Leçon 125 - Extensions de corps. Exemples et applications.

Extrait du rapport de jury

Les extensions de degré fini ont toute leur place dans cette leçon : le théorème de la base télescopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis, sont incontournables. Il est souhaitable d'introduire la notion d'élément algébrique et d'extension algébrique en en donnant des exemples. Il faut savoir calculer le polynôme minimal d'un élément algébrique dans des cas simples, notamment pour quelques racines de l'unité. La leçon peut être illustrée par des exemples d'extensions quadratiques et leurs applications en arithmétique, ainsi que par des extensions cyclotomiques.
Pour aller plus loin, les candidates et candidates et candidats peuvent montrer que l'ensemble des nombres algébriques forme un corps algébriquement clos, par exemple en expliquant comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques. Il est possible de 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 125 intitulée : "Extensions de corps. Exemples et applications.". Les extensions de corps sont des outils très intéressants, car ils permettent, lorsqu'un polynôme P ne possède pas de racines sur un corps commutatif $\mathbb{K}$, d'introduire une racine symbolique du polynôme dans un sur-corps de $\mathbb{K}$ et de travailler dans ce sur-corps.
Dans une première partie, on s'intéresse aux généralités concernant les extensions de corps. Tout d'abord, on commence avec une partie technique sur la caractéristique d'un corps dans laquelle on définit ce qu'est le sous-corps premier ainsi que la caractéristique d'un corps via le morphisme d'anneaux φ. On termine cette première sous-partie avec un résultat important d'isomorphisme concernant le sous-corps premier en fonction de la caractéristique du corps considéré. Dans un deuxième temps, on entre dans le coeur du sujet en parlant d'extension de corps. 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 termine cette deuxième sous-partie en donnant 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. Enfin pour conclure cette première partie, on donne 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.
Dans une deuxième partie, on s'intéresse aux extensions de corps remarquables. Tout d'abord on s'attarde sur les éléments algébriques et transcendants. Ainsi, on commence par introduire la notion d'élément algébrique et transcendant ainsi que quelques exemples basiques, puis l'on donne une caractérisation très pratique des éléments algébriques grâce aux polynômes minimaux et la théorie de la dimension. On montre ensuite que toute extension finie est algébrique mais que la réciproque est fausse et on conclut cette première sous-partie avec la notion de corps algébriquement clos ainsi que quelques exemples classiques. Dans une deuxième sous-partie, on s'intéresse à la notion de corps de rupture et de corps de décomposition (c'est celles-ci qui permettent d'introduire des racines symboliques de polynômes et de travailler dans des sur-corps). On commence 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 au corps de décomposition en donnant sa définition ainsi que quelques exemples classiques avant de continuer sur un résultat d'unité du corps de décomposition. Pour terminer cette sous-partie, on parle également de la clôture algébrique et on énonce le théorème de Steinitz. On conclut cette partie avec un dernier point concernant les corps finis. On commence par deux résultats importants concernant le cardinal des corps finis ainsi que l'existence d'un corps fini de cardinal $q = p^n$ donné à l'isomorphisme près en tant que corps de décomposition du polynômes $X^q - X$ sur $\mathbb{F}_p$. On étudie ensuite les inclusions entre corps finis que l'on illustre avec un trellis. Enfin on termine avec une caractérisation de l'irréductibilité d'un polynôme qui est très utile dans le cas des corps finis.

Enfin, on s'intéresse dans une dernière partie à des applications de la notion d'extension de corps. Une première application concerne les polynômes cyclotomiques qui sont définis à partir des racines primitives n-ièmes de l'unité. On enchaîne avec la proposition 46 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 de déterminer le degré d'une extension cyclotomique donnée. On continue avec une deuxième application qui concerne les théorèmes de l'élément primitif. Il existe deux versions du théorème de l'élément primitif : une en caractéristique nulle et une autre en caractéristique $p > 0$. On continue avec le dénombrement des polynômes irréductibles sur $\mathbb{F}_q$ en introduisant au préalable la fonction de Möbius et en donnant quelques résultats sur cette dernière avant de dénombrer les polynômes irréductibles sur $\mathbb{F}_q$ ainsi que de donner un équivalent de ce nombre lorsque n tend vers $+\infty$. On notera d'ailleurs que ce résultat permet de justifier à nouveau qu'il existe toujours un corps de cardinal $q = p^n$. Enfin, on termine cette leçon par les nombres constructibles à la règle non graduée et au compas. On commence par définir ce qu'est un nombre constructible avant de donner une caractérisation de la constructibilité d'un nombre complexe. On conclut avec le théorème de Gauss-Wantzel qui donne une condition nécessaire et suffisante pour construire un n-gone régulier.

Plan général

Cours détaillé

I Généralités

I.1 Caractéristique d'un corps

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

Définition 1 : 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 2 : 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 3 : [Perrin, p.73]
Si $\operatorname{car}(\mathbb{K}) > 0$, alors l'application :

$$F : \left| \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & x^p \end{array} \right.$$

est un morphisme de corps.
De plus, si $\mathbb{K}$ est fini, alors c'est un automorphisme et si $\mathbb{K} = \mathbb{F}_p$, alors c'est l'identité.

Proposition 4 : [Perrin, p.72]
$*$ $\operatorname{car}(\mathbb{K}) = 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$.
$*$ $\operatorname{car}(\mathbb{K}) > 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

I.2 Extension de corps

Définition 5 : 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 6 : [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 7 : 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 8 :
∗ $\mathbb{C}$ 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 9 : 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 : $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

I.3 Critères d'irréductibilité

Proposition 10 : Critère d'irréductibilité d'Eisenstein [Perrin, p.76] :
Soient A un anneau factoriel et $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$.
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 11 :
∗ Les polynômes $X^n - 2$ et $X^4 - 6X^3 + 3X^2 - 12X + 3$ sont irréductibles dans $\mathbb{Q}[X]$.
∗ Pour tout $n \in \mathbb{N}^*$, il existe au moins une extension de $\mathbb{Q}$ de degré n (c'est $\mathbb{Q}\left(\sqrt[n]{2}\right)$, qui est bien de degré n car $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$).

Proposition 12 : Critère de réduction [Perrin, p.77] :
Soient A un anneau factoriel, 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 13 : [Perrin, p.77]
Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Q}[X]$ par le critère de réduction.

Proposition 14 : [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 $\mathrm{PGCD}(n, m) = 1$, alors P est encore irréductible dans $\mathbb{L}$.

Exemple 15 : [Perrin, p.79]
Le polynôme $X^3 + 4X + 2$ est irréductible sur $\mathbb{Q}[i]$ comme sur $\mathbb{Q}$.

II Extensions remarquables

II.1 Éléments algébriques et transcendants

Définition 16 : 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 17 : [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 18 : 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 19 : 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 20 : [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 21 : [Perrin, p.67]
La proposition 18 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 $\{\alpha \in \mathbb{C} \text{ tq } \alpha \text{ est algébrique sur } \mathbb{Q}\}$!

Définition 22 : 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 23 : [Perrin, p.68]
* $\mathbb{C}$ est un corps algébriquement clos (théorème de D'Alembert-Gauss).
* Le corps A définit dans la remarque 21 est lui aussi algébriquement clos (c'est même la clôture algébrique de $\mathbb{Q}$).

Proposition 24 : [Gourdon, p.67]
Tout corps commutatif algébriquement clos est infini.

II.2 Corps de rupture et corps de décomposition

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

Définition 25 : 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 26 : [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 27 : 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 28 :
* 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 29 : [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.

Définition 30 : Clôture algébrique [Perrin, p.72] :
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 31 : [Perrin, p.72]
* $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$. * A est une clôture algébrique de $\mathbb{Q}$.

Corollaire 32 :
Si $\mathbb{K}$ est algébriquement clos, alors tout endomorphisme d'un $\mathbb{K}$-espace vectoriel E est trigonalisable.

Remarque 33 :
En fait, on a même que tout endomorphisme est trigonalisable sur le corps de décomposition de son polynôme minimal.

Théorème 34 : Théorème de Steinitz [ADMIS] [Berhuy, p.827] :
Tout corps $\mathbb{K}$ commutatif admet une clôture algébrique unique à isomorphisme près.

II.3 Corps finis

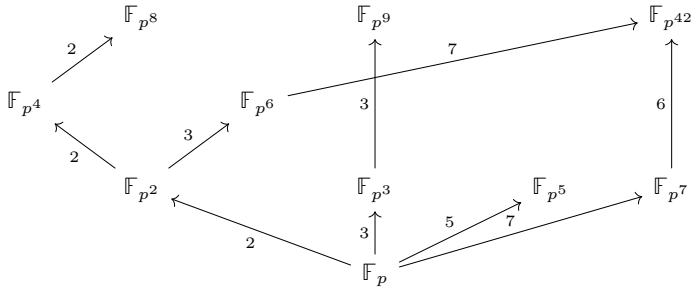
Proposition 35 : [Perrin, p.72]
Soit p un nombre premier.
Tout corps fini commutatif $\mathbb{K}$ de caractéristique p a pour cardinal une puissance de p.

Théorème 36 : [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 37 :
On peut construire un corps à 4 éléments de deux manières :
∗ En tant que corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$.
∗ Grâce à l'isomorphisme $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$.

Corollaire 38 :
Soient p un nombre premier et $n, d \in \mathbb{N}^*$.
Si $\mathbb{K}$ est un corps à p^n éléments, alors il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d si, et seulement si, d divise n.
De plus, un tel sous-corps est alors isomorphe à $\mathbb{F}_{p^d}$.

Exemple 39 :
Pour un nombre premier p quelconque, on a par exemple le trellis suivant :



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 $[\mathbb{L} : \mathbb{K}] \leq \frac{n}{2}$.

Exemple 41 : [Perrin, p.78]
Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

III Applications

III.1 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 $\text{PGCD}(p, n) = 1$.

Définition 42 : 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 $\mu_n^*(\mathbb{K})$ l'ensemble composé de ces éléments).

Définition 43 : 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 44 : [Perrin, p.80]
$\Phi_{n,\mathbb{K}}(X)$ est un polynôme unitaire et de degré $\varphi(n)$.

Exemple 45 : [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 46 : [Perrin, p.80]
On a la formule :

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

Remarque 47 : [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 48 : [Perrin, p.81]
On a $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$.

Développement 1 : [cf. PERRIN]

Théorème 49 : [Perrin, p.82]
Le polynôme $\Phi_{n,\mathbb{Q}}(X)$ est irréductible dans $\mathbb{Q}[X]$.

Corollaire 50 : [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 51 :
Par le corollaire précédent et le théorème de la base télescopique, on a le résultat suivant : $e^{\frac{2i\pi}{5}} \notin \mathbb{Q}\left(e^{\frac{2i\pi}{7}}\right)$

III.2 Théorèmes de l'élément primitif

Théorème 52 : Théorème de l'élément primitif (1) [Gourdon, p.96] :
Soient $\mathbb{K}$ un corps de caractéristique nulle.
Si $\mathbb{L}/\mathbb{K}$ une extension de corps finie, alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

Exemple 53 :
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 $\mathbb{L} = \mathbb{Q}(a)$.

Lemme 54 : [Perrin, p.74]
Soit $\mathbb{K}$ un corps fini commutatif.
Tout sous-groupe de $\mathbb{K}^\times$ est cyclique.

Théorème 55 : 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 $\mathbb{L} = \mathbb{K}(\alpha)$.

III.3 Dénombrement des polynômes unitaires irréductibles sur $\mathbb{F}_q$

Définition 56 : 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 2 : [cf. FRANCINOU]

Lemme 57 : [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 58 : 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 59 : [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 60 : [Francinou, p.189]
En notant $I(n,q) = \text{Card}(A(n,q))$, 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 61 : [Berhuy, p.654]
On a donc en particulier pour tous $n, q \in \mathbb{N}^*$, $I(n,q) \geq 1$. 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.4 Nombres constructibles à la règle non graduée et au compas

Ici, chaque construction commencera de 0 et 1. Durant la construction, nous utiliserons seulement les règles suivantes :
$C1(\alpha, \beta)$: De $\alpha \neq \beta$, on peut tracer la ligne l qui passe par α et β.
$C2(\gamma, \alpha, \beta)$: De $\alpha \neq \beta$ et γ, on peut dessiner le cercle C de centre γ dont le rayon est la distance entre α et β.
$P1$: Le(s) point(s) d'intersection de deux lignes distinctes ℓ_1 et ℓ_2 construites comme ci-dessus.
$P2$: Le(s) point(s) d'intersection d'une ligne ℓ et d'un cercle C construits comme ci-dessus.
$P3$: Le(s) point(s) d'intersection de deux cercles distincts C_1 et C_2 construits comme ci-dessus.

Définition 62 : Nombre constructible [Berhuy, p.762] :
Un nombre complexe α est un **nombre constructible** lorsqu'il existe une suite finie de constructions à la règle non graduée et au compas utilisant $C1$, $C2$, $P1$, $P2$ et $P3$ qui commence avec 0 et 1 et fini avec α.

Exemple 63 : [Berhuy, p.763]
Il est possible de construire une médiatrice d'un segment, le milieu d'un segment, une bissectrice d'un angle, la symétrie centrale et axiale d'un point, une perpendiculaire et une parallèle à une droite donnée.

Dans toute la suite de cette sous-partie, on note $\mathcal{C} := \{\alpha \in \mathbb{C} \text{ tq } \alpha \text{ est constructible}\}$.

Théorème 64 : [Berhuy, p.764 + 765]
L'ensemble $\mathcal{C}$ est un sous-corps de $\mathbb{C}$.
De plus, on a :
$*$ $\alpha := a + ib \in \mathcal{C}$ si, et seulement si, $a, b \in \mathcal{C} \cap \mathbb{R}$.
$*$ Si $\alpha \in \mathcal{C}$, alors chaque racine carrée de α appartient à $\mathcal{C}$.

Théorème 65 : [Berhuy, p.775]
Soit $\alpha \in \mathbb{C}$.
$\alpha \in \mathcal{C}$ si, et seulement si, il existe des sous-corps de $\mathbb{C}$ tels que :

$$\mathbb{Q} := F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n \subseteq \mathbb{C}, \forall i \in [\![0; n-1]\!],\ [F_{i+1} : F_i] = 2 \text{ et } \alpha \in F_n$$

Corollaire 66 : [Berhuy, p.776]
Si $\alpha \in \mathcal{C}$, alors il existe $m \in \mathbb{N}$ tel que $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$.

Remarque 67 :
$*$ Le corollaire précédent implique que tout $\alpha \in \mathcal{C}$ est algébrique sur $\mathbb{Q}$ et que le degré de son polynôme minimal est une puissance de 2. On a alors $\mathbb{Q} \subsetneq \mathcal{C} \subsetneq \mathcal{A}$ avec $\mathcal{A}$ l'ensemble des nombres algébriques sur $\mathbb{Q}$.
$*$ La contraposée du corollaire précédent est très utile car elle permet de voir que pour qu'un nombre n'est pas constructible, il suffit de déterminer le degré de son polynôme minimal sur $\mathbb{Q}$.

Théorème 68 : [Berhuy, p.929]
Soient $\alpha \in \mathbb{C}$ algébrique sur $\mathbb{Q}$ et $\mathbb{L}$ le corps de décomposition du polynôme minimal de α sur $\mathbb{Q}$.
α est constructible si, et seulement si, $[\mathbb{L} : \mathbb{Q}]$ est une puissance de 2.

Corollaire 69 : [Berhuy, p.787 - 788]
La trisection de l'angle, la duplication du cube et la quadrature du cercle sont impossibles à la règle non graduée et au compas.

Théorème 70 : Théorème de Gauss-Wantzel [Berhuy, p.795] :
Soit n un entier naturel supérieur ou égal à 2.
Le n-gone régulier est constructible à la règle non graduée et au compas si, et seulement si, $n := 2^s \prod_{i=1}^{r} p_i$ (avec $s, r \in \mathbb{N}$ et $p_1, ..., p_r$ qui sont r nombres de Fermat distincts).

Exemple 71 : [Berhuy, p.805]
Il est possible de construire le pentagone régulier avec la règle non graduée et le compas.

Remarque 72 :
Certaines constructions à la règle non graduée et au compas ne sont donc pas possibles (construction de l'heptagone régulier, trisection de l'angle, etc.) Mais que se passe-t-il si l'on modifie les règles du jeu (théorème de Mohr-Mascheroni, théorème de Poncelet-Steiner, règle avec deux graduations, allumettes, origamis, etc.) ?

Remarques sur la leçon

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

— Il est possible de parler légèrement de théorie de Galois avec les extensions séparables et normales.

Liste des développements possibles

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

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

Bibliographie

— Daniel Perrin, *Cours d'algèbre*.

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

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

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