b) *Le groupe multiplicatif* K^* *est cyclique d'ordre* $q-1$.

c) *On a* $x^{q-1}=1$ *pour tout* $x \in K^*$, *et* $x^q = x$ *pour tout* $x \in K$.

En effet, comme $\mathbf{Z}$ est infini, K ne peut être de caractéristique 0. Donc il contient $\mathbf{F}_p$, avec p premier. Ainsi K est un espace vectoriel sur $\mathbf{F}_p$; sa dimension s est finie, sinon K serait infini. En tant qu'espace vectoriel, K est isomorphe à $(\mathbf{F}_p)^s$, donc a p^s éléments. L'assertion *b*) résulte du § 6, th. 1. On en déduit aussitôt *c*).

Exemple. Appliquons *b*) à $\mathbf{F}_p$, où p est premier : il existe un entier $x \in \mathbf{Z}$ tel que $0 \leqslant x \leqslant p-1$ et que tout entier y non multiple de p soit congru modulo p à une puissance de x. On dit alors que x est *une racine primitive modulo* p. La recherche des racines primitives modulo p n'est nullement triviale. Par exemple il y a $\varphi(6)=2$ racines primitives modulo 7; ce sont 3 et 5 (en effet on a $1^2 \equiv 6^2 \equiv 1$ (mod. 7) et $2^3 \equiv 4^3 \equiv 1$ (mod. 7); seuls restent 3 et 5).

Remarque. Il résulte de *c*) qu'un corps fini K à q éléments est l'ensemble des racines du polynôme $X^q - X$ (qui n'a que q racines). On peut en déduire que deux corps finis à q éléments sont isomorphes. On note souvent $\mathbf{F}_q$ un corps fini à q éléments.

A titre d'exercice et d'intermède, nous allons démontrer un élégant théorème relatif aux équations diophantiennes sur un corps fini :

THÉORÈME 2 (Chevalley). *Soient* K *un corps fini, et* $F(X_1, \ldots, X_n)$ *un polynôme homogène de degré* d *sur* K. On suppose $d < n$. Il *existe alors un point* $(x_1, \ldots, x_n) \in K^n$ *distinct de l'origine* $(0, \ldots, 0)$ *tel que* $F(x_1, \ldots, x_n)=0$.

Étant donnés un corps K et un entier j, on dit que K est un *corps* C_j si tout polynôme homogène sur K de degré d et à n variables, *tel que* $n > d^j$, admet un zéro non trivial (i.e. distinct de l'origine) dans K^n. Les corps C_0 sont les corps algébriquement clos. Le théorème de Chevalley exprime que les corps finis sont C_1 (on dit aussi « quasi-algébriquement clos »). On montre que, si K est un corps C_j, le corps $K(T)$ des fractions rationnelles à une variable sur K et le corps $K((T))$ des séries formelles à une variable sur K sont des corps C_{j+1} ([5]). On s'est longtemps demandé si les corps p-adiques sont C_2, et on a récemment montré qu'il n'en est rien ([8]).

Démontrons le th. 2. Notons q le cardinal de K et p sa caractéristique (de sorte que $q = p^s$). Soit $V \subset K^n$ l'ensemble des zéros de F, i.e. des points $(x_1, \ldots, x_n) \in K^n$ tels que $F(x)=0$ (nous employons, ici et dans la suite, l'écriture vectorielle où x désigne un point $(x_1, \ldots, x_n)$ de K^n). D'après le th. 1, *c*), on a $F(x)^{q-1}=0$ pour $x \in V$, et $F(x)^{q-1}=1$ pour $x \in K^n - V$; ainsi le polynôme $G(x) = F(x)^{q-1}$ est une *fonction caractéristique de* $K^n - V$, à valeurs dans $\mathbf{F}_p$. Le nombre modulo p de points de $K^n - V$ sera donc donné par la somme $\sum_{x \in K^n} G(x)$; nous allons calculer cette somme et montrer qu'elle est *nulle*. Alors card $(K^n - V)$ sera multiple de p; comme card $(K^n) = q^n = p^{ns}$ est aussi multiple de p,

card (V) sera multiple de p; comme V contient déjà l'origine, il contiendra nécessairement d'autres points, car $p \geqslant 2$; le th. 2 sera ainsi démontré.

Calculons donc $\sum_{x \in K^n} G(x)$. Le polynôme G est combinaison linéaire de monômes $M_\alpha(X) = X_1^{\alpha_1} \ldots X_n^{\alpha_n}$; et on est ramenés à calculer $\sum_{x \in K^n} M_\alpha(x) = \sum_{x \in K^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n} = \left(\sum_{x_1 \in K} x_1^{\alpha_1}\right) \ldots \left(\sum_{x_n \in K} x_n^{\alpha_n}\right)$. Il s'agit donc de calculer des sommes de la forme $\sum_{z \in K} z^\beta (\beta \in \mathbf{N})$.

(*a*) Pour $\beta = 0$, on a $z^\beta = 1$ pour tout $z \in K$, et la somme vaut $q = 0$;

(*b*) Pour $\beta > 0$, le terme 0^β est nul, et la somme se réduit à $\sum_{z \in K^*} z^\beta$. Or K^* est un groupe cyclique d'ordre $q-1$ (th. 1, *b*); soit ω un générateur de celui-ci. Alors $\sum_{z \in K^*} z^\beta = \sum_{j=0}^{q-2} \omega^{\beta j}$, qui est la somme d'une progression géométrique. Donc:

(*b'*) Si la raison ω^β est $\neq 1$, c'est-à-dire si β n'est pas multiple de $q-1$, on a $\sum_{j=0}^{q-2} \omega^{\beta j} = \dfrac{\omega^{\beta(q-1)} - 1}{\omega^\beta - 1} = 0$ (car $\omega^{q-1} = 1$).

(*b''*) Si $\omega^\beta = 1$, c'est-à-dire si β est multiple de $q-1$, on a

$$\sum_{j=0}^{q-2} \omega^{\beta j} = q - 1.$$

Il résulte de (*a*), (*b'*) et (*b''*) que $\sum_{x \in K^n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ est nul *sauf si* tous les α_i sont > 0 et multiples de $q-1$. Le degré $\alpha_1 + \cdots + \alpha_n$ du monôme est, dans ce cas, $\geqslant (q-1)n$. Mais, comme $G = F^{q-1}$, G est de degré $(q-1)d$, et on *a* $(q-1)d < (q-1)n$ d'après l'hypothèse. On a donc $\sum_{x \in K^n} M_\alpha(x) = 0$ pour tout monôme $M_\alpha(X)$ qui figure dans G avec coefficient non nul. D'où, par addition, $\sum_{x \in K^n} G(x) = 0$. Nous avons vu que cette relation entraîne notre conclusion.

On remarquera qu'il aurait, au lieu de supposer F homogène, suffit de supposer F sans terme constant. Naturellement l'inégalité *stricte* $d < n$ entre degré et nombre de variables est essentielle. Par exemple la *norme* de $\mathbf{F}_q n$ à $\mathbf{F}_q$ (cf. chap. II, § 6) fournit un polynôme homogène de degré n et à n variables sur $\mathbf{F}_q$ qui n'a d'autre zéro que l'origine.

Un exemple. Une forme quadratique à 3 variables sur un corps *fini* K « représente 0 » (i.e. a un zéro non trivial). En passant de K^3 au plan projectif $P_2(K)$, ceci veut dire qu'une *conique* sur K admet un point rationnel sur K (i.e. dont les coordonnées homogènes peuvent être choisies dans K). L'exemple de la conique $x^2 + y^2 + z^2 = 0$ sur $\mathbf{R}$ (resp. $x^2 + y^2 - 3z^2 = 0$ sur $\mathbf{Q}$; pour s'assurer que $x^2 + y^2 - 3z^2 = 0$ n'a pas de solution non triviale dans $\mathbf{Q}$, on se ramène au cas où x, y, z sont des entiers premiers entre eux, et on réduit modulo 4) montre qu'il ne s'agit pas d'une propriété vraie sur tout corps.