

Jeudi : Corps finis

Cours de remise à niveau MPRI 2005–2006

David A. Madore
david.madore@ens.fr

22 septembre 2005

Programme du cours

- ▶ Lundi : Entiers (\mathbb{Z})
- ▶ Mardi : Entiers modulaires ($\mathbb{Z}/n\mathbb{Z}$)
- ▶ Mercredi : Polynômes ($k[t]$)
- ▶ Jeudi : Corps finis (\mathbb{F}_q)
- ▶ Vendredi : Extensions de corps (K/k)

9h30 à 11h30 ; salle 0D1 du 19 au 22, 1C1 le 23

Jeudi : Corps finis

David Madore

Programme du
cours

Table des matières

Existence et
unicité

Corps finis et
polynômes

La loi de
réciprocité
quadratique

Table des matières

Existence et unicité

Corps finis et polynômes

La loi de réciprocité quadratique

Jeudi : Corps finis

David Madore

Programme du
cours

Table des matières

Existence et
unicité

Corps finis et
polynômes

La loi de
réciprocité
quadratique

Corps premier d'un corps fini

Si \mathbb{F} est un corps fini, on appelle **corps premier** de \mathbb{F} l'image de \mathbb{Z} dans \mathbb{F} (rappel : il y a un unique morphisme d'anneaux $\mathbb{Z} \rightarrow \mathbb{F}$).

Cette image est un *sous-anneau* de \mathbb{F} , et puisque c'est un anneau intègre fini, c'est un corps.

Comme c'est un *quotient* de \mathbb{Z} , il est de la forme $\mathbb{Z}/p\mathbb{Z}$ pour un nombre premier p qui est la **caractéristique** de \mathbb{F} .

Le corps \mathbb{F} est alors un *espace vectoriel* sur $\mathbb{Z}/p\mathbb{Z}$: si d est sa dimension, on a donc

$$\#\mathbb{F} = p^d$$

On note souvent implicitement $q = \#\mathbb{F}$ le cardinal d'un corps fini et p sa caractéristique, dont q est donc une puissance.

Unicité du corps à q éléments

Si \mathbb{F} est un corps fini à q éléments, son *groupe multiplicatif* \mathbb{F}^\times (ensemble des éléments non nuls) est d'ordre $q - 1$, donc tout $x \in \mathbb{F}$ non nul vérifie $x^{q-1} = 1$. En multipliant par x et en vérifiant pour $x = 0$, on voit que tout $x \in \mathbb{F}$ vérifie le « petit théorème de Fermat » (généralisé),

$$x^q = x$$

Tout corps fini \mathbb{F} à $q = p^d$ éléments se plonge dans la *clôture algébrique* $\bar{\mathbb{F}}$ de $\mathbb{Z}/p\mathbb{Z}$ (qui est celle de \mathbb{F}). En admettant son unicité, on a

$$\mathbb{F} = \{x \in \bar{\mathbb{F}} : x^q = x\}$$

ce qui montre l'unicité du corps à q éléments (à *isomorphisme près* ou bien *dans tout corps plus gros*).

Si E est un corps de caractéristique p , l'application

$$\text{Fr}: x \mapsto x^p$$

s'appelle **(morphisme de) Frobenius**.

On a $\text{Fr}(x + y) = \text{Fr}(x) + \text{Fr}(y)$ (car tous les coefficients C_p^i pour $0 < i < p$ sont multiples de p donc nuls dans E) et $\text{Fr}(xy) = \text{Fr}(x) \text{Fr}(y)$ (clair) : donc Fr est un morphisme (d'anneaux, de corps)...

Pour $q = p^d$, on note Fr_q ou Fr^d le composé d -ième de Fr , soit $x \mapsto x^q$, parfois aussi appelé morphisme de Frobenius.

Existence du corps à q éléments

Soit $q = p^d$, et $\bar{\mathbb{F}}$ une clôture algébrique de \mathbb{F}_p (dont on admet l'existence). Alors

$$\mathbb{F}_q := \{x \in \bar{\mathbb{F}} : x^q = x\}$$

est un *sous-anneau* de $\bar{\mathbb{F}}$; si $x \in \mathbb{F}_q$ est non nul, alors x^{q-2} est son inverse, donc \mathbb{F}_q est en fait un *sous-corps* de $\bar{\mathbb{F}}$.

Comme la dérivée du polynôme $t^q - t \in \mathbb{F}_p[t]$ est -1 , donc ne s'annule jamais, ses racines dans $\bar{\mathbb{F}}$ sont *distinctes* de sorte que $\#\mathbb{F}_q = q$.

Il existe donc bien un corps à q éléments pour tout $q = p^d$.

Inclusion entre les \mathbb{F}_q

Si d, d' sont deux naturels non nuls tels que $d \mid d'$, alors, en posant $q = p^d$ et $q' = p^{d'}$, on a $q' = q^{d'/d}$, donc $\text{Fr}_{q'} = (\text{Fr}_q)^{d'/d}$. En particulier, si x est fixe par Fr_q , il est fixe par $\text{Fr}_{q'}$, donc : $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$.

Si d et d' sont tels que $\text{pgcd}(d, d') = d_0$, alors on peut écrire $sd + s'd' = d_0$ (Bézout), donc pour $q = p^d$ et $q' = p^{d'}$ et $q_0 = p^{d_0}$ on a $(x^{q^s})^{q'^{s'}} = x^{q_0}$. Ceci prouve : $\mathbb{F}_q \cap \mathbb{F}_{q'} = \mathbb{F}_{q_0}$ (dans tout corps contenant).

Exemple : \mathbb{F}_4 n'est pas contenu dans \mathbb{F}_8 : tous deux sont contenus dans \mathbb{F}_{64} et leur intersection est réduite à $\mathbb{F}_2 = \{0, 1\}$.

Bilan : Les corps finis contenant \mathbb{F}_q sont les \mathbb{F}_{q^e} pour $e \in \mathbb{N}^*$.

Existence d'éléments primitifs

Soit $q = p^d$. L'ordre du groupe \mathbb{F}_q^\times est $q - 1$.

Soit ℓ un nombre premier divisant $q - 1$ et $r = v_\ell(q - 1)$

l'exposant de ℓ dans $q - 1$. Parmi les ℓ^r racines de $t^{\ell^r} - 1 = 0$ (toutes sont dans \mathbb{F}_q), il y en a au plus ℓ^{r-1} qui sont racines de $t^{\ell^{r-1}} - 1 = 0$, donc il existe au moins un élément d'ordre exactement ℓ^r dans \mathbb{F}_q^\times .

En écrivant $q - 1$ comme produit de tels ℓ^r (premiers entre eux!), on en déduit l'existence d'un élément d'ordre $q - 1$ dans \mathbb{F}_q^\times , qui l'engendre donc. Un tel élément est dit **primitif**. On a prouvé :

Théorème : Le groupe multiplicatif d'un corps fini est cyclique.

Le nombre d'éléments primitifs est, bien sûr, $\varphi(q - 1)$.

Fait : Soit $x \in \mathbb{F}_{q^e}$. Alors x est racine d'un unique polynôme irréductible (unitaire) sur \mathbb{F}_q , qui est de degré $\leq e$.

Démonstration : Existence : les puissances $1, x, x^2, \dots, x^e$ sont liées car $\dim_{\mathbb{F}_q} \mathbb{F}_{q^e} = e$, donc il existe un $f \in \mathbb{F}_q[t]$ de degré e tel que $f(x) = 0$. Comme x est racine de f , il doit être racine d'un de ses facteurs irréductibles. Unicité : deux polynômes irréductibles distincts sont sans facteur commun (Bézout!) même dans une extension de corps.

Ce polynôme s'appelle **polynôme minimal** de x sur \mathbb{F}_q , et son degré est le **degré** de x sur \mathbb{F}_q .

Remarque : Ces faits sont généraux à toute extension de corps L/K de degré e .

Corps de rupture

Théorème : Soit $f \in \mathbb{F}_q[t]$ un polynôme irréductible de degré e . Alors $\mathbb{F}_q[t]/(f) \cong \mathbb{F}_{q^e}$ et f y a e racines distinctes, qui sont $\bar{t}, \bar{t}^q, \bar{t}^{q^2}, \dots, \bar{t}^{q^{e-1}}$ (où \bar{t} est l'image de $t \in \mathbb{F}_q[t]$ dans $\mathbb{F}_q[t]/(f)$).

Démonstration : $\mathbb{F}_q[t]/(f)$ est un corps car f est irréductible ; étant un \mathbb{F}_q -espace vectoriel de dimension $\deg f = e$, il a q^e éléments, donc c'est \mathbb{F}_{q^e} . Le fait que $f(\bar{t}) = 0$ est la définition de \bar{t} . Mais comme $f(\text{Fr}_q(x)) = \text{Fr}_q(f(x))$ (car f est à coefficients dans \mathbb{F}_q donc fixes par Fr_q et car Fr_q est un morphisme de corps), on a $f((\text{Fr}_q)^i(\bar{t})) = 0$ pour tout i . Si l'ordre de Fr_q appliqué à \bar{t} est $e' < e$, alors \bar{t} est dans un $\mathbb{F}_{q^{e'}}$ donc racine d'un polynôme de degré $\leq e' < e$, qui devrait être multiple de f , contradiction.

Note : Si $f \in \mathbb{F}_q[t]$ irréductible a *une* racine dans une certaine extension $\mathbb{F}_{q'}$, il a *toutes* ses racines dans $\mathbb{F}_{q'}$.

Calculs dans $\mathbb{F}[t]/(f)$

Généralement $q = p$ ici : \mathbb{F}_q est le corps sur lequel on « sait » travailler (évident si $q = p$), et \mathbb{F}_{q^e} est le corps dans lequel on souhaite faire des calculs.

On a vu que si f est irréductible de degré e alors

$\mathbb{F}_q[t]/(f) \cong \mathbb{F}_{q^e}$. Pour calculer dans \mathbb{F}_{q^e} , une fois trouvé un tel f , on va donc calculer dans $\mathbb{F}_q[t]/(f)$. Ceci se fait sur la base $\bar{1}, \bar{t}, \dots, \bar{t}^{e-1}$:

- ▶ l'addition se fait terme à terme,
- ▶ la multiplication se fait en multipliant les polynômes de degré $< e$ puis en effectuant la division euclidienne par f .

Exercice : Sachant que $f = t^3 + t + 1$ est irréductible dans $\mathbb{F}_2[t]$, calculer les puissances successives de \bar{t} dans $\mathbb{F}_8 \cong \mathbb{F}_2[t]/(f)$.

Éléments conjugués

Deux éléments $x, x' \in \mathbb{F}_{q^e}$ sont dits **conjugués** sur \mathbb{F}_q lorsque (conditions équivalentes) :

- ▶ x et x' ont le même polynôme minimal sur \mathbb{F}_q ,
- ▶ il existe i (qu'on peut prendre entre 0 et $e - 1$) tel que $x' = x^{q^i}$.

Toute classe de conjugaison a pour cardinal le plus petit e tel que $x, x' \in \mathbb{F}_{q^e}$, degré commun de x et x' , qui est aussi le degré de leur polynôme minimal commun : ce polynôme a pour racines exactement les e éléments conjugués en question.

Si $x \in \mathbb{F}_{q^e}$ est primitif (engendre $\mathbb{F}_{q^e}^\times$) alors il en va de même de tout conjugué de x . On peut alors dire que la classe de conjugaison, ou le polynôme minimal qui la définit, sont **primitifs**. Un élément primitif est manifestement de degré e exactement.

Décomposition de $t^{q^e} - t$

Une fois de plus, on peut imaginer que $q = p$.

Dans la décomposition en facteurs irréductibles de $t^{q^e} - t$ dans \mathbb{F}_q :

- ▶ chaque polynôme irréductible de degré divisant e sur \mathbb{F}_q apparaît une et une seule fois,
- ▶ chaque facteur correspond à une classe de conjugaison (de cardinal égal au degré du facteur) dans \mathbb{F}_{q^e} ,
- ▶ le nombre de facteurs de degré exactement e est $\frac{1}{e}$ fois le nombre d'éléments appartenant à \mathbb{F}_{q^e} mais à aucun $\mathbb{F}_{q^{e_1}}$ pour e_1 divisant strictement e ,
- ▶ le nombre de facteurs primitifs est $\frac{1}{e} \varphi(q^e - 1)$.

Exercice : Expliquer pourquoi $t^{64} - t$ se décompose en irréductibles sur \mathbb{F}_2 en : 2 facteurs de degré 1, 1 de degré 2, 2 de degré 3 et 9 de degré 6, et pourquoi 6 de ces 9 derniers facteurs sont primitifs. Qu'en est-il sur \mathbb{F}_4 ?

Test de Rabin (1980) : Donné un $f \in \mathbb{F}_q[t]$ de degré e , comment savoir s'il est irréductible ? Il faut et il suffit qu'il vérifie chacune des deux conditions :

- ▶ f est premier avec $t^{q^{e_1}} - t$ pour tout diviseur strict e_1 de e , et
- ▶ f divise $t^{q^e} - t$.

Évidemment q^e et q^{e_1} peuvent être très grands, mais on calcule tout *modulo* f (c'est-à-dire dans $\mathbb{F}_q[t]/(f)$), en utilisant l'écriture binaire de l'exposant q^e et l'élévation au carré successive, pour calculer le reste de la division de $t^{q^e} - t$ par f , et de même pour q^{e_1} .

Test de Butler (1954) : f est irréductible ssi $\dim \ker(\text{Fr}_q - \text{id}) = 1$, où Fr_q et id opèrent sur $\mathbb{F}_q[t]/(f)$.

Comment calculer dans \mathbb{F}_q ?

Ici, $q = p^d$.

- ▶ On sait calculer dans $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.
- ▶ Pour calculer dans \mathbb{F}_q , on le représente comme $\mathbb{F}_p[t]/(f)$ avec f irréductible de degré d , et on utilise la base $\bar{1}, \bar{t}, \dots, \bar{t}^{d-1}$.
- ▶ Pour trouver f irréductible de degré d , il suffit de répéter :
 - ▶ tirer aléatoirement f unitaire de degré d dans $\mathbb{F}_p[t]$,
 - ▶ tester l'irréductibilité,

jusqu'à trouver f qui convient. Le nombre d'essais à faire est statistiquement de l'ordre de d .

- ▶ Pour avoir f primitif, le nombre d'essais sera plutôt $\frac{e q^e}{\varphi(q^e - 1)}$.

Symbole de Legendre

Si p est un *nombre premier impair* et a un entier non multiple de p , on note $\left(\frac{a}{p}\right)$ (**symbole de Legendre**) l'entier qui vaut

- ▶ $+1$ si a est un carré dans \mathbb{F}_p , i.e., si l'équation $x^2 = a$ a une solution dans \mathbb{F}_p , et
- ▶ -1 sinon.

On pose parfois $\left(\frac{a}{p}\right) = 0$ si a est multiple de p .

Si g est un élément primitif modulo p , on peut écrire $a = g^{\iota(a)}$ pour un certain $\iota(a)$ (logarithme discret de a , défini modulo $p-1$) : alors $\left(\frac{a}{p}\right)$ vaut 1 si $\iota(a)$ est *pair*, -1 s'il est *impair*, soit $(-1)^{\iota(a)}$. Or $g^{(p-1)/2} \equiv -1 \pmod{p}$ (pourquoi ?). On peut donc écrire

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

Symbole de Legendre (suite)

Le symbole de Legendre est *multiplicatif* : si a et b sont non multiples de p alors $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
(car $(ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2}$).

Pour calculer la valeur de $\left(\frac{a}{p}\right)$ pour tout a , on cherche donc la valeur lorsque a vaut -1 , ou 2 , ou un nombre premier impair (différent de p).

Le cas de -1 est facile : $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$, qui vaut donc

- ▶ $+1$ si $p \equiv 1 \pmod{4}$
- ▶ -1 si $p \equiv 3 \pmod{4}$

Le cas de 2 est donné par la **formule complémentaire** :

$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$, qui vaut donc

- ▶ $+1$ si $p \equiv 1, 7 \pmod{8}$
- ▶ -1 si $p \equiv 3, 5 \pmod{8}$

Gauß, « **theorema aureum** » : Si p et q sont des nombres premiers impairs distincts, alors

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

En d'autres mots : $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ sauf si p et q sont tous deux $\equiv 3 \pmod{4}$, auquel cas $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Application : Quels sont les p tels que 3 soit un carré modulo p ? Et 6 ? Et -5 ?

Une démonstration possible

Soient p et q deux nombres premiers impairs distincts, et soit ζ une racine primitive p -ième de l'unité dans une extension de \mathbb{F}_q (à savoir $\mathbb{F}_{q'}$ où q' est une puissance de q telle que $p|(q' - 1)$).

On pose

$$S = \sum_{x \in \mathbb{F}_p^\times} \left(\frac{x}{p} \right) \zeta^x \in \mathbb{F}_q$$

(somme de Gauß).

On montre que

- ▶ $S^2 = \left(\frac{-1}{p} \right) p$
- ▶ $S^q = \left(\frac{q}{p} \right) S$

et on conclut en considérant les deux écritures pour S^{q-1} .