Théorème de Dedekind

Diego Izquierdo

Voici une preuve du théorème 11.12 du polycopié :

Soient L le corps de décomposition de f et G le groupe de Galois de f. Soit $\mathcal{O}_L$ l'anneau des entiers de L. Soit $\mathfrak{q}$ un idéal maximal de $\mathcal{O}_L$ qui contient p. On remarque alors bien sûr que $\lambda = \mathcal{O}_L/\mathfrak{q}$ est une extension finie de $\mathbb{F}_p$. Introduisons les groupes suivants :

$$G_\mathfrak{q} = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) | \sigma(\mathfrak{q}) = \mathfrak{q}\}$$
$$g_\mathfrak{q} = \mathrm{Gal}(\lambda/\mathbb{F}_p).$$

Le groupe $g_\mathfrak{q}$ est cyclique. Soit σ un générateur de $g_\mathfrak{q}$.

Lemme : Le morphisme naturel $\varphi : G_\mathfrak{q} \to g_\mathfrak{q}$ est surjectif.

Preuve. Soit $\alpha \in \lambda^\times$ tel que $\lambda = \mathbb{F}_p(\alpha)$. Soit P le polynôme minimal de α et posons $\beta = \sigma(\alpha)$. Soit $\tilde{\alpha}$ un relèvement de α dans $\mathcal{O}_L$ tel que $\alpha \in \mathfrak{q}'$ pour tout idéal maximal de $\mathcal{O}_L$ contenant p autre que $\mathfrak{q}$: un tel $\tilde{\alpha}$ existe d'après le lemme chinois[1]. Soit $\tilde{P}$ le polynôme minimal de $\tilde{\alpha}$. Bien sûr, $\tilde{P}$ est un relèvement de P et donc $\tilde{P}$ possède une racine $\tilde{\beta}$ relevant β. De plus, $\tilde{P}$ étant irréductible, G agit transitivement sur les racines de $\tilde{P}$. Par conséquent, on peut trouver $\tau \in G$ tel que $\tau(\tilde{\alpha}) = \tilde{\beta}$. Soit $\mathfrak{q}' = \tau^{-1}(\mathfrak{q})$. On vérifie aisément que c'est un idéal maximal de $\mathcal{O}_L$ contenant p. Si $\mathfrak{q} \neq \mathfrak{q}'$, alors $\tilde{\alpha} \in \mathfrak{q}'$, et donc $\tau(\tilde{\alpha}) = \tilde{\beta} \in \mathfrak{q}$. Cela impose que $\beta = 0$: absurde ! Donc $\mathfrak{q} = \mathfrak{q}'$ et $\tau \in G_\mathfrak{q}$. Comme $\tau(\tilde{\alpha}) = \tilde{\beta}$, on a $\varphi(\tau) = \sigma$, ce qui achève la preuve du lemme.

Pour prouver le théorème 11.12 du polycopié, il suffit alors de choisir un élément de $G_\mathfrak{q}$ dont l'image par φ est σ.

Remarque : Le groupe $G_\mathfrak{q}$ joue un rôle important en théorie des nombres : on l'appelle le groupe de décomposition en $\mathfrak{q}$. De même, le noyau de φ joue un rôle important en théorie des nombres : on l'appelle le groupe d'inertie de $\mathfrak{q}$.

1. Pour appliquer le lemme chinois, il faut bien sûr savoir que $\mathcal{O}_L$ possède un nombre fini d'idéaux maximaux contenant p. Mais $\mathcal{O}_L$ étant un groupe abélien de type fini, le groupe $\mathcal{O}_L/(p)$ est fini. Ce dernier possède donc un nombre fini de sous-groupes. Cela garantit que $\mathcal{O}_L$ possède un nombre fini d'idéaux maximaux contenant p.