# Introduction à la théorie des corps finis
# Brique CQFD

Hugues Randriam

10 décembre 2004

## 1 Prérequis et rappels sur les structures fondamentales de l'algèbre

On rappelle brièvement les définitions des structures de base de l'algèbre qu'on utilisera continuellement.

Un *groupe* est un ensemble muni d'une loi de composition interne associative qui admet un élément neutre et pour laquelle tout élément est inversible. Le groupe est dit commutatif (ou *abélien*) si sa loi l'est.

Un *anneau* est un ensemble muni de deux lois de composition interne, appelées addition et multiplication, qui vérifient les propriétés suivantes :
- l'addition définit sur l'anneau une structure de groupe abélien, dont l'élément neutre est appelé l'élément nul (ou zéro, noté 0) de l'anneau
- la multiplication est associative, admet un élément neutre (appelé élément unité de l'anneau, noté 1) et est distributive par rapport à l'addition.

L'anneau est dit commutatif si sa multiplication l'est.

Dans ce cours on n'étudiera que des anneaux commutatifs. L'algèbre non-commutative est très riche et intéressante, mais on aura déjà suffisamment à faire avec la théorie commutative. Ainsi, dans la suite du texte, et sauf mention du contraire, *tous les anneaux considérés seront commutatifs.*

Dans un anneau $A$, les éléments inversibles forment un groupe pour la multiplication, noté $A^\times$.

Un *corps* est un anneau dans lequel un élément est inversible si et seulement s'il est non nul (remarquons que cette définition implique $0 \neq 1$).

Un anneau $A$ est dit *intègre* si $0 \neq 1$ et si le produit de deux éléments non nuls est non nul. Cela équivaut à demander qu'il existe un corps admettant $A$ comme sous-anneau. Un corps minimal pour l'inclusion parmi ceux qui possèdent cette propriété est appelé *corps de fractions* de $A$.

Soit $A$ un anneau. On appellera $A$-module la donnée d'un groupe abélien $V$ et d'une application

$$\begin{array}{ccc} A \times V & \longrightarrow & V \\ (a, v) & \mapsto & av \end{array}$$

appelée multiplication scalaire, telle que, notant $0_A$ l'élément nul de $A$, $1_A$ son élément unité, et $0_V$ l'élément neutre de $V$, pour tous $a, b \in A$ et $v, w \in V$ on ait $0_A v = 0_V$, $a0_V = 0_V$, $1_A v = v$, $(ab)v = a(bv)$, $(a+b)v = av + bv$, et $a(v+w) = av + aw$.

Dans le cas particulier où l'anneau $A$ est un corps $K$, on parlera indifféremment de $K$-module ou de *$K$-espace vectoriel.*

Un *morphisme* (ou *homomorphisme*) entre deux groupes, deux anneaux, deux corps, ou deux $K$-espaces vectoriels, est une application entre ces deux ensembles qui respecte leurs structures (envoie élément neutre sur élément neutre, respecte addition, multiplication,...).

**Exemple 1.1.** — Les nombres réels forment un groupe (abélien) pour l'addition, $(\mathbb{R}, +, 0)$. Les nombres réels non nuls forment un groupe (abélien) pour la multiplication, $(\mathbb{R}^\times, \times, 1)$. L'exponentielle (peu importe la base) de $\mathbb{R}$ dans $\mathbb{R}^\times$ est un morphisme de groupes, car on a bien $\exp(0) = 1$ et $\exp(x+y) = \exp(x)\exp(y)$ pour tous $x$ et $y$ dans $\mathbb{R}$.

Un morphisme entre deux $K$-espaces vectoriels est aussi appelé une *application $K$-linéaire.*

Une famille d'éléments d'un $K$-espace vectoriel $V$ est dite *génératrice* si tout élément de $V$ peut s'écrire comme combinaison linéaire (finie, à coefficients dans $K$) d'entre eux. Une famille d'éléments de $V$ est dite *libre* si toute combinaison linéaire non triviale de ces éléments est non nulle. Une telle famille est appelée *base* de $V$ si elle est à la fois libre et génératrice ; cela revient à demander que tout élément de $V$ puisse s'écrire d'une unique façon comme combinaison linéaire de ces éléments. De toute famille génératrice d'un espace vectoriel on peut extraire une base, et toute famille libre peut se compléter en une base.

Toutes les bases de $V$ ont même cardinal (éventuellement infini), appelé *dimension* de $V$ (sur $K$). Dans ce cours on considérera principalement des espaces de dimension finie.

**Exemple 1.2.** — Les applications $K$-linéaires d'un $K$-espace vectoriel de dimension $m$ dans un $K$-espace vectoriel de dimension $n$ forment un $K$-espace vectoriel de dimension $mn$.

Un morphisme d'un objet dans lui-même est appelé *endomorphisme*. Un morphisme bijectif (et dont l'inverse est alors aussi un morphisme) est appelé *isomorphisme*. Un morphisme qui est à la fois un endomorphisme et un isomorphisme est appelé *automorphisme*.

**Exemple 1.3.** — La conjugaison complexe de $\mathbb{C}$ dans lui-même est un automorphisme de corps. En effet, elle est son propre inverse, et on a bien $\overline{0} = 0$, $\overline{1} = 1$, $\overline{x+y} = \overline{x} + \overline{y}$, et $\overline{xy} = \overline{x}.\overline{y}$ pour tous $x$ et $y$ dans $\mathbb{C}$.

# 2 Généralités sur les extensions de corps

**Définition 2.1.** — Soit $L$ un corps. Un *sous-corps* de $L$ est une partie de $L$ qui contient 0 et 1, est stable par addition et multiplication, et telle que ces opérations la munissent d'une structure de corps.

On dira de façon équivalente que $K$ est un sous-corps de $L$ ou que $L$ est une *extension* de $K$.

Un morphisme entre deux extensions $L_1$ et $L_2$ d'un même corps $K$ est un morphisme de corps de $L_1$ dans $L_2$ dont la restriction à $K$ est l'identité.

**Proposition 2.2.** — *Soit $f : K \longrightarrow L$ un morphisme de corps. Alors $f$ est injectif.*

*Démonstration.* Il suffit de montrer que si $x$ n'est pas nul, $f(x)$ non plus. Or tout $x$ non nul admet un inverse $x^{-1}$, et on a

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(1_K) = 1_L \neq 0_L$$

donc $f(x) \neq 0_L$. □

Interprétation de la proposition : $f$ injectif permet d'identifier $K$ à son image $f(K)$ qui est un sous-corps de $L$ ; ainsi tout morphisme de corps permet de considérer le corps d'arrivée comme une extension du corps de départ.

Si $K \subset L$ est une extension de corps, on peut considérer $L$ comme un $K$-espace vectoriel : la structure de groupe abélien de ce $K$-espace vectoriel est définie par l'addition usuelle de $L$, et la multiplication scalaire $K \times L \longrightarrow L$ est définie par la restriction de la multiplication usuelle de $L$.

**Définition 2.3.** — Le *degré* de l'extension $K \subset L$, noté $[K : L]$, est la dimension de $L$ considéré comme $K$-espace vectoriel :

$$[L : K] = \dim_K L.$$

Une extension de degré fini sera aussi parfois appelée une extension *finie.*

**Proposition 2.4** (multiplicativité du degré). — *Soient $K \subset L \subset M$ trois corps extensions l'un de l'autre. Alors*

$$[M : K] = [M : L][L : K].$$

*Démonstration.* Considérons des éléments $e_i \in M$ qui forment une base de $M$ sur $L$ et, de même, des $f_j \in L$ formant une base de $L$ sur $K$. Alors tout élément $m \in M$ s'écrit de façon unique comme combinaison linéaire (finie) $m = \sum_i l_i e_i$ pour des $l_i$ dans $L$, et de même chaque $l_i$ s'écrit de façon unique $l_i = \sum_j k_{i,j} f_j$ pour des $k_{i,j}$ dans $K$. Ainsi $m$ s'écrit de façon unique $m = \sum_{i,j} k_{i,j} e_i f_j$ de sorte que les $e_i f_j$ forment une base de $M$ sur $K$. $\square$

Soient $K \subset L$ une extension de corps de degré fini $n$, et $e_1, \ldots, e_n \in L$ une base de $L$ sur $K$. Deux éléments $x$ et $y$ de $L$ s'écrivent de façon unique $x = \sum_{i=1}^n \lambda_i e_i$ et $y = \sum_{i=1}^n \mu_i e_i$ avec les $\lambda_i$ et $\mu_i$ dans $K$. Il est encore facile d'exprimer la somme de $x$ et $y$ dans la base : on a $x + y = \sum_{i=1}^n (\lambda_i + \mu_i) e_i$.

Pour le produit, on a $xy = \sum_{i,j=1}^n \lambda_i \mu_j e_i e_j$, et on voit qu'il peut être utile de savoir exprimer chaque produit $e_i e_j$ dans la base.

**Définition 2.5.** — Les constantes de structure de la base $(e_1, \ldots, e_n)$ de $L$ sur $K$ sont les $\alpha_{i,j,k} \in K$, pour $i, j, k \in \{1, \ldots, n\}$, définis par

$$e_i e_j = \sum_{k=1}^n \alpha_{i,j,k} e_k.$$

Avec les notations qui précèdent, on a donc

$$xy = \sum_{k=1}^n \nu_k e_k$$

avec

$$\nu_k = \sum_{i,j=1}^{n} \alpha_{i,j,k} \lambda_i \mu_j.$$

On vérifie que la commutativité de la multiplication implique

$$\alpha_{i,j,k} = \alpha_{j,i,k}$$

et l'associativité

$$\sum_{p=1}^{n} \alpha_{i,j,p} \alpha_{p,k,l} = \sum_{q=1}^{n} \alpha_{i,q,l} \alpha_{j,k,q}$$

pour tous $i, j, k, l$. L'existence d'un élément unité et de l'inverse peuvent s'exprimer dans les mêmes termes.

**Exemple 2.6.** — Prenant $K = \mathbb{R}$ et $L = \mathbb{C}$ on a $n = [\mathbb{C} : \mathbb{R}] = 2$, et choisissant la base formée de $e_1 = 1$ et $e_2 = i = \sqrt{-1}$ on trouve $\alpha_{1,1,1} = \alpha_{1,2,2} = \alpha_{2,1,2} = 1$, $\alpha_{1,1,2} = \alpha_{1,2,1} = \alpha_{2,1,1} = \alpha_{2,2,2} = 0$, et $\alpha_{2,2,1} = -1$.

La multiplication de $L$ pouvant se lire sur les constantes de structure, il importe de trouver une base pour laquelle celles-ci sont particulièrement simples.

**Définition 2.7.** — Soit $L$ une extension finie de $K$, de degré $n$. On dit que $L$ est une extension *élémentaire*, ou *simple* (ou encore parfois *primitive*), de $K$ s'il existe $x \in L$ tel que $(1, x, x^2, \ldots, x^{n-1})$ soit une base de $L$ sur $K$.

On dit alors que $x$ est un *générateur* de $L$ sur $K$.

Quelques remarques :

– La définition équivaut à demander qu'il existe un élément $x \in L$ tel que les éléments de $L$ soient exactement les valeurs en $x$ des polynômes à coefficients dans $K$ de degré inférieur ou égal à $n - 1$.
– En particulier l'élément $x^n$ de $L$ doit être égal à la valeur en $x$ d'un polynôme à coefficients dans $K$ de degré inférieur ou égal à $n - 1$ : il existe $a_0, a_1, \ldots, a_{n-1} \in K$ tels que $x^n = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Notant alors $P(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_1 X - a_0$, on a $P(x) = 0$.
– Si $y = F(x) \in L$ et $z = G(x) \in L$, alors $y+z = (F+G)(x)$ et $yz = H(x)$ où $H$ est le reste de la division euclidienne de $FG$ par $P$. En effet, si $FG = PQ + H$, on a $yz = F(x)G(x) = P(x)Q(x) + H(x) = H(x)$ puisque $H(x) = 0$.

**Définition 2.8.** — Soient $K$ un corps et $P \in K[X]$ un polynôme de degré $n$. L'*anneau quotient* $K[X]/P$ est construit comme suit :
- en tant que groupe abélien, c'est l'ensemble des polynômes à coefficients dans $K$ de degré inférieur ou égal à $n-1$, muni de l'addition usuelle ;
- si $F$ et $G$ sont deux éléments de $K[X]/P$, leur produit dans $K[X]/P$ est le reste de la division euclidienne par $P$ du produit usuel $FG$.

Des remarques qui précèdent il découle immédiatement le résultat suivant :

**Lemme 2.9.** — *Soient $K \subset L$ une extension élémentaire de degré $n$ et $x$ un générateur de $L$ sur $K$. Il existe alors un polynôme $P \in K[X]$ de degré $n$ annulant $x$, et l'application de $K[X]/P$ dans $L$ qui envoie $F$ sur $F(x)$ est un isomorphisme d'anneaux.*

On peut encore préciser le lemme comme suit.

**Théorème 2.10.** — *Soit $K$ un corps.*

1. *Soit $P \in K[X]$ un polynôme de degré $n$. Les assertions suivantes sont équivalentes :*
   - *l'anneau quotient $K[X]/P$ est intègre*
   - *le polynôme $P$ est irréductible*
   - *l'anneau quotient $K[X]/P$ est un corps.*

   *Si l'une de ces conditions équivalentes est vérifiée, $K[X]/P$ est alors une extension élémentaire de $K$, de degré $n$.*
2. *Inversement, si $L$ est une extension finie de $K$, alors $L$ est élémentaire si et seulement s'il existe un polynôme* irréductible *$P \in K[X]$ tel que $L$ soit isomorphe à $K[X]/P$ en tant qu'extension de $K$ (on peut choisir par exemple le polynôme $P$ et l'isomorphisme donnés dans le lemme).*

*Démonstration.* Supposons $K[X]/P$ intègre et $P$ non irréductible, de sorte que $P = FG$ avec $\deg F \leq n-1$ et $\deg G \leq n-1$. Le produit de $F$ et $G$ dans $K[X]/P$ est le reste de la division euclidienne par $P$ du produit usuel $FG$, c'est-à-dire 0. Puisque $K[X]/P$ est supposé intègre, on doit donc avoir $F = 0$ ou $G = 0$, ce qui est absurde. Si maintenant $P$ est irréductible et si $A$ est un polynôme non nul de degré inférieur ou égal à $n-1$, alors le théorème de Bézout fournit $B$ et $Q$ de degrés inférieurs ou égaux à $n-1$ et tels que $AB + PQ = 1$, de sorte que $B$ est un inverse de $A$ dans $K[X]/P$. Ainsi $K[X]/P$ est un corps. Tout corps étant intègre, on a démontré l'équivalence des trois assertions. Ceci étant fait, $K[X]/P$ est une extension élémentaire de $K$ puisqu'elle admet $X$ comme générateur.

Si maintenant $L$ est une extension élémentaire de $K$, $x$ un générateur, et $P$ un polynôme de degré $n$ qui annule $x$, l'application donnée dans le lemme étant un isomorphisme d'anneaux, et $L$ étant un corps, $K[X]/P$ est aussi un corps, de sorte que l'irréductibilité de $P$ résulte de la première partie du théorème. L'isomorphisme entre $K[X]/P$ et $L$ est alors un isomorphisme de corps, et puisqu'il laisse les éléments de $K$ inchangés, c'est même un isomorphisme d'extensions de $K$. □

Pour l'étude de la structure de $K[X]/P$ pour un polynôme $P$ quelconque, on consultera l'exercice 7.1.

**Proposition 2.11.** — *Soient $K \subset L$ une extension finie de corps et $x$ un élément de $L$. Alors il existe un unique polynôme irréductible $P$ à coefficients dans $K$ et de coefficient dominant 1 qui annule $x$.*

*Si l'on note $K[x]$ le plus petit sous-anneau de $L$ qui contient $K$ et $x$, alors $K[x]$ est un corps, et plus précisément c'est une extension élémentaire de $K$ isomorphe à $K[X]/P$.*

*Démonstration.* Notons $n$ le plus petit entier naturel tel que $(1, x, \ldots, x^{n-1})$ soit une famille libre dans le $K$-espace vectoriel $L$ (on a donc $n \leq [L : K]$). Alors $x^n$ est combinaison linéaire à coefficients dans $K$ de ces éléments : $x^n = a_{n-1}x^{n-1} + \cdots + a_1x + a_0$. Alors on a $P(x) = 0$ où $P(X) = X^n - a_{n-1}X^{n-1} - \cdots - a_1X - a_0$, et $K[x]$ s'identifie à $K[X]/P$. Cet anneau étant intègre (puisque sous-anneau d'un corps), l'irréductibilité de $P$ et le reste de la proposition découlent du théorème précédent. □

**Définition 2.12.** — Le polynôme irréductible $P$ ainsi défini dans la proposition est appelé le polynôme minimal de $x$ sur $K$.

Un polynôme à coefficients dans $K$ annule $x$ si et seulement s'il est multiple de $P$.

**Proposition 2.13.** — *Toute extension finie de corps s'obtient par composition d'extensions élémentaires.*

*Démonstration.* On procède par récurrence. Soit $K \subset L$ une extension finie de corps. Si $L = K$, l'assertion à prouver est triviale. Sinon, soit $x \in L$, $x \notin K$. Alors on a $K \subset K[x] \subset L$ où $K[x]$ est une extension élémentaire de

$K$, et où $L$ est une extension de $K[x]$ de degré strictement inférieur à $[L : K]$. On peut donc conclure en appliquant l'hypothèse de récurrence à l'extension $K[x] \subset L$. □

Si $L$ est une extension finie de $K$ et si $x_1, \ldots, x_r \in L$, on note $K[x_1, \ldots, x_r]$ le plus petit sous-anneau de $L$ qui contient $K$ et $x_1, \ldots, x_r$. Les faits qui précèdent et une récurrence immédiate montrent que $K[x_1, \ldots, x_r]$ est un corps. On dit que c'est le sous-corps de $L$ engendré par $x_1, \ldots, x_r$ sur $K$.

**Proposition 2.14.** — *Soient $K$ un corps et $P \in K[X]$ un polynôme non constant. Alors il existe une extension finie $L$ de $K$ dans laquelle $P$ admet une racine.*

*Démonstration.* Sans perte de généralité on peut supposer $P$ irréductible. Alors l'extension élémentaire $L = K[X]/P$ de $K$ convient, puisque l'élément $X$ de $L$ est bien racine de $P$. □

**Proposition 2.15.** — *Soient $K$ un corps et $P \in K[X]$ un polynôme de degré $r \geq 1$. Alors il existe une extension finie $L$ de $K$ dans laquelle $P$ se décompose en produit de facteurs linéaires : il existe $c \in K$ et $\alpha_1, \ldots, \alpha_r \in L$ tels que*

$$P(X) = c(X - \alpha_1) \ldots (X - \alpha_r).$$

*Démonstration.* On procède par récurrence sur $r$. Par la proposition précédente il existe une extension finie $K_1$ de $K$ telle que $P$ admette une racine $\alpha_1$ dans $K_1$. Notant alors $P(X) = (X - \alpha_1)P_1(X)$ avec $P_1 \in K_1[X]$, on conclut en appliquant l'hypothèse de récurrence avec $K_1$ et $P_1$ à la place de $K$ et $P$. □

**Définition 2.16.** — On appelle *corps de décomposition* de $P$ sur $K$ une extension $L$ de $K$ de degré minimal dans laquelle $P$ se décompose en produit de facteurs linéaires.

Avec les notations de la proposition, la minimalité du degré signifie que le corps de décomposition $L$ est engendré par les racines de $P$ : on a $L = K[\alpha_1, \ldots, \alpha_r]$.

**Proposition 2.17.** — *Soit $\sigma : K_1 \xrightarrow{\sim} K_2$ un isomorphisme de corps, $P_1$ un polynôme non constant à coefficients dans $K_1$, $P_2 = \sigma(P_1)$, $L_1$ un corps de décomposition de $P_1$ sur $K_1$ et $L_2$ un corps de décomposition de $P_2$*

*sur $K_2$. Alors $L_1$ et $L_2$ sont isomorphes, et plus précisément, il existe un isomorphisme de $L_1$ sur $L_2$ qui étend $\sigma$.*

*En particulier, prenant $K_1 = K_2 = K$ et $\sigma$ l'identité, on voit que le corps de décomposition d'un polynôme est unique (à isomorphisme près).*

*Démonstration.* On procède par récurrence sur le degré de $P_1$. Soit $Q_1$ un facteur irréductible de $P_1$. Par définition d'un corps de décomposition, $Q_1$ admet une racine $x_1$ dans $L_1$, et $Q_2 = \sigma(P_2)$ une racine $x_2$ dans $L_2$. Par la proposition 2.11, $K_1' = K_1[x_1]$ est naturellement isomorphe à $K_1[X]/P_1$, et $K_2' = K_2[x_2]$ à $K_2[X]/P_2$, les isomorphismes envoyant $x_1$ et $x_2$ sur $X$. L'isomorphisme $\sigma$ de $K_1$ sur $K_2$ s'étend naturellement en un isomorphisme de $K_1[X]/P_1$ sur $K_2[X]/P_2$, et donc de $K_1'$ sur $K_2'$, noté $\sigma'$, qui vérifie $\sigma'(x_1) = x_2$. Ecrivant $P_1(X) = (X - x_1)R_1(X)$ avec $R_1 \in K_1'[X]$, $P_2(X) = (X - x_2)R_2(X)$ avec $R_2 = \sigma'(R_1) \in K_2'[X]$, et remarquant que $L_1$ est un corps de décomposition de $R_1$ sur $K_1'$, et $L_2$ de $R_2$ sur $K_2'$, on peut conclure en appliquant l'hypothèse de récurrence. □

# 3 Construction des corps finis et étude de leurs propriétés élémentaires

On supposera connue la théorie des anneaux quotient $\mathbb{Z}/n\mathbb{Z}$, en particulier le fait que $\mathbb{Z}/n\mathbb{Z}$ est intègre (et même, est un corps) si et seulement si $n$ est un nombre premier.

**Proposition 3.1.** — *Soit $K$ un corps. Alors ou bien $K$ est une extension du corps $\mathbb{Q}$ des nombres rationnels, ou bien $K$ est une extension de $\mathbb{Z}/p\mathbb{Z}$ pour un nombre premier $p$ uniquement déterminé.*

**Définition 3.2.** — Dans le premier cas de la proposition on dit que $K$ est de caractéristique 0, et dans le second que $K$ est de caractéristique $p$.

*Démonstration.* On dispose naturellement d'un homomorphisme d'anneaux $f$ de $\mathbb{Z}$ dans $K$ qui envoie $1 \in \mathbb{Z}$ sur l'élément unité de $K$. Si $f$ est injectif, alors $K$ contient son image $f(\mathbb{Z})$ qui est isomorphe à $\mathbb{Z}$, et son corps de fractions qui est isomorphe à $\mathbb{Q}$. Sinon il existe un plus petit entier non nul $p$ tel que $f(p) = 0$. Alors l'image $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, et est intègre (puisque sous-anneau d'un corps), de sorte que $p$ est premier. □

**Proposition 3.3.** — *Soit $K$ un corps fini. Alors le cardinal de $K$ est une puissance d'un nombre premier. Plus précisément, il existe $p$ premier tel que $K$ soit une extension de $\mathbb{Z}/p\mathbb{Z}$, et le cardinal de $K$ vaut $p^r$ où $r = [K : \mathbb{Z}/p\mathbb{Z}]$ est le degré de cette extension.*

*Démonstration.* Le corps $K$ étant fini, il ne peut contenir $\mathbb{Q}$, donc est nécessairement extension d'un $\mathbb{Z}/p\mathbb{Z}$. Notant $r = [K : \mathbb{Z}/p\mathbb{Z}]$, $K$ est alors un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension $r$, donc de cardinal $p^r$. □

**Lemme 3.4.** — *Soit $K$ un corps de caractéristique $p$. Alors pour tous $a, b \in K$ on a $(a+b)^p = a^p + b^p$, et plus généralement, pour tout entier $r \geq 1$,*

$$(a+b)^{p^r} = a^{p^r} + b^{p^r}.$$

*Démonstration.* La formule du binôme donne

$$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$

Or, pour $1 \leq i \leq p-1$, l'entier $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ est divisible par $p$ donc nul dans $\mathbb{Z}/p\mathbb{Z}$. Ceci prouve le cas $r = 1$ du lemme, et le cas général en découle par une récurrence évidente. □

**Théorème 3.5.** — *Soient $p$ un nombre premier et $r \geq 1$ un entier.*

1. *Le corps de décomposition du polynôme $X^{p^r} - X$ sur $\mathbb{Z}/p\mathbb{Z}$ est de cardinal $p^r$.*
2. *Inversement, si $K$ est un corps fini de cardinal $p^r$, alors $K$ est corps de décomposition de $X^{p^r} - X$ sur $\mathbb{Z}/p\mathbb{Z}$. Plus précisément, les racines de $X^{p^r} - X$ sont exactement les éléments de $K$ avec multiplicité 1.*

*Démonstration.* Notons $K$ le corps de décomposition de $X^{p^r} - X$ sur $\mathbb{Z}/p\mathbb{Z}$, de sorte qu'on ait

$$X^{p^r} - X = \prod_{i=1}^{p^r} (X - \alpha_i)$$

pour des $\alpha_i \in K$ qui engendrent $K$ sur $\mathbb{Z}/p\mathbb{Z}$.

Montrons d'abord que les $\alpha_i$ sont tous distincts (*i.e.* que $X^{p^r} - X$ est à racines simples). Dans le cas contraire, si $\alpha_i = \alpha_j = \alpha$, alors on peut écrire

$$X^{p^r} - X = (X - \alpha)^2 Q(X)$$

d'où en dérivant et en utilisant le fait que $p$ est nul dans $\mathbb{Z}/p\mathbb{Z}$,

$$-1 = p^r X^{p^r-1} - 1 = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X),$$

de sorte que $(X-\alpha)$ divise 1, ce qui est absurde.

Les $\alpha_i$ forment donc $p^r$ éléments deux à deux distincts de $K$. Montrons maintenant que l'ensemble $E$ des $\alpha_i$ est un sous-corps de $K$ (d'où l'on déduira, par minimalité du corps de décomposition, que ce sous-corps est $K$ tout entier). On a clairement $0^{p^r} = 0$ et $1^{p^r} = 1$, donc 0 et 1 font bien partie de $E$. Par le lemme, si $\alpha$ et $\beta$ sont dans $E$, alors

$$(\alpha+\beta)^{p^r} = \alpha^{p^r} + \beta^{p^r} = \alpha + \beta,$$

donc $\alpha + \beta \in E$. De la même façon, $(\alpha\beta)^{p^r} = \alpha^{p^r}\beta^{p^r} = \alpha\beta$ donc $\alpha\beta \in E$. Ainsi $E$ est stable par addition et multiplication. Si $\alpha \in E$ est non nul, alors $(\alpha^{-1})^{p^r} = (\alpha^{p^r})^{-1} = \alpha^{-1}$, donc $E \smallsetminus \{0\}$ est stable par inverse. Enfin, reste à voir que si $\alpha$ est dans $E$, alors $-\alpha$ aussi. Si $p = 2$ c'est évident, puisqu'alors $-\alpha = \alpha$, et sinon $p$ est impair, de sorte que $(-\alpha)^{p^r} = -\alpha^{p^r} = -\alpha$, ce qu'il fallait démontrer. Ceci termine la preuve de la première assertion du théorème.

Soit maintenant $K$ un corps de cardinal $p^r$. Alors $K^\times$ est un groupe abélien de cardinal $p^r - 1$, donc par le théorème de Lagrange tout élément $x$ de $K^\times$ vérifie $x^{p^r-1} = 1$. Ainsi tout élément non nul de $K$ est racine de $X^{p^r-1} - 1$, donc de $X^{p^r} - X$. Par ailleurs 0 est aussi clairement racine de $X^{p^r} - X$. Les $p^r$ éléments distincts de $K$ sont donc tous racines de $X^{p^r} - X$, qui est de degré $p^r$, de sorte qu'on peut écrire

$$X^{p^r} - X = \prod_{x \in K} (X - x),$$

et $K$ est bien corps de décomposition de $X^{p^r} - X$. □

**Corollaire 3.6.** — *Tout corps fini est de cardinal une puissance d'un nombre premier. Inversement, si $q = p^r$ est une puissance d'un nombre premier, il existe un corps fini de cardinal $q$, et celui-ci est unique à isomorphisme près.*

*Démonstration.* C'est une conséquence immédiate du théorème, l'unicité résultant de l'unicité du corps de décomposition. □

On notera $\mathbb{F}_q$, ou parfois aussi $GF(q)$, l'unique corps à $q$ éléments. Si $q = p$ est un nombre premier, on a donc $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On prendra garde à l'inverse que si $q = p^r$ avec $r \geq 2$, alors $\mathbb{F}_q$ n'est pas isomorphe à $\mathbb{Z}/q\mathbb{Z}$, ce dernier anneau n'étant même pas intègre.

Décrivons explicitement $\mathbb{F}_q$ pour les petites valeurs de $q$ :

– $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| × | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

– $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\} = \{0, 1, -1\}$

| + | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

| × | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 |
| 2 | 0 | 2 | 1 |

– $\mathbb{F}_4$ n'est pas égal à $\mathbb{Z}/4\mathbb{Z}$ ! En tant que corps de caractéristique 2, il contient $\mathbb{F}_2 = \{0, 1\}$, et deux autres éléments, qu'on notera $\alpha$ et $\beta$. On vérifie que les seules tables d'addition et de multiplication possibles sont les suivantes :

| + | 0 | 1 | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| 0 | 0 | 1 | $\alpha$ | $\beta$ |
| 1 | 1 | 0 | $\beta$ | $\alpha$ |
| $\alpha$ | $\alpha$ | $\beta$ | 0 | 1 |
| $\beta$ | $\beta$ | $\alpha$ | 1 | 0 |

| × | 0 | 1 | $\alpha$ | $\beta$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $\alpha$ | $\beta$ |
| $\alpha$ | 0 | $\alpha$ | $\beta$ | 1 |
| $\beta$ | 0 | $\beta$ | 1 | $\alpha$ |

On vérifie que ces opérations sont associatives et commutatives et que la multiplication est distributive par rapport à l'addition. Le corps $\mathbb{F}_4$ est bien corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$ puisqu'on a $0^4 = 0$, $1^4 = 1$, $\alpha^4 = \alpha$ et $\beta^4 = \beta$, de sorte que

$$X^4 - X = X(X - 1)(X - \alpha)(X - \beta).$$

On vérifie enfin qu'on a $\alpha^2 = \alpha + 1$, de sorte que $\alpha$ est racine de $X^2 + X + 1$ (l'autre racine est $\beta$), d'où l'on tire une représentation

$$\mathbb{F}_4 \simeq \mathbb{F}_2[X]/X^2 + X + 1.$$

– $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$
– Il n'y a pas de corps de cardinal 6.
– $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$
– $\mathbb{F}_8$ est une extension de degré 3 de $\mathbb{F}_2$, qu'on va décrire plus précisément.

Considérons un élément $x \in \mathbb{F}_8 \setminus \mathbb{F}_2$, et notons $K = \mathbb{F}_2[x]$. On a alors $[K : \mathbb{F}_2] > 1$ et $[\mathbb{F}_8 : K][K : \mathbb{F}_2] = [\mathbb{F}_8 : \mathbb{F}_2] = 3$, donc nécessairement $[K : \mathbb{F}_2] = 3$, et $K = \mathbb{F}_8$. Ainsi $\mathbb{F}_8$ est une extension élémentaire de $\mathbb{F}_2$, et tout élément de $\mathbb{F}_8 \setminus \mathbb{F}_2$ en est un générateur ; le polynôme minimal $P$ d'un tel élément est irréductible de degré 3 sur $\mathbb{F}_2$, et on a alors $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/P$.

Quels sont les polynômes irréductibles de degré 3 sur $\mathbb{F}_2$ ? Il y a 8 polynômes de degré 3 sur $\mathbb{F}_2$, parmi lesquels 6 sont multiples de $X$ ou de $X+1$. Éliminant ceux-ci, il reste $X^3+X+1$ et $X^3+X^2+1$, qui sont irréductibles. On dispose donc de deux isomorphismes,

$$\mathbb{F}_8 \simeq \mathbb{F}_2[X]/X^3+X+1 \qquad \text{et} \qquad \mathbb{F}_8 \simeq \mathbb{F}_2[X]/X^3+X^2+1,$$

qui vont donner deux descriptions différentes du même corps $\mathbb{F}_8$.

Notons $\alpha$ une racine de $X^3+X+1$ dans $\mathbb{F}_8$. Les éléments de $\mathbb{F}_8$ sont les polynômes en $\alpha$ de degré au plus 2 :

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}.$$

Utilisant la relation $\alpha^3 = \alpha+1$ on peut décomposer successivement les puissances de $\alpha$ dans la base $(1, \alpha, \alpha^2)$ de $\mathbb{F}_8$ sur $\mathbb{F}_2$. On peut aussi faire la même chose en partant d'une racine $\beta$ de $X^3+X^2+1$, qui vérifie donc $\beta^3 = \beta^2+1$.

On trouve :

| | $\alpha^2$ | $\alpha$ | $1$ |
|---|---|---|---|
| $1$ | 0 | 0 | 1 |
| $\alpha$ | 0 | 1 | 0 |
| $\alpha^2$ | 1 | 0 | 0 |
| $\alpha^3$ | 0 | 1 | 1 |
| $\alpha^4$ | 1 | 1 | 0 |
| $\alpha^5$ | 1 | 1 | 1 |
| $\alpha^6$ | 1 | 0 | 1 |

| | $\beta^2$ | $\beta$ | $1$ |
|---|---|---|---|
| $1$ | 0 | 0 | 1 |
| $\beta$ | 0 | 1 | 0 |
| $\beta^2$ | 1 | 0 | 0 |
| $\beta^3$ | 1 | 0 | 1 |
| $\beta^4$ | 1 | 1 | 1 |
| $\beta^5$ | 0 | 1 | 1 |
| $\beta^6$ | 1 | 1 | 0 |

et $\alpha^7 = \beta^7 = 1$.

Le corps $\mathbb{F}_8$ étant unique à isomorphisme près, ces deux descriptions doivent être équivalentes. On vérifie que les racines de $X^3+X+1$ sont $\{\alpha, \alpha^2, \alpha^4\}$, et celles de $X^3+X^2+1$, $\{\alpha^3, \alpha^5, \alpha^6\}$. On peut donc prendre pour $\beta$ n'importe lequel de ces trois derniers éléments. Choisissant par exemple le premier, on voit que la correspondance $\beta \mapsto \alpha^3$, $\beta^2 \mapsto \alpha^6$, $\beta^3 \mapsto \alpha^2$, $\beta^4 \mapsto \alpha^5$, $\beta^5 \mapsto \alpha$, $\beta^6 \mapsto \alpha^4$ respecte l'addition et la multiplication, de sorte que les écritures en termes de $\alpha$ et en termes de $\beta$ sont bien deux représentations équivalentes de la même structure de corps.

# 4 Polynômes primitifs et structure multiplicative des corps finis

Un phénomène agréable dans l'exemple étudié précédemment est que tous les éléments de $\mathbb{F}_8^*$ sont des puissances de $\alpha$. L'exponention $i \mapsto \alpha^i$ définit un morphisme surjectif de groupes de $\mathbb{Z}$ sur $\mathbb{F}_7^*$ qui, puisque $\alpha$ est d'ordre 7, définit par passage au quotient un isomorphisme

$$\begin{array}{ccc} \mathbb{Z}/7\mathbb{Z} & \longrightarrow & \mathbb{F}_8^* \\ i \mod 7 & \mapsto & \alpha^i. \end{array}$$

Plus généralement :

**Définition 4.1.** — Soient $q$ une puissance d'un nombre premier et $\mathbb{F}_q$ le corps fini à $q$ éléments. On dira qu'un élément $\gamma \in \mathbb{F}_q$ est (multiplicativement) *primitif* s'il est d'ordre $q-1$ dans $\mathbb{F}_q^*$.

Puisque $\mathbb{F}_q^*$ est d'ordre $q-1$, cela revient à demander que tout élément non nul de $\mathbb{F}_q$ soit une puissance de $\gamma$, ou encore que l'application d'exponentiation

$$\begin{array}{ccc} \mathbb{Z}/(q-1)\mathbb{Z} & \longrightarrow & \mathbb{F}_q^* \\ i \mod q-1 & \mapsto & \gamma^i \end{array}$$

soit un isomorphisme de groupes. L'isomorphisme inverse est appelé logarithme en base $\gamma$ :

$$\log_\gamma : \mathbb{F}_{q-1}^* \xrightarrow{\sim} \mathbb{Z}/(q-1)\mathbb{Z}.$$

**Proposition 4.2.** — *Soient $p$ un nombre premier et $n \geq 1$ un entier. On suppose que $\mathbb{F}_{p^n}$ admet un élément primitif $\gamma$. Alors $\mathbb{F}_{p^n}$ est une extension élémentaire de $\mathbb{F}_p$ et $\gamma$ en est un générateur. En particulier, le polynôme minimal de $\gamma$ est de degré $n$.*

**Définition 4.3.** — Un polynôme de degré $n$ à coefficients dans $\mathbb{F}_p$ est dit *primitif* s'il est polynôme minimal d'un élément primitif de $\mathbb{F}_{p^n}$.

Remarquons qu'un polynôme primitif est donc par définition irréductible.

**Lemme 4.4.** — *Soient $G$ un groupe abélien et $m_1, \ldots, m_n$ des entiers deux à deux premiers entre eux. Si, pour tout $i$, $G$ contient un élément d'ordre $m_i$, alors $G$ contient un élément d'ordre $m_1 \ldots m_n$.*

**Définition 4.5.** — Soit $G$ un groupe abélien fini. On appelle *exposant* de $G$, noté $\omega(G)$, le plus petit commun multiple des ordres des éléments de $G$ :

$$\omega(G) = \operatorname*{ppcm}_{g \in G} \omega(g).$$

**Lemme 4.6.** — *Soit $G$ un groupe abélien fini. Alors $G$ admet un élément d'ordre $\omega(G)$.*

On rappelle qu'un groupe abélien fini $G$ est dit cyclique s'il est isomorphe au groupe $\mathbb{Z}/\#G\mathbb{Z}$. Cela revient à demander que $G$ possède un élément d'ordre $\#G$.

**Théorème 4.7.** — *Soit $G$ un groupe abélien fini tel que pour tout $n$ divisant $\#G$, il y ait dans $G$ au plus $n$ éléments d'ordre divisant $n$. Alors $G$ est cyclique.*

**Corollaire 4.8.** — *Soit $K$ un corps. Alors tout sous-groupe fini de $K^*$ est cyclique.*

**Corollaire 4.9.** — *Tout corps fini admet un élément primitif. Pour tout nombre premier $p$ et pour tout entier $n \geq 1$, il existe un polynôme primitif (donc, a fortiori, irréductible) de degré $n$ à coefficients dans $\mathbb{F}_p$.*

Blah table de Zech.
Blah sous-groupes de puissances.

# 5 Extensions de corps finis : propriétés relatives, Frobenius, racines conjuguées, norme et trace

On a vu que tout corps fini contenait un sous-corps premier $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On se propose maintenant d'étudier les extensions $\mathbb{F}_q \subset \mathbb{F}_{q'}$ de corps finis en général.

**Lemme 5.1.** — *Soient $m$ et $n$ deux entiers naturels, $m$ supposé non nul, et $r$ le reste de la division euclidienne de $n$ par $m$. Alors dans $\mathbb{Z}[X]$ on a*

$$X^n - 1 \equiv X^r - 1 \mod X^m - 1.$$

*Démonstration.* Écrivons $n = dm + r$. Alors

$$\begin{aligned}(X^n - 1) - (X^r - 1) &= X^n - X^r \\ &= X^r(X^{dm} - 1) \\ &= X^r(X^m - 1)(X^{(d-1)m} + X^{(d-2)m} + \cdots + X^m + 1)\end{aligned}$$

est bien divisible par $X^m - 1$. □

**Lemme 5.2.** — *Soient $m$, $n$ et $p$ trois entiers naturels, $m$ et $p$ non nuls. Alors $X^{p^m} - X$ divise $X^{p^n} - X$ si et seulement si $m$ divise $n$.*

*Démonstration.* Simplifiant par $X$, la première condition équivaut à demander que $X^{p^m-1} - 1$ divise $X^{p^n-1} - 1$, ce qui par le lemme précédent èquivaut à ce que $p^m - 1$ divise $p^n - 1$. Appliquant à nouveau ce lemme, en évaluant en $p$ les polynômes considérés, on trouve

$$p^n - 1 \equiv p^r - 1 \mod p^m - 1,$$

de sorte que $p^m - 1$ divise $p^n - 1$ si et seulement si $m$ divise $n$. □

**Théorème 5.3.** — *Soient $p$ un nombre premier, $n$ un entier non nul, $q' = p^n$, et $q$ un entier naturel. Alors $\mathbb{F}_{q'}$ admet un sous-corps de cardinal $q$ si et seulement si $q = p^m$ avec $m$ divisant $n$ (i.e. si et seulement si $q'$ est une puissance de $q$), et un tel sous-corps est alors unique : ses éléments sont les racines de $X^q - X$.*

**Corollaire 5.4.** — *Soient $q$ une puissance d'un nombre premier et $d \geq 1$ un entier naturel. Alors $\mathbb{F}_q$ admet une extension élémentaire de degré $d$ (isomorphe à $\mathbb{F}_{q^d}$). Autrement dit, $\mathbb{F}_q[X]$ admet des polynômes irréductibles en tout degré.*

*Démonstration.* En effet, $q^d$ est encore une puissance de nombre premier, et par le théorème, $\mathbb{F}_q$ est un sous-corps de $\mathbb{F}_{q^d}$. Ceci étant, n'importe quel élément primitif de $\mathbb{F}_{q^d}^*$ engendre alors $\mathbb{F}_{q^d}$ comme extension de $\mathbb{F}_q$. □

**Exemple 5.5.** — Les corps $\mathbb{F}_4$ et $\mathbb{F}_8$ sont des extensions de $\mathbb{F}_2$, mais il n'existe pas d'inclusion de $\mathbb{F}_4$ dans $\mathbb{F}_8$. Le plus petit corps fini contenant simultanément $\mathbb{F}_4$ et $\mathbb{F}_8$ est $\mathbb{F}_{64}$.

Soient $q$ une puissance d'un nombre premier et $d \geq 1$ un entier naturel. Considérons l'application

$$\begin{array}{rccc} \varphi : & \mathbb{F}_{q^d} & \longrightarrow & \mathbb{F}_{q^d} \\ & x & \mapsto & x^q. \end{array}$$

On a alors $\varphi(0) = 0$, $\varphi(1) = 1$ et, pour tous $x, y \in \mathbb{F}_{q^d}$, $\varphi(x+y) = x + y$ et $\varphi(xy) = \varphi(x)\varphi(y)$ (l'avant-dernière égalité résultant du lemme 3.4). Ainsi $\varphi$ est un endomorphisme du corps $\mathbb{F}_{q^d}$. Ceci implique que $\varphi$ est injectif (proposition 2.2), donc bijectif puisque $\mathbb{F}_{q^d}$ est fini. En fait pour tout $x \in \mathbb{F}_{q^d}$ on a $\varphi^d(x) = x^{q^d} = x$, de sorte que $\varphi^d$ est l'identité de $\mathbb{F}_{q^d}$, et l'on voit que l'inverse de $\varphi$ est $\varphi^{d-1}$. Remarquons par ailleurs que $\mathbb{F}_{q^d}$ contient $\mathbb{F}_q$ comme sous-corps, et qu'un élément $x$ de $\mathbb{F}_{q^d}$ appartient à $\mathbb{F}_q$ si et seulement s'il vérifie $x^q = x$, autrement dit, si et seulement s'il est laissé invariant par $\varphi$. Les éléments de $\mathbb{F}_q$ étant invariants sous $\varphi$, on conclut que $\varphi$ est un automorphisme de $\mathbb{F}_{q^d}$ vu comme extension de $\mathbb{F}_q$.

**Définition 5.6.** — L'application ainsi définie, notée $\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_q}$ ou $\mathrm{Frob}_{\mathbb{F}_{q^d}/\mathbb{F}_q}$, est appelée automorphisme de Frobenius de $\mathbb{F}_{q^d}$ sur $\mathbb{F}_q$.

**Proposition 5.7.** — *Les corps intermédiaires entre $\mathbb{F}_q$ et $\mathbb{F}_{q^d}$ sont les $\mathbb{F}_{q^k}$ pour $k$ divisant $d$. Pour un tel $k$ on a*

$$\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_{q^k}} = (\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_q})^k$$

*et un élément $x$ de $\mathbb{F}_{q^d}$ appartient à $\mathbb{F}_{q^k}$ si et seulement s'il est invariant sous $\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_{q^k}}$, autrement dit, s'il vérifie $x^{q^k} = x$.*

*Démonstration.* C'est une conséquence directe du théorème 5.3 et de la définition du Frobenius. □

**Lemme 5.8.** — *Soit $\varphi$ un automorphisme d'une extension $L$ d'un corps $K$. Alors pour tous $P \in K[X]$ et $x \in L$ on a*

$$\varphi(P(x)) = P(\varphi(x)).$$

*Démonstration.* Notons $P(X) = \sum_i a_i X^i$, avec $a_i \in K$, de sorte que $\varphi(a_i) =$

$a_i$. Alors

$$\begin{aligned}\varphi(P(x)) &= \varphi(\sum_i a_i x^i) \\ &= \sum_i \varphi(a_i)\varphi(x)^i \\ &= \sum_i a_i \varphi(x)^i \\ &= P(\varphi(x)),\end{aligned}$$

ce qu'il fallait démontrer. □

**Théorème 5.9.** — *Soient $q$ une puissance d'un nombre premier et $d \geq 1$ un entier.*

1. *Si $x$ est un élément de $\mathbb{F}_{q^d}$, le plus petit entier non nul $k$ tel que $x^{q^k} = x$ est un diviseur de $d$. Le polynôme*

$$P(X) = (X - x)(X - x^q)(X - x^{q^2}) \dots (X - x^{q^{k-1}}),$$

   *à coefficients dans $\mathbb{F}_{q^d}$, est en fait à coefficients dans $\mathbb{F}_q$, et est irréductible sur $\mathbb{F}_q$ ; c'est donc le polynôme minimal de $x$ sur $\mathbb{F}_q$.*
2. *Inversement, soient $P \in \mathbb{F}_q[X]$ un polynôme irréductible, et $k$ son degré. Alors $P$ admet une racine $x$ dans $\mathbb{F}_{q^d}$ si et seulement si $k$ divise $d$, et alors $P$ y admet toutes ses racines, qui sont $x$, $x^q$, ..., $x^{q^{k-1}}$.*

*Démonstration.* Les entiers $j$ tels que $x^{q^j} = x$ forment un sous-groupe additif de $\mathbb{Z}$. Ce sous-groupe contenant $d$, son générateur positif $k$ est un diviseur de $d$. Puisque $x^{q^k} = x$, le Frobenius $\varphi_{\mathbb{F}_{q^d}/\mathbb{F}_q}$ induit une permutation de $\{x, x^q, \dots, x^{q^{k-1}}\}$, donc laisse $P$ inchangé. Les éléments de $\mathbb{F}_{q^d}$ invariants sous le Frobenius étant précisément ceux qui appartiennent au sous-corps $\mathbb{F}_q$, on voit que $P$ est bien à coefficients dans $\mathbb{F}_q$. Supposons maintenant $P = QR$ avec $Q$ et $R$ unitaires à coefficients dans $\mathbb{F}_q$. Puisque $x$ est racine de $P$, on peut supposer par exemple $x$ racine de $Q$. Alors, par le lemme (appliqué avec pour $\varphi$ le Frobenius), $x^q$, $x^{q^2}$, ..., $x^{q^{k-1}}$ sont aussi racines de $Q$, et la minimalité de $k$ implique que les $k$ racines ainsi obtenues sont toutes distinctes. On a donc $Q = P$, ce qui prouve l'irréductibilité. Plaçons-nous maintenant sous les hypothèses de la seconde assertion. On peut sans perte de généralité supposer $P$ unitaire. Si $P$ admet une racine $x$ dans $\mathbb{F}_{q^d}$, alors $P$ est le polynôme minimal de $x$ sur $\mathbb{F}_q$, et on conclut à l'aide du point précédent. Inversement, si $P$ est de degré $k$ divisant $d$, considérons une extension $\mathbb{F}_{q^{\lambda d}}$ de $\mathbb{F}_{q^d}$ dans laquelle $P$ admette une racine $x$. Alors $\mathbb{F}_q[x] \simeq \mathbb{F}_q[X]/P$ est un sous-corps de cardinal $q^k$ de $\mathbb{F}_{q^{\lambda d}}$ et donc, par le résultat d'unicité dans le théorème 5.3, coïncide avec l'unique sous-corps de cardinal $q^k$ de $\mathbb{F}_{q^d}$. Ainsi on a $x \in \mathbb{F}_{q^d}$, et on conclut comme précédemment. $\square$

**Corollaire 5.10.** — *Les groupe des automorphismes de $\mathbb{F}_{q^d}$ au-dessus de $\mathbb{F}_q$ est cyclique de cardinal $d$, engendré par le Frobenius.*

*Démonstration.* On rappelle que $\mathbb{F}_{q^d}$ est une extension élémentaire de $\mathbb{F}_q$. Soient $x$ un générateur de cette extension et $\varphi$ un automorphisme de $\mathbb{F}_{q^d}$ au-dessus de $\mathbb{F}_q$. Tout élément de $\mathbb{F}_{q^d}$ peut s'écrire sous la forme $Q(x)$ où $Q$ est un polynôme à coefficients dans $\mathbb{F}_q$, et alors, par le lemme, l'image de cet élément par $\varphi$ est $Q(\varphi(x))$. Ainsi $\varphi$ est déterminé par sa valeur en $x$. Mais par ailleurs, toujours par le lemme, $\varphi$ doit permuter les racines du polynôme minimal de $x$, qui sont précisément les images de $x$ sous les puissances du Frobenius. Ainsi $\varphi$ est bien une puissance du Frobenius. $\square$

**Définition 5.11.** — Soit $K \subset L$ une extension finie de corps. On dit que deux éléments de $L$ sont *conjugués* sur $K$ s'ils ont même polynôme minimal sur $K$.

**Corollaire 5.12.** — *Deux éléments $x$ et $y$ de $\mathbb{F}_{q^d}$ sont conjugués sur $\mathbb{F}_q$ si et seulement s'il existe $j$ tel que $y = x^{q^j}$.*

Soit $K \subset L$ une extension finie de corps. Si $x$ est un élément de $L$, la multiplication par $x$ est un endomorphisme $K$-linéaire du $K$-espace vectoriel $L$.

**Définition 5.13.** — Avec ces notations, on définit la *trace* de $x$, notée $\mathrm{Tr}_{L/K}(x)$, et la *norme* de $x$, notée $\mathrm{N}_{L/K}(x)$, comme la trace et le déterminant de cette application linéaire.

**Remarque 5.14.** — Après choix d'une base de $L$ sur $K$, la construction qui précède permet de voir les éléments de $L$ comme des matrices carrées de taille $n = [L : K]$ à coefficients dans $K$, l'addition et la multiplication de $L$ correspondant à l'addition et à la multiplication usuelle des matrices, et les éléments de $K \subset L$ s'identifiant aux matrices diagonales.

**Exemple 5.15.** — $\mathbb{R} \subset \mathbb{C}$

**Proposition 5.16.** — *Soit $K \subset L$ une extension de corps. Alors la trace est une application $K$-linéaire de $L$ dans $K$, et la norme induit un homomorphisme de groupes de $L^*$ dans $K^*$. Plus précisément, pour $\lambda \in K$ et $x, y \in L$, on a :*

- $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$
- $\mathrm{Tr}(\lambda x) = \lambda \,\mathrm{Tr}(x)$
- $\mathrm{Tr}(1) = [L : K]$
- $N(xy) = N(x)N(y)$
- $N(\lambda) = \lambda^{[L:K]}$.

**Lemme 5.17.** — *$F \subset K \subset L$ $x \in K$ $\mathrm{Tr}_{L/F}(x) = [L : K]\,\mathrm{Tr}_{K/F}(x)$ $\mathrm{N}_{L/F}(x) = \mathrm{N}_{K/F}(x)^{[L:K]}$*

**Théorème 5.18.** — *Trace somme puissances Frobenius, norme produit...*

**Corollaire 5.19.** — *$F \subset K \subset L$ corps finis $\mathrm{Tr}_{L/F} = \mathrm{Tr}_{K/F} \circ \mathrm{Tr}_{L/K}$ $\mathrm{N}_{L/F} = \mathrm{N}_{K/F} \circ \mathrm{N}_{L/K}$*

**Définition 5.20.** — caractère

**Lemme 5.21** (d'indépendance des caractères)**.** —

**Proposition 5.22.** — *corps finis, norme et trace surjectives*

# 6 Algorithme de factorisation de Berlekamp

Blah.

# 7 Exercices

**Exercice 7.1** a) Soient $K$ un corps, $F$ et $G$ deux polynômes à coefficients dans $K$ premiers entre eux, et $P = FG$. Considérons l'application

$$f : \begin{array}{ccc} K[X]/P & \longrightarrow & K[X]/F \times K[X]/G \\ H \mod P & \mapsto & (H \mod F, H \mod G). \end{array}$$

i. Montrer que $f$ est un homomorphisme d'anneaux et de $K$-espaces vectoriels.

ii. Quel est le noyau de $f$ ? Quelles sont les dimensions sur $K$ des espaces de départ et d'arrivée ? En déduire que $f$ est bijectif.

iii. Trouver des éléments de $K[X]/P$ dont l'image par $f$ est $(1, 0)$ ou $(0, 1)$ (on pourra utiliser une relation de Bézout entre $F$ et $G$). Expliciter l'isomorphisme inverse de $f$.

b) Soit $P \in K[X]$ se décomposant en produit $P = P_1^{e_1} \dots P_r^{e_r}$, les $P_i$ étant irréductibles et deux à deux distincts, et les $e_i$ non nuls.

i. Montrer qu'on a un isomorphisme d'anneaux et de $K$-espaces vectoriels
$$K[X]/P \simeq K[X]/P_1^{e_1} \times \cdots \times K[X]/P_r^{e_r}$$
qui envoie $X$ sur $(X, \dots, X)$. Expliciter l'isomorphisme inverse.

ii. On rappelle qu'un élément $a$ d'un anneau est dit *idempotent* s'il vérifie $a^2 = a$, ce qui équivaut à demander que la multiplication par $a$ soit un projecteur. Montrer que le nombre d'idempotents de $K[X]/P$ est égal à $2^r$ (on pourra commencer par montrer que dans un anneau de la forme $K[X]/Q^e$ avec $Q$ irréductible et $e \geq 1$, les seuls idempotents sont 0 et 1).

iii. On rappelle qu'un élément $a$ d'un anneau est dit *nilpotent* si une certaine puissance de $a$ est nulle. Un anneau est dit *réduit* s'il n'admet pas d'élément nilpotent non nul. Montrer que $K[X]/P$ est réduit si et seulement s'il est isomorphe à un produit de corps, ou encore si et seulement si $P$ est sans facteurs multiples dans $K[X]$.

**Exercice 7.2** a) Donner la liste des polynômes irréductibles de degré 1, 2, 3 et 4 sur $\mathbb{F}_2$.

b) Soit $\gamma$ un élément de $\mathbb{F}_{16}$ racine du polynôme $X^4 + X + 1$. Écrire les puissances de $\gamma$ comme des polynômes en $\gamma$ de degré au plus 3 à coefficients dans $\mathbb{F}_2$. En déduire que $X^4 + X + 1$ est primitif sur $\mathbb{F}_2$.

c) Quels sont les sous-groupes du groupe multiplicatif $\mathbb{F}_{16}^*$ ?

d) Quels sont les sous-corps de $\mathbb{F}_{16}$ ?

e) Parmi les polynômes obtenus à la question a), quels sont ceux qui admettent des racines dans $\mathbb{F}_{16}$ ? Pour chacun, dire quelles sont ces racines.

f) Quels sont les polynômes primitifs de degré 4 sur $\mathbb{F}_2$ ?

g) Quel est le degré minimal possible d'un polynôme non nul à coefficients dans $\mathbb{F}_2$ qui s'annule en $\gamma^5$, $\gamma^6$ et $\gamma^7$ ?

**Exercice 7.3** a) Combien y a-t-il de polynômes irréductibles de degré 3 sur $\mathbb{F}_3$ ? Parmi ceux-ci, combien sont-ils primitifs, et combien ne le sont-ils pas ?

b) Même question pour les polynômes de degré 5 sur $\mathbb{F}_2$.

c) Même question pour les polynômes de degré 6 sur $\mathbb{F}_2$.

d) Même question pour les polynômes de degré 12 sur $\mathbb{F}_2$.

Soit $d$ un entier. On rappelle qu'un élément $x$ d'un corps $K$ est dit être une racine primitice $d$-ième de l'unité si on a $x^d = 1$ mais $x^c \neq 1$ pour tout diviseur strict $c$ de $d$.

On définit le $d$-ième polynôme cyclotomique $\Phi_d$, à coefficients dans $\mathbb{Z}$, par la formule

$$\Phi_d(X) = \frac{X^d - 1}{\mathrm{ppcm}(X^c - 1)_{c|d, c\neq d}}.$$

On note $\varphi$ la fonction indicatrice d'Euler.

**Exercice 7.4** a) Montrer que $\Phi_d$ est de degré $\varphi(d)$.

b) Soit $K$ un corps. Montrer qu'un élément $x$ de $K$ est une racine primitive $d$-ième de l'unité si et seulement si $\Phi_d(x) = 0$.

**Exercice 7.5**

Soient $q \geq 2$ une puissance d'un nombre premier et $n \geq 1$ un entier.

a) Notons $\mathcal{S}$ l'ensemble des polynômes irréductibles sur $\mathbb{F}_q$ de degré divisant $n$. Montrer :

$$\prod_{P \in \mathcal{S}} P(X) = X^{q^n} - X.$$

b) Notons $\mathcal{T}$ l'ensemble des polynômes primitifs de degré $n$ sur $\mathbb{F}_q$. Montrer :

$$\prod_{P \in \mathcal{T}} P(X) = \Phi_{q^n - 1}(X).$$

**Exercice 7.6**

Soient $q \geq 2$ une puissance d'un nombre premier et $d$ un entier premier à $q$. Quels sont les entiers $k$ tels que $\mathbb{F}_{q^k}$ contienne une racine primitive $d$-ième de l'unité ?

**Exercice 7.7**

Soient $q \geq 2$ une puissance d'un nombre premier et $P$ un polynôme à coefficients dans $\mathbb{F}_q$.

a) Soit $d$ un diviseur de $q-1$. Notons $\mathcal{U}$ l'ensemble des racines non nulles de $P$ dans $\mathbb{F}_q$ qui sont des puissances $d$-ièmes. Montrer :

$$\operatorname{pgcd}(P(X), X^{\frac{q-1}{d}} - 1) = \prod_{\alpha \in \mathcal{U}} (X - \alpha).$$

b) Soit $n \geq 1$ un entier. Notons $\mathcal{V}$ l'ensemble des racines de $P$ dans $\mathbb{F}_{q^n}$. Montrer que le polynôme

$$\prod_{\alpha \in \mathcal{V}} (X - \alpha)$$

sur $\mathbb{F}_{q^n}$ est en fait à coefficients dans $\mathbb{F}_q$. Donner une formule permettant de calculer facilement ce polynôme.

**Exercice 7.8**
Soient $q \geq 2$ une puissance d'un nombre premier et $n$ un entier. Soit $x$ un élément primitif de $\mathbb{F}_{q^n}$. Montrer que la norme $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)$ de $x$ est un élément primitif de $\mathbb{F}_q$.

**Exercice 7.9**
Factoriser le polynôme

$$X^{11} + X^{10} + X^9 + X^8 + X^7 + X^5 + X^3 + X + 1$$

sur $\mathbb{F}_2$.