Université Claude Bernard Lyon 1

MASTER M1G

Algèbre

Fiche TD 2

Exercice 1 *Manipulations algébriques de base*
Les anneaux sont tous unitaires et commutatifs. L'anneau A est un sous-anneau de B. On note I, J des idéaux de A, avec $I \subset J$. Montrer les isomorphismes suivants :

1. $(A/I)/(J/I) \simeq A/J$.
   Partir de l'anneau qui vous semble le plus universel parmi ceux en présence, puis construire des morphismes naturels. Par morphisme naturel, on entend : surjection canonique, injection canonique et passage au quotient.
2. $A[X,Y]/(X-1) \simeq A[Y]$.
3. $A[X,Y]/(X,Y) \simeq A$.
4. $A/(a)[X] \simeq A[X]/A[X]a$.
5. Soit P un polynôme de $A[X]$: $A[X]/\big(B[X]P \cap A[X]\big) \hookrightarrow B[X]/B[X]P$.
6. $\mathbb{Q}[X]/\mathbb{Q}[X](X^2+1) \simeq \mathbb{Q}[i]$,
7. Si ϕ est un morphisme injectif de A dans un anneau A', $A/I \simeq \phi(A)/\phi(I)$.
8. Si ϕ est un morphisme de A dans un anneau A', $A/I + \ker\phi \simeq \phi(A)/\phi(I)$.
9. p est un entier. $\mathbb{Z}[i]/p\mathbb{Z}[i] \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(\mathbb{Z}/p\mathbb{Z})(X^2+1)$.
   Partir de $A = \mathbb{Z}[X]$, $J = (p, X^2+1)$, et $I = p\mathbb{Z}[X]$ ou $(X^2+1)\mathbb{Z}[X]$, puis, appliquer la question 1).

Exercice 2 *Quotienter, c'est tuer*
Sauras-tu reconnaître ces corps célèbres ?

1. $\mathbb{Q}[X]/(X+1)$, $\mathbb{R}[X]/(X^2+X+1)$, $\mathbb{Z}[X]/(5,X)$

Exercice 3 *Systèmes et polynômes symétriques élémentaires*
Résoudre dans $\mathbb{C}$ le système :

$$\begin{cases} x+y+z = 5 \\ \frac{1}{x}+\frac{1}{y}+\frac{1}{z} = 5 \\ x^2+y^2+z^2 = 15 \end{cases}$$

On écrira tout en fonction des polynômes symétriques élémentaires en x, y, z, puis on résoudra une équation de degré 3 qui possède une racine évidente...

Exercice 4 *Une taupinade*

Soit P un polynôme de $\mathbb{R}[X]$ unitaire. Montrer que P est scindé sur $\mathbb{R}$ si et seulement si pour tout z complexe, on a

$$|P(z)| \geq |\operatorname{Im}(z)|^{\deg(P)}$$

Pour le « si », on suppose que z est une racine de P. Pour le « seulement si », on factorise $P(z)$ et on utilise $|(x-\alpha)+iy| \geq |y|$, pour tout x, y, α réels.

Exercice 5 *Multiplicité des racines pour un polynôme irréductible*

Si P est irréductible dans $\mathbb{K}[X]$, les racines de P sont-elles simples ? Montrer que c'est vrai en caractéristique nulle.
Si une racine de P est non simple, alors, elle annule aussi la dérivée P'. Quel est l'ensemble des polynômes qui annulent α ? Quel en est le polynôme minimal ? Peut-on avoir P' multiple de P ?

Exercice 6 *Polynômes et fonctions polynômes*

Soit $\mathbb{K}$ un corps infini. On considère l'application f qui envoie un polynôme P de $\mathbb{K}[X_1, X_2, \cdots, X_n]$ sur la fonction polynôme f_P de $\mathbb{K}^n$ dans $\mathbb{K}$ telle que

$$f_P(\alpha_1, \alpha_2, \cdots, \alpha_n) = P(\alpha_1, \alpha_2, \cdots, \alpha_n).$$

1. Montrer que f est un morphisme d'algèbres (de quelles algèbres parle-t-on ?). On appelle *algèbre des fonctions polynomiales sur $\mathbb{K}$ à n variables* l'image de f.
2. On suppose ici que $n = 1$. Montrer que f est injective. Que se passe-t-il si $\mathbb{K}$ est fini ?

   L'idée est de dire qu'un polynôme non nul possède un nombre fini de racines. Si $\mathbb{K}$ est fini, on pourra considérer le polynôme $\prod_{\alpha \in \mathbb{K}}(X-\alpha)$.
3. Montrer alors par récurrence sur n que f est injective.

   Un polynôme de $\mathbb{K}[X_1, X_2, \cdots, X_n]$ peut être vu comme un polynôme de $A[X_n]$, avec $A := \mathbb{K}[X_1, X_2, \cdots, X_{n-1}]$. Considérer un polynôme P non nul de $A[X_n]$, et montrer que f_P est non nul.
4. Pourquoi peut-on identifier l'algèbre des polynômes à l'algèbre des fonctions polynômes, lorsque $\mathbb{K}$ est infini ?

Exercice 7 *Relation entre coefficients et racines*

Pour toute famille $z = (z_1, \ldots, z_n)$ de $\mathbb{C}^n$ et tout k de $[1, n]$, on note $e_k(z)$ la k-ième fonction symétrique élémentaire de z définie par l'égalité suivante, valable dans $\mathbb{C}[X]$:

$$(X - z_1) \cdots (X - z_n) = X^n + \sum_{k=1}^{n} (-1)^k e_k(z) X^{n-k}.$$

1. Montrer que l'application $e : \mathbb{C}^n \to \mathbb{C}^n$, $z \mapsto \big(e_1(z), \ldots, e_n(z)\big)$ est surjective et que pour tout $w \in \mathbb{C}^n$, $e^{-1}(w)$ est une orbite sous le groupe symétrique $\mathfrak{S}_n$ (pour l'action par permutation).

   La décomposition d'un polynôme de $\mathbb{C}[X]$ en irréductibles est unique à permutation près.

2. Montrer que e définit par passage au quotient une bijection $\overline{e}$ de $\mathbb{C}^n/\mathfrak{S}_n$ dans $\mathbb{C}^n$.

Remarque 0.1. Finalement, ceci n'est qu'une façon de parler de la relation entre coefficients et racines. Cela peut paraître un peu surfait et poussé dans l'abstraction. Mais l'intérêt de cette construction est que l'on peut y insérer de la topologie. La bijection devient alors un homéomorphisme. Cela donne corps à une idée intuitive que les racines d'un polynôme P, unitaire de degré n, de $\mathbb{C}[X]$, dépendent continûment des coefficients de P. Merci l'abstraction !

Exercice 8 *Un isomorphisme de Harish-Chandra*

On considère la $\mathbb{C}$-algèbre $\mathbb{C}[\mathcal{M}_n(\mathbb{C})]$ des fonctions polynomiales sur $\mathcal{M}_n(\mathbb{C})$, identifiée à l'algèbre de polynômes sur $\mathbb{C}$ à n^2 indéterminées. La $\mathbb{C}$-algèbre

$$\left\{f \in \mathbb{C}[\mathcal{M}_n(\mathbb{C})],\ \forall A \in \mathcal{M}_n(\mathbb{C}), \forall P \in \mathrm{GL}_n(\mathbb{C}),\ f(PAP^{-1}) = f(A)\right\}$$

sera notée $\mathbb{C}[\mathcal{M}_n(\mathbb{C})]^{\mathrm{GL}_n(\mathbb{C})}$.

1. Montrer que la restriction au sous-espace $\mathcal{D}_n$ des matrices diagonales définit un morphisme
$$\rho\,:\,\mathbb{C}[\mathcal{M}_n(\mathbb{C})]^{\mathrm{GL}_n(\mathbb{C})} \longrightarrow \mathbb{C}[\mathcal{D}_n]^{\mathfrak{S}_n},$$
où $\mathbb{C}[\mathcal{D}_n]^{\mathfrak{S}_n}$ est la $\mathbb{C}$-algèbre des fonctions polynomiales symétriques sur $\mathcal{D}_n$ identifiée à l'algèbre des polynômes symétriques à n indéterminées.
2. En utilisant le fait que les matrices diagonalisables sont denses dans $\mathcal{M}_n(\mathbb{C})$, montrer que ρ est injective.
3. Montrer que ρ est un isomorphisme.

Soluce

1. *On peut toujours restreindre un polynôme $f(X_{ij}, 1 \leq i, j \leq n)$ en les coefficients d'une matrice au sous-espace des matrices diagonales. La restriction deviendra le polynôme f, où les X_{ij}, pour $i \neq j$, sont remplacés par 0. Cela reste bien-sûr polynomial en les X_{ii}, $1 \leq i \leq n$.*
   Si f est $\mathrm{GL}_n(\mathbb{C})$-invariant, il est en particulier invariant par les matrices de permutations P_σ, $\sigma \in \mathfrak{S}_n$. Donc, si $D = \mathrm{diag}(d_1, \cdots, d_n)$, alors,
   $$D_\sigma = \mathrm{diag}(d_{\sigma(1)}, \cdots, d_{\sigma(n)}) \text{ et } f(D_\sigma) = f(P_\sigma^{-1}D\ P_\sigma) = f(D),$$
   ce qui prouve que f est une fonction symétrique. D'où l'assertion (on rappelle que, comme on est sur le corps infini $\mathbb{C}$, on peut assimiler les polynômes aux fonctions polynômes).
2. *Comme ρ est un morphisme, on cherche son noyau. Il est constitué des polynômes invariants sur les $\mathrm{GL}_n(\mathbb{C})$-orbites et s'annulant sur les matrices diagonalisables. Or, il est bien connu que les matrices diagonalisables constituent une partie dense de $\mathcal{M}_n(\mathbb{C})$, et les fonctions polynômes sont continues. On en conclut que le noyau est réduit au polynôme nul, et ρ est injective.*

3. *On doit maintenant montrer que le morphisme ρ est surjectif, c'est-à-dire qu'il contient un système de générateurs. Or, l'ensemble des sommes de Newton*

$$S_k := \sum_{i=1}^{n} X_i^k, \ 1 \leq k \leq n$$

constitue un système de générateurs de l'algèbre $\mathbb{C}[X_1, \cdots, X_n]^{\mathfrak{S}_n} \simeq \mathbb{C}[\mathcal{D}_n]^{\mathfrak{S}_n}$. Il suffit donc de trouver des antécédents de ρ pour ces générateurs. On vérifie que si l'on pose P_k qui envoie M sur $\mathrm{tr}(M^k)$, alors

a) P_k est bien polynomial en les coefficients de M,

b) P_k est invariant par conjugaison, puisque

$$\mathrm{tr}\left((PMP^{-1})^k\right) = \mathrm{tr}\left(PM^kP^{-1}\right) = \mathrm{tr}(M^k),$$

c) La restriction de P_k aux matrices diagonales est bien S_k.

On a donc bien l'isomorphisme annoncé.