(141) Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

I/ Polynômes irréductibles

- Rappels : A anneau commutatif intègre
  déf de l'irréductibilité sur A (Perrin)
  A principal, a irréd de $A \Rightarrow A/(a)$ corps
- Déf : Polynôme irréductible de $A[X]$
  + premiers ex
  ⚠ Pas dans Gozard car il y a une erreur !
  Irréductibles de degré ≥ 2 : pas de racine
  D'Alembert-Gauss, irréductibles de $\mathbb{R}[X]$. → exemples
- $A[X]$ factoriel (Perrin)
  déf de contenu, de pol primitif, caractérisation des polynômes irr. de $A[X]$ + ex : $\mathbb{Z}[X]$.
- Critère d'Eisenstein (Gozard)
  évt dans le cas général (Perrin)
  + exemples (Perrin)

II/ Extensions de corps

- Éléments algébriques (Goz) : irréductibilité du pol. minimal
  + Corps des nombres algébriques
- Adjonction de racine (Goz)
  corps de rupture, existence et unicité (à détailler)
  (+ deux propositions de (Goz) sur les racines de P et les extensions
  → à ne pas oublier : degré de l'extension → appl : existence/unicité des corps finis.
- Appli : corps de décomposition, clôture algébrique (Goz)
- Appli : polynômes cyclotomiques (Goz)
  → ils sont irréductibles
  → théorème de Dirichlet - progression arithmétique (FGN)
  évt : polygones constructibles à la règle et au compas

III/ Corps finis

- Polynômes irréductibles sur $\mathbb{F}_p$ (Goz, Lidl)
  → thm d'existence d'un polyn irréd de degré n sur $\mathbb{F}_p$.
  + dénombrement des polynômes irréductibles unitaires. (formule de Möbius)
- Représentations des corps finis (Lidl, Niederreiter)
- Algorithme de factorisation (sur un corps fini)
  . dans le cas P sans facteur carré
  algorithme de Berlekamp (Demazure)
  + généralisation