Leçon 141 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

Extrait du rapport de jury

Les généralités sur les algèbres de polynômes à une variable sont supposées connues. Le bagage théorique permettant de définir corps de rupture et corps de décomposition doit être présenté. Ces notions doivent être illustrées dans différents types de corps (réel, rationnel, corps finis) ; Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$ ou $\mathbb{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques, par exemple les polynômes cyclotomiques. Le théorème de la base télescopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes sont incontournables. Des applications du corps de décomposition doivent être mentionnées, par exemple en algèbre linéaire.
Pour aller plus loin, on peut montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos, s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois.

Présentation de la leçon

Je vais vous présenter la leçon 141 intitulée : "Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.". Les premiers polynômes apparaissent dès l'antiquité, puis vint étude de résolution abstraite jusqu'à l'ordre deux. Cardan et Tartaglia s'attaquent aux équations cubiques, puis Ferrari à la quartique. Le problème reste en suspens jusqu'à ce que Ruffini et Abel s'approchent de la solution de degré supérieur à 5, où les idées de Lagrange seront exploitées pleinement par Galois.
On commence dans une première partie par introduire la notion d'irréductibilité d'un polynôme dans un anneau commutatif intègre avec tout d'abord quelques définitions. On commence par donner la définition d'un polynôme irréductible ainsi que d'une racine d'un polynôme. On donne ensuite un premier critère d'irréductibilité en fonction du degré du polynôme considéré ainsi que les premiers exemples de polynômes irréductibles. On donne ensuite quelques résultats sur l'anneau des polynômes. On termine cette première sous-partie en énonçant le lemme des noyaux qui est très utile dans le cadre de la réduction des endomorphismes. Dans une deuxième sous-partie, on donne les premiers critères d'irréductibilité de polynôme dans le cadre d'un anneau factoriel. On introduit tout d'abord la notion de contenu d'un polynôme afin d'énoncer le lemme de Gauss ainsi que le théorème du transfert. On termine cette deuxième sous-partie en énonçant quelques critères d'irréductibilité utiles : notamment le critère d'Eisenstein (très souvent pour montrer qu'un polynôme est irréductible sur $\mathbb{Q}[X]$) et le critère de réduction (très souvent pour simplifier l'expression d'un polynôme) que l'on agrémente de plusieurs exemples. On conclut cette partie avec un rapide dernier point qui fait le lien avec l'irréductibilité et les anneaux quotients.
Dans une deuxième partie, on s'intéresse aux extensions de corps. On commence tout d'abord par parler d'extensions et d'éléments algébriques. On introduit en premier lieu la notion d'extension de corps ainsi que le degré d'une extension et l'on donne plusieurs exemples d'extensions de corps ainsi que leurs degrés respectifs. On donne ensuite le théorème de la base télescopique qui est un résultat très important et utile dans la pratique pour trouver le degré d'une extension un peu délicate. On termine cette sous-partie en énonçant la définition d'un élément algébrique puis une caractérisation des éléments algébriques par le polynôme minimal avant de finir par la définition d'une extension algébrique. Dans une deuxième sous-partie, on s'intéresse aux corps de rupture et de décomposition en commençant par donner la définition d'un corps de rupture et on montre ensuite qu'il est unique à l'isomorphisme près. Puis on s'intéresse ensuite au corps de décomposition en donnant sa définition ainsi que quelques exemples classiques et en montrant qu'il est également unique à l'isomorphisme près. On termine cette sous-partie avec un premier théorème de l'élément primitif, un lien avec les endomorphismes trigonalisables ainsi que quelques critères d'irréductibilité. On consacre ensuite une dernière sous-partie aux clôtures algébriques en énonçant la définition d'un corps algébriquement clos, d'une clôture algébrique ainsi que quelques exemples classiques et on conclut avec le théorème de Steinitz.
On consacre ensuite une dernière partie à quelques exemples et applications. On

s'intéresse tout d'abord aux corps finis avec deux résultats techniques concernant le sous-corps premier et la caractéristique d'un corps avant de s'intéresser en profondeur aux corps finis avec tout d'abord un résultat sur le cardinal d'un corps fini, l'existence d'un corps fini de cardinal $q = p^n$ puis un deuxième théorème de l'élément primitif et enfin du dénombrement des polynômes unitaires irréductibles sur $\mathbb{F}_q$ grâce à la fonction de Möbius. On donne enfin une deuxième application concernant les polynômes cyclotomiques qui sont définis à partir des racines primitives n-ièmes de l'unité. On enchaîne avec la proposition 69 qui nous donne une relation très utile. En effet, cette relation est intéressante car celle-ci permet de construire de manière récurrente ces polynômes cyclotomiques (inutile désormais de passer par les racines primitives de l'unité pour le déterminer). De plus, ces polynômes possèdent la propriété non immédiate d'être dans $\mathbb{Z}[X]$ et d'être irréductible dans $\mathbb{Q}[X]$! Ce fait nous permet ainsi de déterminer le degré d'une extension cyclotomique donnée.

Plan général

Cours détaillé

I Irréductibilité

I.1 Définitions

Définition 1 : Polynôme irréductible [Perrin, p.46] :
On considère un anneau A commutatif intègre.
Un polynôme $P \in A[X]$ est un **polynôme irréductible** lorsque $P \notin A^\times$ et ses seuls diviseurs dans $A[X]$ sont les éléments inversibles de $A[X]$ et les associés du polynôme P.

Définition 2 : Racine d'un polynôme [Berhuy, p.426] :
On considère un anneau A commutatif intègre et $A \in \mathbb{K}[X]$.
On dit que $a \in A$ est une **racine de** P lorsque $P(a) = 0_A$.

Remarque 3 : [Berhuy, p.426]
La multiplicité de a comme racine de P est le plus grand entier naturel n tel que $P = (X-a)^n Q$ dans $A[X]$ et $Q(a) \neq 0_A$.

Proposition 4 : [Deschamps, p.15]
Soient $\mathbb{K}$ un corps commutatif et $P \in \mathbb{K}[X]$.
∗ Si $\deg(P) = 1$, alors P est irréductible.
∗ Si $\deg(P) > 1$ et P est irréductible, alors P n'a pas de racines dans $\mathbb{K}$.
∗ Si $\deg(P) \in \{2; 3\}$, alors P est irréductible dans $\mathbb{K}[X]$ si, et seulement si, P n'a pas de racines dans $\mathbb{K}$.

Exemple 5 : [Deschamps, p.15]
∗ Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.
∗ Les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 à discriminant strictement négatifs.
∗ Le polynôme $(X^2+1)^2 \in \mathbb{Q}[X]$ n'a pas de racines dans $\mathbb{Q}$ mais n'est pas irréductible.
∗ Le polynôme $2X$ n'est pas irréductible dans $\mathbb{Z}[X]$.

Proposition 6 : [Perrin, p.50]
Si $\mathbb{K}$ est un corps commutatif, alors $\mathbb{K}[X]$ est euclidien.

Proposition 7 : [Perrin, p.51]
Soit A un anneau commutatif.
$A[X]$ est principal si, et seulement si, A est un corps.

Lemme 8 : Lemme des noyaux [Deschamps, p.99] :
Soient $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$ et $P_1, ..., P_r$ des polynômes de $\mathbb{K}[X]$ non nuls et deux à deux premiers entre eux.
Si l'on note $P = \prod_{i=1}^{r} P_i$, alors on a :

$$\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{r} \mathrm{Ker}(P_k(u))$$

Remarque 9 :
La décomposition du polynôme caractéristique en produits de polynômes irréductibles d'un endomorphisme u sur un $\mathbb{K}$-espace vectoriel E assure une décomposition de E en sous-espaces stables par u.

I.2 Critères d'irréductibilité

Dans toute cette sous-partie, on considère un anneau A factoriel.

Définition 10 : Contenu d'un polynôme [Perrin, p.51] :
On considère un polynôme $P \in A[X]$.
On appelle **contenu de** P (et on note $c(P)$) le PGCD (défini modulo $A^\times$) des coefficients de P. De plus, P est dit **primitif** lorsque $c(P) = 1$.

Lemme 11 : Lemme de Gauss [Perrin, p.51] :
∗ Pour tous polynômes P, Q de $A[X]$ non nuls, on a $c(PQ) = c(P)c(Q)$.
∗ Le produit de deux polynômes primitifs est primitif.

Théorème 12 : [Perrin, p.51] :
Les polynômes $P \in A[X]$ irréductibles dans $A[X]$ sont exactement :
∗ Les constantes $p \in A$ irréductibles dans A.
∗ Les polynômes P de degré supérieur ou égal à 1, primitifs et irréductibles dans $\mathrm{Frac}(A)[X]$.

Exemple 13 :
Les polynômes $P \in \mathbb{Z}[X]$ irréductibles dans $\mathbb{Z}[X]$ sont exactement :
∗ Les nombres premiers (au sens usuel) ainsi que leurs opposés.
∗ Le polynômes P de degré supérieur ou égal à 1, primitifs et irréductibles dans $\mathbb{Q}[X]$.

Théorème 14 : Théorème de transfert [Perrin, p.51] :
Si A est factoriel, alors $A[X]$ est factoriel.

Proposition 15 : Critère d'irréductibilité d'Eisenstein [Perrin, p.76] :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$.
S'il existe un élément irréductible p tel que :
∗ p ne divise pas a_n. ∗ Pour tout $i \in [\![0; n-1]\!]$, p divise a_i.
∗ p^2 ne divise pas a_0.
alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 16 :
Les polynômes $X^n - 2$ et $X^4 - 6X^3 + 3X^2 - 12X + 3$ sont irréductibles dans $\mathbb{Q}[X]$.

Proposition 17 : Critère de réduction [Perrin, p.77] :
Soient I un idéal premier de A et $P \in A[X]$ unitaire.
Si $\overline{a}_n \neq 0$ dans A/I et si $\overline{P}$ est irréductible sur A/I ou $\mathrm{Frac}(A/I)$, alors le polynôme P est irréductible sur $\mathrm{Frac}(A)$.

Exemple 18 : [Perrin, p.77]
Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Q}[X]$ par le critère de réduction.

I.3 Irréductibilité et anneaux quotients

Proposition 19 :
Soient $\mathbb{K}$ un corps commutatif et $P \in \mathbb{K}[X]$.
P est irréductible dans $\mathbb{K}[X]$ si, et seulement si, $\mathbb{K}[X]/(P)$ est un corps.

Exemple 20 :
$\mathbb{R}[X]/(X^2+1)$ est un corps (car X^2+1 est irréductible dans $\mathbb{R}[X]$ puisqu'il est de degré 2 et ne possède pas de racine dans $\mathbb{R}[X]$).

II Extensions de corps

II.1 Extensions et éléments algébriques

Définition 21 : Extension de corps [Perrin, p.65] :
On considère $\mathbb{K}$ et $\mathbb{L}$ deux corps commutatifs quelconques.
On dit que $\mathbb{L}$ est une **extension de corps de** $\mathbb{K}$ lorsque $\mathbb{K} \subseteq \mathbb{L}$ et on la note $\mathbb{L}/\mathbb{K}$.

Exemple 22 : [Perrin, p.65]
∗ $\mathbb{C}$ est une extension de corps de $\mathbb{R}$.
∗ $\mathbb{Q}(i)$ est une extension de corps de $\mathbb{Q}$.

Définition 23 : Degré d'un extension de corps [Perrin, p.65] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$.
On appelle **degré de l'extension** $\mathbb{L}/\mathbb{K}$, la dimension de $\mathbb{L}$ vu comme $\mathbb{K}$-espace vectoriel et on la note $\dim_{\mathbb{K}} \mathbb{L}$ (ou encore $[\mathbb{L} : \mathbb{K}]$).

Exemple 24 :
∗ $\mathbb{C}$ est une extension de corps de $\mathbb{R}$ de degré 2.
∗ $\mathbb{Q}(i)$ est une extension de corps de $\mathbb{Q}$ de degré 2.
∗ $\mathbb{R}$ est une extension de corps de $\mathbb{Q}$ de degré infini (car $\mathbb{Q}$ est dénombrable).

Théorème 25 : Théorème de la base télescopique [Perrin, p.65] :
Soient $\mathbb{K}$, $\mathbb{L}$ et $\mathbb{M}$ trois corps commutatifs quelconques tels que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$.
Si $(e_i)_{i\in I}$ est une $\mathbb{K}$-base de $\mathbb{L}$ et $(f_j)_{j\in J}$ une $\mathbb{L}$-base de $\mathbb{M}$, alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ en temps de $\mathbb{K}$-espace vectoriel.
On a alors en particulier : $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 26 : Élément algébrique/transcendant [Perrin, p.66] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$, $\alpha \in \mathbb{L}$ ainsi que le morphisme de corps $\varphi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ tel que $\varphi|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$ et $\varphi(T) = \alpha$.
∗ Lorsque φ est injectif, il n'y a que le polynôme nul qui s'annule en α. On dit alors que α est **transcendant sur** $\mathbb{K}$.
∗ Lorsque φ n'est pas injectif, il existe $\mu_\alpha \in \mathbb{K}[T]$ non nul unitaire tel que $\mathrm{Ker}(\varphi) = (\mu_\alpha)$. On dit alors que α est **algébrique sur** $\mathbb{K}$ et que μ_α est le **polynôme minimal de** α **sur** $\mathbb{K}$.

Exemple 27 : [Perrin, p.66]
∗ Les nombres $\sqrt{2}$, i et $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs $X^2 - 2$, $X^2 + 1$ et $X^3 - 2$.
∗ Les nombres π et e sont transcendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$) [ADMIS].

Proposition 28 : Caractérisation des éléments algébriques [Perrin, p.66] :
Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha \in \mathbb{L}$.
Les assertions suivantes sont équivalentes :
∗ α est algébrique sur $\mathbb{K}$. ∗ On a $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
∗ On a $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < +\infty$ (plus précisément, $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg(\mu_\alpha)$).
∗ Il existe un unique polynôme $\mu_\alpha \in \mathbb{K}[X]$ unitaire et irréductible dans $\mathbb{K}[X]$ tel que $\mu_\alpha(\alpha) = 0_{\mathbb{K}}$.
∗ $\mathbb{K}(\alpha) = \mathrm{Vect}_{\mathbb{K}}(1_{\mathbb{K}}, \alpha, \alpha^2, ..., \alpha^{\deg(\mu_\alpha)-1})$.

Définition 29 : Extension finie/algébrique [Perrin, p.67] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$.
On dit que $\mathbb{L}/\mathbb{K}$ est une extension :
∗ **finie** lorsque $[\mathbb{L} : \mathbb{K}] < +\infty$.
∗ **algébrique** lorsque tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Théorème 30 : [Perrin, p.67]
Si $\mathbb{L}/\mathbb{K}$ une extension de corps, alors $M = \{x \in \mathbb{L} \text{ tq } x \text{ est algébrique sur } \mathbb{K}\}$ est un sous-corps de $\mathbb{L}$.

Remarque 31 : [Perrin, p.67]
La proposition 28 montre donc que toute extension finie est algébrique, cependant la réciproque est fausse comme le montre l'extension $A/\mathbb{Q}$ avec A le sous-corps de $\mathbb{C}$ égal à $\{\alpha \in \mathbb{C} \text{ tq } \alpha \text{ est algébrique sur } \mathbb{Q}\}$!

II.2 Corps de rupture et corps de décomposition

Dans toute cette sous-partie, on considère un corps $\mathbb{K}$ commutatif quelconque.

Définition 32 : Corps de rupture [Perrin, p.70] :
On considère $P \in \mathbb{K}[X]$ un polynôme irréductible dans $\mathbb{K}[X]$.
Une extension de corps $\mathbb{L}/\mathbb{K}$ est appelée **corps de rupture de** P **sur** $\mathbb{K}$ lorsque $\mathbb{L}$ est monogène $\mathbb{L} = \mathbb{K}(\alpha)$, avec $P(\alpha) = 0$.

Théorème 33 : [Perrin, p.70]
Soit $P \in \mathbb{K}[X]$ irréductible.
Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.
De plus, $\mathbb{K}[X]/(P)$ est un corps de rupture de P (si on note α la classe de X dans $\mathbb{K}[X]/(P)$, on a $P(X)$ congru à 0 modulo $P(X)$, c'est-à-dire $P(\alpha) = 0$. Ainsi, α est une racine de P dans $\mathbb{K}[X]/(P)$).

Définition 34 : Corps de décomposition [Perrin, p.71] :
On considère $P \in \mathbb{K}[X]$.
Une extension de corps $\mathbb{L}/\mathbb{K}$ est appelée **corps de décomposition de** P **sur** $\mathbb{K}$ lorsque dans $\mathbb{L}[X]$, P est produit de facteurs de degrés 1 et que le corps $\mathbb{L}$ est minimal pour cette propriété.

Exemple 35 :
∗ Pour $\mathbb{K} = \mathbb{Q}$, $P(X) = X^3 - 2$ a pour corps de décomposition $\mathbb{Q}\left(\sqrt[3]{2}, j\right)$.
∗ Pour $\mathbb{K} = \mathbb{Q}$, $P(X) = X^4 - 2$ a pour corps de décomposition $\mathbb{Q}\left(\sqrt[4]{2}, i\right)$.

Théorème 36 : [Perrin, p.71]
Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$ et il est unique à isomorphisme près.

Théorème 37 : Théorème de l'élément primitif (1) [Gourdon, p.96] :
Soient $\mathbb{K}$ un corps de caractéristique nulle.
Si $\mathbb{L}/\mathbb{K}$ est une extension de corps finie, alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

Exemple 38 :
On considère $\mathbb{L} = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ et $\mathbb{K} = \mathbb{Q}$.
En notant $a = \sqrt{2} + \sqrt{3}$, on a :

$$\left(a - \sqrt{2}\right)^2 = 3 \iff \sqrt{2} = \frac{a^2 - 1}{2a} \in \mathbb{K}(a)$$

$$\left(a - \sqrt{3}\right)^2 = 2 \iff \sqrt{2} = \frac{a^2 + 1}{2a} \in \mathbb{K}(a)$$

Donc $\mathbb{L} = \mathbb{Q}(a)$.

Proposition 39 :
Tout endomorphisme est trigonalisable sur le corps de décomposition de son polynôme minimal.

Proposition 40 : [Perrin, p.78]
Soit $P \in \mathbb{K}[X]$ de degré $n > 0$.
P est irréductible sur $\mathbb{K}$ si, et seulement si, P n'a pas de racines dans toute extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie $[\mathbb{L} : \mathbb{K}] \leq \frac{n}{2}$.

Remarque 41 :
Ce critère sera surtout utilisé avec les corps finis comme nous le verrons dans un exemple en III.1.

Proposition 42 : [Perrin, p.79]
Soient $\mathbb{K}$ un corps commutatif quelconque, $P \in \mathbb{K}[X]$ un polynôme irréductible de degré n et $\mathbb{L}/\mathbb{K}$ une extension de corps de degré m.
Si $\text{PGCD}(n, m) = 1$, alors P est encore irréductible dans $\mathbb{L}$.

Exemple 43 : [Perrin, p.79]
Le polynôme $X^3 + 4X + 2$ est irréductible sur $\mathbb{Q}[i]$ comme sur $\mathbb{Q}$.

II.3 Clôture algébrique

Définition 44 : Corps algébriquement clos [Perrin, p.67] :
On considère un corps $\mathbb{K}$ commutatif quelconque.
On dit que $\mathbb{K}$ est un **corps algébriquement clos** lorsqu'il vérifie l'une des propriétés équivalentes suivantes :
∗ Tout polynôme $P \in \mathbb{K}[X]$ de degré strictement positif admet une racine dans $\mathbb{K}$.
∗ Tout polynôme $P \in \mathbb{K}[X]$ est produit de polynômes de degré 1.
∗ Les éléments irréductibles de $\mathbb{K}[X]$ sont exactement les $X - a$ avec $a \in \mathbb{K}$.
∗ Si une extension $\mathbb{L}/\mathbb{K}$ est algébrique, alors $\mathbb{L} = \mathbb{K}$.

Exemple 45 : [Perrin, p.68]
∗ $\mathbb{C}$ est un corps algébriquement clos (théorème de D'Alembert-Gauss).
∗ Le corps A définit dans la remarque 31 est lui aussi algébriquement clos (c'est même la clôture algébrique de $\mathbb{Q}$).

Proposition 46 : [Gourdon, p.67]
Tout corps commutatif algébriquement clos est infini.

Définition 47 : Clôture algébrique [Perrin, p.72] :
On considère $\mathbb{K}$ un corps commutatif quelconque.
Une extension $\overline{\mathbb{K}}$ de $\mathbb{K}$ est appelée **clôture algébrique de** $\mathbb{K}$ lorsque $\overline{\mathbb{K}}$ est algébriquement clos et que $\overline{\mathbb{K}}$ est algébrique sur $\mathbb{K}$.

Exemple 48 : [Perrin, p.72]
∗ $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$. ∗ A est une clôture algébrique de $\mathbb{Q}$.

Théorème 49 : Théorème de Steinitz [ADMIS] [Berhuy, p.827] :
Tout corps $\mathbb{K}$ commutatif admet une clôture algébrique unique à isomorphisme près.

III Exemples et applications

III.1 Corps finis

Dans toute cette sous-partie, on considère un corps $\mathbb{K}$ commutatif quelconque.

Définition 50 : Sous-corps premier [Perrin, p.72] :
On appelle **sous-corps premier de** $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$ (contenant l'élément $1_{\mathbb{K}}$).

On considère le morphisme d'anneaux :

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \longmapsto & n \cdot 1_{\mathbb{K}} \end{array} \right.$$

Le noyau de φ est un idéal de $\mathbb{Z}$ et par le premier théorème d'isomorphisme, on a $\mathbb{Z}/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi) \subseteq \mathbb{K}$, donc $\operatorname{Ker}(\varphi)$ est un idéal premier de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec $p \in \mathcal{P} \cup \{0\}$.

Définition 51 : Caractéristique d'un corps [Perrin, p.72] :
On appelle **caractéristique de** $\mathbb{K}$ le nombre $p \in \mathcal{P} \cup \{0\}$ qui est le générateur de $\operatorname{Ker}(\varphi)$ et on le note $\operatorname{car}(\mathbb{K})$.

Proposition 52 : [Perrin, p.72]
Soit p un nombre premier.
Tout corps fini commutatif $\mathbb{K}$ de caractéristique p a pour cardinal une puissance de p.

Théorème 53 : [Perrin, p.73]
Soient p un nombre premier et $n \in \mathbb{N}^*$.
Si l'on pose $q = p^n$, alors il existe un corps $\mathbb{K}$ à q éléments (c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$).
En particulier, $\mathbb{K}$ est unique à isomorphisme près et on le note $\mathbb{F}_q$.

Exemple 54 :
$* \ \mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2+X+1)$. $* \ \mathbb{F}_9 \cong \mathbb{F}_3[X]/(X^2+X-1)$.

Lemme 55 : [Perrin, p.74]
Soit $\mathbb{K}$ un corps fini commutatif.
Tout sous-groupe de $\mathbb{K}^\times$ est cyclique.

Théorème 56 : Théorème de l'élément primitif (2) [Gourdon, p.97] :
Soit $\mathbb{K}$ un corps fini commutatif.
$\mathbb{L}/\mathbb{K}$ une extension de corps finie, alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

Remarque 57 : [Perrin, p.77]
Soit $P \in \mathbb{Z}[X]$ unitaire.
S'il existe un nombre premier p (au sens usuel) tel que $\overline{P} \in \mathbb{F}_p[X]$ soit irréductible, alors P est irréductible dans $\mathbb{Z}[X]$ (application du critère de réduction). Ainsi, $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Z}[X]$ par exemple.

Exemple 58 : [Perrin, p.78]
Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$ (application de la proposition 40).

Définition 59 : Fonction de Möbius [Berhuy, p.151] :
On appelle **fonction de Möbius** la fonction μ définie par :

$$\mu : \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \begin{cases} (-1)^r & \text{si } n \text{ est produit de } r \text{ nombres premiers distincts} \\ 0 & \text{s'il existe un nombre premier } p \text{ tel que } p^2 \text{ divise } n \end{cases} \end{array} \right.$$

Développement 1 : [cf. FRANCINOU]

Lemme 60 : [Francinou, p.93]
Pour tout $n \in \mathbb{N}^*$, on a :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

Théorème 61 : Formule d'inversion de Möbius [Francinou, p.93] :
Soient A un groupe abélien et $f : \mathbb{N}^* \longrightarrow A$.
Si l'on pose $g(n) = \sum_{d|n} f(d)$, alors $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

Théorème 62 : [Francinou, p.189]
Si l'on note $A(n,q)$ l'ensemble des polynômes irréductibles, unitaires et de degré n sur $\mathbb{F}_q$, alors $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P(X)$

Corollaire 63 : [Francinou, p.189]
En notant $I(n,q) = \mathrm{Card}(A(n,q))$, on a :

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \text{ et } \forall q \geq 2, \ I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$$

Remarque 64 : [Berhuy, p.654]
On a donc en particulier pour tout $n, q \in \mathbb{N}^*$, $I(n,q) \geq 1$. Ainsi, il existe au moins un polynôme irréductible de degré quelconque n dans $\mathbb{F}_p$ (c'est-à-dire que $\mathbb{F}_{p^n}$ existe toujours en tant que corps).

III.2 Polynômes cyclotomiques

Dans toute cette sous-partie, on suppose que $\mathbb{K}$ est un corps commutatif de caractéristique p, on note $\mu_n(\mathbb{K}) = \{\zeta \in \mathbb{K} \text{ tq } \zeta^n = 1\}$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{K}$ et on suppose que $\mathrm{PGCD}(p,n) = 1$.

Définition 65 : Racine primitive n-ième de l'unité [Perrin, p.80] :
On considère $P(X) = X^n - 1$ et $\mathbb{K}_n$ un corps de décomposition de P.
On appelle **racine primitive n-ième de l'unité**, tout élément $\zeta \in \mathbb{K}_n$ tel que $\zeta^n = 1$ et pour tout $d \in [\![1; n-1]\!]$, $\zeta^d \neq 1$ (et on note $\mu_n^*(\mathbb{K})$ cet ensemble).

Définition 66 : n-ième polynôme cyclotomique [Perrin, p.80] :
On appelle **n-ième polynôme cyclotomique sur** $\mathbb{K}$ le polynôme :

$$\Phi_{n,\mathbb{K}}(X) = \prod_{\zeta \in \mu_n^*(\mathbb{K})} (X - \zeta)$$

Remarque 67 : [Perrin, p.80]
$\Phi_{n,\mathbb{K}}(X)$ est un polynôme unitaire et de degré $\varphi(n)$.

Exemple 68 : [Perrin, p.81]
Sur $\mathbb{Q}$, on a :
$\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$ et $\Phi_4(X) = X^2 + 1$.

Proposition 69 : [Perrin, p.80]
On a la formule :

$$X^n - 1 = \prod_{d|n} \Phi_{d,\mathbb{K}}(X)$$

Remarque 70 : [Perrin, p.81]
La formule de la proposition précédente permet de calculer les polynômes cyclotomiques par récurrence en écrivant :

$$\Phi_{n,\mathbb{K}}(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_{d,\mathbb{K}}(X)}$$

Proposition 71 : [Perrin, p.81]
On a $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

Développement 2 : [cf. PERRIN]

Théorème 72 : [Perrin, p.82]
Le polynôme $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$.

Corollaire 73 : [Perrin, p.83]
Si ζ est une racine primitive n-ième de l'unité dans un corps commutatif de caractéristique nulle, alors son polynôme minimal sur $\mathbb{Q}$ est $\Phi_{n,\mathbb{Q}}$ et $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$.

Exemple 74 :
Par le corollaire précédent et le théorème de la base télescopique, on a le résultat suivant : $e^{\frac{2i\pi}{5}} \notin \mathbb{Q}\left(e^{\frac{2i\pi}{7}}\right)$

Remarques sur la leçon

— On peut faire le lien entre le nombre de polynômes unitaires irréductibles sur $\mathbb{F}_q$ avec le théorème des nombres premiers.

— Il est aussi possible de parler du résultant ainsi que de la théorie de Galois (légèrement).

Liste des développements possibles

— Dénombrement des polynômes unitaires irréductibles sur $\mathbb{F}_q$.

— Irréductibilité des polynômes cyclotomiques sur $\mathbb{Q}[X]$.

Bibliographie

— Daniel Perrin, *Cours d'algèbre*.

— Grégory Berhuy, *Algèbre, le grand combat*.

— Claude Deschamps, *Tout-en-un MP/MP**.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.

— Serge Francinou, *Exercices de mathématiques pour l'agrégation, Algèbre 1*.