Quelques réflexions et exercices sur la leçon : “Corps finis. Applications.”

Richard Leroy

richard.leroy@univ-rennes1.fr
http ://perso.univ-rennes1.fr/richard.leroy/

Préparation à l'agrégation de Mathématiques 2008
Université de Rennes 1

1 Quelques remarques

On commence par quelques remarques sur le plan présenté mercredi.

1. Attention, on ne parle de corps de rupture que pour un polynôme irréductible.
2. Le groupe multiplicatif $\mathbb{F}_q^*$ est cyclique, d'ordre $q-1$, isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$: attention, la loi de groupe pour ce dernier est additive.
3. Une partie sur l'arithmétique sur $\mathbb{F}_q$ est plus qu'envisageable. On pourra y mentionner l'étude des carrés modulo q, la loi de réciprocité quadratique.Il est essentiel de savoir qu'en caractéristique 2, tout élément est un carré (se rappeler de la définition comme corps de décomposition !).
4. Il est important de noter qu'un corps fini n'est jamais algébriquement clos (pourquoi ?), et de connaître sa clôture algébrique, comme il est important de savoir à quelle condition $\mathbb{F}_q \subset \mathbb{F}_{q'}$ (d'ailleurs, quel sens donner à cette inclusion ?).
5. Dans la partie sur les polynômes irréductibles, on peut aussi penser au critère d'Eisenstein.
6. On dispose également d'un test d'irréductibilité dans $\mathbb{F}_q[X]$ ($q = p^n$) : $\mathbb{F}_q[X]$ de degré d est irréductible si et seulement si f vérifie les deux conditions suivantes :

$$\forall k < n, k \mid n,\ \operatorname{pgcd}\left(f, T^{q^k} - T\right) = 1$$
$$f \mid \left(T^{q^d} - T\right)$$

C'est le test de Rabin (1980).

• Le test de Butler (1954) affirme quant à lui que f est irréductible si et seulement si

$$\dim \ker(\text{F-Id}) = 1$$

où F est l'endomorphisme de $E := \mathbb{F}_q[X]/(f)$ défini par :

$$\begin{array}{rccc} F & : & E & \to & E \\ & & x & \mapsto & x^q \end{array}$$

La preuve de l'algorithme de Berlekamp utilise ce résultat.

7. Concernant l'algorithme de Berlekamp, on l'utilise sur des polynômes séparables (*ie* dont les racines dans une extension algébriquement close sont simples). On considère pour cela le quotient $\dfrac{f}{\text{pgcd}(f, f')}$, qui est séparable si f' n'est pas nul. Il est important de noter que l'on peut très bien avoir $f' = 0$, et dans ce cas, $f = g^p$ pour un certain polynôme $g \in \mathbb{F}_q[X]$. Ceci est dû au fait que les corps finis sont parfaits.
On revoit le lecteur à Objectif Agrégation par exemple.
8. La factorisation du polynôme cyclotomique Φ_{p^r-1} sur $\mathbb{F}_p$ (algorithme de Berlekamp) fournit effectivement des polynômes irréductible de degré r tous différents, ce qui permet de construire explicitement le corps $\mathbb{F}_{p^r}$. Cependant, en pratique, on préfère souvent l'approche consistant à tirer au hasard des polynômes de degré r et à tester leur irréductibilité.
9. La formule d'inversion de Möbius fournit l'égalité (pour $n \geq 1$) :

$$I_q^n = \frac{1}{n} \sum_{d|n} q^d \mu\left(\frac{n}{d}\right),$$

ce qui implique en particulier l'existence de polynômes irréductibles unitaires de tout degré $n \geq 1$ dans $\mathbb{F}_q[X]$. On pourra mettre ce résultat en parallèle avec les cas $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
10. Une structure du plan peut être :
    (a) Structure des corps finis (Wedderburn, caractéristique, Frobenius, existence et unicité, clôture algébrique, inclusion des corps finis, groupe multiplicatif)
    (b) Arithmétique dans les corps finis (carrés, réciprocité quadratique, Chevalley-Warning)
    (c) Polynômes sur les corps finis
    (d) Codes correcteurs d'erreurs

2 Quelques exercices

1. Montrer que tout anneau intègre fini est un corps.
2. Montrer qu'un corps fini n'est jamais algébriquement clos.
3. Montrer qu'en caractéristique 2, tout élément est un carré.
4. Le théorème de Chevalley-Warning est un résultat sur le nombre de solutions d'un système polynomial sur un corps fini. Quelle est la situation sur d'autres corps ($\mathbb{R}$, ou $\mathbb{C}$ par exemple) ?
5. Montrer que toute quadrique projective de $\mathbb{F}_q$ (q impair) en $n \geq 3$ variables est non vide.
6. Montrer que pour tout nombre premier p, Φ_p est irréductible sur $\mathbb{Q}$.
7. Montrer que $\mathbb{F}_p(T)$ n'est pas parfait (on pourra considérer le polynôme $X^p - T \in (\mathbb{F}_p(T))[X]$).
8. Soient $a, b, c \in \mathbb{Z}$ dont aucun n'est un carré dans $\mathbb{Z}$, et tel que le produit abc soit un carré dans $\mathbb{Z}$.
   Donner un exemple d'un tel triplet.
   Soit $P = \left(X^2 - a\right)\left(X^2 - b\right)\left(X^2 - c\right)$.
   Montrer que P n'a pas de racine dans $\mathbb{Q}$, mais qu'il en a dans tout $\mathbb{F}_p$.

3 Références

- La page de Pascal Boyer (http ://www.math.jussieu.fr/ boyer/) mérite d'être consultée. Elle contient des indications et des exercices sur plusieurs leçons d'algèbre, notamment celle-ci.
- L'algorithme de Berlekamp est bien expliqué dans Objectif Agrégation.
- Le Perrin et le Demazure sont des valeurs sûres pour cette leçon.