Notations : k, K et L sont des corps commutatifs, A est un anneau commutatif factoriel.

I - Polynômes irréductibles

1°) Définitions et propriétés élémentaires

Déf 1 : $P \in A[X]$ est dit irréductible s'il est non-inversible, non-nul et si : $\forall R, Q \in A[X]$, $P = RQ \Rightarrow R \in A^\times$ ou $Q \in A^\times$

Exe 2 : $\cdot$ 5 est irréductible dans $\mathbb{Z}[X]$ mais pas dans $\mathbb{Q}[X]$,
$\cdot$ X^2+1 est irréductible dans $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.

Prop 3 : Soit $P \in K[X]$, on a :
i) Si $\deg P = 1$, alors P est irréductible
ii) Si $\deg P > 1$ et si P est irréductible, alors P n'a pas de racine dans K
iii) Si $\deg P = 2$ ou 3 et si P n'a pas de racine dans K, alors P est irréductible

Rmq 4 : $(X^2+1)^2$ est réductible dans $\mathbb{R}[X]$ mais n'a pas de racine réelle.

Prop 5 : $P \in K[X]$ est irréductible ssi $K[X]/(P)$ est un corps.

2°) Caractérisation des polynômes irréductibles de $A[X]$

Prop 6 : A est factoriel ssi $A[X]$ l'est.

Rmq 7 : On peut définir un [redacted] pgcd sur un anneau factoriel

Ex. 8 : La factorisation en irréductibles de $X^2+1 \in \mathbb{C}[X]$ est $(X+i)(X-i)$

Déf 9 : Soit $P \in A[X] \setminus \{0\}$. On appelle contenu de P et on note $c(P)$ le pgcd de ses coefficients dans A. Si $c(P) = 1$, P est dit primitif.

Prop 10 : $\forall P, Q \in A[X] \setminus \{0\}$, $c(PQ) = c(P)c(Q)$

Rq 11 : Soit $P \in A[X]$, $\deg P \geq 1$. P est irréductible dans $A[X]$ ssi il est primitif dans $A[X]$ et irréductible dans $\mathrm{Frac}(A)[X]$.

3°) Critères d'irréductibilité de $P \in A[X]$ dans $\mathrm{Frac}(A)[X]$

Th. 12 (Critère d'Eisenstein) : Soit $P = a_n X^n + \dots + a_1 X + a_0 \in A[X]$ tel que $a_n \neq 0$ et $a_0 \neq 0$. S'il existe $p \in A$ irréductible vérifiant :
i) $\forall k \in [\![0, n-1]\!]$, p divise a_k
ii) p ne divise pas a_n
iii) p^2 ne divise pas a_0
Alors P est irréductible dans $\mathrm{Frac}(A)[X]$

Exe 13 : $\forall n \in \mathbb{N}^*$, $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$

Prop 14 : Soit I un idéal premier de A, $P \in A[X] \setminus A$ dont le coefficient dominant n'appartient pas à I. On note $\bar{P}$ la réduction de P modulo I. Si $\bar{P}$ est irréductible dans $\mathrm{Frac}(A/I)[X]$, alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Rmq 15 : La réciproque est fausse, X^4+1 est irréductible sur $\mathbb{Z}$ mais réductible modulo p pour tout p premier.

II - Corps de rupture et de décomposition, clôture algébrique

1°) Extensions algébriques

Prop-dif 16 : Soit L/K une extension, $x \in L$. Les propriétés suivantes sont équivalentes :
i) $K[x]$ est de dimension finie sur K
ii) $K[x] = K(x)$
iii) $\exists P \in K[x] \setminus \{0\}$, $P(x) = 0$
Si elles sont vérifiés, x est dit algébrique sur K.

Déf 17 : Si tous les éléments de L sont algébriques sur K, L/K est une extension algébrique.

Prop-dif 18 : Soient L/K une extension, $x \in L$ algébrique sur K. L'ensemble des polynômes annulateurs de x sur K est un idéal de $K[X]$ engendré par un unique polynôme irréductible unitaire. On l'appelle "polynôme minimal de x sur K" et on le note $\pi_{x,K}$.

Ex. 19 : On note $P_m(\mathbb{C}) = \{\text{racines primitives } m^{\text{ième}} \text{ de l'unité}\}$

Le $m^{\text{ième}}$ polynôme cyclotomique $\Phi_m = \prod_{z \in P_m(\mathbb{C})} (X - z)$ est à coefficients entiers et est le polynôme minimal de n'importe quelle racine primitive $m^{\text{ième}}$ de l'unité sur $\mathbb{Q}$. En particulier, il est irréductible sur $\mathbb{Q}$.

Prop 20 : Une extension finie est algébrique.

~~Rmq 21 : La réciproque est fausse : $\mathbb{Q}$ est une extension algébri~~

Rmq 21 : La réciproque est fausse : l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$ est une extension algébrique non-finie de $\mathbb{Q}$.

Th. 22 (Base télescopique) : Soient L/K et K/k des extensions finies, $(a_i)_{1 \le i \le m}$ (resp. $(b_j)_{1 \le j \le n}$) une base de L sur K (resp. une base de K sur k). Alors L/K est finie et $(a_i b_j)_{1 \le i \le m, 1 \le j \le n}$ est une base de L sur k.

En particulier : $[L : k] = [L : K][K : k]$

2°) Corps de rupture

Déf-Prop 23 : Soit $P \in K[X]$ irréductible, L/K une extension. On dit que L est un corps de rupture de P s'il existe $\alpha \in L$ tel que $P(\alpha) = 0$ et $L = K[\alpha]$.

Exemple 24 : $\mathbb{C} = \mathbb{R}[i]$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$

Prop 25 : Soit $P \in K[X]$ irréductible ; $L = K[X]/(P)$ est un corps de rupture de P sur K. En notant x la classe de X dans L, $(1, x, \dots, x^{\deg P - 1})$ est une K-base de L et $L = K(x)$. En particulier, P est le polynôme minimal de x sur K.

Cor 26 : Soient $P \in K[X]$ et L/K une extension finie de degré premier avec le degré de P. Alors si P est irréductible sur K, il l'est sur L.

Rmq 27 : Un polynôme n'est pas toujours scindé sur son corps de rupture, par exemple $X^3 - 2$ n'est pas scindé sur $\mathbb{Q}(\sqrt[3]{2})$.

Prop 28 : Si L et K sont des corps de rupture de $P \in k[X]$, alors ils sont k-isomorphes.

Prop 29 : Soit $P \in k[X] \setminus k$. P est irréductible ssi pour toute extension finie L/k telle que $[L : K] \le \frac{\deg P}{2}$, P n'a aucune racine dans L.

Ex 30 : $X^4 + X + 1$ est irréductible sur $\mathbb{Z}/2\mathbb{Z}$.

3°) Corps de décomposition

Déf 31 : Soit $P \in K[X]$, L/K une extension. L est un corps de décomposition de P si P est scindé sur L et si $L = K[\alpha_1, \dots, \alpha_n]$ où les α_i sont les racines de P sur L.

Prop. 32 : Soient $P_1, \dots, P_n \in K[X]$ de degrés ≥ 1, alors il existe une extension finie L/K dans laquelle chaque P_i possède au moins une racine.

Cor. 33 : Tout polynôme $P \in K[X]$ a un corps de décomposition L tel que $[L : K] \le (\deg P)!$

Ex 34 : $\mathbb{Q}(e^{2i\pi/n})$ est un corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$.

Prop 35 : Deux corps de décomposition d'un même polynôme sont isomorphes.

4°) Clôture algébrique

Déf. 36 : Soit K un corps, les assertions suivantes sont équivalentes :

i) $\forall P \in K[X] \setminus K$, P est scindé sur K

ii) $\forall P \in K[X] \setminus K$, P a au moins une racine dans K

iii) $\forall P \in K[X]$, P est irréductible ssi $\deg P = 1$

Si elles sont vérifiées, K est dit algébriquement clos.

Ex. 37 : Le théorème de d'Alembert-Gauss affirme que $\mathbb{C}$ est algébriquement clos

Déf 38 : Une extension L de K est appelée clôture algébrique de K si elle est algébriquement close et algébrique sur K.

Ex 39 : $\mathbb{C}$ est "la" clôture algébrique de $\mathbb{R}$. $\mathbb{R}$ n'est pas algébriquement clos car les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de la forme aX^2+bX+c avec $b^2-4ac<0$.

Th. 40 (Steinitz) : 1) Tout corps commutatif admet une clôture algébrique

2) Deux clôtures algébriques de K sont K-isomorphes

III - Applications 1°) Extensions finies d'un corps parfait

Déf 41 : Le corps K est dit parfait s'il est de caractéristique nulle ou si son morphisme de Frobenius $\Phi : \left| \begin{array}{ccc} K & \to & K \\ x & \mapsto & x^{\mathrm{car}(K)} \end{array} \right.$ est surjectif.

Rmq 42 : Les corps finis et les corps algébriquement clos sont parfaits.

Prop 43 : Soit K un corps parfait, $P \in K[X]$ irréductible.
Alors P est à racines simples dans son corps de décomposition.

Rmq 44 : On note $K = \mathbb{F}_p(T)$, le corps des fractions rationnelles à une indéterminée sur $\mathbb{F}_p$. Soit $P = X^p - T \in K[X]$, il est irréductible. Soit L le corps de décomposition de P sur K, et soit $\alpha \in L$ une racine de P. Alors $P = (X-\alpha)^p$, donc L n'est pas parfait.

Th 45 (Théorème de l'élément primitif) :
Si K est parfait et L/K est une extension finie, alors L est un corps de rupture. En d'autres termes, il existe $x \in L$ algébrique sur K tel que $L = K(x)$

↳ DEV. n°1

2°) Constructions des corps finis

Th. 42 : Soit $n \in \mathbb{N}^*$ et $\mathbb{F}$ un corps fini de cardinal $q \in \mathbb{N}^*$.

1) Le corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}$ est de cardinal q^n

2) Tout corps de cardinal q^n est un corps de décomposition de $X^{q^n} - X$ sur $\mathbb{F}$.

Cor 43 : 1) Comme pour tout $p \in \mathbb{N}$ premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps de cardinal p ; il existe un corps de cardinal p^n pour tout $n \in \mathbb{N}$

2) Deux corps finis de même cardinal sont isomorphes

Remarque 44 : En pratique, on construit $\mathbb{F}_{p^n}$ en quotientant $\mathbb{F}_p[X]$ par un polynôme irréductible de degré n ; $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2+X+1)$

Déf 45 : On définit la fonction de Möbius μ sur $\mathbb{N}$ par :

$$\begin{cases} \mu(1) = 1 \\ \mu(p_1 \dots p_k) = (-1)^k \text{ si } p_1, \dots, p_k \text{ sont premiers distincts} \\ \mu(n) = 0 \quad \text{sinon (i.e. } \mu \text{ a un facteur premier de multiplicité } > 1) \end{cases}$$

Prop 46 : Le nombre de polynômes irréductibles de degré n sur $\mathbb{F}_q$ est :

$$I(n,q) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$$

DEV n°2

Prop 47 : $I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$