

Pierre Lissy

April 29, 2010

Soit  $K$  un corps de décomposition de  $\Phi_n$  sur  $\mathbb{Q}$ . et  $\zeta \in K$  une racine  $n$ -ième primitive de 1. Soit  $p$  un nombre premier, ne divisant pas  $n$ . Alors  $\zeta^p$  est encore une racine primitive de l'unité.

Considérons dorénavant  $f \in \mathbb{Q}[X]$  (resp  $g$ ) le polynôme minimal de  $\zeta$  (resp.  $\zeta^p$ ) sur  $\mathbb{Q}$ . Alors  $f$  et  $g$  sont nécessairement des polynômes à coefficients entiers. En effet, par le théorème de transfert de Gauss, l'anneau  $\mathbb{Z}[X]$  est factoriel et on a  $\Phi_n(X) = f_1(X)^{\alpha_1} \dots f_r(X)^{\alpha_r}$  avec  $f_i \in \mathbb{Z}[X]$  irréductible. Comme  $\Phi_n$  est unitaire, on peut supposer quitte à multiplier par -1 que les  $f_i$  le sont aussi. Mais alors  $\zeta$  est nécessairement racine de l'un de ses  $f_i$  unitaire irréductible sur  $\mathbb{Z}$ , donc sur  $\mathbb{Q}$ , et le polynôme minimal est ce  $f_i$ . De même pour  $g$ .

Montrons que  $f = g$ . Sinon, comme  $f$  et  $g$  sont irréductibles et distincts, le produit  $fg$  divise  $\Phi_n$ . Par ailleurs, comme  $g(\zeta^p) = 0$ , ce signifie que  $f$  divise  $g(X^p)$  dans  $\mathbb{Q}[X]$ .  $fh = g$ . Posons de la manière habituelle  $h = a/bh'$  avec  $a$  et  $b$  premiers entre eux et  $h'$  à coefficients entiers primitif (on prend si  $h = \sum a_i/b_i X^i$ , pour  $b$  un ppcm des  $b_i$ , pour  $a$  un pgcd des  $a_i$  et on simplifie éventuellement la fraction obtenue). En passant au contenu, on a  $ac(f)c(h') = bc(g)$  et donc comme  $f$  et  $g$  sont unitaires ils sont primitifs et on obtient  $a = b$ , et donc  $h = h'$  et  $h$  est bien à coefficients entiers.

On projette alors l'égalité dans  $\mathbb{F}_p$ : on note  $\bar{g}, \bar{h}, \bar{f}$  les polynômes correspondant et on utilise le morphisme de Frobenius qui dit que modulo  $p$  on a  $\bar{g}(X^p) = (\bar{g}(X))^p$ . Donc  $\bar{g}(X)^p = \bar{f}\bar{h}$ . De plus, par propriété de la réduction modulo  $p$ , si l'on considère un facteur irréductible  $\varphi$  de  $\bar{f}$ , par le lemme d'Euclide on a  $\varphi | \bar{g}$ . Comme  $fg$  divise  $\Phi_n$  sur  $\mathbb{Z}$ ,  $\bar{f}\bar{g}$  divise  $\bar{\Phi}_n$  sur  $\mathbb{F}_p$ , mais on sait que la réduction du polynôme cyclotomique correspond au polynôme cyclotomique dans  $\mathbb{F}_p$ . Donc  $\varphi^2$  divise  $\bar{\Phi}_n$ , mais dans un corps de décomposition  $\varphi$  a forcément une racine, on obtiendrait donc que  $\bar{\Phi}_n$  aurait une racine double dans un corps de décomposition, ce qui est impossible par propriété des polynômes cyclotomiques lorsque la caractéristique  $p$  est première à  $n$ . Ainsi,  $f = g$ .

On conclut de la manière suivante. Soit  $\zeta' = \zeta^m$  une racine primitive  $n$ -ième de l'unité, avec  $m$  tel que  $m$  et  $n$  sont premiers entre eux. On écrit  $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ . Aucun des  $p_i$  ne divise  $n$ , donc d'après le point précédent, on a avec une récurrence assez immédiate que  $\zeta'$  a le même polynôme minimal que  $\zeta$ , à savoir  $f$ . En effet, on récrit  $m$  sous la forme  $m'p_1$ . Alors on a encore  $m'$  et  $n$  premiers entre eux, donc  $\zeta'^{m'}$  est une racine primitive  $n$ -ième de l'unité et par ce qu'on a fait précédemment les nombres  $\zeta'^{m'}$  et  $\zeta'^m$  ont même polynôme minimal. On amorce donc une récurrence sur  $\sum_p v_p(m)$ , qui est déjà initialisée et dont la transmission se fait comme indiquée au-dessus. Ainsi,  $f$  a au moins  $\varphi(n)$  racines et divise un polynôme de degré  $\varphi(n)$  qui est  $\Phi_n$ , donc nécessairement  $f = \Phi_n$  et ce dernier est irréductible.

## References

[1]