Exercices de khôlle pour la MP*

Année scolaire 1997-1998

Cinquième semaine (polynômes ; evn)

David A. Madore (`david.madore@ens.fr`)

Exercice classiquissime. *Soit K un corps commutatif, et G un sous-groupe fini du groupe multiplicatif $K^\times$ de K. Montrer que G est cyclique. En déduire la classification complète des corps finis.*

"Petit" théorème de Wedderburn. *Soit K un corps fini non nécessairement commutatif. Il s'agit de montrer que K est en fait commutatif. En notant Z le centre de K et q son ordre, n le degré de K sur Z, montrer grâce à l'équation aux classes que*

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{\delta(x)} - 1}$$

où les $\delta(x)$ sont des entiers que l'on définira. Notant Φ_n le n-ième polynôme cyclotomique, montrer que $\Phi_n(q)$ divise tous les termes de l'équation ci-dessus sauf éventuellement $q-1$, et donc qu'il divise celui-ci. Conclure.

> **Remarques :** En combinant les deux exercices ci-dessus, on peut facilement arriver à la conclusion suivante : si G est un sous-groupe fini d'un corps non nécessairement commutatif de caractéristique non nulle, alors G est cyclique. Ceci n'est pas vrai en caractéristique nulle, comme le sous-groupe $\{\pm 1, \pm i, \pm j, \pm k\}$ du corps $\mathbb{H}$ des quaternions le prouve.
>
> Le théorème ci-dessus s'appelle "petit" théorème de Wedderburn par opposition au "grand" théorème de Wedderburn-Artin : si A est un anneau semisimple (c'est-à-dire que tout A-module est somme directe de A-modules simples (i.e. n'ayant pas de sous-module autres que 0 et lui-même)) alors A est isomorphe à un produit direct d'anneaux de matrices sur des corps (non nécessairement commutatifs).
>
> Le petit théorème de Wedderburn admet la généralisation suivante : si A est un anneau dans lequel pour tout x il existe $n(x) \geq 2$ vérifiant $x^{n(x)} = x$ alors A est commutatif. Ce théorème est connu sous le nom de théorème de Jacobson et sa démonstration en est plutôt difficile.
>
> (Pour plus d'informations, cf. T.Y. Lam, *A First Course in Noncommutative Rings*, GTM 131.)

Valuations de $\mathbb{C}(X)$. *Une valuation (discrète normalisée non triviale) de $\mathbb{C}(X)$ (au-dessus de $\mathbb{C}$) est une application $v\colon \mathbb{C}(X) \to \mathbb{Z} \cup \{\infty\}$ vérifiant les propriétés suivantes :*
(N) v prend la valeur 1.
(C) Si $\lambda \in \mathbb{C}^*$ alors $v(\lambda) = 0$; $v(0) = \infty$.
(1) Pour $f, g \in \mathbb{C}(X)$, on a $v(fg) = v(f) + v(g)$.
(2) Pour $f, g \in \mathbb{C}(X)$, on a $v(f+g) \geq \min(v(f), v(g))$.

(L'addition et l'ordre sur $\mathbb{Z} \cup \{\infty\}$ étant définis par $k + \infty = \infty$ et $k \geq \infty$ pour tout $k \in \mathbb{Z} \cup \{\infty\}$.) Déterminer toutes les valuations (discrètes normalisées non triviales)

de $\mathbb{C}(X)$ (au-dessus de $\mathbb{C}$). Montrer la formule dite "du produit" (puisqu'il s'agit d'une somme)

$$\sum_v v(f) = 0$$

pour tout $f \in \mathbb{C}(X) \setminus \{0\}$, la somme étant prise sur toutes les valuations (discrètes normalisées non triviales) de $\mathbb{C}(X)$ (au-dessus de $\mathbb{C}$).

> **Remarque :** Inutile de dire que tout ce fatras a des généralisations faramineuses. Pour plus d'informations, cf. N. Bourbaki, *Algèbre commutative*. Signalons simplement que les valuations trouvées ci-dessus sont en correspondance bijectives avec les points de la "sphère de Riemann" $\mathbb{C} \cup \{\infty\}$; c'est pourquoi on les appelle encore les "places" de $\mathbb{C}(X)$. Plus généralement, si K est un corps algébrique sur $\mathbb{C}(X)$ et engendré par un nombre fini d'éléments sur celui-ci, on peut considérer les places de K, et les réunir en une "courbe", le corps K étant alors le corps des fonctions "rationnelles" sur cette courbe. Par ailleurs, en théorie des nombres, on s'intéresse aux valuations (discrètes normalisées non triviales) de $\mathbb{Q}$, et on montre qu'elles sont en correspondance bijective avec les nombres premiers ; pour recouvrer la formule du produit, il faut alors faire un peu plus de gymnastique (passer aux valeurs absolues...)

Théorème de Hilbert. *On dit qu'un anneau commutatif A est noethérien[*] ssi toute suite d'idéaux de A croissante pour l'inclusion est stationnaire. Montrer que cela revient à affirmer que pour tout idéal I de A il existe un nombre fini $f_1, \ldots, f_n$ d'éléments de A tels que $I = \{g_1 f_1 + \cdots + g_n f_n : g_1, \ldots, g_n \in A\} =: (f_1, \ldots, f_n)$. Montrer que A est noethérien ssi $A[X]$ l'est. Pour l'implication non triviale, on procèdera par l'absurde en choisissant pour chaque n un élément de degré minimal de I qui n'est pas dans $(f_1, \ldots, f_{n-1})$ et en considérant les coefficients dominants.*

Théorème d'inexistence de la mécanique quantique. *Soit E un espace vectoriel normé. Montrer qu'il n'existe pas d'applications linéaires continues $u, v : E \to E$ vérifiant $uv - vu = \mathrm{id}_E$.*

> **Remarque :** Pour que la mécanique quantique existe quand même, on est obligé de considérer (sur, par exemple, un espace de Hilbert) des applications linéaires définies sur des parties denses et dont le graphe est fermé plutôt que des applications linéaires continues définies sur tout l'espace.

Théorème de Banach-Steinhaus. *On rappelle le résultat suivant (théorème de Baire) : dans un espace métrique complet, toute intersection dénombrable d'ouverts denses est dense. Soit E un espace de Banach, et $(\varphi_i)_{i\in I}$ une famille de formes linéaires continues sur E telles que pour tout $x \in E$ la famille $(\varphi_i(x))$ soit bornée ; montrer qu'alors la famille $(\|\varphi_i\|)_{i\in I}$ est bornée. [Indication : considérer les fermés $\{x \in E : \forall i \in I (|\varphi_i(x)| \le n)\}$ pour $n \in \mathbb{N}$, et en particulier leur union.] Supplément : en déduire qu'une partie B d'un espace de Banach E est bornée ssi pour toute forme linéaire φ continue sur E, on a $\varphi(B)$*

[*] *En l'honneur de la mathématicienne allemande Emmy Noether.*

borné. [Indication : appliquer le théorème de Banach-Steinhaus au dual topologique E^* de E, c'est-à-dire à l'espace de Banach des formes linéaires continues sur E.]

Critère d'Eisenstein. *Soit $P = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ et p premier tel que $p | a_i$ si $i < n$, $p \not| a_n$ et $p^2 \not| a_0$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.*

Un résultat dû à Liouville. *Soit $P \in \mathbb{C}[X]$ non constant. Montrer que les racines de P' sont dans l'enveloppe convexe de celles de P.*

Contenu. *Si $P \in \mathbb{Z}[X]$, on appelle <u>contenu</u> de P et on note $c(P)$ le pgcd des coefficients de P. On dit que P est primitif ssi $c(P) = 1$. Montrer que $c(PQ) = c(P)\,c(Q)$. Montrer que les polynômes irréductibles de $\mathbb{Z}[X]$ sont de deux sortes : les polynômes primitifs irréductibles dans $\mathbb{Q}[X]$, et les nombres premiers. Montrer que l'anneau $\mathbb{Z}[X]$ est factoriel (i.e. tout élément de $\mathbb{Z}[X]$ possède une décomposition comme produit d'éléments irréductibles, unique à multiplication près par des unités).*

Exercice menant à la (vraie) géométrie. *Soit E un espace métrique compact : trouver les idéaux maximaux de l'anneau $\mathcal{C}(E, \mathbb{R})$ des fonctions continues sur E à valeurs réelles.*

Exercice un peu taupin. *On considère une suite (α_n) de nombres réels et la partie*

$$\{(x_n) : \forall n \in \mathbb{N}(|x_n| \leq \alpha_n)\}$$

de $\ell^2(\mathbb{R})$. On demande une condition nécessaire et suffisante sur les α_n pour qu'elle soit compacte.