Notes sur le chapitre premier

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1973)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **11.09.2024**

degré q^{m-1}, admet pour racines les q^m éléments de K: absurde): elle est donc surjective, ce qui prouve la première assertion, et ce qui montre en outre que le noyau de Tr est un hyperplan de K; comme $Tr\,(y^q - y) = 0$ pour tout élément y de K, il reste, pour établir l'équivalence de (a) et (b), à prouver que l'ensemble des éléments de la forme $y^q - y$ ($y \in K$) est également un hyperplan de K; et il suffit pour cela de remarquer que l'application $y \mapsto y^q - y$ de K dans K est k-linéaire et de rang $m - 1$, puisque son noyau (formé des $y \in K$ tels que $y^q = y$, donc égal à k: prop. 2, ou prop. 8) est de dimension 1.

3.3. Mêmes données et notations que ci-dessus. Soit maintenant $N\colon K \to k$, l'application *norme.* La proposition 8 montre que, pour tout élément x de K, on a

(3.3.1) $$N(x) = x.x^q \ldots x^{q^{m-1}} = x^{(q^m-1)/(q-1)}.$$

En outre:

PROPOSITION 10. — *L'application $N\colon K^* \to k^*$, est surjective. Si $x \in K^*$, les deux assertions suivantes sont équivalentes :*

(a) $N(x) = 1$;

(b) *il existe $y \in K^*$ tel que $x = y^{q-1}$.*

Démonstration. — N est un homomorphisme du groupe K^* dans le groupe k^*, et il résulte de (3.3.1) et de la proposition 7 (avec $d=(q^m-1)/(q-1)$) que le noyau de N est d'ordre $(q^m-1)/(q-1)$; comme l'ordre de K^* est égal à $q^m - 1$, l'image de N est nécessairement d'ordre $q - 1 = \text{card}\,(k^*)$, d'où la surjectivité de N. Le noyau de N contenant évidemment tous les éléments de K^* de la forme y^{q-1} ($y \in K^*$), qui en constituent un sous-groupe, il reste donc, pour établir l'équivalence de (a) et (b), à montrer que ce sous-groupe est précisément d'ordre $(q^m-1)/(q-1)$; mais il suffit pour cela de remarquer que l'application $y \mapsto y^{q-1}$ de K^* dans K^* est un homomorphisme dont le noyau (formé des $y \in K^*$ tels que $y^{q-1} = 1$, donc égal à k^*) est d'ordre $q - 1$, et dont l'image est alors effectivement d'ordre $(q^m-1)/(q-1)$, puisque K^* est lui-même d'ordre $q^m - 1$.

Notes sur le chapitre premier

Théorème de Wedderburn: pour la démonstration originale, voir Wedderburn (1905); l'idée d'utiliser (comme dans [**1**] ou [**19**]) les propriétés des polynômes cyclotomiques pour simplifier cette démonstration est due à Witt (1931).

§ **1**: la classification des corps (commutatifs) finis (« champs de Galois ») remonte essentiellement à Galois (1830).

§ **2**: le fait que le groupe multiplicatif du corps $\mathbf{F}_p$ est cyclique est dû à Euler (1760); sa démonstration utilisait les propriétés de l'« indicatrice d'Euler ». Ce résultat est un ingrédient essentiel de la théorie des restes quadratiques (Euler, Legendre, Gauss), cubiques (Jacobi, Eisenstein), biquadratiques (Gauss, Jacobi), et plus généralement des restes de puissances quelconques (Kummer, etc.); à ce sujet, voir par exemple Dickson, *History of the Theory of Numbers.*

§ **3**: les propositions 9 et 10 sont des cas particuliers du *théorème* 90 de Hilbert relatif aux extensions cycliques (voir [**10**], pp. 213-215).

CHAPITRE 2

POLYNÔMES ET IDÉAUX DE POLYNÔMES

On sait que si K est un corps *infini*, et si F est un polynôme à une ou plusieurs variables, à coefficients dans K, et *identiquement nul* sur K, alors F est *nul*: tous ses coefficients sont nuls. Ceci n'est plus vrai pour un corps fini: ainsi, sur $k = \mathbf{F}_q$, le polynôme $X^q - X$, non nul, est pourtant identiquement nul (chap. 1, sect. 1.1 et 1.2); c'est à cette particularité des corps finis qu'est consacré le présent chapitre.

Dans tout le cours de ce chapitre (ainsi que dans les chapitres suivants), k désignera un corps fini à $q = p^f$ éléments, n un entier $\geqslant 1$, $X = (X_1, ..., X_n)$ une famille de n variables, et $k[X] = k[X_1, ..., X_n]$ l'anneau des polynômes en $X_1, ..., X_n$ à coefficients dans k; d'autre part, les éléments $\mathbf{a} = (a_1, ..., a_n)$ de k^n seront appelés *points* (ou *points rationnels sur* k, si cette précision est nécessaire); si $F \in k[X]$, si $\mathbf{a}$ est un point de k^n, et si $F(\mathbf{a}) = 0$, on dira que $\mathbf{a}$ est un *zéro* de F.

§ **1.** *Polynômes réduits et polynômes identiquement nuls.*

1.1. Soit F un élément de $k[X]$.