

Développement : Intersection de corps cyclotomiques

Étienne PEILLON

Pour tout entier naturel non nul t , on désigne par ζ_t une racine primitive t -ème de l'unité. L'objectif est de montrer la propriété suivante sur les extensions cyclotomiques de $\mathbb{Q}$.

Proposition

Soient p, q deux entiers non nuls, on note $N = \text{ppcm}(p, q)$ et $d = \text{pgcd}(p, q)$. Alors $\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_q) = \mathbb{Q}(\zeta_N)$ et $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}(\zeta_d)$.

Pour ce faire, on va avoir besoin du résultat préliminaire suivant.

Lemme

Soient k un corps, L une extension et K, F deux corps intermédiaires. Alors KF , le corps engendré par K et F , vérifie $[KF : F] \leq [K : k]$.

Le recasage est le suivant :

- ***** 125 : Extensions de corps. Exemples et applications.
- ***** 127 : Exemples de nombres remarquables. Exemples d'anneaux de nombres remarquables. Applications.
- ***** 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.
- ***** 148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
- **** 102 : Groupe des nombres complexes de module 1. Racines de l'unité. Applications.
- *** 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Développement

Partie 1 : produit de corps. Le résultat est clair si $[K : k] = \infty$. Si $d = [K : k]$ est fini, alors il existe $e_1, \dots, e_d \in K$ formant une k -base de K . Or

$$F[K] = \left\{ \sum_{i=1}^n f_i k_i, n \in \mathbb{N}, f_i \in F, k_i \in K \right\} = \left\{ \sum_{i=1}^d f_i e_i, f_i \in F \right\}.$$

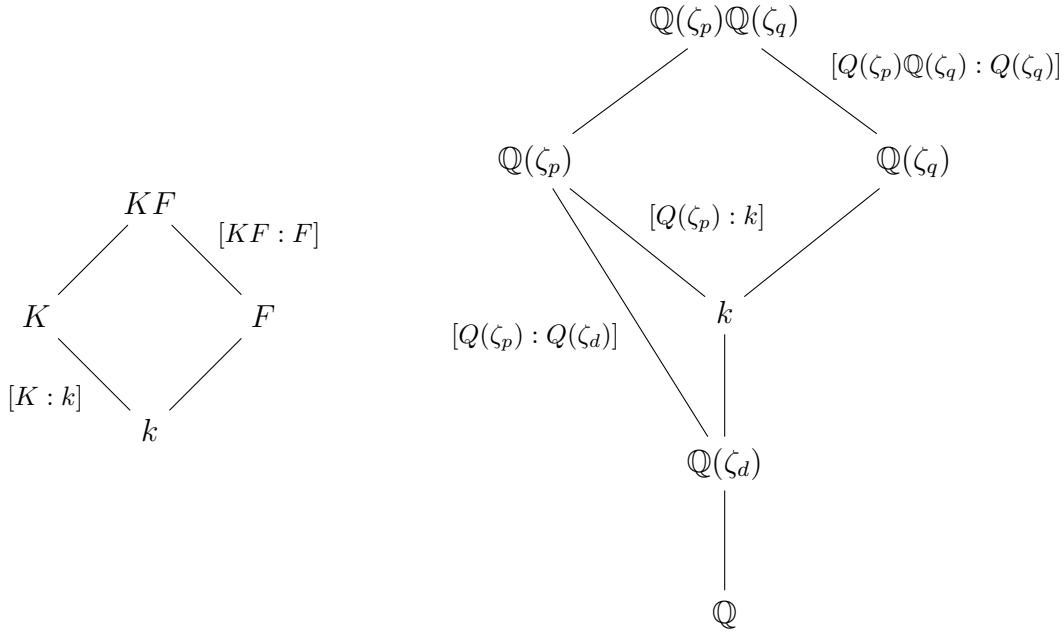


FIGURE 1 – Diagrammes d’extensions de corps dans le cas d’un produit de corps à gauche et le cas pratique des corps cyclotomiques à droite. Ainsi, via les lemmes de multiplication de corps et de multiplicativité des degrés, on visualise clairement la hiérarchie des degrés des extensions en jeu, avec $[K : k] \geq [KF : F]$ à gauche et $[Q(\zeta_p) : Q(\zeta_d)] \geq [Q(\zeta_p) : k] \geq [Q(\zeta_p)Q(\zeta_q) : Q(\zeta_q)]$ à droite.

Ainsi $(e_i)_{i=1,\dots,d}$ est une famille génératrice de $F[K]$ et $F[K]$ est un F -espace vectoriel de dimension fini. Par ailleurs, étant donné $x \in F[K]$ non nul, l’endomorphisme

$$\begin{array}{ccc} F[K] & \longrightarrow & F[K] \\ y & \longmapsto & xy \end{array}$$

est injectif par intégrité de L , et comme $F[K]$ est de dimension finie, c’est un automorphisme. Donc, il existe $y \in F[K]$ de telle sorte que $xy = 1$ et $F[K]$ est un corps. Finalement, $KF = F[K]$ et $[KF : F] \leq d = [K : k]$. On peut se référer à la figure 1 pour visualiser l’inégalité.

Partie 2 : produit de corps cyclotomiques. On commence par la remarque introductive suivante : étant donné deux entiers a, b non nuls, comme $Q(\zeta_{ab})$ est le corps de décomposition de $X^{ab} - 1$ et que $(\zeta_a)^a = 1$, on a $\zeta_a \in Q(\zeta_{ab})$ et $Q(\zeta_a) \subset Q(\zeta_{ab})$.

Supposons d’abord que p et q sont premiers entre eux. Étant donné que $Q(\zeta_p)$ et $Q(\zeta_q)$ sont inclus dans $Q(\zeta_{pq})$, alors $Q(\zeta_p)Q(\zeta_q) \subset Q(\zeta_{pq})$ par définition du produit de corps. Réciproquement, comme $\text{pgcd}(p, q) = 1$, $\zeta_p \zeta_q$ est d’ordre pq . Ainsi, c’est une racine primitive pq -ème, $\zeta_{pq} \in Q(\zeta_p)Q(\zeta_q)$ et on a l’inclusion réciproque.

À présent, prenons p et q quelconques et considérons leurs décompositions en facteurs irréductibles $p = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et $q = p_1^{\beta_1} \dots p_r^{\beta_r}$. Par ailleurs, en notant $\gamma_i = \max(\alpha_i, \beta_i)$, $N = \text{ppcm}(p, q) = p_1^{\gamma_1} \dots p_r^{\gamma_r}$. D’après la remarque précédente, on a $Q(\zeta_p) = Q(\zeta_{p_1^{\alpha_1}}) \dots Q(\zeta_{p_r^{\alpha_r}})$ et $Q(\zeta_q) = Q(\zeta_{p_1^{\beta_1}}) \dots Q(\zeta_{p_r^{\beta_r}})$. Ainsi $Q(\zeta_{p_i^{\alpha_i}})Q(\zeta_{p_i^{\beta_i}}) = Q(\zeta_{p_i^{\gamma_i}})$. Finalement, on a bien $Q(\zeta_p)Q(\zeta_q) = Q(\zeta_N)$.

Partie 3 : intersection de corps cyclotomique. On note $k = \mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_q)$, et on a $\mathbb{Q}(\zeta_d) \subset k$ par définition de $d = \text{pgcd}(p, q)$ et la fait que $\mathbb{Q}(\zeta_a) \subset \mathbb{Q}(\zeta_{ab})$. On veut montrer $[k : \mathbb{Q}(\zeta_d)] = 1$. On rappelle préalablement que $\mathbb{Q}(\zeta_p)$ est une extension de degré $\varphi(p)$ sur $\mathbb{Q}$. Pour ce faire, la figure 1 nous permet d'écrire l'inégalité de degré suivante, justifiée par la première partie et le lemme de multiplicativité des degrés :

$$\frac{\varphi(p)}{\varphi(d)} = [\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_d)] \geq [\mathbb{Q}(\zeta_p) : k] \geq [\mathbb{Q}(\zeta_p)\mathbb{Q}(\zeta_q) : \mathbb{Q}(\zeta_q)] = \frac{\varphi(N)}{\varphi(q)}.$$

Or $pq = Nd$, et par multiplicativité de l'indicatrice d'Euler φ , et en travaillant sur chaque facteur premier, on a $\varphi(p)\varphi(q) = \varphi(N)\varphi(d)$. Ainsi, l'inégalité précédente se trouve être une suite d'égalité et par multiplicativité des degrés, on a le résultat souhaité.

Remerciements Merci à Axel pour sa relecture et ses conseils.

Références

- [Ort04] Pascal ORTIZ. Exercices d'algèbre. Ellipses, 2004.
 [Per96] Daniel PERRIN. Cours d'algèbre. Ellipses, 1996.

Annexe

Une grande partie des propriétés sur les polynômes cyclotomiques proviennent du lemme suivant, appliqué aux racines primitives de l'unité.

Lemme

Soient G un groupe et $a, b \in G$ deux éléments commutant d'ordre fini p et q . Si p et q sont premiers entre eux, alors l'ordre de ab est pq .

Démonstration. On note n l'ordre de ab . D'abord, on a $(ab)^{pq} = (a^p)^q(b^q)^p = 1$, de sorte que n divise pq . Réciproquement, on a $1 = (ab)^{nq} = a^{nq}$, donc $p \mid nq$ et comme $\text{pgcd}(p, q) = 1$, $p \mid n$ d'après le lemme d'Euclide. De même, $q \mid n$ et finalement $n = pq$. $\square$

Ainsi, si p et q sont deux entiers premiers entre eux, alors $\zeta_p \zeta_q = \zeta_{pq}$ est une racine primitive pq -ème de l'unité. On peut aussi se rappeler du calcul explicite $e^{\frac{2i\pi}{p}} e^{\frac{2i\pi}{q}} = e^{2i\pi \frac{p+q}{pq}}$ et de remarquer que la fraction $\frac{p+q}{pq}$ est irréductible si $\text{pgcd}(p, q) = 1$.