Feuille de TD n° 12
Groupe de Galois des quartiques
Réponses

Exercice.
On note V le sous-groupe $\{1, (12)(34), (13)(24), (14)(23)\}$ de S_4.

a) Montrer que V est distingué dans S_4 et que $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
$\forall \sigma \in \mathfrak{S}_4$, $\sigma(12)(34)\sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$

b) Soit G un sous-groupe transitif de S_4. Montrer que G est

$$S_4, A_4, V \text{ ou un sous-groupe conjugué à } \langle (1234) \rangle \text{ ou } D$$

(on note $D := \{1, (1234)^{\pm 1}, (13)(24), (24), (12)(34), (13), (14)(23)\} \simeq D_4$ le groupe diédral d'ordre 8 (c'est le groupe des isométries du carré)).
Comme G agit transitivement sur l'ensemble $\{1, 2, 3, 4\}$, $4||G|$. Donc $|G| = 4, 8, 12,$ ou 24.
Si $|G| = 24$, alors $G = \mathfrak{S}_4$. Si $|G| = 12$, alors $G = \mathfrak{a}_4$, seul sous-groupe d'indice 2 de $\mathfrak{S}_4$. Si $|G| = 8$, alors G est conjugué à D, $2-$Sylow de $\mathfrak{S}_4$. si $|G| = 4$ alors ou bien G contient un $4-$cycle et G est conjugué à $\langle (1234) \rangle$ ou bien G n'a pas de $4-$cycles et alors G contient des transpositions ou des doubles transpositions. Si $G \neq V$, alors G contient une transposition par exemple (12). Comme G est d'ordre 4, G contient une autre transposition qui commute avec (12). C'est forcément (34). Donc $G = \langle (12), (34) \rangle$ Mai ce n'est pas un sous-groupe transitif ! (aucun élément n'envoie 1 sur 3 par exemple). Donc $G = V$.

c) Soit $P(X) = X^4 + pX^2 + qX + r$ un polynôme irréductible à coefficients dans un corps k de caractéristique $\neq 2, 3$. Vérifier que $P(X)$ a 4 racines distinctes, x_1, x_2, x_3, x_4 dans son corps de décomposition L.
Comme k est de caractéristique différente de 2, $P' \neq 0$ Donc $P \wedge P' = 1$ (car le pgcd est de degré $< \deg P$ et divise P qui est irréductible. Donc P et P' n'ont pas de racines communes et les racines de P sont simples.

d) On pose

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

Montrer que $R(X) = (X-\theta_1)(X-\theta_2)(X-\theta_3) = X^3 - 2pX^2 + (p^2-4r)X + q^2$.
On a : $P = (X - x_1)(X - x_2)(X - x_3)(X - x_4) \Rightarrow x_1 + x_2 + x_3 + x_4 = 0$. Donc $\theta_1 = -(x_1 + x_2)^2$, $\theta_2 = -(x_1 + x_4)^2$, $\theta_3 = -(x_1 + x_3)^2$. Donc $R(X) = X^3 - (\theta_1 + \theta_2 + \theta_3)X^2 + (\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3)X - \theta_1\theta_2\theta_3$.
Or,

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

$$= -(x_1^2 + x_2^2 + x_3^2 + x_4^2) = -(x_1 + x_2 + x_3 + x_4)^2 + 2(x_1x_2 + x_1x_3 + \ldots) = 2p$$

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

$$= ((x_1 + x_2)(x_1 + x_4))^2 + ((x_1 + x_2)(x_1 + x_3))^2 + ((x_1 + x_4)(x_1 + x_3))^2$$

$$= (x_1(x_1 + x_2 + x_4) + x_2x_4)^2 + \ldots$$

$$= (x_1(-x_3)+x_2x_4)^2+... = (x_1x_3-x_2x_4)^2+(x_1x_4-x_2x_3)^2+(x_1x_2-x_3x_4)^2$$

$$= (x_1x_2)^2 + (x_1x_3)^2 + (x_1x_4)^2 + (x_2x_3)^2 + (x_2x_4)^2 + (x_3x_4)^2 - 6x_1x_2x_3x_4$$

$$= p^2 - 2x_1^2x_2x_3 - 2x_1^2x_2x_4 - 2x_1x_2^2x_3 - ... - 6x_1x_2x_3x_4 - 6x_1x_2x_3x_4$$

$$= p^2-2x_1x_2x_3(x_1+x_2+x_3)-2x_1x_2x_4(x_1+x_2+x_4)-2x_1x_3x_4(x_1+x_3+x_4)-2x_2x_3x_4(x_2+x_3+x_4)$$

$$-12r$$

$$= p^2 + 8x_1x_2x_3x_4 - 12r = p^2 + 4r$$

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

$$= -\frac{((x_1 + x_1)(x_1 + x_2)(x_1 + x_3)(x_1 + x_4))^2}{4x_1^2}$$

$$= -\frac{((-x_1 - x_1)(-x_1 - x_2)(-x_1 - x_3)(-x_1 - x_4))^2}{4x_1^2}$$

$$= -\frac{P(-x_1)^2}{4x_1^2} = -\frac{(x_1^4 + px_1^2 - qx_1 + r)^2}{4x_1^2}$$

$$= -\frac{(-qx_1 - r - qx_1 + r)^2}{4x_1^2}$$

$$= -q^2 \ .$$

e) Montrer que $\theta_1 - \theta_2 = (x_3 - x_1)(x_2 - x_4)$. En déduire que $R(X)$ et $P(X)$ ont le même discriminant Δ.

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

Or,

$$\Delta_R = (\theta_1 - \theta_2)^2(\theta_1 - \theta_3)^2(\theta_2 - \theta_3)^2$$

$$= (x_1 - x_3)^2(x_2 - x_4)^2(x_1 - x_4)^2(x_2 - x_3)^2(x_1 - x_2)^2(x_3 - x_4)^2 = \Delta_P \ .$$

f) Soit G le groupe de Galois de L sur k. On note $G_1 = G \cap V$. Montrer que

$$L^{G\cap V} = k(\theta_1, \theta_2, \theta_3)$$

le corps de décomposition de $R(X)$ sur k. On pose $M = k(\theta_1, \theta_2, \theta_3)$.

Il est clair que $\theta_1, \theta_2, \theta_3$ sont invariants par les permutations de V donc $M = k(\theta_1, \theta_2, \theta_3) \leq L^{G\cap V}$. En particulier, $[L : M] \geq |G \cap V|$ (*).Soit $H = \mathrm{Gal}(L/M)$. Alors $M = L^H$ et $[L : M] = |H|$. Or si $\sigma \in H$, $\sigma \in V$. En effet, si σ était une transposition, par exemple (12), alors $\sigma(\theta_2) = \theta_3 \neq \theta_2$ absurde ! Si σ était un $3-$cycle, par exemple (123), alors $\sigma(\theta_1) = \theta_2 \neq \theta_1$ absurde ! Si σ était un $4-$cycle, par exemple (1234), alors $\sigma(\theta_1) = \theta_2 \neq \theta_1$ absurde ! Donc $H \leq G \cap V \Rightarrow [L : M] \leq |G \cap V|$. don c d'après (*), $[L : M] = |G \cap V| = [L : L^{G\cap V}] \Rightarrow M = L^{G\cap V}$.

g) Montrer que le tableau suivant décrit bien toutes les possibilités pour le groupe de Galois du polynôme $P(X)$ sur k :

$\Delta \notin k^2$	$R(X)$ 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	$G \cong D_4$
$\Delta \notin k^2$	$R(X)$ a une racine dans k	$P(X)$réductible sur M	$G \cong \mathbb{Z}/4\mathbb{Z}$

Justifions les cases de ce tableau ligne par ligne en lisant de droite à gauche.
Si $G = \mathfrak{S}_4$, alors $\Delta \notin k^2$ car $G \not\leq \mathfrak{a}_4$. Comme $G \cap V = V$, $[M : k] = |G/G \cap V| = 6$. Or M est le corps de décomposition du polynôme R sur k. Comme R est de degré 3, les θ_i sont de degrés 1, 2 ou 3 sur k. Donc au moins une des racines θ_i de R est de degré 3. Donc R est son polynôme minimal et est irréductible sur k.
Si $G = \mathfrak{a}_4$, alors $\Delta \in k^2$. Comme Comme $G \cap V = V$, $[M : k] = |G/G \cap V| = 3$. Donc comme ci-dessus, une des racines θ_i est de degré 3 sur k. Donc R est irréductible sur k.
Si $G = V$, alors $G = V \leq \mathfrak{a}_4$ donc $\Delta \in k^2$. Comme $[M : k] = |G/G \cap V| = 1$, $M = k$ et les $\theta_i \in K$. donc R est scindé dans k.
Si G est conjugué à D, alors $V \leq G$. Donc $[M : k] = |G/V| = \frac{8}{4} = 2$. Donc R n'est pas irréductible sur k (sinon θ_1 serait de degré 3 sur k). Donc R a une racine dans k. Comme $D \not\leq \mathfrak{a}_4$, on a $\notin k^2$. Le goupe de Galois du polynôme P sur M est $G \cap V = V$ qui agit transitivement sur les racines x_1, x_2, x_3, x_4 de P. Donc P est irréductible sur M.
Si G est engendré par un $4-$cycle, alors $G \not\leq \mathfrak{a}_4$ donc $\Delta \notin k^2$. On a $G \cap V$ d'ordre 2 donc $[M : k] = 2$. Comme précédemment, aucun des θ_i n'est de degré 3 sur k donc R n'est pas irréductible sur k et donc a au moins une racine dans k. Le groupe de Galois de P sur M est $G \cap V$ d'ordre 2 et donc ne peut agir transitivement sur l'ensemble des 4 racines de P. Donc P n'est pas irréductible sur M.

h) *Applications :* Montrer que si le polynôme $X^4 + bX^2 + d$ est irréductible sur k, alors son groupe de Galois est V si d est un carré dans k, $\mathbb{Z}/4\mathbb{Z}$ si $d \notin k^2$ et $\frac{b^2}{d} - 4 \in k^2$ et D_4 sinon.
Déterminer les groupes de Galois sur $\mathbb{Q}$ des polynômes $X^4 - X - 1$ et $X^4 + 8X + 12$.
Le polynôme $X^4 - X - 1$ est irréductible sur $\mathbb{F}_2$ donc sur $\mathbb{Q}$. De plus dans ce cas, $R = X^3 + 4X + 1$, donc $\Delta = \Delta_R = -4(16^3) - 27 = -283 \notin \mathbb{Q}^2$. LE polynôme R est irréductible sur $\mathbb{Q}$ (car ± 1 ne sont pas racines). Donc

$$\mathrm{Gal}_{\mathbb{Q}}(X^4 - X - 1) = \mathfrak{S}_4$$

d'après le tableau ci-dessus.
Soit $P(X) = X^4 + 8X + 12$. On a $P(X - 1) = X^4 - 4X^3 + 6X^2 + 4X - 19$. Si $P(X - 1) = P_1 P_2$ avec $P_1, P_2 \in \mathbb{Q}[X]$ unitaires de degrés > 0, alors $P_1, P_2 \in \mathbb{Z}[X]$. Donc si on note $a_1, ..., a_r$ les racines de P_1, $a_{r+1}, ..., a_4$ les

racines de P_2, on a $|a_1...a_r||a_{r+1}...a_4| = 19$. Ce sont des entiers donc un des facteurs est 1 l'autre 19. Si par exemple $|a_1...a_r| = 1$, alors au moins un des $|a_i| \leq 1$. Mais on aurait : $a_i^4 - 4a_i^3 + 6a_i^2 + 4a_i = 19$. C'est absurde car :

$$|a_i^4 - 4a_i^3 + 6a_i^2 + 4a_i| \leq |a_i|^4 + 4|a_i|^3 + 6|a_i|^2 + 4|a_i| \leq 1 + 4 + 6 + 4 = 15 < 19\,.$$

Donc $P(X-1)$ est irréductible sur $\mathbb{Q}$. Donc P aussi.
On a $R(X) = X^3 - 48X + 64$. C'est irréductible $\mod 5$ (pas de racines) donc sur $\mathbb{Q}$. De plus $\Delta = \Delta_R = -4(-48)^3 - 27.(64)^2 = 2^{14}.3^3 - 3^3 2^{12} = (2^{14} - 2^{12}).3^3 = 2^{12}.3^4 \in \mathbb{Q}^2$.
Donc

$$\mathrm{Gal}_{\mathbb{Q}}(X^4 + 8X + 12) = \mathfrak{a}_4$$

d'après le tableau ci-dessus.