Examen 2ème Session 2020/2021
4M002 - Algèbre et théorie de Galois
Anna Cadoret

## Avertissement.

Sont autorisés: le polycopié du cours, les notes manuscrites du cours, les dictionnaires de langues papier. Sont interdits les corrigés polycopiés et manuscrits des travaux dirigés. Les réponses peuvent être rédigées en français ou en anglais.

Tous les anneaux considérés sont commutatifs, associatifs, unitaires.

**Exercice.** Soit $p$ un nombre premier. On note $\mathcal{S}_p$ le groupe des permutations de $\{1, \ldots, p\}$.

(1) (a) Soit $c \in \mathcal{S}_p$ un $p$-cycle et $\tau \in \mathcal{S}_p$ une transposition. Montrer que le groupe $\mathcal{S}_p$ est engendré par $c$ et $\tau$.

(b) Montrer que les seuls éléments d'ordre $p$ de $\mathcal{S}_p$ sont les $p$-cycles.

(2) Soit $P(T) \in \mathbb{Q}[T]$ irréductible de degré $p$ ayant exactement deux racines non réelles. On note $K/\mathbb{Q}$ le corps de décomposition de $P$ sur $\mathbb{Q}$.

(a) Rappeler pourquoi $K/\mathbb{Q}$ est galoisienne; on note $G := Gal(K|\mathbb{Q})$ son groupe de Galois.

(b) Montrer que $G$ est un sous-groupe de $\mathcal{S}_p$ qui agit transitivement sur $\{1, \ldots, p\}$.

(c) En déduire que $p||G|$ puis que $G$ contient un $p$-cycle.

(d) Montrer que $G$ contient une transposition et en déduire que $G = \mathcal{S}_p$.

(3) Calculer le groupe de Galois du corps de décomposition de $P(T) = T^5 - 6T + 3$ sur $\mathbb{Q}$.

**Problème.** Soit $\phi : A \to B$ un morphisme d'anneaux (qui munit donc $B$ d'une structure de $A$-algèbre donc de $A$-module) et $M$ un $B$-module. Une $A$-dérivation $d : B \to M$ est un morphisme de $A$-modules tel que

(i) (les éléments de $A$ sont constants) $\phi(A) \subset \ker(d)$;
(ii) (Règle de Leibnitz) $d(bb') = bdb' + b'db,\ b, b' \in A$.

On note $Der_A(B, M)$ l'ensemble des $A$-dérivations $d : B \to M$.

(1) Montrer que $Der_A(B, M)$ est naturellement muni d'une structure de $B$-module, que l'on explicitera.

(2) On note $F := \oplus_{b \in B} Bdb$ le $B$-module libre de base indexée par les éléments de $B$ et $R \subset F$ le sous-$B$-module engendré par les éléments de la forme $d(bb') - bdb' - b'db$, $d(b + b') - db - db'$, $b, b' \in B$ et $da$, $a \in A$. Soit $d_{B|A} : B \to F/R =: \Omega^1_{B|A}$ la composée de l'application $B \hookrightarrow F$, $b \mapsto db$ et de la projection canonique $F \twoheadrightarrow \Omega^1_{B|A}$.

(a) Vérifier que $d_{B|A} : B \to F/R =: \Omega^1_{B|A}$ est une $A$-dérivation.

(b) Montrer que $d_{B|A} : B \to \Omega^1_{B|A}$ a la propriété universelle suivante: pour tout $B$-module $M$ et $A$-dérivation $\delta : B \to M$, il existe un unique morphisme de $B$-modules $\phi : \Omega^1_{B|A} \to M$ tel que

$$\begin{tikzcd} B \arrow[r, "d_{B|A}"] \arrow[d, "\delta"'] & \Omega^1_{B|A} \arrow[dl, dotted, "\exists!\phi"] \\ M & \end{tikzcd}$$

Autrement dit, on a un isomorphisme canonique de $B$-modules $-\circ d_{B|A} : Hom_B(\Omega^1_{B|A}, M) \tilde{\to} Der_A(B, M)$.

**Rem.** On notera que $\Omega^1_{B|A}$ est engendré, comme $B$-module, par les $db$, $b \in B$.

(3) On suppose que $B = A[\underline{T}] := A[T_1, \ldots, T_r]$ est la $A$-algèbre des polynômes à $r$ indéterminées sur $A$. Montrer que si $\delta : A[\underline{T}] \to M$ est une $A$-dérivation alors

$$(*)\ \ \delta P = \sum_{1 \leq i \leq r} \frac{\partial P}{\partial T_i} dT_i.$$

En déduire que $\Omega^1_{A[\underline{T}]|A} \tilde{\to} \oplus_{1 \leq i \leq r} A[\underline{T}]\delta T_i$.

(4) Soit $\psi : B \to C$ un morphisme de $A$-algèbre.

(a) En utilisant les propriétés universelles de $\otimes$, $d_{B|A} : B \to \Omega^1_{B|A}$ etc. construire des morphismes canoniques de $C$-modules

$$g : \Omega^1_{B|A} \otimes_B C \to \Omega^1_{C|A}, \ \ h : \Omega^1_{C|A} \to \Omega^1_{C|B}$$

que l'on explicitera.

(b) Montrer que la suite de $C$-modules

$$\Omega^1_{B|A} \otimes_B C \xrightarrow{g} \Omega^1_{C|A} \xrightarrow{h} \Omega^1_{C|B} \to 0$$

est exacte.

(c) Supposons que $\psi : B \twoheadrightarrow C$ est surjective; on note $I := \ker(\psi) \subset B$ son noyau, qui est un idéal de $B$ de sorte que $\psi : B \twoheadrightarrow C$ s'identifie au morphisme quotient $p_I : B \twoheadrightarrow B/I$.

(i) Montrer que $\Omega^1_{C|B} = 0$;

(ii) Vérifier que $I/I^2$ est muni d'une structure de $C(= B/I)$-module et montrer qu'il existe un morphisme canonique de $C$-modules $f : I/I^2 \to \Omega^1_{B|A} \otimes_B C$ que l'on explicitera.

(iii) Montrer que la suite de $C$-modules

$$I/I^2 \xrightarrow{f} \Omega^1_{B|A} \otimes_B C \xrightarrow{g} \Omega^1_{C|A} \to 0$$

est exacte.

(5) Revenons à la situation de (3). Fixons $P \in A[\underline{T}] \setminus A$ et notons $\psi : A[\underline{T}] \twoheadrightarrow C := A[\underline{T}]/PA[\underline{T}]$ l'anneau quotient. Montrer que

$$\Omega^1_{C|A} \tilde{\to} (\oplus_{1 \leq i \leq r} C dT_i)/C dP$$

(6) Soit $K/k$ une extension de corps finie.

(a) Montrer que $K/k$ admet une plus grande sous-extension $k \subset K^s \subset K$ telle que $K^s/k$ est séparable.

(b) Montrer que si $K/k$ n'est pas séparable, on peut toujours écrire $K = K_0(x)/K_0$ avec $k \subset K_0 \subset\neq K$ une sous-extension et $a \in K$ inséparable sur $K_0$.

(c) Montrer que si $K/k$ est séparable si et seulement si $\Omega^1_{K|k} = 0$.

*anna.cadoret@imj-prg.fr*
IMJ-PRG- Sorbonne Université.