valeur de d, la formule $n = \sum_{d \mid n} \varphi(d)$ montrerait que le nombre d'éléments de H est $< n$, contrairement à l'hypothèse. En particulier, il existe un élément $x \in \mathrm{H}$ d'ordre n, et H coïncide avec le groupe cyclique (x).

Le théorème 2 résulte du lemme 2, appliqué à $\mathrm{H} = \mathbf{F}_q^*$ et $n = q - 1$; il est en effet évident que l'équation $x^d = 1$, qui est de degré d, a au plus d solutions dans $\mathbf{F}_q$.

Remarque. — La démonstration ci-dessus montre que, plus généralement, tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

§ 2. Equations sur un corps fini

Soit q une puissance d'un nombre premier p, et soit K un corps à q éléments.

2.1. *Sommes de puissances.*

LEMME. — *Soit u un entier $\geqslant 0$. La somme $\mathrm{S}(\mathrm{X}^u) = \sum_{x \in \mathrm{K}} x^u$ est égale à 1 si u est $\geqslant 1$ et divisible par $q - 1$; elle est égale à 0 sinon.*

(On convient que $x^u = 1$ si $u = 0$, *même si* $x = 0$.)

Si $u = 0$, tous les termes de la somme sont égaux à 1, d'où $\mathrm{S}(\mathrm{X}^u) = q.1 = 0$, puisque K est de caractéristique p.

Si u est $\geqslant 1$, et divisible par $q - 1$, on a $0^u = 0$ et $x^u = 1$ si $x \neq 0$; d'où $\mathrm{S}(\mathrm{X}^u) = (q-1).1 = -1$.

Enfin, si u est $\geqslant 1$, et non divisible par $q - 1$, le fait que K^* soit cyclique d'ordre $q - 1$ (th. 2) montre qu'il existe $y \in \mathrm{K}^*$ tel que $y^u \neq 1$. On a

$$\mathrm{S}(\mathrm{X}^u) = \sum_{x \in \mathrm{K}^*} x^u = \sum_{x \in \mathrm{K}^*} y^u x^u = y^u \mathrm{S}(\mathrm{X}^u),$$

d'où $(1 - y^u).\mathrm{S}(\mathrm{X}^u) = 0$, et cela entraîne bien $\mathrm{S}(\mathrm{X}^u) = 0$.

(*Variante.* — Utiliser le fait que, si $d \geqslant 2$, la somme des racines d-ièmes de l'unité est nulle.)

2.2. *Le théorème de Chevalley.*

THÉORÈME 3 (Chevalley-Warning). — *Soient*

$$f_\alpha \in \mathrm{K}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$$

des polynômes à n variables tels que $\sum \deg(f_\alpha) < n$, et soit V *l'ensemble de leurs zéros communs dans* K^n. *On a*

$$\mathrm{Card}\,(\mathrm{V}) \equiv 0 \pmod{p}.$$

Posons $\mathrm{P} = \prod_\alpha (1 - f_\alpha^{q-1})$, et soit $x \in \mathrm{K}^n$. Si $x \in \mathrm{V}$, tous les $f_\alpha(x)$ sont nuls, et l'on a $\mathrm{P}(x) = 1$; si $x \notin \mathrm{V}$, l'un des $f_\alpha(x)$ est non nul, et $f_\alpha^{q-1}(x) = 1$, d'où $\mathrm{P}(x) = 0$. Ainsi, P est la *fonction caractéristique* de V. Si, pour tout polynôme f, on pose $\mathrm{S}(f) = \sum_{x \in \mathrm{K}^n} f(x)$, on a donc :

$$\mathrm{Card}\,(\mathrm{V}) \equiv \mathrm{S}(\mathrm{P}) \pmod{p},$$

et tout revient à montrer que $\mathrm{S}(\mathrm{P}) = 0$.

Or, l'hypothèse $\sum \deg(f_\alpha) < n$ entraîne

$$\deg(\mathrm{P}) < n(q-1);$$

donc P est combinaison linéaire de monômes

$$\mathrm{X}^u = \mathrm{X}_1^{u_1} \ldots \mathrm{X}_n^{u_n}$$

avec $\sum u_i < n(q-1)$; il suffit de prouver que, pour un tel monôme X^u, on a $\mathrm{S}(\mathrm{X}^u) = 0$. Mais cela résulte du lemme, puisque l'un au moins des u_i est $< q - 1$, c.q.f.d.

COROLLAIRE 1. — *Si $\sum \deg(f_\alpha) < n$, et si les f_α sont sans terme constant, les f_α ont un zéro commun non trivial.*

En effet, si V était réduit à $\{0\}$, on aurait $\mathrm{Card}\,(\mathrm{V}) = 1$, et Card (V) ne serait pas divisible par p.