M1 arithmétique; rappels sur les corps finis.
J-F. Mestre.

1 Extensions de corps

Définition.- *Soit k et K deux corps; on dit que K est une* **extension** *de k si k est un sous-corps de K; c'est une* **extension finie** *de k si le k-espace vectoriel K est de dimension finie. Le* **degré** *de l'extension est alors la dimension du k-espace vectoriel K.*

On note parfois K/k l'extension K de k. Attention: il ne s'agit pas d'un quotient !

Proposition.- *Si L est une extension finie de K de degré n et K une extension finie de k de degré m, L est une extension finie de k de degré nm.*

Proposition et définition.- *Soit K une extension finie d'un corps k, α un élément de K, et $f:\ k[X] \to K$ l'application définie par $f(P) = P(\alpha)$; f est une application k-linéaire, et un morphisme d'anneaux non injectif; le générateur unitaire P_α de $\ker f$ s'appelle le* **polynôme minimal de** *α, c'est un polynôme irréductible, et le* **degré** *de α (dans l'extension K/k) est le degré de P_α.*

De plus, $f(k[X])$ est un sous-corps de K, isomorphe au corps $k[X]/(P_\alpha)$. C'est une extension de degré égal au degré de α. En particulier, pour tout $x \in K$, le degré de x divise le degré de l'extension K/k.

Il est clair que f est une application k-linéaire. Elle n'est pas injective, car $k[X]$ est de dimension infinie, et K de dimension finie; de même, il est clair que f est un morphisme d'anneaux; n'etant pas injectif, son noyau $\ker f$ n'est pas réduit à $\{0\}$, et il existe donc un unique polynôme unitaire l'engendrant. C'est le polynôme unitaire de $k[X]$ de plus petit degré s'annulant sur α, il est donc irréductible.

2 Anneaux quotients de polynômes

Soit k un corps, $P = \sum_{i=0}^{n} a_i X^i$ un élément de $k[X]$ de degré $n \geq 1$, A l'anneau quotient $k[X]/(P)$, et $\rho:\ k[X] \to A$ le morphisme d'anneau qui à tout $Q \in k[X]$ associe sa classe modulo P; A est un k-e.v. de dimension n, admettant comme base $\{1, \alpha, \ldots, \alpha^{n-1}\}$, où $\alpha = \rho(X)$. Le morphisme ρ restreint à k est injectif, et dans ce qui suit on identifie k à son image $\rho(k)$; pour tout polynôme constant $a \in k[X]$, par abus de notation, on note donc a, plutôt que $\rho(a)$, son image dans A par ρ.

Remarque importante.- Comme $\ker \rho = (P)$, on a

$$0 = \rho(P) = \sum \rho(a_i)\rho(X)^i = \sum a_i \alpha^i = P(\alpha)$$

donc l'élément α de A est une racine du polynôme P.

En particulier, si P est irréductible, A est un corps, contenant k après l'identification précédente; c'est donc une extension de k de degré n.

Soit P un polynôme irréductible de $k[X]$. On a ainsi construit une extension K de k, à savoir $k[X]/(P)$, dans lequel le polynôme P a une racine, à savoir $\alpha = \rho(X)$.

Proposition.- *Soit k un corps, et $P \in k[X]$ un polynôme de degré $n \geq 1$. Il existe une extension de K dans laquelle P est scindé (i.e. produit de polynômes de degré 1).*

La démonstration se fait par récurrence sur n, le cas $n = 1$ étant trivial; on suppose la proposition démontrée pour $n - 1$; soit $Q \in k[X]$ un facteur irréductible de P. D'après ce qui précède, il existe une extension K de k dans laquelle Q a une racine α; il existe donc $P_1 \in K[X]$, de degré $n - 1$, tel que $P(X) = (X - \alpha)P_1(X)$. D'après l'hypothèse de récurrence, il existe une extension L de K où P_1 est scindé; L est donc une extension de k où P est scindé.

3 Corps finis

Dans ce qui suit, p est un nombre premier. On note $\mathbf{F}_p$ le corps $\mathbf{Z}/p\mathbf{Z}$.

Proposition.- *Si k un corps fini de caractéristique p, il existe n tel que son cardinal est p^n.*

En effet, k est un e.v. de dimension finie sur $\mathbf{F}_p$.

Proposition.- *Soit k un corps de caractéristique p; l'application $F : k \to k$ définie par $F(x) = x^p$, appelée le Frobenius, est un morphisme d'anneaux injectif, et bijectif dès que k est fini.*

Pour $1 \leq i \leq p - 1$, le coefficient du binôme C_p^i est divisible par p (par exemple parce que $iC_p^i = pC_{p-1}^{i-1}$.) Donc pour tous $x, y \in k$, $(x + y)^p = x^p + y^p$.

Corollaire.- *Soit k un corps de caractéristique p, n un entier, et $q = p^n$. L'application $G : k \to k$ définie par $x \mapsto x^q$ est un morphisme d'anneaux injectif, et bijectif dès que k est fini.*

En effet, $G = F^n$.

Dans ce qui suit, n est un entier fixé, et on pose $q = p^n$.

Proposition.- *Soit K un corps de cardinal q; le groupe multiplicatif K^* est cyclique, et les éléments de K sont les q racines du polynôme $X^q - X$.*

K^* étant fini, il est cyclique. De plus, K^* ayant $q - 1$ éléments, pour tout $x \in K$, on a $x^{q-1} = 1$. Tout élément de K^* est donc racine de $X^{q-1} - 1$, et donc tout élément de K est racine de $X^q - X$, qui a donc au moins q racines; étant de degré $\leq q$, il a au plus q racines; il en a donc q.

Théorème.- *Il existe un corps fini de cardinal q.*

Soit une extension L de $\mathbf{F}_p$ où le polynôme $P = X^q - X$ est scindé, et soit $K \subset L$ l'ensemble des racines de P. Comme $P' = -1$, les racines de P

sont simples, et K a q éléments; K étant le noyau du morphisme de groupes $\phi : (L,+) \to (L,+)$ défini par $x \mapsto F^q(x) - x$, c'est un sous-groupe de $(L,+)$; K^*, étant le noyau du morphisme de groupes $\psi : L^* \to L^*$ défini par $x \mapsto x^{q-1}$, est un sous-groupe de $(L^*, \times)$; K est donc un corps à q éléments.

Proposition.- *Tout polynôme $P \in \mathbf{F}_p[X]$ irréductible de degré n divise $X^q - X$.*

Soit $K = \mathbf{F}_p[X]/(P)$, qui est un corps à q éléments. L'image du polynôme $X^q - X$ par l'application $f : \mathbf{F}_p[X] \to \mathbf{F}_p[X]/(P)$ est nulle, donc $X^q - X$ est un élément du noyau de f, *i.e.* un multiple de P.

Proposition.- *Soit K un corps à q éléments. Il existe un polynôme irréductible $P \in \mathbf{F}_p[X]$, de degré n, tel que K est isomorphe à $\mathbf{F}_p[X]/(P)$.*

Soit $\alpha \in K$ un générateur du groupe cyclique K^*, et $P \in \mathbf{F}_p[X]$ son polynôme minimal. Le morphisme d'anneaux $f : \mathbf{F}_p[X] \to K$ défini par $f(Q) = Q(\alpha)$ est surjectif, tout élément de K étant l'image d'un monôme. Par suite, K est isomorphe au corps $\mathbf{F}_p[X]/(P)$, qui est donc de degré n, comme K.

Théorème.- *Soit L un corps à q éléments. Si K est un sous-corps de L, son degré est un diviseur de n. Réciproquement, si d est un diviseur de L, il existe un unique sous-corps de L de cardinal p^d; c'est l'ensemble des racines du polynôme $X^{p^d} - X$.*

Si d divise n, $p^d - 1$ divise $p^n - 1 = q - 1$, donc $X^{p^d-1} - 1$ divise $X^{q-1} - 1$ et $X^{p^d} - X$ divise $X^q - X$, qui est scindé dans L; il en est donc de même de $X^{p^d} - 1$, dont les racines forment un sous-corps à p^d éléments de L.

Théorème.- *Soit L un corps à q éléments, et $P \in \mathbf{F}_p[X]$ un polynôme irréductible de degré d. Les assertions suivantes sont équivalentes:*
i) d divise n.
ii) P est scindé dans L.
iii) P a une racine dans L.
iv) $\mathbf{F}_p[X]/(P)$ est isomorphe à un sous-corps de L.

Si i) est vrai, le polynôme $X^{p^d} - X$ est scindé dans L, donc P aussi, d'où ii), qui implique trivialement iii). Si iii) est vrai, et si α est une racine de P, P est le polynôme minimal de α, et $\mathbf{F}_p[X]/(P)$ est un sous-corps de L, d'où iv); si iv) est vrai, comme $\mathbf{F}_p[X]/(P)$ est de degré d sur $\mathbf{F}_p$, on a i).

Théorème.- *Deux corps finis de même cardinal sont isomorphes.*

Soit K et L deux corps à q éléments; il existe $P \in \mathbf{F}_p[X]$ de degré n tel que K est isomorphe à $\mathbf{F}_p[X]/(P)$, qui, d'après ce qui précède, est isomorphe à un sous-corps de L, de même cardinal que L, donc à L.

Remarque.- *On note souvent $\mathbf{F}_q$ un corps fini à q éléments.*