ACCQ204 Décembre 2015

Enseignant: Aslan Tchamkerten *Crédit: Wenceslas Godel*

Intermède algébrique

1 Corps finis

$F = (S, +, \cdot)$

1. $+$ et $\cdot$ satisfont certaines conditions:
   - fermés,
   - commutatifs,
   - et admettent des identités ("0" pour $+$ et "1" pour $\cdot$).
2. Inverses: $\forall\ a \in S \Rightarrow$ unique inverse -a
   $\forall\ a \neq 0 \in S \Rightarrow$ unique inverse a^{-1}.
3. Distributivité: $a \cdot (a + b) = ab + ac$.

Theorem 1 *Tout corps fini a cardinalité p^s où p est un nombre entier et $s \geq 1$ entier.*

Exemple 2 $F = (\{0, 1\}, +, \cdot)$
$F = (\{0, 1, \ldots, p-1\}, +_p, \cdot_p)$ *Les opérations sont réalisées modulo p.*

Theorem 3 $\forall q = p^s\ \exists!$ *corps avec q éléments (sans compter les isomorphismes).*

Remarque $(S, \cdot, +)$ et $(S', \odot, \oplus)$
ϕ isomorphisme
$\phi : S \longrightarrow S'$ conserve les opérations.

Theorem 4 *Tout corps fini a un élément π, appelé élément "primitif" de F tq. $S = \{0, \pi^0, \pi^1, \ldots, \pi^{q-2}\}$.*

2 Polyômes et corps finis

Definition 5 *Étant donné F_q, on définit $F_q[X] = \{\sum_0^\infty \alpha_i X^i, \alpha_i \in F_q\}$.*

Definition 6 *$P(X) = \sum_1^d \alpha_i X^i, \alpha_d \neq 0$, d est le degré de P(X).*

Exemple 7 *Les $F_q[X]$ avec les lois d'addition et de multiplication sont des anneaux.*

Definition 8 *$\alpha \in F_q$ est une racine de P(X) si $P(\alpha) = 0$.*

Theorem 9 (Fondamental de l'algèbre) *Un polynôme non nul de degré d a au plus d racines (peu importe F_q).*

Definition 10 *$P(X) \in F_q[X]$ est dit "irréductible" si pour tout $Q_1(X), Q_2(X) \in F_q[X]$ tq. $Q_1(X) \cdot Q_2(X) = P(X)$, on a $min(deg(Q_1), deg(Q_2)) = 0$.*

Remarque Les polynômes irréductibles sur l'ensemble des polynômes jouent le même rôle que les nombres premiers sur l'ensemble des entiers.

Exemple 11 *$X^2 + X + 1$ irréductible sur F_2.*
$X^2 + 1 = (X + 1) \cdot (X + 1)$ n'est pas irréductible sur F_2.

3 Extensions d'un corps

$F_q \longrightarrow F_q^m \overset{isomorphe}{\leftrightarrow} F_{q^m}$.
Avec F_{q^m} on n'insiste plus sur la représentation vectorielle mais polynômiale.
$F_q^m = \{(\alpha_0, \alpha_1, \ldots, \alpha_{m-1})\}, \forall i, \alpha_i \in F_q$.
E(X) est un polynôme irréductible de degré m.
$+ : (\alpha_0, \alpha_1, \ldots, \alpha_{m-1}) \times (\beta_0, \beta_1, \ldots, \beta_{m-1}) \longmapsto (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \ldots, \alpha_{m-1} + \beta_{m-1})$
On peut considérer commme représentation alternative: $P(X) = \sum_0^{m-1} \alpha_i X^i$.
Alors l'addition des polyômes revient à l'addition des vecteurs.
$\cdot$: multiplication des polyômes modulo E(X).
Cela nous assure que l'on reste dans l'ensemble des polyômes de degré m-1.
On note $F/E(X)$.
Remarque Si $|F| < \infty$, $\exists$ des polyômes irréductibles de n'importe quel degré.