 = x^p + y^p - z^p \equiv 3x^p \pmod{\mathfrak{P}},$$

et x est dans \mathfrak{P} , ce qui n'est pas. D'où l'exercice.

IV. Démonstration du deuxième cas du théorème

Exercice 13

Puisque $xyz \neq 0$, il existe x' , y' et z' tels que $x = \lambda^r x'$, $y = \lambda^s y'$, $z = \lambda^t z'$ et que $x'y'z'$ ne soit pas divisible par λ i.e. ne soit pas dans \mathfrak{P} , et r , s et $t \geq 0$. Si un seul des entiers x , y et z est divisible par λ , l'assertion est immédiate. Supposons que x , y et z soient divisibles par λ . On obtient alors

$$\lambda^{rp} x'^p + \lambda^{sp} y'^p = \lambda^{tp} z'^p.$$

avec r , s et t sont des entiers ≥ 1 . Puisque le premier cas du théorème est vrai, r , s , et t ne sont pas tous égaux. Supposons $t > r$. Dans ce cas, on a $r = s$, et l'on a alors

$$x'^p + y'^p = \lambda^{(t-r)p} z'^p,$$

d'où le résultat dans ce cas. Si $t < r$, on a $t = s$ puis

$$\lambda^{r-t} x'^p + y'^p = z'^p.$$

Si $t = r$, on a $s > t$, d'où

$$x'^p + \lambda^{s-t} y'^p = z'^p,$$

et de nouveau le résultat. D'où le fait que S soit non vide.

Exercice 14

Soient I_j des idéaux de A vérifiant la condition (1) de l'énoncé de l'exercice 4. L'indice j_0 étant celui intervenant dans ces égalités, quitte à remplacer β par $\zeta^{j_0} \beta$, et à réindexer les idéaux I_j , on peut supposer que $j_0 = 0$. On a alors les égalités

$$(\alpha + \beta)A = \mathfrak{P}^{p(m-1)+1} I'_0 I_0^p,$$

$$(\alpha + \zeta^j \beta)A = \mathfrak{P} I'_j I_j^p \quad \text{si } 1 \leq j \leq p-1,$$

avec $I' = \text{pgcd}(\alpha A, \beta A)$ et où les I_j sont premiers entre eux deux à deux et non divisibles par \mathfrak{P} . On en déduit que pour tout j entre 1 et $p-1$, on a

$$\mathfrak{P}^{(m-1)p} \cdot (\alpha + \zeta^j \beta) A \cdot I_0^p = (\alpha + \beta) A \cdot I_j^p.$$

L'idéal fractionnaire $(I_j/I_0)^p$ est donc principal. Puisque p est **régulier**, I_j/I_0 est donc principal. Il existe ainsi des éléments μ_j et ν_j de A avec $\nu_j \neq 0$, tels que

$$\frac{I_j}{I_0} = \left(\frac{\mu_j}{\nu_j} \right) A.$$

On peut supposer que $\mu_j \nu_j \not\equiv 0 \pmod{\lambda}$ (car les I_j ne sont pas divisibles par \mathfrak{P} : on a déjà évoqué cet argument dans l'exercice 8). Pour tout j entre 1 et $p-1$, il existe donc une unité $u_j \in A$ vérifiant la condition annoncée.

Exercice 15

On explicite l'égalité obtenue dans l'exercice 14 avec $j=1$ et $j=2$. On obtient

$$(\alpha + \zeta \beta) \lambda^{p(m-1)} = u_1 (\alpha + \beta) \left(\frac{\mu_1}{\nu_1} \right)^p \quad \text{et} \quad (\alpha + \zeta^2 \beta) \lambda^{p(m-1)} = u_2 (\alpha + \beta) \left(\frac{\mu_2}{\nu_2} \right)^p.$$

En multipliant la première égalité par $1+\zeta$ puis en soustrayant la deuxième à celle obtenue, on obtient

$$\lambda^{p(m-1)} \zeta (\alpha + \beta) = (\alpha + \beta) \left((1 + \zeta) u_1 \left(\frac{\mu_1}{\nu_1} \right)^p - u_2 \left(\frac{\mu_2}{\nu_2} \right)^p \right),$$

d'où

$$\lambda^{p(m-1)} \zeta (\nu_1 \nu_2)^p = (1 + \zeta) u_1 (\mu_1 \nu_2)^p - u_2 (\mu_2 \nu_1)^p,$$

ce qui, en divisant par $(1 + \zeta) u_1$, entraîne le résultat.

Exercice 16

1) D'après l'exercice 3 que l'on a $m \geq 2$. Par suite, λ^p divise $\alpha'^p + \varepsilon \beta'^p$. Puisque λ ne divise pas β' , l'idéal $\beta' A$ n'est pas contenu dans \mathfrak{P} et \mathfrak{P} étant maximal, on a donc

$$\lambda A + \beta' A = A.$$

Il existe donc $\omega \in A$ tel que

$$\omega \beta' \equiv 1 \pmod{\lambda},$$

d'où

$$(\omega \beta')^p \equiv 1 \pmod{\lambda^p}.$$

En multipliant l'égalité obtenue dans l'exercice 15 par ω^p , on en déduit que

$$(\alpha' \omega)^p + \varepsilon \equiv 0 \pmod{\lambda^p},$$

d'où l'existence d'un élément $\rho \in A$ tel que l'on ait $\varepsilon \equiv \rho^p \pmod{\lambda^p}$. Il existe $r \in \mathbb{Z}$ tel que $\rho \equiv r \pmod{\lambda}$. On obtient ainsi $\varepsilon \equiv r^p \pmod{\lambda^p}$, et d'après le lemme de Kummer, ε est donc une puissance p -ième dans A .

2) Posons $\varepsilon = \delta^p$ où δ est une unité de A . On a

$$\alpha'^p + (\delta\beta')^p = \varepsilon'(\gamma'\lambda^{m-1})^p.$$

Les éléments α' , β' et γ' ne sont pas divisibles par λ et $m-1$ appartient donc à l'ensemble S (on a $m \geq 2$). Le caractère minimal de m entraîne alors une contradiction. D'où le résultat.