Automorphismes d'un corps cyclotomique

Aurélien Guerder

2023-2024

Source : LESESVRE, MONTAGNON, LE BARBENCHON, PIERRON, 131 développements pour l'oral

Notons μ_n le groupe des racines n-ièmes de 1 dans $\mathbb{C}$. Soit $\xi \in \mu_n$ primitive (c'est-à-dire d'ordre n) et G le groupe des $\mathbb{Q}$-automorphismes de corps de $\mathbb{Q}(\xi)$.

Dans un premier temps, nous allons décrire les $\mathbb{Q}$-automorphismes de corps de $\mathbb{Q}(\xi)$. Il suffit pour cela de les décrire sur μ_n car celui-ci est une famille génératrice de $\mathbb{Q}(\xi)$.

Théorème 1. *$\forall \sigma \in G$, il existe un unique $a_\sigma \in (\mathbb{Z}/n\mathbb{Z})^\times$ tel que $\forall x \in \mu_n, \sigma(x) = x^{a_\sigma}$.*

Démonstration. Soit $\sigma \in G$. Alors $\sigma(\xi)^n = \sigma(\xi^n) = \sigma(1) = 1$ et $\forall k \in [\![1, n-1]\!], \sigma(\xi)^k = \sigma(\xi^k) \neq 1$, d'où $\sigma(\xi)$ est d'ordre n. De plus, comme ξ est primitive, elle engendre le groupe μ_n donc il existe $k \in \mathbb{Z}$ tel que $\sigma(\xi) = \xi^k$ et comme l'ordre de $\sigma(\xi)$ est n, $k \wedge n = 1$ d'où $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$.
Soit $x = \xi^k \in \mu_n$. Alors $\sigma(x) = \sigma(\xi)^l = \xi^{kl} = x^k$ et on a donc l'existence avec $\overline{k} = a_\sigma$.
Pour l'unicité, si b_σ convient, on a alors $\xi^{a_\sigma - b_\sigma} = 1$ donc comme ξ est primitive, $a_\sigma - b_\sigma = 0$ dans $\mathbb{Z}/n\mathbb{Z}$. □

Maintenant, nous allons décrire la structure du groupe G.

Proposition 1. *Si p est premier ne divisant pas n, alors ξ et ξ^p ont le même polynôme minimal dans $\mathbb{Q}[X]$.*

Remarque : ici, on n'a pas besoin de supposer ξ primitive.

Pour prouver cette proposition, on aura besoin d'une version du lemme de Gauss :

Lemme 1. *Soit $P, Q \in \mathbb{Q}[X]$. Si P et Q sont unitaires et si PQ est à coefficients entiers, alors P et Q sont à coefficients entiers.*

Démonstration. (de la Proposition) Soit f (respectivement g) le polynôme minimal de ξ (resp. ξ^p) sur $\mathbb{Q}$. Par l'absurde, supposons que $f \neq g$.

Etape 1 : f et g sont à coefficients entiers :
f et g sont des polynômes minimaux donc ils sont irréductibles. Or, ils divisent $X^n - 1$ (car ξ et ξ^p en sont racines) et sont distincts et unitaires, donc $fg | X^n - 1$. Soit $h \in \mathbb{Q}[X]$ tel que $fgh = X^n - 1$. f, g, h sont unitaires, et $X^n - 1 \in \mathbb{Z}[X]$ donc par le lemme de Gauss, ils sont à coefficients entiers.

Etape 2 : $\overline{f}$ et $\overline{g}$ (modulo p) sont premiers entre eux :
On a $\overline{f}\,\overline{g} | X^n - 1$. Or $(X^n - 1)' = nX^{n-1} \neq 0$ car p ne divise pas n, donc comme $X^n - 1 \wedge X^{n-1} = 1$, $X^n - 1$ est à racines simples dans une clôture algébrique. Donc $\overline{f}$ et $\overline{g}$ n'ont pas de racine commune dans une

clôture algébrique et donc $\overline{f} \wedge \overline{g} = 1$.

Etape 3 : Conclusion
Comme $g(X^p)$ annule ξ, $f | g(X^p)$. Il existe donc $k \in \mathbb{Q}[X]$ tel que $kf = g(X^p)$ et par le lemme de Gauss, $k \in \mathbb{Z}[X]$. Modulo p, on a que $\overline{g}(X^p) = \overline{g}^p$ donc $g^p = \overline{f}\,\overline{k}$, donc un facteur irréductible de $\overline{f}$ divise $\overline{g}$, ce qui contredit l'étape 2, d'où la contradiction. □

Théorème 2.

$$\begin{array}{ccccc} \psi & : & G & \to & (\mathbb{Z}/n\mathbb{Z})^\times \\ & & \sigma & \mapsto & a_\sigma \end{array}$$

est un isomorphisme.

Démonstration. Etape 1 : Morphisme :
Soit $\sigma, \tau \in G$. On a $(\sigma \circ \tau)(\xi) = \xi^{a_{\sigma\tau}}$ et $\sigma(\tau(\xi)) = \sigma(\xi^{a_\tau}) = \xi^{a_\sigma a_\tau}$.
Par l'unicité dans le théorème 1, $a_{\sigma\tau} = a_\sigma a_\tau$.

Etape 2 : Injectivité :
Soit $\sigma \in \ker\psi$, c'est-à-dire $a_\sigma = 1$. Alors $\sigma(\xi) = \xi$ et donc $\forall x \in \mathbb{Q}(\xi), \sigma(x) = x$ d'où $\sigma = \mathrm{id}$.

Etape 3 : Surjectivité : Attention, c'est la partie difficile.
Montrons qu'un $\mathbb{Q}$-morphisme σ de $\mathbb{Q}(\xi)$ est un $\mathbb{Q}$-automorphisme si et seulement si ξ et $\sigma(\xi)$ ont le même polynôme minimal :
D'une part, si ξ et $\sigma(\xi)$ ont le même polynôme minimal f, alors $\sigma(\xi)$ est d'ordre n : comme ξ est d'ordre n, on a f divise $X^n - 1$ mais pas $X^k - 1$ pour $k < n$ donc $\sigma(\xi)$ n'est pas racine de $X^k - 1$ pour $k < n$, d'où les racines de f sont toutes d'ordre n. $\sigma(\xi)$ engendre donc μ_n et donc σ est surjectif.
D'autre part, si σ est un $\mathbb{Q}$-automorphisme, si $f \in \mathbb{Q}[X]$, on a $f(\sigma(\xi)) = \sigma(f(\xi))$ et donc $\sigma(\xi)$ et ξ ont les mêmes polynômes annulateurs donc le même polynôme minimal.
Pour conclure, on va montrer que $\forall a \in (\mathbb{Z}/n\mathbb{Z})^\times$, ξ et ξ^a ont le même polynôme minimal.
Soit $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Notons $a = p_1 \ldots p_r$ où les p_i sont premiers. Comme $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $\forall i, p_i$ ne divise pas n. Donc ξ et ξ^{p_1} ont le même polynôme minimal d'après la proposition 1, et $\xi^{p_1} \in \mu_n$. On réitère avec ξ^{p_1} et $\xi^{p_1 p_2}$, etc... par récurrence. On obtient finalement que ξ et ξ^a ont le même polynôme minimal, d'où le $\mathbb{Q}$-morphisme σ défini par $\sigma(\xi) = \xi^a$ est un $\mathbb{Q}$-automorphisme et on a $\sigma \in G$ et $a_\sigma = \overline{a}$.
□

Ce développement est long et technique. On peut le raccourcir si besoin par exemple en s'arrêtant à l'injectivité, ou en admettant le résultat montré dans la preuve de la surjectivité.