Master 1 – Université Lyon I **mercredi 5 avril 2022**
2021–2022

CC~~1~~ 2 : Anneaux et corps et commutatifs

Durée : 1h30

Les documents ne sont pas autorisés
Les réponses doivent être justifiées

Exercice 1 1. Donner la liste des polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$.

X^2+1 , X^2+X-1 , X^2-X-1 (discriminant $=-1$)

2. Montrer que chacun de ces polynômes divise $X^9 - X$ dans $\mathbb{F}_3[X]$.

Soit P irréductible de degré 2 sur $\mathbb{F}_3$. Alors le corps $K = \mathbb{F}_3[X]/(P)$ est de cardinal 9 donc $\forall x \in K$, $x^9 = x$. Donc $X^9 = X \mod P$ c-à-d: $P \mid X^9 - X$.

Exercice 2 Soit $P \in \mathbb{Q}[X]$ un polynôme séparable et $\alpha_1, \cdots, \alpha_n$ ses racines. On sait que le discriminant $\Delta_P = \delta^2$ où $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$. On désigne par $\mathrm{Gal}(P)$ le groupe de Galois de P sur $\mathbb{Q}$. Rappelons que $\mathrm{Gal}(P)$ agit sur $\{\alpha_1, \cdots, \alpha_n\}$ et est consideré comme sous-groupe du groupe symétrique S_n.

1. Montrer que si $\sigma \in \mathrm{Gal}(P)$ alors $\sigma(\delta) = \epsilon(\sigma)\delta$ où $\epsilon(\sigma) \in \{\pm 1\}$. En déduire que l'application $\epsilon : \mathrm{Gal}(P) \to \{\pm 1\}$ est un homomorphisme.

Comme $\delta^2 \in K$, $\forall \sigma \in Gal(P)$, $\sigma(\delta^2) = \delta^2 \Leftrightarrow \sigma(\delta)^2 = \delta^2 \Leftrightarrow \sigma(\delta) = \pm\delta$.
Posons $\varepsilon(\sigma) = \frac{\sigma(\delta)}{\delta}$ (P séparable $\Rightarrow \delta \neq 0$). On a : $\forall \sigma, \tau \in Gal(P)$,
$\varepsilon(\sigma\tau) = \frac{\sigma(\tau(\delta))}{\delta} = \frac{\sigma(\varepsilon(\tau)\delta)}{\delta} = \varepsilon(\tau)\frac{\sigma(\delta)}{\delta} = \varepsilon(\tau)\varepsilon(\sigma)$.

2. On désigne par A_n le sous-groupe alterné de S_n. Montrer que $\mathrm{Gal}(P) \subset A_n$ si et seulement si $\Delta \in (\mathbb{Q}^*)^2$.

Identifions $Gal(P)$ à un sous-groupe de S_n via : $\forall i$, $\sigma(\alpha_i) = \alpha_{\sigma(i)}$.
Alors $\sigma(\delta) = \prod_{1\le i<j\le n}(\alpha_{\sigma(i)} - \alpha_{\sigma(j)}) = sgn(\sigma)\prod_{1\le i<j\le n}(\alpha_i - \alpha_j)$.
Donc $\varepsilon(\sigma) = sgn(\sigma)$. D'où $Gal(P) \leqslant A_n \Leftrightarrow \forall \sigma \in Gal(P)$, $sgn(\sigma) = 1$
$\Leftrightarrow \forall \sigma \in Gal(P)$, $\varepsilon(\sigma) = 1$
$\Leftrightarrow \forall \sigma \in Gal(P)$, $\sigma(\delta) = \delta \Leftrightarrow \delta \in \mathbb{Q}^\times$
$\Leftrightarrow \Delta \in (\mathbb{Q}^\times)^2$

Exercice 3 Soient $P(X) = X^3 - 3X - 1$ et $Q(X) = X^3 - 4X - 1$ des polynômes dans $\mathbb{Q}[X]$. On note Δ_P et Δ_Q les discriminants de P et Q.

1. Montrer que P et Q sont irréductibles sur $\mathbb{Q}$.

Si $x \in \mathbb{Q}$ était racine de P, alors $x \in \mathbb{Z}$ car P unitaire dans $\mathbb{Z}[X]$. Mais alors $P(x) = 0 \Leftrightarrow x^3 - 3x - 1 = 0 \Rightarrow x \mid 1 \Rightarrow x = \pm 1$. Or $P(1), P(-1) \neq 0$. Donc P n'a pas de racines dans $\mathbb{Q}$ donc P irréductible sur $\mathbb{Q}$. De même, Q irréductible sur $\mathbb{Q}$.

2. Justifier que chacun des polynômes P et Q a trois racines réelles distinctes.

On note x_1, x_2, x_3 les racines de P et y_1, y_2, y_3 celles de Q.

$\Delta_P = -4\cdot(-3)^3 - 27\cdot(-1)^2 = 3^3\cdot(4-1) = 3^4 > 0$. $\Delta_Q = -4(-4)^3 - 27\cdot(-1)^2 = 4^4 - 3^3 > 0$. Donc les racines de P et de Q sont réelles et deux à deux distinctes.

3. En calculant Δ_P et Δ_Q décrire à isomorphisme près

(a) le groupe $\mathrm{Gal}(P)$, et

P irréductible donc $3 \mid |Gal(P)|$. Or $Gal(P) \leq \mathfrak{S}_3$. Donc $Gal(P) = A_3$ ou $\mathfrak{S}_3$. Or $\Delta_P = 3^4 = (3^2)^2 \in (\mathbb{Q}^\times)^2 \Rightarrow Gal(P) = A_3$

(b) le groupe $\mathrm{Gal}(Q)$.

On a aussi $Gal(Q) = A_3$ ou $\mathfrak{S}_3$: Or $\Delta_Q = 4^4 - 3^3 = 16^2 - 3^3$
$\Rightarrow 15^2 < \Delta_Q < 16^2$
$\Rightarrow \Delta_Q \notin (\mathbb{N})^2 \Rightarrow \Delta_Q \notin (\mathbb{Q}^\times)^2 \Rightarrow Gal(Q) = \mathfrak{S}_3$

Justifier ses réponses.

4. A-t-on :

(a) $\mathbb{Q}(x_1) = \mathbb{Q}(x_1, x_2, x_3)$,

Comme P irréductible, $[\mathbb{Q}(x_1) : \mathbb{Q}] = \deg P = 3$
$= |A_3| = |Gal(P)| = [\mathbb{Q}(x_1, x_2, x_3) : \mathbb{Q}]$
Or $\mathbb{Q}(x_1) \leq \mathbb{Q}(x_1, x_2, x_3)$ donc $\mathbb{Q}(x_1) = \mathbb{Q}(x_1, x_2, x_3)$

(b) $\mathbb{Q}(y_1) = \mathbb{Q}(y_1, y_2, y_3)$?

$\mathbb{Q}(y_1) \neq \mathbb{Q}(y_1, y_2, y_3)$ car $[\mathbb{Q}(y_1) : \mathbb{Q}] = 3 < 6 = |\mathfrak{S}_3| = |Gal(Q)| = [\mathbb{Q}(y_1, y_2, y_3) : \mathbb{Q}]$.

Justifier ses réponses.