Corrigé de l'EXAMEN du 29 janvier 2004

I

1. Il suffit de montrer qu'il existe un élément transcendant dans $k(X)$ pour montrer que l'extension $k(X)|k$ n'est pas algébrique. L'élément X est transcendant. En effet, l'homomorphisme d'anneaux $k[T] \mapsto k(X)$ qui à $P(T)$ associe $P(X)$ est injective. Comme toute extension finie est algébrique, l'extension $k(X)|k$ est infinie.

Le fait que G est un groupe est une question de cours.

2. On a $\sigma_Y(1) = 1$, $\sigma_Y(F_1 + F_2) = (F_1 + F_2)(Y) = F_1(Y) + F_2(Y) = \sigma_Y(F_1) + \sigma_Y(F_2)$ et, par un calcul analogue, $\sigma_Y(F_1F_2) = \sigma_Y(F_1)\sigma_Y(F_2)$ (F_1, $F_2 \in k(X)$).

3. Comme Y est de degré d, l'un des deux polynômes U ou V est de degré d. Notons a et b les coefficients de degré d de U et V. Le coefficient de degré d de S est $a - bY$ et le degré de Y est $\leq d$. Comme a et b sont dans k et que Y n'est pas dans k, et que a et b ne sont pas tous les deux nuls, $a - bY$ est non nul ; c'est donc le coefficient dominant de S, qui est donc de degré d.

On a $S(X) = U(X) - YV(X) = U(X) - (U(X)/V(X))V(X) = 0$.

Comme l'extension $k(X)|k$ est engendrée par X sur k, et que $k(Y)$ contient k, l'extension $k(X)|k(Y)$ est engendrée par X. Comme X est racine d'un polynôme de degré $\leq d$ sur $k(Y)$, l'extension $k(X)|k(Y)$ est de degré $\leq d$.

4. Pour montrer que le degré de cette extension est > 1, il suffit de montrer que $k(X)$ est différent de $k(Y)$. Montrons que X n'appartient pas à $k(Y)$. Supposons que X s'écrive $X = F(Y)$ avec $F \in K(Y)$. Posons $Y = U/V$ comme dans la question **3**. Observons que $K(Y) = K(1/Y)$. Quitte à changer Y en $1/Y$, on peut supposer que le degré de U est supérieur ou égal au degré de V. Nous allons donc montrer que le degré d de U est 1.

Soient x_1, x_2 ... x_d les zéros de U dans $\bar{k}$ comptés avec multiplicités. On a donc $X - F(0) = F(U/V) - F(0)$. Le polynôme de gauche a un unique zéro en $F(0)$, le polynôme de droite a, entre autres, pour zéros (comptés avec multiplicité) x_1, x_2 ... x_d. On a donc $d = 1$.

5. Examinons la situation pour $Y = X^2 + 1$. Comme $\mathbf{R}$ est un corps de caractéristique 0, l'extension $k(X)|k(Y)$ est séparable. L'extension $k(X)|k(Y)$ est de degré ≤ 2 et > 1, c'est donc une extension de degré 2. On a vu en cours que les extensions de degré 2 sont normales. L'extension $k(X)|k(Y)$ est donc galoisienne.

Dans le cas $Y = X^3 + 1$, l'extension est bien séparable. Mais, elle n'est pas normale. En effet, le polynôme $T^3 + 1 - Y \in k(Y)[T]$ admet X comme racine dans $\mathbf{R}(Y)$ et jX et j^2X dans $\mathbf{C}(Y)$ (où $j = e^{2i\pi/3}$). Or on a $jX \notin \mathbf{R}(Y)$.

6. Pour que σ_Y soit un automorphisme il faut et il suffit que ce soit une bijection, car on sait que c'est un homomorphisme d'anneaux d'après **2**.

Pour que σ_Y soit un automorphisme, il faut que l'image de σ_Y soit $k(X)$, c'est-à-dire que $k(X) = k(Y)$. Cela impose que le degré de Y est 1 d'après la question **4**.

Supposons le degré de Y égal à 1. Posons $Y = (aX + b)/(cX + d)$ avec a, b, c et $d \in k$ et $ad - bc \neq 0$. L'homomorphisme σ_Y est injectif. En effet son noyau est un idéal de $k(X)$, qui est un corps et n'a donc pour idéal que 0 et lui-même. Comme σ_Y n'est pas identiquement nul, c'est un homorphisme injectif. Il est surjectif, en effet, il suffit pour cela de montrer que $k(Y)$ contient X. Comme $Y = (aX + b)/(cX + d)$, on a $X = (dX - b)/(-cX + a)$ et donc $X \in k(Y)$.

7. Montrons qu'on a un homomorphisme de groupes. On a $\sigma_{(aX+b)/(cX+d)} \circ \sigma_{(a'X+b')/(c'X+d')}(F) = \sigma_{(aX+b)/(cX+d)}(F((a'X+b')/(c'X+d'))) == \sigma_{(AX+B)/(CX+D)}$, où $\begin{pmatrix} A & C \\ B & D \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}$, par un calcul direct.

Le noyau de ϕ est formé par les matrices $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ telle que $(aX+b)/(cX+d) = X$, c'est-à-dire telles que $c = 0$, $b = 0$, $a = d \in k^*$.

8. C'est l'image par l'homomorphisme de la question **7** de l'ensemble $\{\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} / b \in k\}$ qui est un sous-groupe de $\mathrm{GL}_2(k)$. C'est donc un sous-groupe de G.

II

1. C'est $q(q+1)(q-1)^2$. Le noyau de l'homomorphisme ϕ de la question **7** a pour ordre $q-1$. Par conséquent G a pour ordre $q(q+1)(q-1)$.
2. Un p-sous groupe de Sylow de G a pour ordre la plus grande puissance de p qui divise $q(q+1)(q-1)$, c'est-à-dire q. Or G_0 a même ordre que k c'est-à-dire q.
3. C'est $\mathbf{Z}/n\mathbf{Z}$ (cours).
4. Comme l'extension $\mathbf{F}_q|\mathbf{F}_p$ est galoisienne, tout élément de G' laisse stable $\mathbf{F}_q$. Par conséquent on a bien un homomorphisme de groupes $G' \to H$. Le noyau de cet homomorphisme est formé par les éléments qui opèrent trivialement sur $\mathbf{F}_q$. Il est bien constitué par les éléments de G.
5. On a $k(X)^G \subset k(X)^{G_0} \subset k(X)$, car $\{1\} \subset G_0 \subset G$.
6. Il suffit de démontrer cela lorsque F est un polynôme, en effet toute fraction rationnelle est quotient de deux polynômes. On a $a^q = a$ $(a \in \mathbf{F}_q)$. Posons $F(X) = a_0 + a_1X + ... + a_dX^d$. On a $F(X)^q = a_0^q + a_1^qX^q + ... + a_d^qX^{dq} = a_0 + a_1X^q + ... + a_dX^{dq} = F(X^q)$.

On a donc pour $b \in k$, $\sigma_{X+b}(X^q - X) = (X+b)^q - (X+b) = X^q - X + b^q - b = X^q - X$.
7. C'est un calcul direct (mais un peu fastidieux) utilisant l'identité $F(X)^q = F(X^q)$.