Fiche 5
12 mars 2014

Exercice 1 (Manque de séparabilité).
On fixe un nombre premier p, un corps k de caractéristique p et deux indéterminées X, Y sur k. En d'autres termes, X et Y sont algébriquement indépendants sur k. On définit $E = k(X, Y)$ et $K = k(X^p, Y^p)$.

1. Montrer que $X \notin K$ et $Y \notin K(X) = K[X]$.
2. Déduire de 1 que $T^p - X^p$ est irréductible dans $K[T]$ et que $T^p - Y^p$ est irréductible dans $K(X)[T]$. Conclure que $[E : K] = p^2$.
3. Montrer que si $\alpha \in E$ alors $[K(\alpha) : K] \leq p$. En déduire que l'extension E/K ne contient pas d'élément primitif.
4. Déduire du point précédent et de la preuve du théorème primitif pour les corps infinis que pour tous $t_1, t_2 \in K$, $K(X + t_1Y) = K(X + t_2Y)$ si et seulement si $t_1 = t_2$. (*L'extension E/K a donc une infinité de sous-extensions, et en particulier, elle n'est pas galoisienne. En effet, E/K n'est pas une extension séparable.*)

Exercice 2 (Eléments primitifs).
Déterminer le corps de décomposition L sur $\mathbb{Q}$ de $X^5 - 2$. Déterminer un élément primitif pour $L/\mathbb{Q}$.

Exercice 3 (Bases normales).
Vérifiez les assertions $(a), (b), (c)$ et (d) sur la page 23 des notes de cours.

Exercice 4 (Résolvantes).
Soit $f(X_1, ..., X_n) \in \mathbb{Z}[X_1, ..., X_n]$. Soit G un sous-groupe de S_n. On note H le sous-groupe des $\sigma \in G$ tels que $f^\sigma = f$.

On suppose que $P(X)$ est un polynôme séparable de degré n sur un corps k. On note L/k un corps de décomposition de P sur k et $x_1, ..., x_n$ ses racines dans L. On définit :

$$R_G(f, P) = \prod_{\sigma H \in G/H} (X - f(x_{\sigma(1)}, ..., x_{\sigma(n)})) \in L[X] \quad .$$

(a) Montrer que si $\mathrm{Gal}(L/k) \subseteq G$, alors $R_G(f, P) \in k[X]$.
(b) Montrer que si de plus, $R_G(f, P)$ a une racine simple dans k, alors $\mathrm{Gal}(L/k)$ est conjugué à un sous-groupe de H.

Exercice 5 (Groupe de Galois des quartiques).
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 $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(b) Soit G un sous-groupe transitif de S_4. Montrer que G est

$$S_4, A_4, V \text{ ou un sous-groupe isomorphe à } \mathbb{Z}/4\mathbb{Z} \text{ ou } D_8$$

(on note D_8 le groupe diédral d'ordre 8 (c'est le groupe des isométries du carré)).
(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.
(d) On pose $f = (X_1 + X_2)(X_3 + X_4)$. On note $R(X) = R_{S_4}(f, P)$. Montrer que $R(X) = (X - \theta_1)(X - \theta_2)(X - \theta_3)$ où :

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

(e) Montrer que $R(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$.
(f) 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.
(g) 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 $M = k(\theta_1, \theta_2, \theta_3)$.
(h) 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	$G \cong D_8$
$\Delta \notin k^2$	$R(X)$ a une racine dans k	$P(X)$réductible sur M	$G \cong \mathbb{Z}/4\mathbb{Z}$

(i) *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_8 sinon.
Déterminer les groupes de Galois sur $\mathbb{Q}$ des polynômes $X^4 - X - 1$ et $X^4 + 8X + 12$.