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

Corrigé de la feuille de TD numéro 2.

1. a) Par définition du corps de rupture, Q possède une racine x dans F, qui est aussi une racine de P car Q divise P. Posons $M = K[x]$, alors M est un corps de rupture de P sur K, on a donc $[M : K] = n$. Comme $M \subset F$ (puisque F contient K et x), la multiplicativité des degrés donne que n divise $[F : K]$.

b) On a $[F : K] = [F : L].[L : K]$, ce qui montre d'après a) que n divise $m[F : L]$. Comme n est premier avec m, il divise $[F : L]$. Mais $[F : L]$ n'est autre que le degré de Q car F est un corps de rupture de Q sur L. Ainsi Q est de degré divisible par $n = \deg P$, et comme $P = QR$, on obtient que R est constant. Finalement, les seuls facteurs irréductibles de P sur L ont même degré que P, ce qui montre que P est irréductible sur L.

2. a) Les polynômes P et Q sont irréductibles avec K de caractéristique zéro. Ils n'ont donc pas de racine multiple d'après l'exercice 1)b) de la feuille numéro 1.

b) Il suffit de prendre t non nul différent de tous les $\frac{x-x_i}{y_j-y}$, ce qui est possible parce que K est infini (il est de caractéristique zéro); noter aussi que $y_j - y$ est bien non nul d'après a).

c) Comme P est à coefficients dans $K \subset K'$ et $z - tX$ est un polynôme à coefficients dans K', on a bien $F \in K'[X]$. On observe déjà que $X - y$ divise Q, et il divise également F car $F(y) = F(x) = 0$. Pour montrer que $X - y$ est le pgcd de Q et F, on peut faire le calcul dans M, corps sur lequel Q est scindé à racines simples d'après a); il s'agit alors de montrer que $(X - y_j)$ ne divise pas F, i.e. que $F(y_j) \neq 0$. Mais si on avait $F(y_j) = F(z - ty_j) = 0$, alors $z - ty_j = x + ty - ty_j$ serait égal à x ou à l'un des x_i, ce qui est exclu d'après b).

d) Comme F et Q sont dans $K'[X]$, leur pgcd $X - y$ aussi, ce qui impose $y \in K'$. Comme K' contient z, t, et y, il contient aussi x, donc aussi $L = K[x, y]$. Finalement $L = K'$ car l'inclusion $K' \subset L$ est évidente.

e) On peut écrire $F = K[x_1, ..., x_n]$. Supposons $n \geq 2$; en écrivant $F = F'[x_{n-1}, x_n]$, où F' est le corps $K[x_1, ..., x_{n-2}]$ (il s'agit bien d'un corps car tous les x_i sont algébriques sur K), on peut appliquer d) pour obtenir que F s'écrit $F = K'[z_{n-1}] = K[x_1, ..., x_{n-2}, z_{n-1}]$. On obtient alors le résultat en raisonnant par récurrence sur n.

3. 1. Il suffit de montrer que Q et Q' sont premiers entre eux. Or la dérivée de Q est -1 car q^n est divisible par la caractéristique p de $\mathbf{F}_q$ (c'est même une puissance de p) d'où le résultat.

2. a) Le dit corps de rupture a pour degré d sur $\mathbf{F}_q$, donc son cardinal est q^d. En particulier $x^{q^d} = x$ comme on l'a vu en cours (cette équation est satisfaite par tous les éléments d'un corps de cardinal q^d). Comme $n = ed$ avec e entier, on a $x^{q^n} = x$ (en élevant $e - 1$ fois à la puissance q^d l'égalité $x^{q^d} = x$).

b) Prenons comme corps de de rupture de P le corps $\mathbf{F}_q[X]/(P)$, et comme racine la classe $x = \overline{X}$ de X. En appliquant a), on obtient que $Q(\overline{X}) = 0$ ou encore $\overline{Q(X)} = 0$, ce qui signifie exactement que P divise Q.

3. a) C'est le même argument que celui vu en cours quand $q = p$: l'ensemble R des racines de Q dans K est déjà un corps (facile en utilisant le fait qu'on est en caractéristique p) donc $R = K$. Du coup K est de cardinal q^n (le degré de Q) vu que Q est scindé à racines simples dans K. Notons que cela implique que $[K : \mathbf{F}_q] = n$ car K est isomorphe à $\mathbf{F}_q^{[K:\mathbf{F}_q]}$ comme $\mathbf{F}_q$-ev.

b) Il suffit de prendre le corps $\mathbf{F}_q[a]$, où a est une racine de a dans K.

c) Par multiplicativité des degrés, le degré sur $\mathbf{F}_q$ du corps de rupture (cf. b)) divise le degré de K sur $\mathbf{F}_q$. Avec a), on obtient que s divise n.

4. La question 2.b) dit que tout polynôme irréductible unitaire dont le degré divise n divise aussi Q, donc est l'un des P_i (par unicité de la décomposition en produit d'irréductibles). La question 3.c) dit réciproquement que chaque P_i a un degré divisant n (et les P_i sont irréductibles unitaires) d'où le résultat.

5. On écrit que le degré de Q est la somme des degrés des P_i. On obtient alors le résultat avec 4., en regroupant les P_i par leur degré.