Examen 2022/2023 - Correction
4M003 - Algèbre commutative
Anna Cadoret

Exercice 1.

(1) Récurrence sur n en développant

$$P_{n+1}(T_1,\dots,T_{n+1},X)=P_n(T_1,\dots,T_n,X)(X-T_{n+1})=(X^n+\sum_{1\leq k\leq n}(-1)^kS_k^nX^k)(X-T_{n+1})$$

on a $S_k^{n+1}=S_{k-1}^nT_{n+1}+S_k^n=\sum_{1\leq i_1<\dots<i_k\leq n+1}T_{i_1}\cdots T_{i_k}$, $2\leq k\leq n$, $S_1^{n+1}=S_1^n+T_{n+1}=\sum_{1\leq k\leq n+1}T_k$ et $S_{n+1}^{n+1}=T_1\cdots T_{n+1}$.

(2) En développant $P_n(T_1,\dots,T_{n-1},0,X)=XP_{n-1}(T_1,\dots,T_{n-1},X)$ et en identifiant les coefficients de X^{n-k}, $k=1,\dots,n$ on obtient bien $S_k^{n-1}=S_k^n(T_1,\dots,T_{n-1},0)$, $k=1,\dots,n-1$.

(3) Il suffit d'écrire.

(4) Pour tout $\sigma\in\mathcal{S}_n$, il résulte de la question précédente en observant que l'application

$$\sigma\cdot:A[T_1,\dots,T_n]\to A[T_1,\dots,T_n],\ P\mapsto\sigma\cdot P$$

est un automorphisme de A-algèbre que

$$\mathbb{Z}[T_1,\dots,T_n]^\sigma:=\{P\in\mathbb{Z}[T_1,\dots,T_n]\mid\sigma\cdot P=P\}\subset\mathbb{Z}[T_1,\dots,T_n]$$

est une sous-$\mathbb{Z}$-algèbre. On conclut en utilisant que $\Sigma[T_1,\dots,T_n]=\cap_{\sigma\in\mathcal{S}_n}A[T_1,\dots,T_n]^\sigma\subset A[T_1,\dots,T_n]$ est une sous-A-algèbre comme intersection de sous-A-algèbres.

(5) (a) Comme $P(T_1,\dots,T_{n-1},0)\in\Sigma[T_1,\dots,T_{n-1}]$ et est de degré $\leq d$ par définition / construction, H$(n-1)$ implique immédiatement qu'il existe $Q_1\in\Sigma[T_1,\dots,T_{n-1}]$ de poids $\leq d$ tel que $P(T_1,\dots,T_{n-1},0)=Q_1(S_1^{n-1},\dots,S_{n-1}^{n-1})=Q_1(S_1^n,\dots,S_{n-1}^n)(T_1,\dots,T_{n-1},0)$, où la deuxième égalité est la question (2). Notons que Q_1 est de degré total $\leq d$ dans $\mathbb{Z}[T_1,\dots,T_{n-1}]$ (donc aussi dans $\mathbb{Z}[T_1,\dots,T_{n-1},T_n]$).

(b) En effectuant la division euclidienne de P_1 par T_n dans $\mathbb{Z}[T_1,\dots,T_{n-1}][T_n]$: il existe $Q\in\mathbb{Z}[T_1,\dots,T_n]$ et $R\in\mathbb{Z}[T_1,\dots,T_{n-1}]$ tels que

$$P_1=T_nQ(T_1,\dots,T_n)+R(T_1,\dots,T_{n-1})$$

Mais par construction, on a $0=P_1(T_1,\dots,T_{n-1},0)=R(T_1,\dots,T_{n-1})$. Donc en fait $P_1=T_nQ(T_1,\dots,T_n)$. De plus, en utilisant la transposition $\tau_k=(k,n)\in\mathcal{S}_n$, on a $P_1=\tau_k\cdot P_1=\tau_k\cdot T_n\tau_k\cdot Q(T_1,\dots,T_n)=T_k\tau_k\cdot Q(T_1,\dots,T_n)$, $k=1,\dots,n-1$. Cela montre que $T_1,\dots,T_n$ divise P_1 dans $\mathbb{Z}[T_1,\dots,T_n]$. De plus $T_1,\dots,T_n$ sont irréductibles deux à deux distincts dans $\mathbb{Z}[T_1,\dots,T_n]$ qui est factoriel, donc $T_1\cdots T_n$ divise P_1 dans $\mathbb{Z}[T_1,\dots,T_n]$.

(c) Ecrivons donc $P_1=T_1\cdots T_nP_2$ avec $P_2\in\mathbb{Z}[T_1,\dots,T_n]$. Comme $P_1,T_1\cdots T_n\in\Sigma[T_1,\dots,T_n]$ et que $\mathbb{Z}[T_1,\dots,T_n]$ est intègre, on a automatiquement $P_2\in\Sigma[T_1,\dots,T_n]$. En outre, $deg(P_2)=deg(P_1)-n\leq d-n<d$. Donc si on raisonne maintenant par récurrence sur $d\geq 0$ (en observant là encore que l'assertion pour $d=0$ - qui correspond aux polynômes constants- est tautologique) on en déduit qu'il existe $Q_2\in\mathbb{Z}[T_1,\dots,T_n]$ de poids $\leq d-n$ tel que $P_2=Q_2(S_1^n,\cdots,S_n^n)$. On conclut en prenant $Q=Q_1(T_1,\dots,T_{n-1})+T_nQ_2(T_1,\dots,T_{n-1},T_n)\in\mathbb{Z}[T_1,\dots,T_n]$, qui est bien de poids $\leq d$.

(6) On raisonne par récurrence sur n. Comme le cas $n=1$ est tautologique (puisque $\Sigma[T_1]=\mathbb{Z}[T_1]$), il faut seulement montrer que H$(n-1)$) implique H(n). Soit $Q\in\mathbb{Z}[X_1,\dots,X_n]$ tel $Q(S_1^n,\dots,S_n^n)=0$. Comme $\mathbb{Z}[X_1,\dots,X_n]$ est intègre - et même factoriel, on peut supposer Q irréductible. Ecrivons $Q=\sum_{0\leq k\leq d}Q_kX_n^k\in\mathbb{Z}[X_1,\dots,X_{n-1}][X_n]$ *i.e.* avec $Q_k\in\mathbb{Z}[X_1,\dots,X_{n-1}]$, $k=0,\dots,d$ et $Q_d\neq 0$. La condition $Q(S_1^n,\dots,S_n^n)=0$ implique en particulier $0=Q(S_1^n,\dots,S_n^n)(T_1,\dots,T_{n-1},0)=Q(S_1^{n-1},\dots,S_{n-1}^{n-1},0)$ (on utilise à nouveau la question (2)). D'après H$(n-1)$, cela force

$$Q_0=Q(X_1,\dots,X_{n-1},0)=0.$$

Mais alors X_n diviserait Q dans $\mathbb{Z}[X_1,\dots,X_n]$, contredisant l'irréductibilité de Q.

(7) Par propriété universelle de $\mathbb{Z}[X_1,\dots,X_n]$, il existe un unique morphisme de $\mathbb{Z}$-algèbre $\phi:\mathbb{Z}[X_1,\dots,X_n]\to\Sigma[T_1,\dots,T_n]$ tel que $\phi(T_k)=S_k^n$, $k=1,\dots,n$. Ce morphisme est surjectif par la question (5) et injectif par la question (6) donc c'est un isomorphisme.

(8) D'après la question (7) $\Sigma[T_1,\dots,T_n]$ est factoriel (puisqu'il est isomorphe à l'anneau factoriel $\mathbb{Z}[X_1,\dots,X_n]$). En outre, l'isomorphisme e de $\mathbb{Z}$-algèbre $\phi : \mathbb{Z}[X_1,\dots,X_n] \to \Sigma[T_1,\dots,T_n]$ induit une bijection au niveau des irréductibles. Donc les irréductibles de $\Sigma[T_1,\dots,T_n]$ sont exactement les polynômes de la forme $P(S_1^n,\dots,S_n^n)$ avec $P \in \mathbb{Z}[T_1,\dots,T_n]$ irréductible dans $\mathbb{Z}[T_1,\dots,T_n]$.

Exercice 2. Soit A un anneau principal de corps des fractions $A \hookrightarrow K$.

(1) Immédiat.

(2) L'élément $g \in N_{\mathrm{GL}_n(K)}(\mathrm{GL}_n(A))$ induit un isomorphisme de A-modules $g : A^{\oplus n}\tilde{\to}M$ donc M est un A-module libre de rang n.

(3) Pour tout $h \in \mathrm{GL}_n(A)$, on a $g^{-1}hg \in \mathrm{GL}_n(A)$ puisque $g \in N_{\mathrm{GL}_n(K)}(\mathrm{GL}_n(A))$. Donc $hM = hg(A^{\oplus n}) = gg^{-1}hg(A^{\oplus n}) = g(A^{\oplus n}) = M$.

(4) Soit $m_1,\dots,m_n$ une A-base de M. Pour $j = 1,\dots,n$ on a, dans $e_1,\dots,e_n$: $m_j = \sum_{1\leq i\leq n} x_{i,j}e_i$ avec $x_{i,j} \in K$. Mais comme K est le corps des fractions de A, il existe $0 \neq a \in A$ tel que $ax_{i,j} \in A$, $1 \leq i,j \leq n$.

(5) Par théorème de la base adaptée appliqué à $aM \subset A^{\oplus n}$, il existe une A-base $f_1,\dots,f_n$ de $A^{\oplus n}$ et $d = d_1|\cdots|d_n$ dans A tels que

$$aM = \oplus_{1\leq i\leq n} Ad_if_i \subset A^{\oplus n} = \oplus_{1\leq i\leq n} Af_i$$

donc

$$\frac{a}{d}M = \oplus_{1\leq i\leq n} A\frac{d_i}{d_1}f_i \subset A^{\oplus n} = \oplus_{1\leq i\leq n} Af_i$$

avec $\delta_i := \frac{d_i}{d_1} \in A$, $i = 1,\dots,n$. En posant $N = \oplus_{2\leq i\leq n} A\frac{d_i}{d_1}f_i$, on a bien $\frac{a}{d}M = Af_1 \oplus N \subset A^{\oplus n} = \oplus_{1\leq i\leq n} Af_i$ comme A-modules.

(6) Pour $i = 1,\dots,n$, on a $L_ie_i = f_1 \in \frac{a}{d}M$ donc, comme $L_i^{-1}in\mathrm{GL}_n(A)$ et M (donc $\frac{a}{d}M$) est $\mathrm{GL}_n(A)$-stable par la question (3), $e_i = L_i^{-1}f_1 \in \frac{a}{d}M$.

(7) Comme $e_1\dots,e_n$ est une A-base de $A^{\oplus n}$, on a $\frac{d}{a}M \supset A^{\oplus n}$ et comme $\frac{d}{a}M \subset A^{\oplus n}$ par construction, on a bien $\frac{a}{d}M = A^{\oplus n}$. Cela montre en particulier que $\frac{d}{a}ge_1,\dots,\frac{d}{a}ge_n$ est une A-base de $A^{\oplus n}$ donc que $\frac{d}{a}g \in \mathrm{GL}_n(A)$.

Exercice 3: (Calculs de produits tensoriels)

(1) Notons $A := \mathbb{Z}$, $S := A \setminus \{0\} \subset A$, qui est une partie multiplicative tel que $\mathbb{Q} = S^{-1}A$. On a alors $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} = S^{-1}A \otimes_A S^{-1}A \simeq S^{-1}(S^{-1}A) \simeq S^{-1}A = \mathbb{Q}$ et $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{R} = S^{-1}A \otimes_A \mathbb{R} \simeq S^{-1}\mathbb{R} \simeq \mathbb{R}$. Par ailleurs si M, N sont des A modules comme $M \otimes_A N$ est engendré comme A-module par les éléments de la forme $m \otimes_A n$, $m \in M$, $n \in N$ on a $M \otimes_A N = 0$ ssi $m \otimes_A n = 0$, $m \in M$, $n \in N$. Or pour tout $a/b, a'/b' \in \mathbb{Q}$, on a $a/b \otimes \overline{a'/b'} = (ab')/(bb') \otimes \overline{a'/b'} = a/(bb') \otimes \overline{a'b'/b'} = a/(bb') \otimes \overline{a'} = a/(bb') \otimes \overline{0} = 0$. De même $\overline{a/b} \otimes \overline{a'/b'} = \overline{(ab')/(bb')} \otimes \overline{a'/b'} = \overline{a/(bb')} \otimes \overline{a'b'/b'} = \overline{a/(bb')} \otimes \overline{a'} = \overline{a/(bb')} \otimes \overline{0} = 0$.

(2) *Cf.* TD. 5, Exercice 1 (2).

(3) *Cf.* TD. 5, Exercice 1 (3).

(4) Pour tout $n \in \mathbb{Z}$, $n \geq 1$, on fixe $\zeta_n \in \mathbb{C}$ une racine primitive n-ième de 1 (*i.e.* un élément d'ordre n du groupe multiplicatif $\mathbb{C}^\times$) et on note $\mathbb{Q}(\zeta_n) \subset \mathbb{C}$ le plus petit sous-corps de $\mathbb{C}$ contenant ζ_n et $\mathbb{Q}$.

(a) Comme $\zeta_n^n - 1 = 0$, l'unique morphisme de $\mathbb{Q}$-algèbre $ev_{\zeta_n} : \mathbb{Q}[T] \twoheadrightarrow \mathbb{Q}[\zeta_n] \subset \mathbb{C}$, $T \mapsto \zeta_n$ contient $T^n - 1$ dans son noyau donc n'est pas injectif. Comme $\mathbb{Q}[T]$ est principal, $\ker(ev_{\zeta_n}) = \mathbb{Q}[T]\Phi_n$ pour un certain polynôme - que l'on peut supposer unitaire (donc en particulier non-nul) $\Phi_n \in \mathbb{Q}[T]$. En outre $ev_{\zeta_n} : \mathbb{Q}[T] \twoheadrightarrow \mathbb{Q}[\zeta_n]$ se factorise en un isomorphisme de $\mathbb{Q}$-algèbres $\overline{ev}_{\zeta_n} : \mathbb{Q}[T]/\Phi_n\tilde{\to}\mathbb{Q}[\zeta_n]$. Comme $\mathbb{Q}[\zeta_n]$ est intègre (comme sous-anneau de $\mathbb{C}$), $\mathbb{Q}[T]/\Phi_n$ est intègre donc $\mathbb{Q}[T]\Phi_n$ est un idéal premier de $\mathbb{Q}[T]$ donc maximal (en utilisant à nouveau que $\mathbb{Q}[T]$ est principal). Cela montre que $\mathbb{Q}[T]/\Phi_n$ est un corps donc $\mathbb{Q}[\zeta_n]$ aussi; autrement dit $\mathbb{Q}[\zeta_n] = \mathbb{Q}(\zeta_n)$. On a donc $\mathbb{Q}(\zeta_n)\tilde{\to}\mathbb{Q}[T]/\Phi_n$ de $\mathbb{Q}$-dimension finie égale au degré de Φ_n.

(b) Critère d'Eisenstein appliqué à $\Phi_p(T+1)$ - *cf.* TD. 2, Exercice 10 (1) (b). Comme $T^p - 1 = (T-1)\Phi_p(T)$ on voit que $\Phi_p(\zeta_p) = 0$ donc $\mathbb{Q}[T]\Phi_p \subset \ker(ev_p) \subsetneq \mathbb{Q}[T]$ et comme $\Phi_p \in \mathbb{Q}[T]$ est

irréductible, $\mathbb{Q}[T]\Phi_p$ est maximal donc $\mathbb{Q}[T]\Phi_p = \ker(ev_p)$. L'argument de la question précédente montre que $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = deg(\Phi_p) = p - 1$.

(c) On a $\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_q) = \mathbb{Q}^{\oplus p-1} \oplus_{\mathbb{Q}} \mathbb{Q}^{\oplus q-1} \simeq \mathbb{Q}^{\oplus (p-1)(q-1)}$ puisque $\otimes$ et $\oplus$ commutent. Donc $\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_q)$ est de $\mathbb{Q}$-dimension $(p-1)(q-1)$. Pour déterminer la structure de $\mathbb{Q}$-algèbre de $\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_q)$, on peut utiliser (*cf.* TD. 5, Exercice 2 (2)):

$$\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_q) \simeq \mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{Q}[T]/\Phi_q \simeq \mathbb{Q}(\zeta_p)[T]/\Phi_q.$$

Si $p = q$, $\Phi_p = \prod_{1 \leq i \leq p-1}(T - \zeta_p^i)$ dans $\mathbb{Q}(\zeta_p)[T]$ donc, par le lemme Chinois, $\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_q) \simeq \mathbb{Q}(\zeta_p)^{p-1}$ comme $\mathbb{Q}$-algèbre (et même comme $\mathbb{Q}(\zeta_p)$-algèbre). Comme $\mathbb{Q}(\zeta_p)$ est un corps, les idéaux premiers de $\mathbb{Q}(\zeta_p)^{p-1}$ sont exactement les idéaux de la forme $\mathbb{Q}(\zeta_p) \times \cdots \times \{0\} \times \cdots \times \mathbb{Q}(\zeta_p)$ (il y en a $p-1$). Si $p \neq q$, Φ_q reste irréductible dans $\mathbb{Q}(\zeta_p)[T]$ donc $\mathbb{Q}(\zeta_p) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_q)$ est un corps, extension de degré $(p-1)(q-1)$ de $\mathbb{Q}$. En fait, que Φ_q reste irréductible dans $\mathbb{Q}(\zeta_p)[T]$ n'est pas tout à fait immédiat. Supposons avoir choisi $\zeta_n = e^{2i\pi/n}$. Il faut d'abord voir que $\mathbb{Q}(\zeta_p, \zeta_q) = \mathbb{Q}(\zeta_{pq})$ (l'inclusion $\subset$ est immédiate, l'inclusion $\supset$ résulte de Bézout: $up + vq = 1$ implique $\zeta_{pq} = \zeta_p^v \zeta_q^u$) puis savoir que le polynôme minimal de ζ_{pq} est le polynôme cyclotomique Φ_{pq} défini dans le TD 2 Exercice 11, qui est de degré $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$ (ici $\varphi(n)$ est l'indicatrice d'Euler *i.e.* le cardinal de $(\mathbb{Z}/n)^\times$). Cela montre que $\mathbb{Q}(\zeta_p, \zeta_q) = \mathbb{Q}(\zeta_p)(\zeta_q)$ est de degré $(p-1)(q-1)$ sur $\mathbb{Q}$. Mais comme $\mathbb{Q}(\zeta_p)$ est de degré $p-1$ sur $\mathbb{Q}$, cela impose en particulier que le polynôme minimal de ζ_q sur $\mathbb{Q}(\zeta_p)$ est de degré $q-1$. Comme il doit diviser Φ_q (qui est déjà de degré $q-1$) dans $\mathbb{Q}(\zeta_p)[T]$, cela impose que Φ_q est le polynôme minimal de ζ_q sur $\mathbb{Q}(\zeta_p)$ donc est irréductible dans $\mathbb{Q}(\zeta_p)[T]$.