Corps finis

CloudSea

Cadre

On sait qu'un corps fini est une extension de $\mathbb{F}_p$ de degré fini n donc à $q = p^n$ éléments
On montre que le corps de décomposition de $X^q - X$ est l'unique corps fini à q éléments, qu'on note alors $\mathbb{F}_q$
On montre ensuite que $\mathbb{F}_q^\times$ est cyclique, et on en déduit une 2e construction comme corps de rupture d'un polynôme irréductible de degré n

Recasages :
- [[120 Anneau Z sur nZ]]
- [[123 Corps finis]]
- [[125 Extensions de corps]]
- [[141 Polynômes irréductibles]]
- [[144 Racines de polynômes]]

Backup
- [[121 Nombres premiers]] a mettre dans le plan mais pas en faire un DEV

Références : Perrin et Algèbre I de Daniel Guin

Déroulé du développement

Construction avec le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$

Soit $P = X^q - X \in \mathbb{F}_p[X]$ et soit K un corps de décomposition de P
On a $P' = qX^{q-1} - 1 = 0 - 1 = -1$ donc P est simplement scindé sur K, soit E l'ensemble des q racine de P dans K, montrons que E est un sous corps de K

Il est clair que $0, 1 \in E$
Soient $\alpha, \beta \in E$ on a

$$\begin{aligned} P(\alpha-\beta) &= (\alpha-\beta)^q - \alpha + \beta \\ &= \alpha^q - \beta^q - \alpha + \beta \\ &= 0 + 0 \\ &= 0 \end{aligned}$$

Donc $\alpha - \beta \in E$

Et si $\beta \neq 0$

$$\begin{aligned} P(\alpha\beta^{-1}) &= (\alpha\beta^{-1})^q - \alpha\beta^{-1} \\ &= \alpha^q(\beta^q)^{-1} - \alpha\beta^{-1} \\ &= \alpha\beta^{-1} - \alpha\beta^{-1} \\ &= 0 \end{aligned}$$

Donc $\alpha\beta^{-1} \in E$
Donc E est bien un corps

Donc E est un corps de décomposition de P inclus dans K donc $E = K$, donc K est bien un corps fini à q éléments

Réciproquement si K est un corps fini à q éléments, pour tout $x \in K$ on a $x^q = x$ donc $P(x) = 0$. Donc K est un corps de décomposition de P

Donc il existe un unique corps fini à q éléments qu'on va noter $\mathbb{F}_q$

Montrer que $n = \sum_{d|n} \varphi(d)$

On se place sur $\mathbb{Z}/n\mathbb{Z}$
$\mathbb{Z}/n\mathbb{Z}$ admet un unique sous groupe d'ordre d, qu'on va noter H
H est cyclique, donc il est isomorphe à $\mathbb{Z}/d\mathbb{Z}$
Donc les éléments d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ sont les éléments d'ordre d de H, donc les $\varphi(d)$ générateurs de $\mathbb{Z}/d\mathbb{Z}$
Donc en partitionnant $\mathbb{Z}/n\mathbb{Z}$ selon l'ordre des éléments, on obtient bien $n = \sum_{d|n} \varphi(d)$

Montrer que tout sous groupe fini de $K^\times$ est cyclique

Soit K un corps et G un sous groupe fini de $K^\times$ de cardinal n
Pour d diviseur de n, soit $N(d)$ le nombre d'éléments de G d'ordre d, on va montrer que $N(d) = 0$ ou $\varphi(d)$

Si $N(d) \neq 0$, soit x d'ordre d et $H = \langle x \rangle$
H est d'ordre d, donc H contient les d racines du polynôme $X^d - 1$. Donc pour tout $y \notin H$, y n'est pas racine de $X^d - 1$, donc en particulier y n'est pas d'ordre d
Donc les éléments d'ordre d de G sont les éléments d'ordre d de H, donc comme H est cyclique il y en a $\varphi(d)$

Donc $n = \#G = \sum_{d|n} N(d)$, donc comme $n = \sum_{d|n} \varphi(d)$, on a pour tout d $N(d) = \varphi(d)$
En particulier $N(n) = \varphi(n) > 0$, donc G est bien cyclique

Construction avec le corps de rupture

On a vu que $\mathbb{F}_q^\times$ est cyclique, soit α un générateur
On a alors $\mathbb{F}_q = \mathbb{F}_p(\alpha)$, donc $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$, donc $\deg(\mu_\alpha) = n$
Donc pour tout n il existe un polynôme irréductible sur $\mathbb{F}_p$ de degré n, donc on peut aussi construire $\mathbb{F}_q$ comme le corps de rupture d'un tel polynôme, et c'est comme ça qu'on fait en pratique pour manipuler les corps finis avec des ordinateurs

Détail de certains points

Montrer que $\mathbb{Z}/n\mathbb{Z}$ admet un unique sous groupe d'ordre d (où d est un diviseur de n)

Soit $x = \overline{n/d} \in \mathbb{Z}/n\mathbb{Z}$
On a $dx = \overline{n} = 0$, et pour $0 < k < d$ on a $0 < k\frac{n}{d} < n$ donc $kx \neq 0$. Donc x est d'ordre d, donc $\mathbb{Z}/n\mathbb{Z}$ admet bien un sous groupe d'ordre d (à savoir $\langle x \rangle$). Reste à montrer que c'est le seul

Soit H un sous groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d, montrons que $H = \langle x \rangle$
H est un sous groupe d'un groupe cyclique, donc H est cyclique. Soit $\overline{k}$ un générateur de H avec $0 \leq k < n$
Soit p le pgcd de n et k. p divise k donc $H \subseteq \langle \overline{p} \rangle$. Et Bézout donne u, v tels que $p = nu + kv$.
Donc dans $\mathbb{Z}/n\mathbb{Z}$ on obtient $\overline{p} = 0 + v\overline{k} \in H$, donc $\langle \overline{p} \rangle \subseteq H$, donc $H = \langle \overline{p} \rangle$
Or p divise n, donc $\overline{p}$ est d'ordre n/p. Donc comme H est d'ordre d, on a $d = n/p$, donc $p = n/d$. Donc on a bien $H = \langle x \rangle$

Version révisions

On se propose de donner deux constructions des corps finis

Soit $q = p^n$, on considère le polynôme $P = X^q - X$ sur $\mathbb{F}_p$

1. Montrer que P est simplement scindé sur son corps de décomposition K
2. Soit E l'ensemble des racines de P sur K, montrer que E est un corps
3. En déduire que K est un corps fini à q éléments
4. Réciproquement montrer qu'un corps fini à q éléments est nécessairement un CDD de P

Deuxième construction
Soit K un corps et G un sous groupe fini de K^* de cardinal n. Pour d divisant n, soit $N(d)$ le nombre d'éléments de G d'ordre d

5. Montrer que $n = \sum_{d|n} \varphi(d)$
6. Montrer que $N(d) = 0$ ou $\varphi(d)$
7. En déduire à partir de la 5. qu'en fait $N(d) = \varphi(d)$
8. En déduire que G est cyclique
9. Revenons à $\mathbb{F}_q$, montrer qu'il existe un polynôme irréductible sur $\mathbb{F}_p$ dont $\mathbb{F}_q$ est le corps de rupture