Leçon 123 : Corps finis. Applications

1 Extensions de corps

Les corps considérés dans cette leçon seront supposés commutatifs.

1.1 Notion d'extension de corps

Définition 1 (BER 767)**.** Une extension de $\mathbb{K}$ est un corps $\mathbb{L}$ contenant $\mathbb{K}$ comme sous-corps. On le note $\mathbb{L}/\mathbb{K}$.

Définition 2 (BER 767)**.** On appelle degré de $\mathbb{L}/\mathbb{K}$ la dimension de $\mathbb{L}$ comme $\mathbb{K}$-espace vectoriel. On le note $[\mathbb{L} : \mathbb{K}]$.

Définition 3 (BER 768)**.** Une sous-extension de $\mathbb{L}/\mathbb{K}$ est une extension $\mathbb{L}'/\mathbb{K}$ tel que $\mathbb{L}'$ soit un sous-coprs de $\mathbb{L}$.

Théorème 4 (BER 769)**.** [base télescopique] Soient $\mathbb{M}/\mathbb{K}$ et $\mathbb{L}/\mathbb{M}$ des extension de corps. Alors $\mathbb{L}/\mathbb{K}$ est de degré fini si et seulement si $\mathbb{L}/\mathbb{M}$ et $\mathbb{M}/\mathbb{K}$ le sont.

Dans ce cas, $[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}]$.

Définition 5 (BER 770)**.** Soit I une partie de $\mathbb{L}$. On note $\mathbb{K}(I)$ l'intersection des sous-corps de $\mathbb{L}$ contenant $\mathbb{K}$ et I. C'est donc la plus petite sous-extension de $\mathbb{L}/\mathbb{K}$ contenant I.
L'extension $\mathbb{K}(I)/\mathbb{K}$ s'appelle la sous-extension de $\mathbb{L}/\mathbb{K}$ engendré par I.

Notation 6 (BER 770)**.** Si $I = \{s_1, .., s_n\}$, on note $\mathbb{K}(s_1, ..., s_r)/\mathbb{K}$

1.2 Corps de rupture

Définition 7 (PER 70, ROM 418, BER 816)**.** On dit qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de rupture d'un polynôme non constant $P \in \mathbb{K}[X]$ si le polynôme P a une racine ω dans $\mathbb{L}$ telle que $\mathbb{L} = \mathbb{K}(\omega)$.

Théorème 8 (PER 70)**.** Soit $P \in \mathbb{K}[X]$ irréductible. Il existe un corps de rupture de P sur K, unique à isomorphisme près.

Exemple 9 (BER 818)**.** Prenons $P = X(X^2+1) \in \mathbb{Q}[X]$. $\mathbb{Q}/\mathbb{Q}$ et $\mathbb{Q}(i)/\mathbb{Q}$ sont deux corps de rupture de P. Ceci montre qu'il n'y a pas unicité. De plus ces extension ne sont pas isomorphe car elles n'ont pas le même degré A voir la derniere rem!!!

Exemple 10 (BER 818, PER 71)**.** Considérons $P = X^3 - 2 \in \mathbb{Q}[X]$. Un corps de rupture de P est par exemple $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Notons que ce corps n'admet pas d'éléments complexes alors que P admet 2 autres racines complexes. On constate donc qu'un polynôme n'a pas forcément toutes ses racines dans un même coprs de rupture. Ceci emmène à la définition suivante.

1.3 Corps de décomposition

Définition 11 (BER 819, PER 71)**.** Soit $P \in \mathbb{K}[X]$ non constant. Un corps de décomposition de P est une extension $\mathbb{L}/\mathbb{K}$ vérifiant :

1. P se décompose en facteurs de degré 1 dans $\mathbb{L}[X]$
2. $\mathbb{L} = \mathbb{K}(\alpha_1, .., \alpha_n)$, où $\alpha_1, ..., \alpha_n \in \mathbb{L}$ sont les racines de P dans $\mathbb{L}$.

Théorème 12 (PER 71)**.** Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$, unique à isomorphisme près. On le note $D_{\mathbb{K}}(P)$.

Application 13. Dans BER application à F_q, à voir soit là soit parite app

Exemple 14 (PER 72)**.** Si on reprend le polynôme $P = X^3 - 2$, on a $D_{\mathbb{Q}}(P)$.

2 Corps finis

2.1 Premier exemple de corps fini

Proposition 15 (BER 393)**.** Soit A un anneau. Alors A contient un sous-anneau isomorphe à $\mathbb{Z}/car(A)\mathbb{Z}$.

Proposition 16 (BER 399)**.** Soit $n \geq 1$. Alors $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier. Dans le cas $\mathbb{Z}/n\mathbb{Z}$ est un corps.

Corollaire 17 (BER 399)**.** La caractéristique d'un anneau intègre est soit nulle, soit un nombre premier.

Proposition 18 (BER 651)**.** Soit K un corps fini. Alors $|K|$ est une puissance non triviale d'un nombre premier p. De plus, $car(K) = p$

question qui se pose : existe t-il au moins un corps à q éléments (si q puissance d'un nombre premier) et si oui combien à isomorphisme près ?

2.2 Théorème de Wedderburn : motivation

Définition 19 (TL1 309)**.** Le $n-$ème polynôme cyclotomique est le polynôme unitaire ϕ_n dont les racines sont les racines primitives $n-$ème de l'unité : $\phi_n(X) = \prod_{\xi \in \mathbb{U}_n^*} (X - \xi)$

Lemme 20 (ROM 420)**.** Pour tout entier $n \geq 2$ et tout entier $a \geq 2$, on a $|\phi_n(a)| > a - 1$.

Définition 21 (ROM 419)**.** Un anneau à division est un anneau unitaire dans lequel tout élément non nul est inversible

On considère $\mathbb{K}$ un anneau à division

Notation 22 (ROM 419/420)**.** On note $Z(\mathbb{K})$ le centralisateur de $\mathbb{K}$ et pour tout $x \in \mathbb{K}^*$, on introduit $Z_x := \{y \in \mathbb{K} | xy = yx\}$.

Lemme 23 (ROM 419,420 ; Need théorie extension de corps)**.**
1. $Z(\mathbb{K})$ est un corps commutatif et il existe un entier $r \geq 1$ tel que $card(\mathbb{K}) = (card(Z(\mathbb{K})))^r$.
2. Pour tout $x \in \mathbb{K}^*$, Z_x est un corps qui contient $Z(\mathbb{K})$ et il existe un entier $r_x \geq 1$ qui divise r tel que $card(Z_x) = (card(Z(\mathbb{K})))^{r_x}$

Théorème 24 (BER 648, ROM 421)**.** [Wedderburn] Tout anneau à division fini est commutatif.

Ce théorème nous dit donc que tout corps fini est commutatif, ce qui nous ouvre la théorie de la partie précédente à tout corps finis.

Là changer : 1 partie sur existence et unicité corps fini (corps décompo ; autre construction : corps de rupture + dev !

2.3 Existence et unicité des corps fini

Soit p un nombre premier et soit $n \in \mathbb{N}^*$. On pose $q = p^n$.

Théorème 25 (PER 73)**.**
1. Il existe un corps K à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.
2. En particulier, $\mathbb{K}$ est unique, à isomorphisme près. On le note $\mathbb{F}_q$.

On a l'existence et l'unicité, on sait le construir avec les corps de décomposition mais on aimerait se ramener aux corps de rupture car plus sympatique avec lesquelles travailler.

2.4 Construction polynôme irréductible

Proposition 26 (BER 615)**.** Soit $\mathbb{K}$ un corps et soit $P \in \mathbb{K}[X]$ un polynôme de degré $d \geq 1$. Alors l'anneau quotient $\mathbb{K}[X]/(P)$ est une $\mathbb{K}-$algèbre de dimension d de base $(\overline{1}, ..., \overline{X^{d-1}})$.

Corollaire 27 (BER 651)**.** Soit $P \in \mathbb{F}_p$ un polynôme irréductible de degré $n \geq 1$. Alors $\mathbb{F}_p[X]/(P)$ est un corps. De plus, c'est aussi un $\mathbb{F}_p-$espace vectoriel de base $(\overline{1}, \overline{X}, ..., \overline{X}^{n-1})$. En particulier, il a p^n éléments.

Méthode 28 (BER 651)**.** Si l'on dispose d'un polynôme irréductible $P \in \mathbb{F}_p$ de degré $n \geq 1$, on peut donc construire un corps à p^n éléments facilement.

question qui vient : étant donné un nombre premier p, existe t-il des polynômes irréductibles à coefficients dans $\mathbb{F}_p$ de tout degré ?

Notation 29 (ROM 422)**.** Dans la suite, on considère P_n le polynôme $X^{p^n} - X$ où $n \in \mathbb{N}$ et $p \geq 2$ est un nombre premier.
On note également $U_n(p)$ l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré n ; et $I_n(p)$ le cardinal de cet ensemble.

Lemme 30 (ROM 422, DEV1)**.** 1. Soit $P \in \mathbb{F}_p[X]$. $P|P_n \implies deg(P)|n$
2. Soit $d|n$. Tout $P \in U_d(p)$ divise P_n.

Proposition 31 (ROM 422,DEV1)**.** $\forall n \in \mathbb{N}^*$, $nI_n(p) = \sum_{d|n} \mu(\frac{n}{d})p^d$ où μ est la fonction de Möbius

Corollaire 32 (BER 656)**.** Il existe un polynôme irréductible unitaire de degré n dans $\mathbb{F}_p[X]$.

Théorème 33 (BER 656, A voir)**.** Soit $q = p^n$, où p est un nombre premier et $n \geq 1$. Alors il existe un corps fini à q éléments, unique à isomorphisme près. De plus, tout morphisme entre deux corps finis à q éléments est un isomorphisme de $\mathbb{F}_q-$algèbres.

3 Application

3.1 Résolution d'équations de degré 2

Considérons $q = p^n$ où p est un nombre premier. On pose $\mathbb{F}_q = \{x \in \mathbb{F}_q | \exists y \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{2*} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$.

Proposition 34 (PER 74, BER)**.** 1. Pour $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$.
2. Pour $p > 2$, on a $|\mathbb{F}_q| = \frac{q-1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Proposition 35 (PER 75,BER)**.** [caractérisation des carrés] On suppose $p > 2$. Alors on a

$$x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$$

Exemple 36 (PER 75,BER)**.** Si $q = 7$, on a $\mathbb{F}_q = \mathbb{Z}/7\mathbb{Z}$ et $\frac{q-1}{2} = 3$. On a par exemple $2^3 = 8 \equiv 1 \pmod 7$ et $3^3 = 27 \equiv -1 \pmod 7$ donc 2 est un carré dans $\mathbb{F}_7$ mais pas 3.

Proposition 37 (PER 75,BER)**.** -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \pmod 4$.

Définition 38 (ROM 428,BER)**.** [Symbole de Legendre] def symbole de Legendre

Exemple 39 (ROM 438,BER)**.** $\left(\frac{1}{p}\right) = 1$
$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = ...$

Théorème 40 (ROM 434,BER)**.** [Admis] Loi de réciprocité quadratique

Exemple 41. BER 508 $\left(\frac{103}{173}\right)$

3.2 Irréductibilité

Théorème 42 (PER 82, DEV 2)**.** Pour $n \geq 1$, $\varphi_n(X) \in \mathbb{Z}[X]$ est un polynôme irréductible et unitaire, donc irréductible dans $\mathbb{Q}[X]$ également.

Théorème 43 (GOU 62)**.** [Eisenstein] Soit $P = a_nX^n + .. + a_1X + a_n \in \mathbb{Z}[X]$ et p un nombre premier. Si on a :
1. p ne divise pas a_n
2. p divide a_i, pour tout $1 \leq i \leq n-1$
3. p^2 ne divise pas a_0

Alors P est irréductible dans $\mathbb{Q}[X]$.