Université Paris-Sud
Mathématiques générales (algèbre).
D4M4U9, 2008/2009

Corrigé du TD1.

1. a) Soit R le p.g.c.d. de P et Q dans $K[X]$. Alors R est aussi dans $L[X]$, donc comme il divise P et Q dans $L[X]$, il divise le p.g.c.d. S de P et Q dans $L[X]$. D'autre part, le p.g.c.d. de P/R et Q/R dans $K[X]$ est 1, ce qui permet d'écrire une identité de Bezout, puis d'avoir

$$AP + BQ = R$$

avec A, B dans $K[X]$. Comme A, B sont aussi dans $L[X]$, on obtient que S divise R. Finalement $R = S$.

b) Comme P est irréductible, il est en particulier non constant. Comme K est de caractéristique zéro, P' est non nul et de degré $< \deg P$. Ceci implique que P et sa dérivée P' sont premiers entre eux dans $K[X]$ vu que P est irréductible. Ils le sont donc aussi dans $L[X]$ d'après a), d'où le résultat.

c) D'après ce qui précède, le seul cas ennuyeux est celui où $P' = 0$. Alors P est de la forme

$$P = a_0 + a_1 X^p + ... + a_r X^{pr}$$

Comme K est parfait, on peut écrire chaque a_i sous la forme $a_i = b_i^p$ avec $b_i \in K$. Ainsi

$$P = b_i^p + b_1^p X^p + ... + b_r^p X^{pr} = (b_1 + b_2 X + ... + b_r X^r)^p$$

vu qu'on est en caractéristique p, ce qui contredit l'irréductibilité de P.

d) On prend $K = \mathbf{Z}/2\mathbf{Z}(T)$ et $P(X) = X^2 - T$. Il est immédiat que P est irréductible car il est de degré 2 et n'a pas de racine dans K. D'autre part si a est une racine de P dans un corps de rupture L de P, on a $a^2 = T$, d'où, sur L, la factorisation

$$P(X) = X^2 - a^2 = (X - a)^2$$

vu qu'on est en caractéristique 2.

2. a) Ceci sera vu en cours, et résulte de ce que K est un espace vectoriel de dimension finie sur son sous-corps premier (lequel est de cardinal p).

b) On considère le morphisme de groupes multiplicatifs $f : x \mapsto x^2$ de K^* dans K^*. Son noyau est $\{\pm 1\}$, qui est de cardinal 2 si $p \neq 2$, et de cardinal 1 si $p = 2$. Comme $\#K^* = \#\ker f . \#\mathrm{Im}\, f$, on en déduit le résultat (en remarquant que le cardinal de K^* est $q - 1$).

c) Notons que 0 est toujours un carré dans K, donc le nombre de carrés dans K est $(q + 1)/2$. Comme a et b sont non nuls, il y a $(q + 1)/2$ éléments de la forme ax^2 dans K, et $(q + 1)/2$ éléments de la forme $1 - by^2$. Comme $(q + 1)/2 + (q + 1)/2 > \#K$, il y a au moins un élément de K qui est des deux formes ci-dessus, ce qui donne le résultat voulu.

3. a) Un calcul immédiat montre que $(H,+,.)$ est un anneau. L'inverse de $\begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$ est

$$\frac{1}{\mid a \mid^2 + \mid b \mid^2} \begin{pmatrix} \bar{a} & \bar{b} \\ -b & a \end{pmatrix}$$

qui reste dans H. D'autre part H n'est pas commutatif car les matrices obtenues en faisanr $a = 0, b = 1$ et $a = 0, b = i$ ne commutent pas. Enfin, la dimension de H sur $\mathbf{R}$ est clairement 4. Il s'agit du "corps gauche" (il vaut mieux dire *algèbre à divisions*) des *quaternions* de Hamilton.

b) En posant $x = \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix}$, on obtient $x^2 + 1 = 0$ dès que

$$a + \bar{a} = 0 \quad a^2 = b\bar{b} - 1$$

ce qui est réalisé en posant $a = i\lambda$ ($\lambda \in \mathbf{R}$) et $\mid b \mid^2 = 1 - \lambda^2$; il y a des solutions dès que $-1 \leq \lambda \leq 1$, ce qui en fait une infinité.

4. a) Si $x^m = 1$ et $y^n = 1$, alors $(xy)^{mn} = 1$. Si $x^m = 1$, alors $(x^{-1})^m = 1$. Enfin $1^1 = 1$.

b) L'application $x \mapsto e^{2i\pi x}$ est un morphisme de $(\mathbf{Q},+)$ dans $\mu(\mathbf{C})$. Il est clairement surjectif car toute racine n-ième de 1 s'écrit $e^{2i\pi(k/n)}$ avec $k \in \mathbf{Z}$. Comme son noyau est $\mathbf{Z}$, le résultat découle du théorème de factorisation.

Remarque : En fait le groupe de toutes les racines de l'unité d'un corps algébriquement clos de caractéristique zéro K est toujours isomorphe à $\mathbf{Q}/\mathbf{Z}$ (plus difficile...).