

## Examen : Anneaux et corps commutatifs

Durée : 3 heures

L'énoncé comporte deux pages.  
Les documents ne sont pas autorisés.  
Les réponses doivent être justifiées.

Donner les formulations :

- du théorème de Hilbert pour la base,  
Si  $A$  est un anneau noethérien, alors l'anneau  $A[X]$  l'est aussi
- du théorème de Hilbert pour les zéros ,  
Soit  $k$  un corps algébriquement clos, soit  $I \leq k[X_1, \dots, X_n]$  un idéal, alors  $I(V(I)) = \sqrt{I}$ .
- du théorème qui relie les sous-extensions d'une extension galoisienne  $L/k$  avec les sous groupes de  $\text{Gal}(L/k)$ .

$$\{\text{sous-groupes de } (L/k)\} \longleftrightarrow \{K \mid K \text{ est un corps et } k \leq K \leq L\}$$

$$H \longmapsto L^H$$

$$(L/K) \longleftarrow K$$

sont des bijections réciproques l'une de l'autre.

**Exercice 1.** Soit  $P(X) = X^4 + X^3 + X^2 + X + 1$ . On note  $K$  le corps de décomposition de  $P$  sur  $\mathbb{Q}$  dans  $\mathbb{C}$ .

- Quel est l'unique polynôme irréductible de degré 2 sur  $\mathbb{F}_2$  ?  
 $X^2 + X + 1$
- Montrer que  $P$  est irréductible sur  $\mathbb{F}_2$ . On note  $k$  le corps  $k = \mathbb{F}_2[X]/(P)$ . Quel est l'ordre du groupe  $k^*$  ? Si  $P$  était réductible, alors  $P$  aurait un facteur de degré 1 ou serait le produit de deux facteurs de degré 2 irréductibles. Ce n'est pas le cas car  $P$  n'a pas de racine dans  $\mathbb{F}_2$  et  $P \neq (X^2 + X + 1)^2$ .  
Comme  $P$  est de degré 4,  $k$  est un  $\mathbb{F}_2$ -espace vectoriel de dimension 4 donc  $|k^*| = 2^4 - 1 = 15$ .
- On pose  $\alpha = X \pmod{P}$  dans  $k$ . Quel est l'ordre de  $\alpha$  dans le groupe  $k^*$  ? Montrer que  $1, \alpha, \alpha^2, \alpha^3$  est une base de  $k$  comme  $\mathbb{F}_2$ -espace vectoriel. Montrer que comme groupes :

$$\langle 1 + \alpha \rangle = k^*.$$

Dans  $k$ ,  $\alpha^5 - 1 = (\alpha - 1)(1 + \alpha + \dots + \alpha^4) = 0$  donc  $\alpha^5 = 1$  et  $\alpha$  est d'ordre 5. Dans  $\mathbb{F}_2[X]/(P)$ ,  $1, X, X^2, X^3, X^4 \pmod{P}$  forment une base donc  $1, \alpha, \dots, \alpha^4$  est une base de  $k$  comme  $\mathbb{F}_2$ -espace vectoriel. On a :

$$\begin{aligned} (1 + \alpha)^3 &= 1 + \alpha + \alpha^2 + \alpha^3 \neq 1 \\ (1 + \alpha)^5 &= (1 + \alpha)^4(1 + \alpha) = (1 + \alpha^4)(1 + \alpha) = 1 + \alpha^4 + \alpha + \alpha^5 \\ &= 1 + 1 + \alpha + \alpha^2 + \alpha^3 + \alpha + 1 = 1 + \alpha^2 + \alpha^3 \neq 1 \end{aligned}$$

Donc  $(1 + \alpha)$  n'est pas d'ordre 3 ni 5. Comme  $|k^*| = 15$ , on a  $\alpha^{15} = 1$ . Comme  $15 = 5 \cdot 3$ , on en déduit que  $1 + \alpha$  est d'ordre 15 et  $\langle 1 + \alpha \rangle = k^*$ .

4. Quel est le groupe de Galois de  $P$  sur  $\mathbb{F}_2$  (à isomorphisme près)? ( $k/\mathbb{F}_2$ ) est cyclique d'ordre 4 engendré par le morphisme de Frobenius  $xx^2$ , c'est  $\mathbb{Z}/4\mathbb{Z}$ .

5. Montrer que  $P$  est le polynôme minimal de  $e^{\frac{2i\pi}{5}}$  sur  $\mathbb{Q}$ . On a  $P(e^{\frac{2i\pi}{5}}) = 1 + e^{\frac{2i\pi}{5}} + \dots + (e^{\frac{2i\pi}{5}})^4 = \frac{(e^{\frac{2i\pi}{5}})^5 - 1}{e^{\frac{2i\pi}{5}} - 1} = 0$ . Donc le polynôme minimal de  $e^{\frac{2i\pi}{5}}$  sur  $\mathbb{Q}$  divise  $P$ . Or  $P$  est irréductible sur  $\mathbb{Q}$  (car irréductible mod 2) et unitaire donc  $P$  est bien le polynôme minimal.

6. Soit  $K = \mathbb{Q}(e^{\frac{2i\pi}{5}})$ . Montrer que  $K$  est galoisienne sur  $\mathbb{Q}$ . On notera  $G = \text{Gal}(K/\mathbb{Q})$ . Quel est l'ordre de  $G$ ?

Comme  $\mathbb{Q}$  est de caractéristique nulle, toute extension de  $\mathbb{Q}$  est séparable. Or les racines de  $P$  sont  $(e^{\frac{2i\pi}{5}})^l$ ,  $1 \leq l \leq 4$  donc  $\mathbb{Q}(e^{\frac{2i\pi}{5}})$  est le corps de décomposition de  $P$  sur  $\mathbb{Q}$ . Donc  $\mathbb{Q}(e^{\frac{2i\pi}{5}})$  est galoisienne sur  $\mathbb{Q}$  et son groupe de Galois est d'ordre  $[K : \mathbb{Q}] = 4$  (car  $P$  irréductible sur  $\mathbb{Q}$ ).

7. Montrer que si  $x$  est une racine de  $P$ , alors  $(x-1)P'(x) = 5x^4$ . En déduire que  $\Delta_P = 5^3$ . On a  $P(X)(X-1) = X^5 - 1 \Rightarrow P'(X)(X-1) + P(X) = 5X^4 \Rightarrow P'(x)(x-1) = 5x^4$  si  $P$  est une racine de  $P$ .

Comme  $P$  est de degré 4,  $\Delta_P = P'(x_1)P'(x_2)P'(x_3)P'(x_4)$  où  $x_1, x_2, x_3, x_4$  sont les racines de  $P$ . Alors  $\Delta_P = \prod_{i=1,2,3,4} \frac{5x_i^4}{x_i-1}$ . Or  $P(X) = (X-x_1)\dots(X-x_4)$  donc  $\Delta_P = \frac{5^4 \cdot 1}{P(1)} = 5^3$ .

8. Montrer que  $\mathbb{Q}(\sqrt{5}) = K \cap \mathbb{R}$ .

On a  $\Delta_P = 5^3 = \prod_{1 \leq i < j \leq 4} (x_i - x_j)^2 \Rightarrow 5\sqrt{5} = \pm \prod_{1 \leq i < j \leq 4} (x_i - x_j) \in K = \mathbb{Q}(x_1, x_2, x_3, x_4)$ . Donc  $\mathbb{Q}(\sqrt{5}) \leq K \cap \mathbb{R}$ . Or

$$4 = [K : \mathbb{Q}] = [K : K \cap \mathbb{R}][K \cap \mathbb{R} : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$$

$$\Rightarrow [K \cap \mathbb{R} : \mathbb{Q}(\sqrt{5})] = \frac{2}{[K : K \cap \mathbb{R}]}$$

or,  $e^{\frac{2i\pi}{5}} \notin \mathbb{R}$  donc  $[K : K \cap \mathbb{R}] \geq 2$  d'où  $[K \cap \mathbb{R} : \mathbb{Q}(\sqrt{5})] \leq 1$  et  $K \cap \mathbb{R} = \mathbb{Q}(\sqrt{5})$ .

9. Montrer qu'il existe  $\theta \in G$  tel que  $\theta(e^{\frac{2i\pi}{5}}) = e^{\frac{4i\pi}{5}}$ . Vérifier que  $G = \langle \theta \rangle$ .

Comme  $P$  est irréductible sur  $\mathbb{Q}$ , comme  $e^{\frac{2i\pi}{5}}$  et  $e^{\frac{4i\pi}{5}}$  sont des racines de  $P$ , il existe un morphisme de corps  $\theta : K \rightarrow \mathbb{C}$  tel que  $\theta(e^{\frac{2i\pi}{5}}) = e^{\frac{4i\pi}{5}}$ . Puisque  $e^{\frac{4i\pi}{5}} \in K$ ,  $\theta \in G$ . Or  $G$  est d'ordre 4 =  $[K : \mathbb{Q}]$ .

Soit  $z = e^{\frac{2i\pi}{5}}$ . On a  $\theta^2(z) = \theta(z^2) = z^4 \neq z$ . On a aussi  $\theta^4(z) = (z^4)^4 = z^{16} = z$ . Donc  $\theta$  est d'ordre 4 =  $|G|$  donc  $G = \langle \theta \rangle$ .

10. Déterminer les sous-groupes de  $G$  d'ordre 2 et les corps intermédiaires correspondants entre  $\mathbb{Q}$  et  $K$ .

Comme  $G$  est cyclique d'ordre 4,  $G$  a un seul sous-groupe d'ordre 2 :  $\langle \theta^2 \rangle$ . Le corps correspondant est  $L = K^{\langle \theta^2 \rangle}$ . De plus  $[K : L] = 2 \Rightarrow [L : \mathbb{Q}] = 2$ . Donc c'est  $L = \mathbb{Q}(\sqrt{5})$ .

**Exercice 2.** 1. Soit  $E = \{(t, t^n) : t \in \mathbb{C}\}$  où  $n \in \mathbb{N}^*$ .

(a) Trouver un polynôme irréductible  $P \in \mathbb{C}[X, Y]$  tel que  $E = V(P)$ .

$P = X^n - Y$  est irréductible car de degré 1 en  $Y$ .

(b) Montrer que  $I(E) = (P)$ .

D'après le théorème des zéros de Hilbert,  $I(E) = \sqrt{(P)}$ . Or  $P$  irréductible  $\Rightarrow (P)$  premier  $\Rightarrow I(E) = \sqrt{(P)} = (P)$ .

(c) L'idéal  $I(E)$  est-il premier? maximal?  $I(E)$  est premier no maximal car inclus strictement dans  $(X, Y)$ .

2. Soit  $E = \{(e^t, t^n) : t \in \mathbb{C}\}$  où  $n \in \mathbb{N}^*$ .

(a) Montrer que  $I(E) = (0)$ . (Indication : Rappelons que  $\mathbb{C}[X, Y] = \mathbb{C}[Y][X]$  et  $\lim_{t \rightarrow \infty} \frac{P(t)}{e^t} = 0$  pour tout  $P \in \mathbb{C}[Y]$ .)

Soit  $P(X, Y) \in I(E)$ , alors  $t \in \mathbb{C}$ ,  $P(e^t, t^n) = 0$ .

Si  $P \neq 0$ , alors  $P(X, Y) = a_0(Y) + \dots + a_d(Y)X^d$  où  $d > 0$  et  $0 \leq i \leq d$ ,  $a_i(Y) \in \mathbb{C}[Y]$  et  $a_d \neq 0$ . Mais alors :

$$t \in \mathbb{R}, a_d(t^n) = -a_0(t^n)e^{-dt} - \dots - a_{d-1}(t^n)e^{-t}$$

c'est absurde car le terme de gauche est constant non nul si  $a_d(Y)$  est constant ou bien tend vers  $\pm$  en  $+$  et celui de droite vers 0.

Donc  $P = 0$ .

- (b) Existe-t-il un idéal  $I$  dans  $\mathbb{C}[X, Y]$  tel que  $E = V(I)$ ? Justifier.

Si on avait  $E = V(I)$ , on aurait  $I(E) = \sqrt{I} \Rightarrow (0) = \sqrt{I} \Rightarrow I = 0 \Rightarrow E = \mathbb{C}^2$  ce qui est absurde car  $(0, 0) \notin E$ .

**Exercice 3.** Soit un polynôme irréductible  $P \in \mathbb{Q}[X]$  de degré  $\geq 2$  et  $\alpha \in \mathbb{C}$  une racine de  $P$ . Notons par  $K$  un corps maximal parmi les sous-corps de  $\overline{\mathbb{Q}}$  qui ne contiennent pas  $\alpha$ . (L'existence d'un tel corps  $K$  pourrait être démontré facilement à l'aide du lemme de Zorn.)

1. Montrer que  $0 < [K(\alpha) : K] < \infty$ .

Comme  $\alpha \notin K$ ,  $[K(\alpha) : K] > 0$ . Comme  $P \in \mathbb{Q}[X] \leq K[X]$ , on a  $[K(\alpha) : K] \leq \deg P < \infty$ .

2. D'abord, on se propose de montrer que l'extension  $K(\alpha)/K$  est galoisienne. Supposons par l'absurde que  $K(\alpha)/K$  n'est pas galoisienne et notons par  $L$  le corps de décomposition de  $P$  sur  $K$ .

- (a) Justifier que  $L \neq K(\alpha)$  et  $L/K$  est une extension galoisienne.

L'extension  $L/K$  est galoisienne car normale (c'est un corps de décomposition) et séparable (la caractéristique est nulle). En particulier  $L \neq K(\alpha)$ .

- (b) Soit  $G = \text{Gal}(L/K)$  et  $H = \text{Gal}(L/K(\alpha))$ . Montrer que  $\{e\} \subsetneq H \subsetneq G$ .

$|G/H| = \frac{[L:K]}{[L:K(\alpha)]} = [K(\alpha) : K] \neq 1$  car  $\alpha \notin K$ . On a aussi  $|G/H| \neq |G| = [L : K]$  car  $K(\alpha) \neq L$ . Donc  $\{e\} \neq H \neq G$ .

- (c) Soit  $\sigma \in G \setminus H$ . Montrer que  $K = \{x \in L : \sigma(x) = x\}$ . (Indication : On se rappelle la définition de  $K$ .)

Comme  $\sigma \notin H$ ,  $\sigma(\alpha) \neq \alpha$  donc  $\alpha \notin L^{\langle \sigma \rangle}$ . Par maximalité de  $K$  pour la propriété de ne pas contenir  $\alpha$ , on a  $K = L^{\langle \sigma \rangle}$ .

- (d) En déduire que si  $\sigma \in G \setminus H$  alors  $G = \langle \sigma \rangle$ .

Comme  $L/K$  est galoisienne,  $L^G = L^{\langle \sigma \rangle} \Leftrightarrow \langle \sigma \rangle = G$ .

- (e) Conclure.

Comme  $G$  est cyclique,  $H$  est distingué dans  $G$  donc  $K(\alpha)/K$  est galoisienne : *contradiction!*

3. Maintenant, soit  $G = \text{Gal}(K(\alpha)/K)$ .

- (a) Montrer que  $K$  et  $K(\alpha)$  sont les seuls sous-corps de  $K(\alpha)$  contenant  $K$ . (Indication : La même que pour 2(c).)

Si  $K \leq F \leq K(\alpha)$  est un corps tel que  $F \neq K(\alpha)$ , alors si  $H = \text{Gal}(K(\alpha)/F)$ , on a  $\alpha \notin K(\alpha)^H = F$ . Par maximalité de  $K$ ,  $K = F$  donc  $H = G$  donc  $F = K(\alpha)^G = K$ .

- (b) Montrer que le groupe  $G$  est cyclique d'ordre premier.

D'après la correspondance de Galois,  $G$  n'a pas de sous-groupe propre autre que le groupe trivial. Donc  $G$  est en particulier un groupe simple. Or, si  $1 \neq g \in G$ , on a forcément  $\langle g \rangle = G \Rightarrow G$  cyclique  $\Rightarrow G$  est simple cyclique donc d'ordre premier!