125 : Extensions de corps. Exemples et applications.

I Extensions de corps et extensions algébriques.

A Degrés et extensions simples. Per

Définition 1 : Etant donné un corps $\mathbb{K}$, on appelle extension de $\mathbb{K}$ tout corps $\mathbb{L}$ contenant un sous corps isomorphe à $\mathbb{K}$.

Exemple 2 : $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Remarque 3 : Soit $\mathbb{L}$ une extension de $\mathbb{K}$, alors $\mathbb{L}$ est un $\mathbb{K}$-ev avec $\forall (\lambda, x) \in \mathbb{K} \times \mathbb{L}$, $\lambda \cdot x = f(\lambda) x$ avec $f : \mathbb{K} \to \mathbb{L}$ le morphisme de corps.

Définition 4 : Soit $\mathbb{L}$ une extension de $\mathbb{K}$ (on note $L:K$), alors $[L:K]$ est appelé degré de l'extension $L:K$. Si L est dimension finie sur K, on dit que L est une extension de degré fini sur K et $[L:K] = \dim_K L$. Sinon l'extension est de degré infini sur K.

Exemple 5 : $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{K}:\mathbb{K}] = 1$.
Remarque : si $L:K$ sont des corps finis on a $|L| = |K|^m$ où $m = [L:K]$

Théorème 6 (de la base téléscopique)
Soient $K \subset L \subset H$ des corps, $(e_i)_{i \in I}$ une base de L sur K, $(f_j)_{j \in J}$ une base de H sur L. Alors la famille $(e_i f_j)_{i,j \in I \times J}$ est une base de H sur K.

Corollaire 7 (multiplicativité du degré).
Dans ce cas, si les degrés sont finis, on a $[H:K] = [H:L][L:K]$

Exemple 8 : $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$

Définition 9 : Soit $K \subset L$ une extension et A une partie de L. On dit que A engendre L sur K et on écrit alors $L = K(A)$ si L est le plus petit sous corps de L contenant K et A. Si A est fini, $A = \{\alpha_1, \dots, \alpha_n\}$, on note $L = K(\alpha_1, \dots, \alpha_n)$.
L'extension $K \subset L$ est dite monogène s'il existe $\alpha \in L$ tel que $L = K(\alpha)$.

Exemple 10 : $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ est monogène.

Remarque 11 : Soit $L:K$ et $a \in L$, alors $K(a) = \{P(a), P \in \mathrm{Frac}\, K[X]\}$ et $K[a] = \{P(a), P \in K[X]\}$

B Eléments algébriques et extensions algébriques. Per

On considère une extension de corps $L:K$.

Définition 12 : Soit $\alpha \in L$. Soit $\varphi : K[X] \to L$ l'homomorphisme défini par $\varphi_{|K} = \mathrm{id}_K$ et $\varphi(X) = \alpha$.
i) Si φ est injectif, on dit que α est transcendant sur K.
ii) Sinon on dit que α est algébrique sur K. Ceci signifie qu'il existe un polynôme $P(X)$ non nul tel que $P(\alpha) = 0$. Plus précisément si $I = \ker \varphi$, I est un idéal principal non nul donc $I = (P)$ avec $P \neq 0$ d'après supposons P unitaire. Alors P est le polynôme minimal de α sur K.
Exemple 13 : e et π sont transcendants sur $\mathbb{Q}$ mais pas sur $\mathbb{R}$.
Les nombres $\sqrt{2}, i, \sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$.

Théorème 14 : Soit $\alpha \in L$. On a équivalence entre :
i) α est algébrique
ii) on a $K[\alpha] = K(\alpha)$
iii) on a $\dim_K K(\alpha) < +\infty$.
Précisément, si P est le polynôme minimal de α, P est irréductible et on a alors $\dim_K K[\alpha] = [K[\alpha] : K] = d°P$. Cet entier s'appelle le degré de α.

Définition 15 : Une extension $K \subset L$ est dite algébrique si pour tout $\alpha \in L$, α est algébrique sur K.

Remarque 16 : d'après le théorème 14, toute extension finie est algébrique.
Réciproque fausse.

Théorème 17 : Soient $L:K$ et $H:L$ des extensions de corps. Alors : Jos
$(L:K$ et $H:L$ algébriques$) \Rightarrow H:K$ algébrique.

Théorème 18 : On pose $M = \{x \in L \mid x$ est algébrique sur $K\}$. Alors M est un sous corps de L.

Exemple 19 : Soit $A = \{\alpha \in \mathbb{C} \mid \alpha$ algébrique sur $\mathbb{Q}\}$, A est un corps, algébrique sur $\mathbb{Q}$, mais l'extension $\mathbb{Q} \subset A$ n'est pas finie car il existe des éléments de A de degré arbitrairement grand, par exemple $\sqrt[n]{2}$ qui est de degré n car le polynôme $X^n - 2$ est irréductible sur $\mathbb{Q}$ (corollaire du critère d'Eisenstein).

II Construction de corps, lien avec les polynômes.

A Corps de rupture. Per

Définition 20 : Soit $P \in K[X]$ irréductible. Une extension $L : K$ est appelé corps de rupture de P sur K si L est une extension monogène $L = K(\alpha)$ avec $P(\alpha) = 0$.

Proposition 21 : Soit $P \in K[X]$ irréductible, alors $K[X]/(P)$ est un corps dans lequel K s'injecte et si x est l'image de X dans $K[X]/(P)$, on a $P(x) = 0$ et $K(x) = K[X]/(P)$.

Exemple 22 : $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$ est un corps de rupture de X^2+1.
$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[X]/(X^3-2)$ est un corps de rupture de X^3-2.

Théorème 23 : Il existe un unique corps de rupture de P sur K à isomorphisme près.

Lemme 24 : Soient K, K' deux corps, $i : K \to K'$ un isomorphisme que l'on étend de manière évidente en un isomorphisme, noté encore i, de $K[X]$ sur $K'[X]$ en envoyant X sur X. Soit $P \in K[X]$ irréductible et soit $P' = i(P)$. Soit L (resp L') un corps de rupture de P sur K (resp P' sur K') engendré par une racine de P, x (resp x' de P'). Alors il existe un unique isomorphisme φ de L sur L' prolongeant i et vérifiant $\varphi(x) = x'$.

Remarque 25 : Si L est un corps de rupture de P, le polynôme P n'est pas, en général entièrement factorisé sur L.

Exemple 26 : $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de X^3-2 sur $\mathbb{Q}$ mais X^3-2 n'est pas scindé sur $\mathbb{Q}(\sqrt[3]{2})$ car $j\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$ et $(X^3-2)(j\sqrt[3]{2}) = 0$.

B Corps de décomposition Par X.G

Définition 27 : Soit $P \in K[X]$ un polynôme, irréductible ou non de degré n. On appelle corps de décomposition de P sur K une extension L de K telle que :
i) dans $L[X]$, P est produit de facteurs de degré 1 (ou encore, P a toutes ses racines dans L).
ii) le corps L est minimal pour cette propriété (ou encore, les racines de P engendrent L).

Théorème 28 : Pour tout $P \in K[X]$, il existe un unique corps de décomposition de P sur K (à isomorphisme près). On le note $D_K(P)$.

Lemme 29 : Soient K, K' deux corps, $i : K \to K'$ un isomorphisme, que l'on étend en un isomorphisme, noté encore i, de $K[X]$ sur $K'[X]$. Soient $P \in K[X]$ un polynôme, $P' = i(P)$ et L (resp L') un corps de décomposition de P sur K (resp de P' sur K'). Alors il existe un unique isomorphisme φ de L sur L', prolongeant i.

Exemple 30 : i) Pour $K = \mathbb{Q}$, $P(X) = X^3 - 2$, on a $D_K(P) = \mathbb{Q}(\sqrt[3]{2}, j)$
ii) Pour $K = \mathbb{Q}$, $P(X) = X^4 - 2$, on a $D_K(P) = \mathbb{Q}(\sqrt[4]{2}, i)$

Application 31 : (Théorème de l'élément primitif)
Soit L une extension de degré fini de K, si K est de caractéristique 0 alors L est monogène i.e $\exists a \in L$, $L = K(a)$. Problème 2.5.9 X.G page 96.

Lemme 32 : Soit $P, Q \in K[X]$ et $L : K$, alors $\mathrm{PGCD}_{K[X]}(P,Q) = \mathrm{PGCD}_{L[X]}(P,Q)$.

Remarque 33 : Le résultat reste vrai si K est fini.

C Corps algébriquement clos et clôture algébrique Par

Définition 34 : On dit que K est algébriquement clos s'il vérifie l'une des quelconques propriétés équivalentes suivantes :
i) tout polynôme $P \in K[X]$ de degré ≥ 1 admet une racine dans K.
ii) tout polynôme $P \in K[X]$ est produit de polynôme de degré 1.
iii) les éléments irréductibles de $K[X]$ sont les $X - a$, $a \in K$.
iv) si une extension $K \subset L$ est algébrique, on a $L = K$.

Exemple 35 : $\mathbb{C}$ est algébriquement clos (d'Alembert Gauss).

Théorème 36 (Admis) : tout corps K admet une extension algébriquement close (Steinitz)

Définition 37 : Une extension $\overline{K}$ de K est appelée une clôture algébrique de K si elle vérifie :
i) $\overline{K}$ est algébriquement clos.
ii) $\overline{K}$ est algébrique sur K.

Exemple 38 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Théorème 39 : Tout corps K admet une clôture algébrique, plus précisément si L est une extension de K alors l'ensemble $\overline{K}$ des $a \in L$ tels que a est algébrique sur K est une clôture algébrique de K.

Théorème 40 : Tout corps admet une unique clôture algébrique (à isomorphisme près)

III Applications

A Irréductibilité de polynômes et réduction Par

Soit A un anneau factoriel, on note $K = \mathrm{Frac}\, A$.

Définition 41 : On définit pour $P \in A[X]$, $P \neq 0$ le contenu de P noté $c(P)$: si $P(X) = a_n X^n + \dots + a_0$, on pose $c(P) = \mathrm{pgcd}(a_0, \dots, a_n)$, l'élément $c(P)$ est défini modulo $A^\times$. Si $c(P) = 1$, P est dit primitif.

Lemme 42 (Gauss) : On a $c(PQ) = c(P)c(Q)$ modulo $A^\times$

Proposition 43 : Les polynômes $P(X) \in A[X]$ irréductibles dans $A[X]$ sont :
i) les constantes $p \in A$, irréductibles dans A,
ii) les polynômes $P(X)$, de degré ≥ 1, primitifs et irréductibles dans $K[X]$.

Développement (Critère d'Eisenstein)
Soit $P(X) = a_n X^n + \dots + a_0$ avec $a_i \in A$. Soit $p \in A$ un élément irréductible. On suppose :
i) $p \nmid a_n$ ii) $\forall i \in [\![0, n-1]\!]$, $p \mid a_i$ iii) $p^2 \nmid a_0$.
Alors P est irréductible dans $K[X]$ (donc aussi dans $A[X]$ si $c(P) = 1$).

Application 44 : Soit $p \in \mathbb{P}$ impair, alors $\Phi_p(X) = X^{p-1} + \dots + 1$ est irréductible dans $\mathbb{Z}[X]$.

Théorème 45 (réduction) : Soit I un idéal premier de A et $B = A/I$ qui est un anneau intègre de corps de fractions L. Soit $P(X) = a_n X^n + \dots + a_0 \in A[X]$ et $\bar{P}$ sa réduction modulo I. On suppose $\bar{a_n} \neq 0$ dans B. Alors si $\bar{P}$ est irréductible sur B ou L, le polynôme P est irréductible sur K.

Exemple 46 : $X^p - X - 1$ est irréductible sur $\mathbb{F}_p$.

Théorème 47 : Soit k un corps et $P \in k[X]$ de degré $n > 0$. Alors, P est irréductible sur k si et seulement si P n'a pas de racines dans les extensions K de k qui vérifient $[K : k] \leq \frac{n}{2}$.

Exemple 48 : $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2$. Il suffit de vérifier qu'il n'a pas de racines dans $\mathbb{F}_2$ ni $\mathbb{F}_4$. Pour $\mathbb{F}_2$ c'est clair, pour $\mathbb{F}_4$ on note que l'on a $\mathbb{F}_4 = \mathbb{F}_2[j]$ avec $j^2 + j + 1 = 0$. Si $x \in \mathbb{F}_4 \setminus \mathbb{F}_2$, on a $x = j$ ou $x = j+1 = -j^2$ donc $x^3 = 1$ et $x^4 + x + 1 = 2x + 1 = 1 \neq 0$.

Théorème 49 : Soit $P \in k[X]$ irréductible de degré n et soit K une extension de degré m, $m \wedge n = 1$. Alors P est encore irréductible sur K.

Remarque 50 : c'est faux si $m \wedge n \neq 1$. $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais pas sur $\mathbb{Q}(i)$: on a $X^4 + 1 = (X^2 + i)(X^2 - i)$.

Exemple 51 : $X^3 + X + 1$ est irréductible sur $\mathbb{Q}(i)$ comme sur $\mathbb{Q}$.

B Cyclotomie. Par

Soit $n \in \mathbb{N}^*$.

Définition 52 : Le n-ième polynôme cyclotomique $\Phi_n \in \mathbb{C}_n[X]$ est donné par
$$\Phi_n(X) = \prod_{u \in \mu_n^\times} (X - u)$$

Proposition 53 : on a $X^n - 1 = \prod_{d \mid n} \Phi_d(X)$.

Exemple 54 : $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$.

Corollaire 55 : $n = \sum_{d \mid n} \varphi(d)$ avec φ l'indicatrice d'Euler

Développement $\Phi_n(X) \in \mathbb{Z}[X]$ est irréductible unitaire et irréductible dans $\mathbb{Z}[X]$.

Théorème 56 : (Wedderburn) Tout corps fini est commutatif.

Références :

D. Perrin Cours d'Algèbre Per

Extensions de corps Josette Calais Jos

X G Algèbre X.G

Pour dire qu'on peut le lemme de Steinitz
on peut utiliser le lemme de Zorn