Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 19 (1973)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI
Autor: Joly, Jean-René
Kapitel: §1. Relations de Stickelberger.
DOI: https://doi.org/10.5169/seals-46287

désigne la valeur absolue p-adique dans $\mathbf{Q}$: cette dernière inégalité équivaut bien à $q^b \mid N$.

En fait, on travaillera avec les *valuations* $\mathfrak{P}$-adiques, et non avec les valeurs absolues; d'autre part, la phase (2) de la démonstration (qui est indépendante de la phase (1)) sera traitée en premier, au paragraphe 1; les phases (1) et (3) seront traitées au paragraphe 2. Quelques conséquences ou généralisations du théorème 1 (et notamment l'extension du théorème 1 au cas d'un système d'équations) sont indiquées au paragraphe 3.

§ 1. *Relations de Stickelberger.*

1.1. Soit k un corps fini à $q = p^f$ éléments. Notons ω et ζ une racine primitive $(q-1)$-ième et une racine primitive p-ième de l'unité dans le corps des nombres complexes, posons $K = \mathbf{Q}(\omega)$, $L = \mathbf{Q}(\omega, \zeta) = K(\zeta)$, et soient A l'anneau des entiers de K et B l'anneau des entiers de L. Les théorèmes généraux sur la décomposition des idéaux premiers dans les corps cyclotomiques (voir [3], chap. 3 et 5, ou [11], chap. IV) permettent d'énoncer:
(1.1.1) L'idéal $p\mathbf{Z}$ est non ramifié dans K, il se décompose dans A en produit de g idéaux premiers de degré f: $pA = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_g$; g est déterminé par l'égalité $fg = [K: \mathbf{Q}]$, et chaque corps résiduel $A/\mathfrak{p}_i$ est isomorphe à k.
(1.1.2) Chaque idéal $\mathfrak{p}_i$ est totalement ramifié dans L, l'indice de ramification étant égal à $[L: K] = p - 1$; la décomposition de $\mathfrak{p}_i$ dans B est de la forme $\mathfrak{p}_i B = \mathfrak{P}_i^{p-1}$; le degré résiduel en $\mathfrak{P}_i \mid \mathfrak{p}_i$ est égal à 1, et le corps résiduel $B/\mathfrak{P}_i$ s'identifie au corps résiduel $A/\mathfrak{p}_i$, donc à k.
Il résulte de (1.1.1) et (1.2.2) que l'idéal $p\mathbf{Z}$ se décompose dans B de la façon suivante:

$$(1.1.3) \qquad p\mathbf{Z} = \mathfrak{P}_1^{p-1}\mathfrak{P}_2^{p-1} \dots \mathfrak{P}_g^{p-1}.$$

Dans ce qui suit, on suppose choisis une fois pour toutes un idéal $\mathfrak{P}_i$ et l'idéal $\mathfrak{p}_i$ correspondant; on les note simplement $\mathfrak{P}$ et $\mathfrak{p}$, et *on identifie* $B/\mathfrak{P}$ *et* $A/\mathfrak{p}$ *au corps* k.

1.2. Soit maintenant T^* le sous-groupe de L^* engendré par ω; T^* est cyclique, d'ordre $q - 1$, et la restriction à T^* de l'homomorphisme $B \to B/\mathfrak{P} = k$ est évidemment un isomorphisme de T^* sur k^*; l'isomorphisme inverse $k^* \to T^*$ est un *caractère multiplicatif* d'ordre $q - 1$ de k, qu'on notera θ.

1.3. Une dernière notation: pour tout élément non nul α de L, on notera $\mathrm{ord}(\alpha)$ l'exposant de $\mathfrak{P}$ dans la décomposition en facteurs premiers

de l'idéal fractionnaire αB de B (ord est donc tout simplement la « valuation $\mathfrak{P}$-adique normalisée » de L); les propriétés suivantes sont alors évidentes:

(1.3.1) Quels que soient α, β non nuls dans L, on a

$$\mathrm{ord}(\alpha\beta) = \mathrm{ord}(\alpha) + \mathrm{ord}(\beta)\,;\ \mathrm{ord}(\alpha+\beta) \geqslant \inf\big(\mathrm{ord}(\alpha), \mathrm{ord}(\beta)\big)\,.$$

(1.3.2) Si $\alpha \in B$, on a $\mathrm{ord}(\alpha) \geqslant 0$.

(1.3.3) Si $\alpha \in K$, on a $\mathrm{ord}(\alpha) \equiv 0 \pmod{p-1}$.

(1.3.4) Enfin, $\mathrm{ord}(p) = p - 1$.

((1.3.4) résulte de (1.1.3); pour prouver (1.3.3), commencer par décomposer dans K l'idéal premier αA de A, puis utiliser (1.1.2)).

1.4. Soit alors j un entier rationnel, et considérons la somme de Gauss

$$\tau(\theta^{-j} \mid \beta) = \sum_{x \in k^*} \theta^{-j}(x)\,\beta(x)\,, \tag{1.4.1}$$

β étant le caractère additif de k défini par $\beta(x) = \zeta^{Tr(x)}$ ($x \in k$; Tr désigne comme toujours la trace relative à l'extension $k/\mathbf{F}_p$); le choix de ω, ζ, $\mathfrak{P}$, et d'une identification entre $B/\mathfrak{P}$ et k, détermine entièrement θ et β; la somme de Gauss introduite en (1.4.1) ne dépend donc en fait que de j: *on posera pour simplifier* $\tau(j) = \tau(\theta^{-j} \mid \beta)$; en outre, on pourra se borner à étudier $\tau(j)$ pour $0 \leqslant j < q-1$, puisque θ est d'ordre $q-1$. Cela étant, la valuation $\mathfrak{P}$-adique $\mathrm{ord}(\tau(j))$ de $\tau(j)$ est donnée par la proposition suivante, due à Stickelberger:

PROPOSITION 1. — *Soit j un entier tel que $0 \leqslant j < q-1$, et soit*

$$j = j_0 + j_1 p + \ldots + j_{f-1} p^{f-1}$$

l'écriture de j en base p, avec $0 \leqslant j_i \leqslant p-1$ pour $i = 0, \ldots, f-1$; posons $\sigma(j) = j_0 + j_1 + \ldots + j_{f-1}$ (somme des chiffres de j en base p); on a alors:

$$\mathrm{ord}(\tau(j)) = \sigma(j)\,. \tag{1.4.2}$$

Démonstration. — Pour tout entier j, posons a priori $s(j) = \mathrm{ord}(\tau(j))$; il s'agit alors de prouver que si $0 \leqslant j < q-1$, on a $s(j) = \sigma(j)$; or, la fonction s possède les propriétés (i) à (vi) ci-dessous:

(i) *Quel que soit j, $s(j) \geqslant 0$; de plus, $s(0) = 0$.*

En effet, $\tau(j)$ est un entier de L, et $\tau(0) = -1$ est une unité de L. (Pour l'égalité $\tau(0) = -1$, voir chap. 5, sect. 2.2, (i)).

(ii) *Quels que soient j et k, on a $s(j+k) \leqslant s(j) + s(k)$.* ($k$ désigne ici un entier: aucun risque de confusion avec le *corps* k).

Pour j ou $k = 0$, il n'y a rien à prouver, puisque $s(0) = 0$; pour $j + k = q - 1$, on a $s(j+k) = s(0) = 0$, et là encore, il n'y a rien à prouver, puisque $s(j)$ et $s(k)$ sont non négatifs. Supposons donc $0 < j < q - 1$, $0 < k < q - 1$, et $j + k \neq q - 1$; on a dans ce cas

$$\tau(j)\tau(k) = \pi(\theta^{-j}, \theta^{-k})\tau(j+k) \tag{1.4.3}$$

(chap. 5, prop. 9, (ii)), et l'inégalité à démontrer résulte de la première formule (1.3.1) et de (1.3.2), puisque la somme de Jacobi $\pi(\theta^{-j}, \theta^{-k})$ est dans B.

(iii) *Quels que soient j et k, on a $s(j+k) \equiv s(j) + s(k) \pmod{p-1}$.*

Pour j ou $k = 0$, il n'y a rien à prouver, puisque $s(0) = 0$; pour $j + k = q - 1$, on a $\tau(j)\tau(k) = q\theta^j(-1) = p^f\theta^j(-1)$, donc, compte tenu de (1.3.1) et (1.3.4), $s(j) + s(k) = f(p-1) \equiv 0 \pmod{p-1}$; on a d'autre part $s(j+k) = s(0) = 0$; la congruence à démontrer se trouve donc établie dans ce cas particulier (la valeur de $\tau(j)\tau(k)$ résulte de la prop. 7 du chap. 5). Supposons maintenant $0 < j < q - 1$, $0 < k < q - 1$ et $j + k \neq q - 1$; l'égalité (1.4.3) et la première formule (1.3.1) donnent

$$s(j) + s(k) = s(j+k) + \operatorname{ord}\left(\pi(\theta^{-j}, \theta^{-k})\right);$$

la congruence à démontrer résulte alors de (1.3.3), puisque la somme de Jacobi $\pi(\theta^{-j}, \theta^{-k})$ est dans K.

(iv) *Quels que soient j, et $i \geqslant 0$, on a $s(jp^i) = s(j)$.*

En effet, pour tout $x \in k$, on a $\theta^{-jp^i}(x) = \theta^{-j}(x^{p^i})$; on a également $Tr(x^{p^i}) = Tr(x)$, puisque x et x^{p^i} sont conjugués sur $\mathbf{F}_p$ (chap. 1, prop. 8); il suffit alors de faire le changement de variable $y = x^{p^i}$ dans la formule de définition de la somme de Gauss $\tau(jp^i)$ pour obtenir $\tau(j) = \tau(jp^i)$, d'où évidemment l'égalité à démontrer.

(v) *Pour la valeur particulière $j = 1$, on a $s(1) = 1$.*

Posons $\lambda = \zeta - 1$; le polynôme minimal de ζ sur K (ou sur $\mathbf{Q}$) étant $X^{p-1} + \ldots + X + 1 = (X^p - 1)/(X-1)$, le polynôme minimal de λ est évidemment $((X+1)^p - 1)/X = X^{p-1} + pX^{p-2} + \ldots + p$, donc un polynôme d'Eisenstein relativement à p ([**11**], chap. II, § 5): il en résulte que

$$\operatorname{ord}(\lambda) = 1 \tag{1.4.4}$$

(utiliser (1.3.4) et la deuxième formule (1.3.1)). Ecrivons d'autre part la définition de $\tau(1)$ en y remplaçant ζ par $1+\lambda$:

$$\tau(1) = \sum_{x \in k^*} \theta^{-1}(x)(1+\lambda)^{Tr(x)},$$

soit, en développant $(1+\lambda)^{Tr(x)}$ par la formule du binôme et en utilisant (1.4.4):

$$\tau(1) \equiv \sum_{x \in k^*} \theta^{-1}(x)\big(1+\lambda r(x)\big) \pmod{\mathfrak{P}^2}, \tag{1.4.5}$$

$r(x)$ désignant l'unique entier rationnel compris entre 0 et $p-1$ et dont l'image dans $\mathbf{F}_p$ soit égale à $Tr(x)$. Dans le second membre de (1.4.5), faisons le changement de variable $t = \theta(x)$; comme $r(x) \equiv t + t^p + \ldots + t^{p^{f-1}} \pmod{\mathfrak{P}}$ (chap. 1, (3.2.1)), la congruence (1.4.5) devient

$$\tau(1) \equiv \sum_{t \in T^*} t^{-1} + \sum_{t \in T^*} t^{-1}(t+t^p+\ldots+t^{p^{f-1}}) \pmod{\mathfrak{P}^2}; \tag{1.4.6}$$

mais T^* est le groupe des racines $(q-1)$-ièmes de l'unité dans le corps des nombres complexes; on a donc, pour tout entier rationnel u,

$$\sum_{t \in T^*} t^u = \begin{cases} q-1, \text{ si } u \equiv 0 \pmod{q-1}; \\ 0, \text{ sinon}; \end{cases}$$

comme par ailleurs $q = p^f \equiv 0 \pmod{\mathfrak{P}^2}$, la congruence (1.4.6) se réduit à

$$\tau(1) \equiv -\lambda \pmod{\mathfrak{P}^2}; \tag{1.4.7}$$

d'où évidemment, compte tenu de la deuxième formule (1.3.1), $s(1) = \operatorname{ord}(\tau(1)) = \operatorname{ord}(\lambda) = 1$ (utiliser (1.4.4)), C.Q.F.D.

(vi) *On a enfin l'égalité* $\sum_{0 \leq j < q-1} s(j) = f(p-1)(q-2)/2$.

En effet, on a déjà remarqué (voir la démonstration de (iii)) que

$$s(j) + s(q-1-j) = f(p-1); \tag{1.4.8}$$

comme $s(0) = s(q-1) = 0$, la relation (1.4.8) donne, en faisant varier j de 1 à $q-2$ et en additionnant,

$$\sum_{0 \leq j < q-1} \big(s(j)+s(q-1-j)\big) = 2 \sum_{0 \leq j < q-1} s(j) = f(p-1)(q-2),$$

ce qui implique (vi).

Ces diverses propriétés étant établies, prouvons maintenant (toujours en supposant $0 \leqslant j < q-1$) que $\sigma(j) = s(j)$; les propriétés (i), puis (v), puis (ii) et (iii), montrent d'abord que pour $0 \leqslant j \leqslant p-1$, on a $s(j) = j = j_0 = \sigma(j)$; les propriétés (ii) et (iv) donnent d'autre part

$$s(j) \leqslant s(j_0) + s(j_1) + \ldots + s(j_{f-1});$$

comme $0 \leqslant j_i \leqslant p-1$ pour $i = 0, \ldots, f-1$, ces deux remarques impliquent, pour $0 \leqslant j < q-1$,

$$s(j) \leqslant j_0 + j_1 + \ldots + j_{f-1} = \sigma(j); \tag{1.4.9}$$

l'égalité $s(j) = \sigma(j)$ résulte alors de (1.4.9), de la propriété (vi), et de l'égalité $\sum_{0 \leqslant j < q-1} \sigma(j) = f(p-1)(q-2)/2$, qui se vérifie facilement par récurrence sur f. La proposition 1 se trouve ainsi démontrée.

§ 2. *Démonstration du théorème* 1.

Cette démonstration se fera en quatre étapes.

2.1. *Introduction du polynôme* $C(Y)$. Soit T le sous-ensemble de B formé de 0 et des éléments de T^*; pour tout $t \in T$, soit $\bar{t}$ l'image de t dans $k = B/\mathfrak{P}$; l'application $t \mapsto \bar{t}$ est alors une bijection de T sur k (sect. 1.1 et 1.2), dont la bijection inverse est le caractère θ, prolongé comme toujours par $\theta(0) = 0$. Soit d'autre part β le caractère additif de k défini par $\beta(x) = \zeta^{Tr(x)}$ $(x \in k)$; comme card $(T) = q$, il existe évidemment un polynôme à une variable Y et un seul, soit $C(Y)$, de degré $q-1$, à coefficients dans L, et tel que $C(t) = \beta(\bar{t})$ pour tout $t \in T$; posons

$$C(Y) = c_0 + c_1 Y + \ldots + c_{q-1} Y^{q-1}. \tag{2.1.1}$$

Lemme 1. — *Avec les notations du paragraphe* 1, *on a*

$$c_0 = 1;\ c_{q-1} = -q/(q-1);\ \textit{et}\ c_j = \tau(j)/(q-1) \tag{2.1.2}$$
$$\textit{pour}\ 1 \leqslant j \leqslant q-2.$$

En effet, pour $0 \leqslant j \leqslant q-1$, on a, par définition de $\tau(j)$, de θ et de $C(Y)$,

$$\tau(j) = \sum_{x \in k^*} \theta^{-j}(x)\beta(x) = \sum_{t \in T^*} t^{-j}\beta(\bar{t}) = \sum_{t \in T^*} t^{-j} C(t);$$