Références :

- Analyse, Gourdon
- Cours d'algèbre, Perrin
- Théorie de Galois, Gozard

Développements :

- Polynômes irréductibles sur un corps fini
- Théorème de Gauss-Wantzel

On fixe un anneau commutatif unitaire **intègre** A.

1. Irréductibilité

1.1. Définitions et premières propriétés

- Définition
- Exemples
- Un polynôme irréductible n'a pas de racines
  - Réciproque fausse : $X^4 + 1 \in \mathbb{R}[X]$
  - Réciproque partielle sur un corps en degrés 2 et 3
- Si K est un corps, alors $K[X]$ est euclidien
- Corollaire : décomposition en produit d'irréductibles

1.2. Critères d'irréductibilité

- Réduction modulo un nombre premier : si $P \in \mathbb{Z}[X]$ est unitaire et irréductible sur $\mathbb{F}_p$ pour un p premier, alors P est irréductible sur $\mathbb{Z}$
  - Réciproque fausse : $X^4 + 1$
- Critère d'Eisenstein
- App : irréductibilité de Φ_p sur $\mathbb{Q}$ pour p premier

1.3. Irréductibles de $A[X]$ pour A factoriel

- Contenu, lemme de Gauss
- Description des irréductibles de $A[X]$ pour A factoriel
  - App : irréductibilité de Φ_p sur $\mathbb{Z}$ pour p premier
- Thm (Gauss) : A factoriel entraîne $A[X]$ factoriel
  - Cor : si K est un corps, alors $K[X_1, \dots, X_n]$ est factoriel

2. Adjonction de racines

2.1. Extensions de corps et polynômes

- Théorème de la base télescopique
- Polynôme minimal d'un élément algébrique
  - Irréductibilité
  - Ex : X^2+2 pour $\sqrt{2}$ sur $\mathbb{Q}$
- Structure des extensions monogènes [Gozard]

2.2. Corps de rupture

- Si K est un corps et $P \in K[X]$, alors $K[X]/P$ est un corps ssi P est irréductible
- Définition
- Exemples
- Existence et unicité à ("unique") isomorphisme près
  - Rmq : P n'est pas toujours scindé sur son corps de rupture

2.3. Corps de décomposition

- Définition
- Exemples
  - Cas de $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2}) \hookrightarrow \mathbb{Q}(\sqrt[3]{2}, j)$
- Existence et unicité à (unique) isomorphisme près, avec $[L:K] \leq (\deg P)!$
- Corps finis
  - Construction de $\mathbb{F}_q$ comme corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$
  - Corps de rupture = corps de décomposition ici

2.4. Étude des irréductibles suivant le corps de base

- Thm (d'Alembert-Gauss)
  - App : classification des irréductibles de $\mathbb{C}[X]$ et $\mathbb{R}[X]$
  - App : tout $\mathbb{C}$-endomorphisme est trigonalisable en dimension finie
- Cas des corps finis
  - $X^{q^n} - X = \prod_{d|n} \prod_{Q \in I(d,q)} Q$
  - **Développement : Dénombrement des irréductibles unitaires de $\mathbb{F}_q[X]$
  - En particulier il existe des irréductibles de tout degré sur $\mathbb{F}_p$ pour construire les corps finis comme corps de rupture

3. Une application en géométrie : les nombres constructibles à la règle et au compas

- Définition
- Constructions élémentaires
- Thm (Wantzel)
  - Résolution des 3 problèmes de l'Antiquité
- Polygones réguliers constructibles
- **Développement : Gauss-Wantzel**