Fiche V, exercice 1 :

Soit $f(X) = X + a_1 X^{n-1} + ...$ un polynôme irréductible sur k avec n racines distinctes dans une extension algébrique de k. On pose : $L := k(x_1, ..., x_n)$ le corps de décomposition de f sur k.

On pose $G := \mathrm{Gal}_k(f) := \mathrm{Gal}(L/k)$. On peut identifier G à un sous-groupe de S_n : si $\sigma \in G$ on note encore σ la permutation de $\{1, ..., n\}$ telle que pour toute racine x_i, $\sigma(x_i) = x_{\sigma(i)}$.

Soit $\Delta := \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in k$ le discriminant de f. On note : $\delta := \prod_{1 \leq i < j \leq n} (x_i - x_j)$ une racine carrée de Δ.

Alors Δ est un carré dans $k \Leftrightarrow \delta \in k \Leftrightarrow {}^{\forall}\sigma \in G,\ \sigma(\delta) = \delta$.

Or, $\sigma(\delta) = \epsilon(\sigma)\delta$. En effet : $\epsilon(\sigma) = (-1)^{l(\sigma)}$ où $l(\sigma)$ est le nombre de couples (i, j) tels que $1 \leq i < j \leq n$ et $\sigma(i) > \sigma(j)$ (c'est le nombre d'inversions de σ).

Donc Δ est un carré dans k si et seulement si $G \subseteq A_n = \ker \epsilon$.

Comme f est irréductible, f est le polynôme minimal de x_i sur k pour tout i donc $k(x_i) \simeq k[X]/(f)$ pour tout i. Donc si $1 \leq i \leq n$, il existe un $k-$isomorphisme de corps $\sigma : k(x_1) \to k(x_i)$ qui envoie x_1 sur x_i. Cet isomorphisme se prolonge en un automorphiseme que l'on note encore σ : $L \to L$. Donc il existe $\sigma \in G$ tel que $\sigma(x_1) = x_i$ *i.e.* $\sigma(1) = i$.

Ainsi G est un sous-groupe transitif de S_n. Donc l'ensemble $\{1, ..., n\}$ est une seule orbite de G et $n || G|$.

En particulier si $n = 3$, $G = A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ ou $G = S_3$.

On a donc pour un polynôme irréductible f sur k de degré 3 séparable (si f est irréductible, le pgcd de f et f' est 1 ou f. Pour des raisons de degrés, cette dernière possibilité n'a lieu que si $f' = 0$ ce qui est impossible en caractéristique $\neq 3$) :

$$\mathrm{Gal}_k(f) = A_3 \Leftrightarrow \Delta_f \in k^2$$

$$\mathrm{Gal}_k(f) = S_3 \Leftrightarrow \Delta_f \notin k^2 \ .$$

.

Par exemple : si $f = X^3 - X - 1$, f est irréductible sur $\mathbb{Z}$ en effet, le pgcd des coefficients de f est 1 et si f se factorisait on aurait au moins un facteur de degré 1 :

$$X^3 - X - 1 = (X - \alpha)(X^2 + aX + b)$$

avec $\alpha, a, b \in \mathbb{Z}$. Mais alors, $\alpha b = -1 \Rightarrow \alpha = \pm 1$. Or, ni 1 ni -1 ne sont racines. Donc f est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

On a $\Delta_f = -23 \notin \mathbb{Q}^2 \Rightarrow \mathrm{Gal}_{\mathbb{Q}}(f) = S_3$.

Si $g = X^3 + X^2 - 2X - 1$, g est irréductible sur $\mathbb{Q}$. de plus g a le même discriminant que $g(X - 1/3) = X^3 - 7/3X - 7/27$. Donc $\Delta_g = 49 = 7^2 \in \mathbb{Q}^2 \Rightarrow \mathrm{Gal}_{\mathbb{Q}}(g) = A_3$.

Fiche V exo 3 :

Soit $V := \{1, (12)(34), (13)(24), (14)(23)\} < S_4$.

Soit G un sous-groupe de S_4 transitif. Alors, l'ordre de G divise 24 et est divisble par 4. Donc $|G| = 24, 12, 8$ ou 4.

Si $|G| = 24$, $G = S_4$. Si $|G| = 12$, alors $G = A_4$. Si $|G| = 8$, alors $G \cap V$ est d'ordre $1, 2$ ou 4. Or $G/G \cap V$ est un sous-groupe de $S_4/V \simeq S_3$. Donc $G/G \cap V$ est d'ordre qui divise 6.

Donc $G \cap V$ est d'ordre 4 et $G \cap V = V \Rightarrow V \subseteq G$.

Comme G est d'ordre 8, G n'est pas contenu dans A_4. Soit $g \in G \setminus A_4$. Alors g est soit un $4-$cycle soit une transposition. De plus, comme $g \notin V$ et comme G est d'ordre 8, G est engendré par V et g.

Si g est un $4-$cycle, par exemple $g = (1234)$, alors $(13) = (1234)^{-1} \underbrace{(12)(34)}_{\in V} \in G$ et $G = \langle (1234), (13) \rangle \simeq D_8$.

Rappelons que D_8 est le groupe des isométries du carré.

Si g est une transposition, par exemple (13), alors $(1234) = (13)(12)(34) \in G$ et $G = \langle (1234), (13) \rangle \simeq D_8$.

Si G est d'ordre 4, alors $G \cap V$ est pour les mêmes raisons que ci-dessus d'ordre 2 ou 4. Si $|G \cap V| = 4$, alors $V \subseteq G \Rightarrow G = V$.

Si $|G \cap V| = 2$, soit $g \in G \setminus V$. On a g d'ordre 2 ou 4. Si g est d'ordre 4, c'est un $4-$cycle et $G = \langle g \rangle \simeq \mathbb{Z}/4\mathbb{Z}$.

Si g est d'odre 2, g est une transposition. Supposons par exemple que $(12)(34)$ est l'élément non trivial de $G \cap V$. on a $1 \neq g(12)(34)g^{-1} \in G \cap V \Rightarrow g(12)(34)g^{-1} = (12)(34) \Rightarrow g = (12)$ ou (34). Mais alors $G = \{1, (12)(34), (12), (34)\}$ qui n'est pas transitif !

Soit $X^4 + pX^2 + qX + r \in k[X]$ un polynôme irréductible sur k. On note x_1, x_2, x_3, x_4 ses racines (dans un corps de décomposition) que l'on suppose deux à deux distinctes.

On pose $\theta_1 := (x_1 + x_2)(x_3 + x_4), \theta_2 := (x_2 + x_3)(x_1 + x_4), \theta_3 := (x_3 + x_1)(x_2 + x_4)$.

On a :

$$\theta_1 + \theta + \theta_3 = 2x_1x_2 + 2x_1x_3 + ... = 2p \ .$$

$$\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 = x_1^2x_2^2 + x_1^2x_3^2 + ...$$

$$+3x_1^2x_2x_3 + 3x_1x_2^2x_3 + 3x_1x_2x_3^2 + 3x_1^2x_2x_4 + ...$$

$$+6x_1x_2x_3x_4$$

$$= p^2 - 4r \ .$$

$$\theta_1\theta_2\theta_3 = -(x_1 + x_2)^2(x_1 + x_3)^2(x_1 + x_4)^2$$

$$= -(x_1^3 + x_1^2(x_2+x_3+x_4) + x_1(x_2x_3+x_2x_4+x_3x_4) + x_2x_3x_4)^2$$
$$= -(x_1^3 - x_1^3 + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)^2$$
$$= -q^2 \ .$$

On a donc :

$$R(X) := (X-\theta_1)(X-\theta_2)(X-\theta_3) = X^3 - 2pX^2 + (p^2-4r)X + q^2 \ .$$

On a :

$$\theta_1-\theta_2 = (x_3-x_1)(x_2-x_4), \theta_2-\theta_3 = (x_1-x_2)(x_3-x_4), \theta_3-\theta_1 = (x_2-x_3)(x_1-x_4)$$

donc :

$$\Delta_P = \prod_{1\le i<j\le 4}(x_i-x_j)^2 = (\theta_1-\theta_2)^2(\theta_2-\theta_3)^2(\theta_1-\theta_3)^2$$
$$= \Delta_R \neq 0 \ .$$

Soit $L := k(x_1,x_2,x_3,x_4)$. On a $k(\theta_1,\theta_2,\theta_3) \subseteq L^{G\cap V}$. Soit $M := k(\theta_1,\theta_2,\theta_3)$. Si $g \in \mathrm{Gal}(L/M)$, alors :

$$^\forall i = 1,2,3 \ , \ g(\theta_i) = \theta_i$$

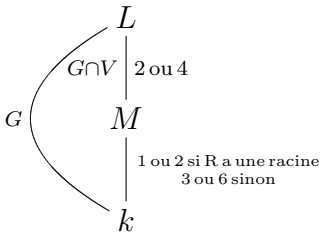
Soit $H := \langle V, (12)\rangle$. C'est un sous-groupe de S_4 d'ordre 8. On a de plus $S_4/H = \{H, (123)H, (132)H\}$. Or, pour tout $h \in H$, $h.\theta_1 = \theta_1$, $(123)h.\theta_1 = \theta_2$, $(132)h.\theta_1 = \theta_3$. Donc $gH = H$ *i.e.* $g \in H$. Or $H/V = \{V, (12)V\}$. Comme pour tout $v \in V$, $(12)v\theta_2 = \theta_3$, on a forcément $gV = V$ *i.e.* $g \in V$.

Donc $\mathrm{Gal}(L/M) \subseteq V$ et $\mathrm{Gal}(L/M) \subseteq G \cap V$. Mais alors :

$$M = L^{\mathrm{Gal}(L/M)} \supseteq L^{G\cap V}$$

et finalement, $M = L^{G\cap V}$.

On a le diagramme suivant avec à gauche les groupes de Galois et à droite les degrés des extensions :



Si $P(X)$ est irréductible (et séparable), alors G est un sous-groupe transitif de S_4 donc $G = S_4, A_4, V$ ou $G \simeq D_8$ ou $\mathbb{Z}/4\mathbb{Z}$. Si $R(X)$ est irréductible sur k, alors θ_1 est de degré 3 sur k. Donc $[M : k]$ est divisible par 3. Donc $[L : k] = |G|$ est dividible par 3 donc $G = S_4$ ou A_4.

D'où les 2 premières lignes du tableau ci-dessous.

Si $R(X)$ est scindé sur k, alors $M = k(\theta_1, \theta_2, \theta_3) = k$ et $G = \mathrm{Gal}(L/M) = G \cap V \Rightarrow G = V$ cae G est d'ordre au moins 4. Dans ce cas forcément $\Delta \in k^2$ car $V \subseteq A_4$ d'ouù la troisième ligne du tableau.

Si $R(X)$ n'a qu'une seule racine dans k, par exemple $\theta_1 \in k$, alors $R(X) = (X - \theta_1)\underbrace{(X - \theta_2)(X - \theta_3)}_{\in k[X]}$. Donc $\theta_2 + \theta_3 \in k$ et $M = k(\theta_2, \theta_3) = k(\theta_2)$ est de degré 2 sur k.

Le corps L est aussi le corps de décomposition de Lsur M. Si $P(X)$ est irréductible sur M, alors le groupe $G \cap V = \mathrm{Gal}(L/M)$ agit transitivement sur les racines x_1, x_2, x_3, x_4 de P. Donc $G \cap V$ est d'ordre 4 et G est d'ordre 8.

Si $P(X)$ est réductible sur M, alors $G \cap V = \mathrm{Gal}(L/M)$ n'est pas un sous-groupe transitif de S_4 donc $G \cap V \underset{\neq}{\subset} V$ et $|G \cap V| = 2 \Rightarrow G \simeq \mathbb{Z}/4\mathbb{Z}$.

On a ainsi les deux dernières lignes du tableau.

$\Delta \notin k^2$	$R(X)$ irréductible sur k		$G = S_4$
$\Delta \in k^2$	$R(X)$ irréductible sur k		$G = A_4$
$\Delta \in k^2$	$R(X)$ scindé sur k		$G = V$
$\Delta \notin k^2$	$R(X)$ a une racine dans k	$P(X)$irréductible sur M	$G \simeq D_8$
$\Delta \notin k^2$	$R(X)$ a une racine dans k	$P(X)$réductible sur M	$G \simeq \mathbb{Z}/4\mathbb{Z}$

Applications : si $P(X) = X^4 + bX^2 + d \in k[X]$. Les racines d'un tel polynôme sont de la forme $\pm\alpha, \pm\beta$ où α et β sont les deux racines de $T^2 + bT + d$. Donc les factorisations possibles en deux polynômes de degré 2 sont :

$$P(X) = (X^2 - \alpha^2)(X^2 - \beta^2)$$

$$P(X) = (X^2 - (\alpha + \beta)X + \alpha\beta)(X^2 + (\alpha + \beta)X + \alpha\beta)$$
$$P(X) = (X^2 - (\alpha - \beta)X - \alpha\beta)(X^2 + (\alpha - \beta)X - \alpha\beta) \ .$$

Donc

$$\Big(\alpha^2 \notin k \text{ et } \alpha \pm \beta \notin k\Big)$$
$$\Rightarrow P(X)\text{irréductible sur } k \ .$$

La réciproque est vraie car $2\alpha\beta = (\alpha+\beta)^2 - \alpha^2 - \beta^2 = (\alpha+\beta)^2 + b$.
Or, $\alpha^2 \in k \Leftrightarrow b^2 - 4d \in k^2$ et $(\alpha \pm \beta)^2 = -b \pm 2\sqrt{d}$. Donc

$$P(X)\text{irréductible sur } k \ .$$

$$\Leftrightarrow b^2 - 4d \notin k^2, -b \pm 2\sqrt{d} \notin k^2 \ .$$

On a $R(X) = X^3 - 2bX^2 + (b^2-4d)X = X(X^2 - 2bX + (b^2-4d))$. Donc si $P(X)$ est irréductible sur k (et séparable), alors le groupe de Galois G de P sur k est V ou isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou D_8. C'est V si et seulement si le discriminant de P est un carré dans k.

Or $\Delta_P = \Delta_R = 16(b^2-4d)^2 d$. Donc $G = V \Leftrightarrow d \in k^2$. Si $d \notin k^2$, alors $G = \mathbb{Z}/4\mathbb{Z} \Leftrightarrow P(X)$ est réductible sur $M = k(\sqrt{d}) \Leftrightarrow b^2 - 4d, -b + 2\sqrt{d}$ ou $-b - 2\sqrt{d} \in k(\sqrt{d})^2$. Or, $-b \pm 2\sqrt{d} = (x + y\sqrt{d})^2$ avec $x, y \in k \Leftrightarrow$:

$$x^2 + dy^2 = -b \text{ et } xy = \pm 1$$

$$\Rightarrow b^2 - 4d = (x^2 - dy^2)^2 \in k^2$$

ce qui est impossible si $P(X)$ est irréductible sur k. Donc $G \simeq \mathbb{Z}/4\mathbb{Z} \Leftrightarrow b^2 - 4d \in k(\sqrt{d})^2$.

Or, $b^2 - 4d = (x + y\sqrt{d})^2$ avec $x, y \in k \Leftrightarrow$:

$$b^2 - 4d = x^2 + dy^2 \text{ et } xy = 0$$

$$\Leftrightarrow b^2/d - 4 \in k^2$$

car $b^2 - 4d \notin k^2$.