ÉNS Lyon — Algèbre 1
L3 — 2010–2011

TD 10

Exercice 1.

1. Montrer qu'un anneau commutatif, intègre et fini est un corps.
2. Montrer qu'un anneau A est un corps si et seulement s'il admet exactement deux idéaux : $\{0\}$ et A. En déduire que tout morphisme de corps [1] est injectif.
3. Montrer que si tous les idéaux d'un anneau commutatif sont premiers, l'anneau est un corps. (*Indication :* pour montrer que x est inversible, on pourra chercher à exploiter la primalité de l'idéal (x^2).)

Exercice 2. Peut-on construire un corps K tel que les groupes additif $(K,+)$ et multiplicatif $(K^\times,\cdot)$ soient isomorphes ? (*Indication :* on pourra considérer les éléments d'ordre 2.)

Exercice 3.

1. Écrire les tables de multiplication et d'addition du corps $\mathbb{F}_4$.
2. Montrer que les anneaux $\mathbb{F}_4$, $\mathbb{F}_2 \times \mathbb{F}_2$ et $\mathbb{Z}/4\mathbb{Z}$ ne sont pas isomorphes.
3. Trouver un autre (à isomorphisme près) anneau à 4 éléments.

Exercice 4. Si K et L sont deux corps, on note $\mathrm{Hom}(K,L)$ l'ensemble des morphismes de corps de K dans L. Déterminer les ensembles de morphismes $\mathrm{Hom}(\mathbb{Q},\mathbb{C})$, $\mathrm{Hom}(\mathbb{C},\mathbb{Q})$, $\mathrm{Hom}(\mathbb{R},\mathbb{R})$ et $\mathrm{Hom}(K,L)$ quand K et L n'ont pas la même caractéristique. (*Indication :* Pour déterminer les morphismes de $\mathbb{R}$ dans lui-même, on pourra commencer par prouver qu'un réel positif doit être envoyé par un morphisme sur un réel positif, puis que le morphisme est nécessairement une fonction continue.)

Exercice 5. Soit L/K une extension de corps (*i.e.* deux corps K et L avec $K \subset L$) et $\alpha \in L$.

1. On considère l'application

$$\mathrm{év}_\alpha : \begin{array}{ccc} K[T] & \to & L \\ P & \mapsto & P(\alpha) \end{array}.$$

   Montrer que c'est un morphisme d'anneaux. On notera $K[\alpha]$ son image.
2. Montrer que $\mathrm{év}_\alpha$ est injectif si et seulement si α est transcendant (*i.e.* non algébrique) sur K et que, dans le cas contraire, $\ker \mathrm{év}_\alpha$ est engendré par un polynôme unitaire $P_\alpha \in K[T]$. Montrer qu'un tel polynôme est unique. On l'appelle le *polynôme minimal* de α sur K.
3. On note $K(\alpha)$ le plus petit-sous corps de L contenant K et α. Montrer que $K(\alpha)$ est égal à $K[\alpha]$ si α est algébrique et isomorphe au corps des fractions rationnelles $K(T)$ si α est transcendant.

[1] Un morphisme de corps est simplement un morphisme d'anneaux entre deux corps.

4. Dans chacun des cas suivants, dire si l'élément $\alpha \in L$ est algébrique ou transcendant sur K et, le cas échéant, exhiber son polynôme minimal :
   - $K = \mathbb{Q}$, $L = \mathbb{C}$, $\alpha = i$, $\alpha = \sqrt[3]{2}$, $\alpha = (1 + i\sqrt{19})/2$;
   - $K = \mathbb{C}$, $L = \mathbb{C}(X)$, $\alpha = X$, $\alpha = X^2$;
   - $K = \mathbb{C}(X^2)$, $L = \mathbb{C}(X)$, $\alpha = X$, $\alpha = X^2$.
5. On suppose que $[L : K] = \dim_K L$ est finie. Montrer qu'alors l'extension est *algébrique*, c'est-à-dire que tous les éléments de L sont algébriques sur K.
6. Soient $K \subset L \subset M$ trois corps inclus les uns dans les autres. Montrer que le degré $[M : K]$ est fini si et seulement si $[L : K]$ et $[M : L]$ le sont et que dans ce cas on a l'égalité
$$[M : K] = [M : L] \cdot [L : K].$$
7. En déduire que si L/K est une extension de corps, les éléments de L algébriques sur K forment un sous-corps de L.
8. Dans le cas $K = \mathbb{Q}$, $L = \mathbb{C}$, déterminer le polynôme minimal de $\sqrt{3} + \sqrt{2}$. (*Indication :* on pourra démontrer que $\mathbb{Q}(\sqrt{3} + \sqrt{2})$ est égal au plus petit sous-corps de $\mathbb{C}$ contenant $\sqrt{2}$ et $\sqrt{3}$, que l'on note $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.)
9. Montrer que l'ensemble
$$\overline{\mathbb{Q}} = \left\{ z \in \mathbb{C} \,\middle|\, z \text{ est algébrique sur } \mathbb{Q} \right\}.$$
est un corps dénombrable, de caractéristique nulle et algébriquement clos. En déduire l'existence d'éléments de $\mathbb{C}$ transcendants sur $\mathbb{Q}$.

Exercice 6. Si $\mathscr{P}$ est une partie de $A = \mathbb{C}[X_1, \ldots, X_n]$, on note $V(\mathscr{P})$ l'ensemble des points $(x_1, \ldots, x_n) \in \mathbb{C}^n$ tels que $\forall P \in \mathscr{P}, P(x_1, \ldots, x_n) = 0$. Le but de cet exercice est de montrer le résultat suivant, appelé *Nullstellensatz* (ou théorème des zéros de Hilbert) faible :

Théorème. Soit $I \lhd A$ un idéal différent de A tout entier. Alors $V(I)$ est non vide.

1. Montrer que pour toute partie $\mathscr{P} \subset A$, on a $V(\mathscr{P}) = V(\langle \mathscr{P} \rangle)$, où $\langle \mathscr{P} \rangle \subset A$ est l'idéal engendré par $\mathscr{P}$.
2. En déduire que de toute partie $\mathscr{P} \subset A$ on peut extraire une partie finie $\{P_1, \ldots, P_s\}$ telle que $V(\mathscr{P}) = V(\{P_1, \ldots, P_s\})$.
3. Montrer que si le Nullstellensatz faible est vrai pour les idéaux maximaux, il est vrai en général. En déduire une preuve du théorème dans le cas $n = 1$.
4. Soit donc I un idéal maximal de A et K le quotient A/I. Montrer que K est une extension de dimension au plus dénombrable de $\mathbb{C}$.
5. Montrer que la famille $(1/(T - t))_{t \in \mathbb{C}}$ est une famille libre du $\mathbb{C}$-espace vectoriel $\mathbb{C}(T)$. En déduire qu'une extension $K/\mathbb{C}$ de dimension au plus dénombrable est nécessairement algébrique et qu'alors $K = \mathbb{C}$.
6. En considérant les images $x_i \in K = \mathbb{C}$ des éléments $X_i \in A$, démontrer que $I = (X_1 - x_1, \ldots, X_n - x_n)$ et conclure la preuve du Nullstellensatz faible.
7. Démontrer que le Nullstellensatz faible devient faux si on remplace dans son énoncé $\mathbb{C}$ par un corps qui n'est pas algébriquement clos.