Zeitschrift: L'Enseignement Mathématique

Band: 19 (1973)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: ÉQUATIONS ET VARIÉTÉS ALGÉBRIQUES SUR UN CORPS FINI

Kapitel: §2. Seconde démonstration du théorème de Chevalley- Warning.

Autor: Joly, Jean-René

DOI: https://doi.org/10.5169/seals-46287

PROPOSITION 1. — *Si un corps commutatif K possède la propriété* (C_1), *alors il possède la propriété* (B_0).

Démonstration. — Soit en effet L un corps gauche de centre K et de degré fini n sur K. On sait que n est un carré (soit $n=d^2$) et que si $e_1, ..., e_n$ est une base de L sur K (en tant qu'espace vectoriel), la norme réduite $Nrd_{L/K}(x)$ d'un élément quelconque $x = x_1e_1 + ... + x_ne_n$ de L est un polynôme homogène et de degré d, à coefficients dans K, par rapport aux composantes $x_1, ..., x_n$ de x, qui sont dans K (voir par exemple Bourbaki, Algèbre, chap. VIII, § 12; dans le cas bien connu du corps $\mathbf{H}$ des quaternions ordinaires sur $\mathbf{R}$, rapporté à la base canonique 1, i, j, k, on a $n = 4 = 2^2$ et $Nrd_{\mathbf{H}/\mathbf{R}}(x) = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2$); cette norme réduite ne s'annule que pour $x = 0$, donc pour $x_1 = ... = x_n = 0$; comme K est supposé posséder la propriété (C_1), on a nécessairement $n = d^2 \leqslant d$, donc $d = 1$, $n = 1$ et $L = K$, C.Q.F.D.

Redémontrons alors le théorème de Wedderburn; soit L un corps fini, non supposé commutatif, et soit k son centre; k est un corps fini *commutatif*, et il possède la propriété (C_1) (cor. 2), donc la propriété (B_0) (prop. 1); mais comme L est évidemment de degré fini sur k, on a alors $L = k$ (par définition de (B_0)), et par conséquent L est commutatif, C.Q.F.D.

§ 2. *Seconde démonstration du théorème de Chevalley-Warning.*

2.1. Cette seconde démonstration, indépendante de la théorie des polynômes réduits, repose sur le théorème suivant (dont on aura également besoin au § 3):

THÉORÈME 2. — *Soit $F \in k\,[X]$ un polynôme à n variables, et de degré d. Alors, si $d < n\,(q-1)$, on a*

$$\sum_{\mathbf{x} \in k^n} F(\mathbf{x}) = 0\,. \tag{2.1.1}$$

Démonstration. — Par linéarité, on peut se ramener au cas où F est un monôme ${X_1}^{u_1} \ldots {X_n}^{u_n}$, avec $d = u_1 + ... + u_n < n\,(q-1)$; on a alors

$$\sum_{\mathbf{x} \in k^n} F(\mathbf{x}) = \prod_{i=1}^{n} \Big(\sum_{x_i \in k} {x_i}^{u_i} \Big)\,; \tag{2.1.2}$$

l'inégalité relative à d montre que pour un i au moins, $u_i < q - 1$, et il suffit évidemment de prouver que, dans (2.1.2), le i-ème facteur du membre de droite est alors nul, ce qui résulte du lemme suivant:

LEMME 1. — *Soit u un entier $\geqslant 0$, et posons $S_u = \sum_{x \in k} x^u$; alors*

(i) *si u est non nul et divisible par $q - 1$, $S_u = -1$;*

(ii) *sinon, $S_u = 0$.*

En particulier, si $u < q - 1$, $S_u = 0$.

Prouvons ce lemme; comme $x^q = x$ pour tout $x \in k$, on ne restreint pas la généralité de la démonstration en supposant $0 \leqslant u \leqslant q - 1$; on est ainsi amené à distinguer trois cas:

(1) $u = 0$: S_u est alors somme de q termes égaux à 1; comme q est divisible par la caractéristique p de k, on a bien $S_u = 0$;

(2) $u = q - 1$: alors $x^u = 0$ pour $x = 0$, et $x^u = 1$ sinon; S_u est donc somme de $q - 1$ termes égaux à 1, et on conclut comme en (1);

(3) $0 < u < q - 1$: la proposition 7 (chap. 1) avec $d = u$ montre qu'il existe dans k^* un élément a tel que $a^u \neq 1$; comme $x \mapsto ax$ est une bijection de k sur k, on peut écrire $S_u = \sum_{x \in k} (ax)^u = a^u S_u$; mais ceci donne $(a^u - 1) S_u = 0$, donc, en simplifiant par $a^u - 1 \neq 0$, $S_u = 0$, C.Q.F.D.

On aurait également pu régler les cas (2) et (3) de la façon suivante: soit g un générateur de k^*; les éléments x de k sont alors 0, et les g^i avec $0 \leqslant i \leqslant q - 2$; S_u est donc égal à la somme de la progression géométrique $1 + g^u + g^{2u} + \ldots + g^{(q-2)u}$; d'où $S_u = (1 - g^{(q-1)u})/(1 - g^u)$, ce qui vaut bien 0, puisque $g^{q-1} = 0$. Remarquons par ailleurs que la nullité des $q - 2$ quantités S_u $(0 < u < q - 1)$ équivaut, compte tenu des *formules de Newton*, à la nullité des $q - 2$ fonctions symétriques élémentaires des éléments de k^* autres que le produit (voir chap. 1, sect. 1.1).

2.2. Utilisons maintenant le théorème 2 pour redémontrer le théorème de Chevalley-Warning. Considérons le polynôme $\bar{F}$ défini par (1.1.2) (sect. 1.1); il est de degré $d(q-1) < n(q-1)$, puisqu'on a supposé $n > d$; le théorème 2 permet donc d'écrire

(2.2.1) $$\sum_{\mathbf{x} \in k^n} \bar{F}(\mathbf{x}) = 0;$$

mais $\bar{F}(\mathbf{x})$ vaut 1 si $\mathbf{x} \in V$, et 0 si $\mathbf{x} \notin V$; d'où une seconde égalité:

(2.2.2) $$\sum_{\mathbf{x} \in k^n} \bar{F}(\mathbf{x}) = N.1;$$

(2.2.1) et (2.2.2) donnent alors $N.1 = 0$, soit, puisque k est de caractéristique p, $N \equiv 0 \pmod p$, C.Q.F.D.