Université Paris 7-Denis Diderot
M1 mathématiques

Algèbre – Année 2005-06
F. Conduché - M. Couillens - L. Merel

CORRIGÉ de l'EXAMEN du 13 janvier 2006

I

1. On a $\Phi_3^+(X) = X + 1$ et $\Phi_5^+(X) = X^2 + X - 1$.
2. Le polynôme $\Phi_p^+(X)$ est produit de $(p-1)/2$ facteurs de degré 1. Il est de degré $(p-1)/2$.
3. On a $X^{(p-1)/2}\Phi_p^+(X+1/X) = \prod_{\zeta\in\mu_p^+}(X^2+1-\zeta X-\zeta^{-1}X) = \prod_{\zeta\in\mu_p^+}(X-\zeta)(X-\zeta^{-1}) = \Phi_p(X)$. En effet, on la réunion disjointe $\mu_p = \mu_p^+ \cup \mu_p^-$, où $\mu_p^- = \{\zeta^{-1}/\zeta \in \mu_p^+\}$ (car $p \neq 2$).
4. Supposons que $\Phi_p^+(X) = \sum_{n=0}^{(p-1)/2} a_n X^n \notin \mathbf{Z}[X]$. Soit n_0 le plus grand entier tel que $a_{n_0} \notin \mathbf{Z}$. On a $X^{(p-1)/2}a_n(X+1/X)^n \in \mathbf{Z}[X]$ lorsque $n > n_0$ et $\Phi_p(X) = X^{(p-1)/2}\Phi_p^+(X+1/X) \in \mathbf{Z}[X]$. On a donc $\sum_{n=0}^{n_0} a_n(X+1/X)^n \in \mathbf{Z}[X]$. Le terme de plus haut degré de ce dernier polynôme est $a_{n_0}X^{n_0+(p-1)/2}$. On a donc $a_{n_0} \in \mathbf{Z}$. Contradiction.
5. Si $\Phi_p^+(X)$ est réductible sur $\mathbf{Q}$, il existe A, $B \in \mathbf{Z}[X]$ non constants de degrés a et b respectivement tels que $\Phi_p^+ = AB$. On a $a+b = (p-1)/2$ et $\Phi_p(X) = X^{(p-1)/2}\Phi_p^+(X+1/X) = X^aA(X+1/X)X^bB(X+1/X)$. Or $X^aA(X+1/X)$ et $X^bB(X+1/X)$ sont des polynômes non constants de $\mathbf{Z}[X]$ de produit Φ_p. Cela contredit l'irréductibilité de Φ_p.

II

1. Comme le polynôme Φ_p^+ est irréductible sur $\mathbf{Q}$ et de degré $(p-1)/2$ ses corps de rupture sont tous de degré $(p-1)/2$ sur $\mathbf{Q}$.
2. Comme $\mathbf{C}$ est algébriquement clos, il y a $(p-1)/2$ tels plongements.
3. Les valeurs possibles de $\sigma(\zeta_0+\zeta_0^{-1})$ sont les racines de Φ_p^+ : les nombres de la formes $\zeta+\zeta^{-1}$ ($\zeta \in \mu_p^+$).
4. Lorsque $\sigma(\zeta_0+\zeta_0^{-1}) = \zeta+\zeta^{-1}$, avec $\zeta \in \mu_p^+$. L'image de σ est $\mathbf{Q}(\zeta+\zeta^{-1})$. Il suffit de montrer que $\zeta+\zeta^{-1} \in \mathbf{R}$. Cela découle du fait que le conjugué complexe de ζ est ζ^{-1}.
5. Cela résulte du fait que ζ_0, $\zeta_0^{-1} \in \mathbf{Q}(\mu_p)$.

III

1. Le groupe $\{\sigma_1, \sigma_{-1}\}$ est un sous-groupe d'ordre 2 de $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$, qui est un groupe d'ordre $p-1$. L'extension $\mathbf{Q}(\mu_p)^+|\mathbf{Q}$ est de degré l'indice de $\{\sigma_1, \sigma_{-1}\}$ dans $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$. Cet indice est $(p-1)/2$.
2. L'élément σ_{-1} échange ζ_0 et ζ_0^{-1}. On a donc $\sigma_{-1}(\zeta_0+\zeta_0^{-1}) = \zeta_0+\zeta_0^{-1}$. C'est pourquois $\zeta_0+\zeta_0^{-1} \in \mathbf{Q}(\mu_p)^+$ et donc $\mathbf{Q}(\zeta_0+\zeta_0^{-1}) \subset \mathbf{Q}(\mu_p)^+$.
3. Comme $\mathbf{Q}(\mu_p)^+$ et $\mathbf{Q}(\zeta_0+\zeta_0^{-1})$ sont de même degré sur $\mathbf{Q}$, ils sont égaux (compte-tenu de $\mathbf{Q}(\zeta_0+\zeta_0^{-1}) \subset \mathbf{Q}(\mu_p)^+$). Le corps $\mathbf{Q}(\mu_p)^+$ contient toutes les racines de $\Phi_p^+(X)$. En effet, $\sigma_{-1}(\zeta+\zeta^{-1}) = \zeta+\zeta^{-1}$ pour tout $\zeta \in \mu_p{}^+$. Donc $\mathbf{Q}(\mu_p)^+$ est bien le sous-corps de $\mathbf{C}$ engendré par toutes les racines de $\Phi_p^+(X)$.
4. L'extension $\mathbf{Q}(\mu_p)^+|\mathbf{Q}$ est galoisienne car elle est séparable (les corps sont de caractéristique 0) et normale ($\mathbf{Q}(\mu_p)^+$ est un corps de décomposition sur $\mathbf{Q}$).
5. Le groupe de Galois s'identifie à $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})/\{\sigma_1, \sigma_{-1}\}$, qui s'identifie à $(\mathbf{Z}/p\mathbf{Z})^*/\{-1, 1\}$.

IV

1. Posons $P(X) = \prod_{i=1}^r(X-\alpha_i) = \prod_{n=0}^r a_nX^n$ et $Q(X) = \prod_{j=1}^s(X-\beta_j) = \prod_{m=0}^s b_mX^m$. On a $\mathrm{R}(P,Q) = \prod_{i,j}(\alpha_i-\beta_j)$. Ce produit comporte rs facteurs. Si on échange les α_i et les β_j, il est modifié par un facteur $(-1)^{rs}$.

Par ailleurs, $R(P,Q)$ est un polynôme à coefficients dans $\mathbf{Z}$ en les a_n et les b_m. Par conséquent la réduction modulo q de $R(P,Q)$ est la valeur de la réduction modulo q de ce polynôme. Cette valeur est le résultant de $\tilde{P}$ et $\tilde{Q}$.

2. On a $\tilde{\Phi}_q(X) = (X^q-1)/(X-1) = (X-1)^q/(X-1) = (X-1)^{q-1}$. Par conséquent, on a $\tilde{\Phi}_q^+(X) = (X-2)^{(q-1)/2}$. On a donc $\mathrm{R}(\tilde{\Phi}_q^+, \tilde{\Phi}_p^+) = \mathrm{R}((X-2)^{(q-1)/2}, (\tilde{\Phi}_p^+) = \prod_{i=1}^{(q-1)/2} \tilde{\Phi}_p^+(2) = \prod_{i=1}^{(q-1)/2} \tilde{\Phi}_p^+(1+1) = \prod_{i=1}^{(q-1)/2} \tilde{\Phi}_p(1) = \tilde{p}^{(q-1)/2}$.

3. Considérons l'homomorphisme de groupe $\phi : (\mathbf{Z}/q\mathbf{Z})^* \to (\mathbf{Z}/q\mathbf{Z})^*$ qui à a associe $a^{(q-1)/2}$. Comme $a^{q-1} = 1$, on a $a^{(q-1)/2} = \pm 1$ ($a \in (\mathbf{Z}/q\mathbf{Z})^*$). L'homomorphisme ϕ est donc à valeurs dans $\{-1, 1\}$. Il y a $(q-1)/2$ éléments d'ordre $(q-1)/2$ dans le groupe cyclique $(\mathbf{Z}/q\mathbf{Z})^*$ d'ordre $q-1$. Par conséquent, le noyau de ϕ est un sous-groupe d'ordre $(q-1)/2$. Par ailleurs, tout élément a qui est un carré, *i.e.* qui s'écrit $a = b^2$ avec $b \in (\mathbf{Z}/q\mathbf{Z})^*$) est dans le noyau de ϕ, car $\phi(a) = a^{(p-1)/2} = b^{p-1} = 1$. Or il y a $(p-1)/2$ tels carrés, donc $\{a/\phi(a) = 1\}$ est l'ensemble des carrés de $(\mathbf{Z}/q\mathbf{Z})^*$.

4. On utilise d'abord la formule $\mathrm{R}(\Phi_q^+, \Phi_p^+) = \prod_{\lambda \in \mu_q^+} \Phi_p^+(\lambda + \lambda^{-1})$. Utilisons ensuite la formule reliant Φ_p^+ à Φ_p : on a $\Phi_p^+(\lambda + \lambda^{-1}) = \lambda^{-(p-1)/2}\Phi_p(\lambda) = \lambda^{(p-1)/2}\Phi_p(\lambda^{-1})$. En utilisant ces deux expressions, on obtient $\mathrm{R}(\Phi_q^+, \Phi_p^+)^2 = \prod_{\lambda \in \mu_q^+} \lambda^{-(p-1)/2}\Phi_p(\lambda)\lambda^{(p-1)/2}\Phi_p(\lambda^{-1}) = \prod_{\lambda \in \mu_q} \lambda^{-(p-1)/2}\Phi_p(\lambda)$.

On a $\prod_{\lambda \in \mu_q} \lambda^{-(p-1)/2}\Phi_p(\lambda) = (\prod_{\lambda \in \mu_q} \lambda)^{-(p-1)/2}(\prod_{\lambda \in \mu_q} (\lambda^p - 1)/(\lambda - 1))$. Le premier facteur est égal à 1 (on regroupe λ avec λ^{-1}). Lorsque λ parcourt μ_q, λ^p parcourt encore μ_q, si bien que le second facteur vaut aussi 1. On a donc $\mathrm{R}(\Phi_q^+, \Phi_p^+)^2 = 1$ et donc $\mathrm{R}(\Phi_q^+, \Phi_p^+)^2 \in \{-1, 1\}$.

5. Deux entiers distincts qui sont congrus modulo q diffèrent d'au moins q. Or les questions précédentes entraînent que les entiers $\mathrm{R}(\Phi_q^+, \Phi_p^+)$ et $\left(\frac{p}{q}\right)$ sont congrus modulo q et sont contenus dans $\{-1, 1\}$. Comme $q > 2$, ces entiers sont égaux.

On a, puisque les polynômes Φ_p^+ et Φ_q^+ sont de degrés $(p-1)/2$ et $(q-1)/2$ respectivement, $\left(\frac{p}{q}\right) = \mathrm{R}(\Phi_q^+, \Phi_p^+) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\mathrm{R}(\Phi_p^+, \Phi_q^+) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$.