Algèbre Commutative 2021/2022
D.M.

Exercice 1: L'objectif de cet exercice est de montrer que l'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais non euclidien.

(1) Soit A un anneau euclidien. Montrer qu'il existe un élément $a \in A$, $a \notin A^\times$ tel que l'application $p_{Aa} : A^\times \cup \{0\} \to A/Aa$ soit surjective.

Dans ce qui suit, on note $\alpha := \frac{1+i\sqrt{19}}{2}$ et $\overline{\alpha} := \frac{1-i\sqrt{19}}{2}$, $A := \mathbb{Z}[\alpha] \subset \mathbb{C}$.

(2) Montrer qu'on a un isomorphisme canonique d'anneaux $\mathbb{Z}[X]/X^2 - X + 5 \tilde{\to} A$;

(3) Montrer que $A/2A$ et $A/3A$ sont des corps;

(4) Déterminer $A^\times$ et en déduire que A n'est pas euclidien;

(5) Montrer que pour tout $0 \neq a, b \in A$ il existe $q, r \in A$ tels que $r = 0$ ou $|r| < |b|$ et soit $a = qb + r$ soit $2a = qb + r$;

(6) En déduire que A est principal.

(1) Soit $0 \neq a \in A \setminus A^\times$ et de stathme $\sigma(a) \geq 0$ minimal. Alors pour tout $b \in A$ il existe un $q, r \in A$ tel que $b = qa + r$ et $r = 0$ ou $\sigma(r) < \sigma(a)$. Mais par minimalité de $\sigma(a)$, si $r \neq 0$ on doit avoir $r \in A^\times$.

(2) Se traite exactement comme la question (1) de l'Exercice 7.

(3) D'après la question (2), $A/2A \tilde{\to} \mathbb{Z}[X]/((X^2-X+5)\mathbb{Z}[X]+2\mathbb{Z}[X]) \tilde{\to} \mathbb{F}_2[X]/X^2+X+1$ qui est bien un corps puisque X^2+X+1 est irréductible dans $\mathbb{F}_2[X]$ et que $\mathbb{F}_2[X]$ est principal. De même $A/3A \tilde{\to} \mathbb{F}_2[X]/X^2 - X - 1$ est un corps puisque $X^2 - X - 1$ est irréductible dans $\mathbb{F}_3[X]$.

(4) Le morphisme de monoïdes multiplicatifs $|-|^2 : (\mathbb{C}, \cdot) \to (\mathbb{N}, \cdot)$, $z \mapsto z\overline{z}$ induit par restriction un morphisme de monoïdes $N : (A, \cdot) \to (\mathbb{N}, \cdot)$. En particulier, pour tout $x = a + \alpha b \in A^\times$, $a^2 + ab + 5b^2 = N(x) = 1$, ce qui n'est possible que si $b = 0$ et $a = \pm 1$. Donc $A^\times = \{\pm 1\}$. D'après la question (1), si A était euclidien, il existerait $a \in A$, $a \notin A^\times$ tel que A/Aa soit de cardinal 2 ou 3. Dans le premier cas, A/Aa serait de caractéristique 2 donc $2A \subset Aa$ et $A/2A \twoheadrightarrow A/Aa$. Mais comme $A/2A$ est un corps, ses seuls idéaux sont 0 ou $A/2A$, ce qui impose $A/2A \tilde{\to} A/Aa$. Mais $A/2A \tilde{\to} \mathbb{F}_2[X]/X^2 + X + 1$ est de cardinal $4 > 2$. Dans le second cas, A/Aa serait de caractéristique 3 donc $3A \subset Aa$ et $A/3A \twoheadrightarrow A/Aa$. Mais comme $A/3A$ est un corps, ses seuls idéaux sont 0 ou $A/3A$, ce qui impose $A/3A \tilde{\to} A/Aa$. Mais $A/3A \tilde{\to} \mathbb{F}_2[X]/X^2 - X - 1$ est de cardinal $9 > 3$.

(5) Il suffit de montrer que pout tt $0 \neq x \in \mathbb{C}$ il existe $q \in A$ tq $|x - q| < 1$ ou $|2x - q| < 1$ (on applique ensuite ça à $x = a/b$...) Ecrivons $x = a + ib$, $a, b \in \mathbb{R}$. soit $n \in \mathbb{Z}$ tq $|\frac{2b}{\sqrt{19}} - n| \leq 1/2$. En remplaçant x par $x - n\alpha$, on est ramené au cas où $-\sqrt{19}/4 \leq b \leq \sqrt{19}/4$ puis, si $-\sqrt{19}/4 \leq b \leq 0$, en remplaçant x par $-x$, on est ramené au cas où $0 \leq b \leq \sqrt{19}/4$. On distingue ensuite selon que $0 \leq b < \sqrt{3}/2$ ou $\sqrt{3}/2 \leq b \leq \sqrt{19}/4$. Si $0 \leq b < \sqrt{3}/2$, soit $n \in \mathbb{Z}$ tq $|a - n| \leq 1/2$; on a alors $|x - n|^2 < 1/4 + 3/4 \leq 1$. Si $\sqrt{3}/2 \leq b \leq \sqrt{19}/4$, en remplaçant x par $\alpha - *2 * x$, on est ramené au cas où $0 \leq b < \sqrt{3}/2$.

(6) Soit $0 \subsetneq I \subsetneq A$ un idéal de A et $0 \neq a \in I$ tel $|a| = min|I|$. On a bien sûr $Aa \subset I$ et, d'après la question (4), $2I \subset Aa$. Supposons $Aa \subsetneq I$ donc il existe $\alpha \in I$ tel que $\alpha \notin Aa$. Comme $2\alpha \in Aa$, on peut écrire $2\alpha = qa \in 2A$. D'après la question (5) cela impose $q \in 2A$ ou $a \in 2A$. Mais comme $\alpha \notin Aa$, on a forcément $a \in 2A$. Ecrivons donc $a = 2b$. On a alors $2Ab \subsetneq I \subset Ab$. Comme A est intègre, le morphisme de multiplication par b $L_b : A \to A$ est injectif. On vérifie en outre que $L_b^{-1}(I) \subset A$ est encore un idéal de A. On a donc $2A \subsetneq L_b^{-1}(I) \subset A$. Mais comme $A/2A$ est un corps, cela force $L_b^{-1}(I) = A$ donc $I = Ab$: contradiction. Donc $Aa = I$.

Exercice 2 Soit B un anneau et $A \subset B$ un sous-anneau.

(1) Montrer que pour $b \in B$ les PSSE:
   (a) Il existe un polynôme unitaire non nul $0 \neq P_b \in A[T]$ tel que $P_b(b) = 0$;
   (b) La sous A-algèbre $A[b] \subset B$ est de type fini comme A-module;

(c) Il existe une sous-A-algèbre $C \subset B$ contenant $A[b]$ qui est de type fini comme A-module.

On dit qu'un élément $b \in B$ qui vérifie les propriétés équivalentes (a), (b), (c) ci-dessous est entier sur A.

(2) Montrer que l'ensemble $B^A \subset B$ des éléments de B entiers sur A est une sous-A-algèbre de B. Si $A = B^A$, on dit que A est intégralement clos dans B. Si $B^A = B$ on dit que B est entier sur A.

(3) Supposons B entier sur A. Montrer que si $I \subset B$ est un idéal alors B/I est entier sur $A/A \cap I$ et que si $S \subset A$ est une partie multiplicative alors $S^{-1}B$ est entier sur $S^{-1}A$.

(4) Supposons A, B intègres et B entier sur A. Montrer que A est un corps ssi B est un corps.

(5) Supposons B entier sur A. Montrer que

(a) pour tout $\mathfrak{q} \in spec(B)$, $\mathfrak{q} \in spm(B)$ ssi $\mathfrak{q} \cap A \in spm(A)$.

(b) pour tout $\mathfrak{q}, \mathfrak{q}' \in spec(B)$ tels que $\mathfrak{q} \subset \mathfrak{q}'$, $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$ implique $\mathfrak{q} = \mathfrak{q}'$.

(c) pour tout $\mathfrak{p} \in spec(A)$ il existe $\mathfrak{q} \in spec(B)$ tel que $\mathfrak{p} = \mathfrak{q} \cap A$ (Ind.: on pourra considérer un idéal maximal du localisé de B en $A \setminus \mathfrak{p}$).

(d) pour toute suite d'idéaux premiers $\mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_m$ de A, toute suite d'idéaux premiers $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_n$ de B telle que $\mathfrak{p}_i = \mathfrak{q}_i \cap A$, $i = 1, \dots, n$ peut se prolonger en une suite d'idéaux premiers $\mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_m$ de B telle que $\mathfrak{p}_i = \mathfrak{q}_i \cap A$, $i = 1, \dots, m$.

(1) (a) $\Rightarrow$ (b): Par déf de P_b, Le morphisme surjectif de A-algèbres canonique $A[T] \twoheadrightarrow A[b]$, $T \mapsto b$ (prop. univ. de $A[T]$) se factorise en un morphisme de A-algèbres surjectif $A5T]/P_b \twoheadrightarrow A[b]$. Comme $P_b \in A[T]$ est unitaire, on peut effectuer la division euclidienne par P_b dans $A[T]$: pour tout $P \in A[T]$ il existe $Q, R \in A[T]$ tq $P = P_bQ + R$ avec $R = 0$ ou $deg(R) < deg(P_b)$. On en déduit que $A[T]/P_b$ - et donc *a fortiori* $A[b]$ - est un A-module de type fini (engendré par les classes de $1, T, \dots, T^{deg(P_b)-1}$.

(b) $\Rightarrow$ (c): prendre $C = A[b]$...

(c) $\Rightarrow$ (a): Soit $c_1, \dots, c_r$ des générateurs de C comme A-module. pour $i = 1, \dots, r$ on a $bc_j = \sum_{1 \leq i \leq r} b_{i,j}c_i$ avec $M = (b_{i,j})_{1 \leq i,j \leq r} \in M_r(A)$. Par construction $(bI_r - M)(c_i)_{1, \leq i \leq r} = 0$ donc en utilisant ${}^tCom(bI_r - M)(bI_r - M) = det(bI_r - M)I_r$, on a $det(bI_r - M)c_i = 0$, $i = 1, \dots, r$. Mais comme $c_1, \dots, c_r$ engendre C comme A-module (et en particulier $1_A \in \sum_{1 \leq i \leq r} Ac_i$), on en déduit $det(bI_r - M) = 0$; on peut donc prendre $P_b = det(TI_r - M) \in A[T]$, qui est bien unitaire.

(2) On a clairement $A \subset B^A$ (si $a \in A$, prendre $P_a = T - a$...). Soit $b, b' \in B^A$. Par (b), $A[b], A[b'] \subset B$ dont des sous-A-modules de type fini donc $A[b, b'] \subset B$ est aussi un sous-A-module de type fini. Or $A[bb'], A[b - b'] \subset A[b, b']$ donc, par (c) $bb', b - b' \in B^A$.

(3) Si $b \in B$ est annulé par $0 \neq P_b \in A[T]$ unitaire alors l'image $\bar{b}$ de b dans B/I est annulé par la réduction $\overline{P}_b \in (A/A \cap I)[T]$ modulo $I \cap A$ de $P_b \in A[T]$, qui est encore unitaire. Si $b \in B$ est annulé par $0 \neq P_b = T^r + \sum_{0 \leq i \leq r-1} a_iT^i \in A[T]$ unitaire alors b/s est annulé par $T^r + \sum_{0 \leq i \leq r-1} a_i/s^{r-i}T^i \in S^{-1}A[T]$, qui est encore unitaire.

(4) Si A est un corps et $0 \neq b \in B$ annulé par $0 \neq P_b = T^r + \sum_{0 \leq i \leq r-1} a_iT^i \in A[T]$ unitaire *de degré minimal*, on a $a_0 \neq 0$ sinon, comme B est intègre, b serait annulé par $T^{r-1} + \sum_{1 \leq i \leq r-1} a_iT^{i-1} \in A[T]$. Donc, comme A est un corps, $-a_0^{-1}(b^{r-1} + \sum_{1 \leq i \leq r-1} a_ib^{i-1})b = 1$. Inversement, si B est un corps, on veut mq pour tt $0 \neq a \in A$, $b := a^{-1} \in B$ est en fait dans A. Soit donc $0 \neq P_b = T^r + \sum_{0 \leq i \leq r-1} a_iT^i \in A[T]$ unitaire annulant P. En muktipliant $P_b(b) = 0$ par a^{r-1} on obient $b = -\sum_{0 \leq i \leq r-1} a_ia^{r-1-i} \in A$.

(5) Il suffit de montrer que pour tt $0 \neq x \in \mathbb{C}$ il existe $q \in A$ tq $|x - q| < 1$ ou $|2x - q| < 1$ (on applique ensuite ça à $x = a/b$). Ecrivons $x = a + ib$, $a, b \in \mathbb{R}$.

(a) Pour tout $\mathfrak{q} \in spec(B)$, $\mathfrak{q}_A := \mathfrak{q} \cap A \in spec(A)$ donc $B/\mathfrak{q}$ et $A/\mathfrak{q}_A$ sont intègres. De plus, par (3), $B/\mathfrak{q}$ est encore entier sur $A/\mathfrak{q}_A$. Donc par (4) $B/\mathfrak{q}$ est un corps ssi $A/\mathfrak{q}_A$ est un corps.

(b) Soit $\mathfrak{q}, \mathfrak{q}' \in spec(B)$ tels que $\mathfrak{q} \subset \mathfrak{q}'$ et $\mathfrak{p} := \mathfrak{q} \cap A = \mathfrak{q}' \cap A$. Notons $S := A \setminus \mathfrak{P} \subset A$. Par (3), $S^{-1}B$ est encore entier sur $S^{-1}A$. Par ailleurs, pour tt $b/s \in S^{-1}\mathfrak{q}$ (avec $b \in \mathfrak{q}, s \in S$), si $b/s \in S^{-1}A$ il existe $t, t' \in S, a \in A$ tq $t'(tb - sa) = 0$ dc $t'sa = t'tb \in \mathfrak{q}$. Mais comme $\mathfrak{q} \in spec(B)$ et $t, t' \notin \mathfrak{q}$, cela force $a \in \mathfrak{q}$. Donc $S^{-1}\mathfrak{q} \cap S^{-1}A = S^{-1}\mathfrak{p}$. De même, $S^{-1}\mathfrak{q}' \cap S^{-1}A = S^{-1}\mathfrak{p}$. Or $S^{-1}\mathfrak{p} \in spm(S^{-1}A)$ donc par (5) (a), $S^{-1}\mathfrak{q}, S^{-1}\mathfrak{q}' \in spm(S^{-1}B)$ et comme $S^{-1}\mathfrak{q} \subset S^{-1}\mathfrak{q}'$, $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{q}'$. En part., pour tout $q' \in \mathfrak{q}'$ il existe $q \in \mathfrak{q}$, $s, t \in S$ tq $t(sq' - q) = 0$ *i.e.* $tsq' = tq \in \mathfrak{q}$. Mais comme $\mathfrak{q} \in spec(B)$ et $s, t \notin \mathfrak{q}$, cela force $q' \in \mathfrak{q}$. On a bien mq $\mathfrak{q}' \subset \mathfrak{q}$.

(c) On suit l'indication de l'énoncé. Notons $S := A \setminus \mathfrak{p}$ et $\iota_S : B \to S^{-1}B$ le morphisme de localisation. Comme $\mathfrak{p}S^{-1}B \subset B$ est un idéal propre, il est contenu dans un idéal maximal $S^{-1}\mathfrak{q} \in spm(S^{-1}B)$, où $\mathfrak{q} \in spec(B)$ (on utilise ici la structure des idéaux premier du localisé vu en cours). Par (3), $S^{-1}B$ est entier sur $S^{-1}A = A_\mathfrak{p}$ donc par (5) (a), $S^{-1}\mathfrak{q} \cap A_\mathfrak{p} \in spm(A_\mathfrak{p})$. Mais comme $A_\mathfrak{p}$ est local d'unique idéal maximal $\mathfrak{p}A_\mathfrak{p}$, cela impose $S^{-1}\mathfrak{q} \cap A_\mathfrak{p} = \mathfrak{p}A_\mathfrak{p}$ et donc

$$\mathfrak{p} = \iota_S^{-1}(\mathfrak{p}A_\mathfrak{p}) = \iota_S^{-1}(S^{-1}\mathfrak{q} \cap A_\mathfrak{p}) = \iota_S^{-1}(S^{-1}\mathfrak{q}) \cap A = \mathfrak{q} \cap A.$$

(d) Il suffit de traiter le cas $m = n + 1 = 2$. Soit donc $\mathfrak{p}_1 \subset \mathfrak{p}_2$ deux idéaux premiers de A et $\mathfrak{q}_1 \in spec(B)$ tq $\mathfrak{p}_1 = \mathfrak{q}_1 \cap A$. D'après (3), $B/\mathfrak{q}_1$ est encore entier sur $A/\mathfrak{p}_1$ et d'après (5) (c) il existe $\overline{\mathfrak{q}}_2 \in spec(B/\mathfrak{q}_1)$ tq $\overline{\mathfrak{q}}_2 \cap A/\mathfrak{p}_1 = \overline{\mathfrak{p}}_2$. Notons $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset B$ l'image inverse de $\overline{\mathfrak{q}}_2$ par la projection canonique $B \twoheadrightarrow B/\mathfrak{q}_1$. Par construction $\mathfrak{p}_2 = \mathfrak{q}_2 \cap A$.

Exercice 3: (Différentielles de Kähler). Soit A un anneau. On rappelle que si B et C sont deux A-algèbres, $A \to B \otimes_A C$, $a \mapsto a \otimes 1 = 1 \otimes a$ est naturellement muni d'une structure de A-algèbre pour le produit $(b \otimes c)(b' \otimes c') = (bb') \otimes (cc')$ et que les applications $B \to B \otimes_A C$, $b \mapsto b \otimes 1$ et $C \to B \otimes_A C$, $c \mapsto 1 \otimes c$ sont des morphismes de A-algèbres. Cela s'applique en particulier au cas $B = C$. Dans ce cas en outre, comme l'application produit $B \times B \to B$, $(b, b') \mapsto bb'$ est 2-A-linéaire, elle se factorise de façon unique en un morphisme de A-modules $B \otimes_A B \to B$, $b \otimes b' \mapsto bb'$

(1) Vérifier que $B \otimes_A B \to B$ est un morphisme de A-algèbres.

(2) Montrer que l'idéal $I := \ker(B \otimes_A B \to B) \subset B \otimes_A B$ est engendré par les éléments de la forme $b \otimes 1 - 1 \otimes b$.

(3) On note $\Omega_{B|A} := I/I^2$. C'est un $B \otimes_A B$-module. En considérant les morphismes de A-algèbres $\phi_1 : B \to B \otimes_A B$, $b \mapsto b \otimes 1$ et $\phi_2 : B \to B \otimes_A B$, $b \mapsto 1 \otimes b$, on peut munir $\Omega_{B|A}$ de deux structures de B-module *a priori* distinctes: $\phi_{1*}\Omega_{B|A}$ et $\phi_{2*}\Omega_{B|A}$. Montrer qu'en fait ces deux structures de B-module coïncident.

(4) Soit M un B-module. Une A-dérivation sur B à valeur dans M est une application A-linéaire $d : B \to M$ telle que $d(bb') = bdb' + b'db$. Montrer que l'ensemble $Der_A(B, M)$ est naturellement muni d'une structure de B-module.

(5) Montrer que l'application $d := d_{B|A} : B \to \Omega_{B|A}$, $b \mapsto db = \overline{b \otimes 1 - 1 \otimes b}$ est une A-dérivation.

(6) Rappeler quelle est la structure de B-module sur l'ensemble $Hom_B(\Omega_{B|A}, M)$ des morphismes de B-modules $\Omega_{B|A} \to M$ et montrer que l'application $\mathrm{Hom}_B(\Omega_{B|A}, M) \to Der_A(B, M)$, $\phi \mapsto \phi \circ d$ est un isomorphisme de B-modules.

(7) Soit $I \subset A$ un idéal. Montrer que $\Omega_{A/I|A} = 0$.

(8) Soit $S \subset A$ une partie multiplicative. Montrer que $\Omega_{S^{-1}A|A} = 0$.

(9) Supposons $B = A[X_1, \dots, X_r]$.

(a) Montrer que $\Omega_{B|A}$ est engendré comme B-module par $dX_1, \dots, dX_r$ et, plus précisément, que pour tout $P(\underline{X}) \in B$, $dP = \sum_{1 \leq i \leq r} \frac{\partial P}{\partial X_i} dX_i$ (où $\frac{\partial P}{\partial X_i}$ est le "polynôme dérivé de $P(\underline{X})$ selon la variable X_i").

(b) Montrer que pour $i = 1, \dots, r$, l'application $\partial_i : B \to B$, $P \mapsto \frac{\partial P}{\partial X_i}$ est une A-dérivation à valeur dans B. D'après la question (6) il existe donc un unique morphisme de B-modules $\phi_i : \Omega_{B|A} \to B$ tel que $\phi_i \circ d_{B|A} = \partial_i$.

(c) Montrer que $\phi_i(d_{B|A}X_j) = \delta_{i,j}$, $1 \leq i, j \leq r$. En déduire que

$$\Omega_{B|A} \simeq \bigoplus_{1 \leq i \leq r} BdX_i \ \text{ et } \ \mathrm{Hom}_B(\Omega_{B|A}, B) \simeq \bigoplus_{1 \leq i \leq r} B\partial_i.$$

(1) Notons $\mu : B\otimes_A B \to B$ le morphisme canonique de A-modules défini par le produit $B\times B\to B$. On a $\mu(1\otimes 1) = 1\cdot 1 = 1$ et

$$\mu((b_1\otimes b_2)\cdot(b_1'\otimes b_2')) \overset{(1)}{=} \mu((b_1b_1')\otimes(b_2b_2')) \overset{(2)}{=} (b_1b_1')(b_2b_2') \overset{(3)}{=} (b_1b_2)(b_1'b_2') \overset{(2)}{=} \mu(b_1\otimes b_2)\mu(b_1'\otimes b_2'),$$

où (2) est par déf. de μ, (1) est par déf du produit sur $B\otimes_A B$ et (3) par commutativité de B.

(2) Notons $J\subset B\otimes_A B$ l'idéal engendré par les éléments de la forme $b\otimes 1 - 1\otimes b$, $b\in B$. Par déf de μ, $J\subset I := \ker(\mu)$. Inversement, pour tout $x = \sum_{1\leq i\leq r} b_i\otimes b_i' \in B\otimes_A B$, $x\in I$ ssi $\sum_{1\leq i\leq r} b_ib_i' = 0$ donc on a aussi

$$x = \sum_{1\leq i\leq r} b_i\otimes b_i' - \sum_{1\leq i\leq r}(b_ib_i')\otimes 1 = \sum_{1\leq i\leq r}(b_i\otimes 1)\cdot(1\otimes b_i' - b_i'\otimes 1)\in J.$$

(3) Pour tout $x\in I$ et pour tout $b\in B$, on a

$$\phi_1(b)\cdot\overline{x} = \overline{(b\otimes 1)\cdot x} = \overline{(b\otimes 1)\cdot x} = \overline{(1\otimes b)\cdot x} + \overline{((b\otimes 1)-(1\otimes b))\cdot x} = \phi_2(b)\cdot\overline{x} + \overline{((b\otimes 1)-(1\otimes b))\cdot x}.$$

Mais comme $(b\otimes 1)-(1\otimes b), x\in I$, on a $((b\otimes 1)-(1\otimes b))\cdot x\in I^2$ dc $\phi_1(b)\cdot\overline{x} = \phi_2(b)\cdot\overline{x}$.

(4) Il suffit de mq $Der_A(B,M)$ est un sous B-module de $\mathrm{Hom}_A(B,M)$ *i.e.* que pour tt $d\in Der_A(B,M)$, $b,b'\in B$, $bd+b'd'\in Der_A(B,M)$. Or pour tt $\beta,\beta'\in B$,

$$(bd+b'd)(\beta\beta') = b(\beta d\beta' + \beta' d\beta) + b'(\beta d'\beta' + \beta' d'\beta) = \beta(bd+b'd')(\beta') + \beta'(bd+b'd')(\beta).$$

(5) On calcule

$$\begin{aligned} d_{B|A}(bb') - bd_{B|A}b' - b'd_{B|A}b &= \overline{(bb')\otimes 1 - 1\otimes(bb')} - b\cdot\overline{b'\otimes 1 - 1\otimes b'} - b'\cdot\overline{b\otimes 1 - 1\otimes b}\\ &= \overline{(bb')\otimes 1 - 1\otimes(bb')} - \overline{(bb')\otimes 1 - b\otimes b'} - \overline{b\otimes b' - 1\otimes b'b}\\ &= 0,\end{aligned}$$

(où, dans la deuxième égalité, on a utilisé (4)). Le fait que $d_{B|A}$ est un morphisme de A-modules se vérifie immédiatement sur la déf.

(6) $\mathrm{Hom}_B(\Omega_{B|A},M)$ est muni de la structure de B-module définie par $(b\phi+b'\phi')(\omega) = b\phi(\omega)+b'\phi'(\omega)$. Pour cette structure, on vérifie sur les déf. que l'application $Hom_B(\Omega_{B|A},M)\to\mathrm{Hom}_A(B,M)$, $\phi\mapsto\phi\circ d$ est morphisme de B-modules et que son image est contenue dans $Der_A(B,M)$. Montrons que le morphisme de B-modules induit $\Phi : Hom_B(\Omega_{B|A},M)\to Der_A(B,M)$ est un isomorphisme:
- Injectivité: Cela résulte du fait que, d'après (2), $\Omega_{B|A} = I/I^2$ est engendré par les $d_{B|A}b$, $b\in B$.
- Surjectivité: Pour tout $d\in Der_A(B,M)$, l'application $B\times B\to M$, $(b,b')\mapsto bdb'$ est A-bilinéaire dc par prop. univ. du produit tensoriel se factorise en un morphisme de A-modules $\delta : B\otimes_A B\to M$. De plus, pour tt $b,b'\in B$ on a

$$\delta((b\otimes 1 - 1\otimes b)(b'\otimes 1 - 1\otimes b')) = \delta(bb'\otimes 1 - b'\otimes b - b\otimes b' + 1\otimes bb') = -b'db - bdb' + d(bb') = 0,$$

(où on a utilisé que $d1 = 0$ puisque $d1 = d(1\cdot 1) = d1 + d1\ldots$). Comme I^2 est engendré par les éléments de la forme $(b\otimes 1 - 1\otimes b)(b'\otimes 1 - 1\otimes b')$, cela mq $I^2\subset\ker(\delta|_I)$ donc que $\delta|_I : I\to M$ se factorise en un morphisme de A-modules $\phi_d := \overline{\delta|_I} : I/I^2\to M$. Par construction, pour tt $b\in B$, $\phi_d\circ d_{B|A}(b) = \phi_d(\overline{b\otimes 1 - 1\otimes b}) = db$.

(7) Cela du fait que $\Omega_{A/I|A}$ est engendré par les $d_{A/I|A}\overline{a}$ et que $d_{A/I|A}\overline{a} = d_{A/I|A}(a\cdot\overline{1}) = ad_{A/I|A}\overline{1} = 0$.

(8) Cela du fait que $\Omega_{S^{-1}A|A}$ est engendré par les $d_{S^{-1}A|A}(a/s)$ et que $d_{S^{-1}A|A}(a/s) = ad_{S^{-1}A|A}(1/s)$ or $0 = d_{S^{-1}A|A}(1) = d_{S^{-1}A|A}(s/s) = sd_{S^{-1}A|A}(1/s)$ dc, puisque $s\in(S^{-1}A)^\times$, $d_{S^{-1}A|A}(1/s) = 0$.

(9) (a) Par A-linéarité, il suffit de traiter le cas $r=1$ $P = X^n$, ce qui se fait par réc sur n: $d1 = 0$, $dX = dX$, $dX^2 = XdX + XdX = 2XdX$, $d(X^n) = Xd(X^{n-1}) + X^{n-1}dX = (n-1)XX^{n-2}dX + X^{n-1}dX = nX^{n-1}dX$.

(b) Exo.

(c) Par déf., pour $1\leq i,j\leq r$, $\phi_i(d_{B|A}X_j) = \partial_i(X_j) = \delta_{i,j}$. D'après (9) (a), le morphisme canonique de B-modules $\bigoplus_{1\leq i\leq r} BdX_i\to\Omega_{B|A}$, $dX_i\mapsto d_{B|A}X_i$ est surjectif. C'est aussi un isomorphisme car pour tt $\sum_{1\leq i\leq r} P_idX_i\in\bigoplus_{1\leq i\leq r} BdX_i$, $\sum_{1\leq i\leq r} P_id_{B|A}X_i = 0$ implique $0 = \phi_j(\sum_{1\leq i\leq r} P_id_{B|A}X_i) = P_j$. *Via* l'isomorphisme $\mathrm{Hom}_B(\Omega_{B|A},B)\to Der_A(B,B)$, $\phi\mapsto\phi\circ d_{B|A}$ de (6), ∂_i, $1\leq i\leq r$ correspond à la base duale de $d_{B|A}X_i$, $1\leq i\leq r$.