ENS de Lyon
2025-2026

Leçon Agreg

Leçon 125

I. Thèmes pour le plan et de développements

Les éléments marqués « DEV » dans cette section sont des éléments qui peuvent être mis en item dans ce plan et réutilisés comme développements dans au moins une autre leçon. Attention, ce ne sont pas tous les meilleurs développements possibles pour cette leçon.

1. Choses classiques

Je conseille de jeter au moins un coup d'œil à ces éléments.

- Critère d'Eisenstein et application : si p est premier, $n \in \mathbb{N}^*$, alors $X^n - p$ est irréductible.
- Étude de l'extension $\mathbb{Q}[\sqrt[p]{a}]/\mathbb{Q}$, si $a \in \mathbb{Z}$ et p premier.
- Irréductibilité sur $\mathbb{Q}[X]$ vs sur $\mathbb{Z}[X]$. $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{F}_p[X]$ implique irréductible sur $\mathbb{Q}[X]$. Applications à des calculs de degrés d'extensions.
- Invariants par extension de corps : pgcd entre polynômes, rang d'une matrice
- Corps de rupture comme quotient d'anneaux de polynômes, unicité.
- Corps de décomposition d'un polynôme P. Son degré est borné par $\deg(P)!$.
- Unicité du corps de décomposition. La preuve de l'unicité utilise le théorème (capital) :

  Théorème 1. Prolongement des morphismes *Soit $\sigma : \mathbb{K} \to \mathbb{K}'$ un isomorphisme entre deux corps. Soit $\mathbb{L}/\mathbb{K}$ et $\mathbb{L}'/\mathbb{K}'$ deux extensions de corps. Soit $x \in \mathbb{L}$ et $x' \in \mathbb{L}'$ deux éléments algébriques sur $\mathbb{K}$, de polynômes minimaux P et P'.*
  Alors, si et seulement si $P' = \sigma \cdot P$, il existe un morphisme de corps $\mathbb{K}[x] \to \mathbb{K}'[x']$ envoyant x sur x' et prolongeant σ.
- Théorème de l'élément primitif en caractéristique nulle

2. Pistes pour enrichir

Ces éléments sont très bien pour s'amuser un peu plus, rajouter du contenu. Ce genre de contenu de plan se recase bien.

- Théorie de Galois. Conseil : se restreindre à la caractéristique nulle, et être au courant que $\mathbb{F}_p(X)$ n'est pas un corps parfait et que donc rien de la théorie de Galois n'y marche. Savoir prouver tout ce qu'on dit. Savoir calculer des exemples (pas forcément hyper compliqués). L'extension $\mathbb{Q}\left[\sqrt{4+\sqrt{5}}\right]/\mathbb{Q}$ est-elle normale ? Quel est le groupe de Galois de sa clôture normale ?
  - Exemple de calcul d'un groupe de Galois. Discriminant et critère pour que $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ soit inclus dans $\mathfrak{A}_n$.
  - Extensions de Kummer (c'est des extensions toutes gentilles avec une belle application de la réduction des endomorphismes).
  - Résolubilité par radicaux. Exemple de polynômes non résolubles par radicaux ($X^5 - p^2X + p$ pour p premier, c.f. Berhuy je crois).
  - Exemple rigolo : les polynômes réciproques. Le polynôme $X^6 + 3X^4 + 2X^3 + 3X^2 + 1$ est irréductible (ce qu'on peut prouver par réduction mod 7. Essayer déjà avec SageMath). Il est réciproque donc (voir exos) l'ordre de son groupe de Galois divise 48. Il est donc (par application classique du théorème de Sylow ou Burnside) résoluble par radicaux.
  - Existence (sur un corps de caractéristique nulle, ou parfait) de la décomposition $M = D + N$ de Dunford avec D semi-simple (dans le cas où χ_M n'est pas forcément scindé).
- Entiers algébriques. Les entiers algébriques de $\mathbb{Q}[e^{\frac{2\pi i}{n}}]$ sont $\mathbb{Z}[e^{\frac{2\pi i}{n}}]$ (pas trop dur à prouver pour n premier). Un entier algébrique qui est rationnel est entier. Applications aux représentations (théorie des caractères, théorème de Burnside pour les groupes d'ordre $p^\alpha q^\beta$).
- Existence d'une clôture algébrique. Au moins celle de $\mathbb{F}_p$, constructible « à la main », puisqu'elle est à voir comme $\bigcup_{n \geqslant 1} \mathbb{F}_{p^n}$.
- Séparabilité, corps parfaits, théorème de l'élément primitif pour une extension finie séparable d'un corps.
- Trace et norme dans une extension finie (DEV famille $\mathbb{Q}$-libre par la trace)
- (seulement si ça vous passionne) quelques éléments de p-adiques.

II. Développements pour cette leçon

Ils font aussi de supers items de plans. Liste non exhaustive.

— Condition suffisante pour que ton petit cousin lise ta table de caractères

— Théorème de descente de Springer pour les formes quadratiques

— Famille $\mathbb{Q}$-libre par la trace (dév sur agreg-maths, abordable et très recasable)

— Algorithme de Berlekamp

— Φ_n irréd + Dirichlet faible (bonus : + les groupes abéliens sont des groupes de Galois)

— Théorème de Gauss-Wantzel

— Dénombrer les polynômes irréductibles sur un corps fini

— Théorème de Kronecker-Weber pour les extensions quadratiques.

III. Exercices

Exercice 1. — Soit $\mathbb{K}/\mathbb{Q}$ une extension finie et $a \in \mathbb{K}$. Décrire les valeurs propres de l'endomorphisme $\mathbb{Q}$-linéaire $m_a : \left| \begin{array}{ccc} \mathbb{K} & \longrightarrow & \mathbb{K} \\ x & \longmapsto & ax \end{array} \right.$. Quel est son polynôme caractéristique ?

Exercice 2. — Soit $\mathbb{L}$ une extension algébrique de $\mathbb{K}$ et σ un endomorphisme $\mathbb{K}$-linéaire de $\mathbb{L}$. Montrer que σ est un automorphisme.

Exercice 3. — Montrer que $\overline{\mathbb{Q}} := \{z \in \mathbb{C} \,|\, z \text{ est algébrique}\}$ est une clôture algébrique de $\mathbb{Q}$ (i.e. algébriquement clos et une extension algébrique de $\mathbb{Q}$).

Exercice 4. (Un argument de « densité ») Soit k un corps, $A, B \in \mathcal{M}_n(k)$. Montrer que $\chi_{AB} = \chi_{BA}$.

Exercice 5. (Une question d'oral) Quel est le groupe des automorphismes du corps $\mathbb{Q}[\sqrt[4]{2}, i]$?

Exercice 6. — Soit $n \geqslant 3$. Soit $a_n = \cos\left(\frac{2\pi i}{n}\right)$ et $b_n = \sin\left(\frac{2\pi i}{n}\right)$. Montrer que $\mathbb{Q}(a_n) = \mathbb{Q}(b_n)$.

Exercice 7. — **1.** Soit $a_1, \ldots, a_r \in \mathbb{N}^*$ premiers entre eux deux à deux et non carrés. On note $\mathbb{L} = \mathbb{Q}[\sqrt{a_1}, \ldots, \sqrt{a_r}]$. On voudrait montrer que $(\sqrt{a_1}, \ldots, \sqrt{a_r})$ est une famille $\mathbb{Q}$-libre. Soit $\lambda_1, \ldots, \lambda_r \in \mathbb{Q}$ tels que $\sum_{i=1}^{r} \lambda_i \sqrt{a_i} = 0$, et tels que $S := \{i \in [\![1, r]\!] \,|\, \lambda_i \neq 0\}$ soit de cardinal minimal.

a. Soit $i, j \in S$, distincts. Montrer qu'il existe un morphisme de corps $\sigma : \mathbb{L} \to \mathbb{L}$ tel que $\frac{\sigma(\sqrt{a_i})}{\sqrt{a_i}} \neq \frac{\sigma(\sqrt{a_j})}{\sqrt{a_j}}$.

b. Conclure.

2. Quel est le degré de l'extension $\mathbb{L}/\mathbb{Q}$? [(a)]

3. Montrer que $\sum_{i=1}^{r} \sqrt{a_i}$ est un élément primitif de cette extension.

4. *Calculer $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$.

Exercice 8. — **1.** Degré de l'extension $\mathbb{Q}\left[\sqrt{4+\sqrt{5}}\right]/\mathbb{Q}$.

2. *Degré du plus petit corps de décomposition sur $\mathbb{Q}$ qui la contient ?

Exercice 9. — Soit k un corps, soit $P \in k[X]$ un polynôme réciproque de degré $2n$ (i.e. $P(X^{-1}) = X^{-2n}P(X)$) . Soit $L = Dec_k(P)$. Montrer que l'ordre de $\mathrm{Aut}(L/k)$ divise $n!2^n$.

(a). N.B. Ce résultat est faisable sous forme de développement. Soit par la méthode ici présente (quoi que ça puisse faire un peu court, soit par une méthode assez directe et calculatoire donc très abordable, soit par une très jolie méthode très recasable que vous trouverez sur agreg-maths, nommée "famille Q-libre par la trace".