ENS Lyon 2013 - 2014
Master 1 – Algèbre avancée Pour le 11.10.2013

Devoir à la maison 2

La rédaction et la clarté des arguments employés seront pris en compte dans l'évaluation de la copie.

Groupes de Galois et relations algébriques

Soit K un corps. Dans tout le problème, on se donne un polynôme $P \in K[T]$ unitaire, irréductible, séparable, de degré $n \geq 1$.

Soit L un corps de décomposition de P sur K. On note $x_1, \ldots, x_n$ les racines de P dans L. Par définition, une *relation algébrique entre les racines de* P est un polynôme $R \in K[X_1, \ldots, X_n]$ tel que $R(x_1, \ldots, x_n) = 0$. On note I_P l'ensemble des relations algébriques entre les racines de P.

1. Montrer que I_P est un idéal de $K[X_1, \ldots, X_n]$ et montrer l'existence d'un isomorphisme de K-algèbres entre $K[X_1, \ldots, X_n]/I_P$ et L.

On munit $K[X_1, \ldots, X_n]$ d'une action du groupe symétrique $\mathfrak{S}_n$ en posant

$$\sigma \cdot P(X_1, \ldots, X_n) = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) \qquad (\sigma \in \mathfrak{S}_n).$$

Soit G_P l'ensemble des permutations $\sigma \in \mathfrak{S}_n$ telles que $\sigma \cdot I_P \subset I_P$.

2. Montrer que G_P est un sous-groupe de $\mathfrak{S}_n$ isomorphe à $\mathrm{Gal}(L/K)$.

On cherche maintenant des générateurs de l'idéal I_P.
On pose $K_0 = K$ et $K_i = K(x_1, \ldots, x_i)$ pour tout $i \in \{1, \ldots, n\}$. On note $\mu_i \in K_{i-1}[T]$ le polynôme minimal de x_i sur K_{i-1}, et on pose $d_i = \deg(\mu_i)$.

3. Montrer que pour tout $i \in \{1, \ldots, n\}$, il existe un unique polynôme $R_i \in K[X_1, \ldots, X_i]$ vérifiant les propriétés suivantes :
   (a) R_i est unitaire de degré d_i en X_i ;
   (b) Pour tout $1 \leq j \leq i-1$, on a $\deg_{X_j}(R_i) \leq d_j - 1$;
   (c) $R_i(x_1, \ldots, x_{i-1}, T) = \mu_i(T)$.
4. Montrer que $I_P = (R_1, \ldots, R_n)$.
   On pourra montrer par récurrence sur i que l'on a un isomorphisme de K-algèbres

$$\phi_i : K[X_1, \ldots, X_i]/(R_1, \ldots, R_i) \xrightarrow{\sim} K_i.$$

5. Calculer explicitement des générateurs de I_P dans les cas suivants :
   (a) $K = \mathbf{F}_2$ et $P = X^3 + X + 1$;
   (b) $K = \mathbf{Q}$ et $P = X^3 - 2$;
   (c) $K = \mathbf{Q}$ et $P = X^4 - 2X^2 + 2$.
   Dans le cas (c), le groupe de Galois de P est d'ordre 8.

On cherche maintenant à établir une formule explicite générale pour les polynômes R_i.
On pose $G = \mathrm{Gal}(L/K) = \{\sigma_1, \ldots, \sigma_N\}$. Pour tout $y \in L$, on définit le vecteur

$$Gy := (\sigma_1(y), \ldots, \sigma_N(y)) \in L^N.$$

6. Soient $y_1, \ldots, y_r \in L$. Montrer que les conditions suivantes sont équivalentes :
   (a) $y_1, \ldots, y_r$ sont K-linéairement indépendants dans L ;
   (b) $Gy_1, \ldots, Gy_r$ sont L-linéairement indépendants dans L^N.
   On pourra s'inspirer de la démonstration du théorème d'Artin.

Dans la suite, on fixe un entier $i \in \{1, \dots, n\}$.

7. Montrer que R_i est l'unique polynôme de $L[X_1, \dots, X_i]$ qui vérifie (3a), (3b) et qui s'annule en $(\sigma(x_1), \dots, \sigma(x_i))$ pour tout $\sigma \in G$.

L'extension L/K_i est galoisienne ; on note $G_i = \mathrm{Gal}(L/K_i)$ son groupe de Galois, qui est un sous-groupe de G.

8. Montrer que pour $\sigma \in G$ et $1 \leq j \leq i$, l'élément $\sigma(x_j)$ ne dépend que de la classe de σ dans l'ensemble quotient (à droite) G/G_i.

Pour tout $\sigma \in G$, on définit l'ensemble

$$C_{\sigma,i} = \{\tau(x_i) : \tau \in G \text{ et } \tau|_{K_{i-1}} = \sigma|_{K_{i-1}}\} \backslash \{\sigma(x_i)\}.$$

9. Montrer que $C_{\sigma,i}$ ne dépend que de la classe de σ dans G/G_i. Quel est le cardinal de $C_{\sigma,i}$?
10. Montrer la formule d'interpolation

$$R_i = X_i^{d_i} - \sum_{[\sigma] \in G/G_i} \sigma(x_i)^{d_i} \Big(\prod_{y_1 \in C_{\sigma,1}} \frac{X_1 - y_1}{\sigma(x_1) - y_1} \Big) \cdots \Big(\prod_{y_i \in C_{\sigma,i}} \frac{X_i - y_i}{\sigma(x_i) - y_i} \Big).$$

Pour en savoir plus...

Les résultats de ce problème sont tirés de l'article suivant : M. Lederer, *Explicit constructions in splitting fields of polynomials*. Riv. Mat. Univ. Parma (7) 3* (2004), pp. 233-244.

Note historique. La définition du groupe de Galois du polynôme P au moyen du groupe G_P est proche de la définition originelle de Galois, que l'on trouvera ci-dessous :

PROPOSITION I.

Théorème. « Soit une équation donnée, dont a, b, c, ... sont les » m racines. Il y aura toujours un groupe de permutations des lettres » a, b, c,... qui jouira de la propriété suivante :
» 1°. Que toute fonction des racines, invariable [*] par les substi- » tutions de ce groupe, soit rationnellement connue ;
» 2°. Réciproquement, que toute fonction des racines, déterminable » rationnellement, soit invariable par les substitutions. »