

### fiche XIII Anneau des entiers d'un corps cyclotomique

Soit  $p$  un nombre premier et soit  $z$  une racine primitive  $p^r$ -ième de l'unité.

On va montrer que l'anneau des entiers de  $\mathbb{Q}(z)$  est  $\mathbb{Z}[z]$ .

On note  $B$  l'anneau des entiers de  $\mathbb{Q}(z)$ . Le polynôme minimal de  $z$  sur  $\mathbb{Q}$  est le polynôme :

$$\Phi_{p^r}(X) = \Phi_p(X^{p^{r-1}}) = 1 + X^{p^{r-1}} + \dots + X^{p^{r-1}(p-1)} .$$

Soit  $\pi := 1 - z$ . On a :

$$N_{\mathbb{Q}(z)/\mathbb{Q}}(\pi) = \prod_i (1 - z_i)$$

où les  $z_i$  sont les conjugués de  $z$  *i.e.* les racines primitives  $p^r$ -ièmes de l'unité.  
Donc :

$$N_{\mathbb{Q}(z)/\mathbb{Q}}(\pi) = \Phi_{p^r}(1) = p .$$

Soit  $\underline{e} := (e_1, \dots, e_n)$  une  $\mathbb{Z}$ -base de  $B$  (où  $n = p^r$ ). Soit  $P$  la matrice de passage de  $(e_1, \dots, e_n)$  dans  $\underline{z} := (1, \dots, z^{n-1})$  (ce sont deux bases de  $\mathbb{Q}(z)$  comme  $\mathbb{Q}$ -espace vectoriel).

Soit  $J := \mathbb{Z}[z]$ . C'est un sous- $\mathbb{Z}$ -module libre de  $B$ . Donc d'après le théorème de la base adaptée, il existe une base  $\underline{f} := (f_1, \dots, f_n)$  de  $B$ ,  $d_1, \dots, d_n$  des entiers tels que :

$$d_1 | d_2 | \dots | d_n \text{ et } \underline{f}' := (d_1 e_1, \dots, d_n e_n)$$

est une base de  $J$ . Alors :

$$\begin{aligned} B/J &\simeq \mathbb{Z}/d_1 \times \dots \times \mathbb{Z}/d_n \\ \Rightarrow |B/J| &= d_1 \dots d_n . \end{aligned}$$

Soient  $P_{\underline{e}, \underline{f}}, P_{\underline{f}, \underline{f}'}, P_{\underline{f}', \underline{z}}$  les matrices de passage de  $\underline{e}$  à  $\underline{f}$ , de  $\underline{f}$  à  $\underline{f}'$  et de  $\underline{f}'$  à  $\underline{z}$ . Alors :

$$P = P_{\underline{e}, \underline{f}} P_{\underline{f}, \underline{f}'} P_{\underline{f}', \underline{z}}$$

donc  $\det P = \pm \det P_{\underline{f}, \underline{f}'} = \pm d_1 \dots d_n$  (car  $P_{\underline{e}, \underline{f}}$  et  $P_{\underline{f}', \underline{z}}$  sont des matrices dans  $\text{GL}_n(\mathbb{Z})$  (donc de déterminants  $\pm 1$ ) en tant que matrices de passage entre deux bases d'un même  $\mathbb{Z}$ -module libre).

On considère la forme bilinéaire :

$$b : \mathbb{Q}(z) \times \mathbb{Q}(z) \rightarrow \mathbb{Q}, (x, y) \mapsto \text{Tr}(xy)$$

où  $\text{Tr}$  est la trace relativement à l'extension  $\mathbb{Q}(z)/\mathbb{Q}$ .

Dans la base  $1, \dots, z^{n-1}$ , le déterminant de  $b$  est  $\text{Disc}(1, \dots, z^{n-1})$ . Donc, en utilisant les formules de changement de bases pour les matrices des formes bilinéaires, on trouve :

$$\text{Disc}(1, \dots, z^{n-1}) = \det P^2 d$$

où  $d$  est le discriminant de la base  $e_1, \dots, e_n$ .

Donc :

$$\text{Disc}(1, \dots, z^{n-1}) = |B/J|^2 d .$$

Or,  $\text{Disc}(1, \dots, z^{n-1})$  est aussi le discriminant du polynôme cyclotomique  $\Phi_n(X) = \Phi_{p^r}(X)$ . C'est donc une puissance de  $p$ . Donc  $B/J$  est un groupe fini d'ordre  $p^N$  pour un certain  $N$ . On a alors  $p^N B/J = 0$  i.e.  $p^N B \subseteq J$ .

Comme  $N(\pi) = p$ ,  $p \in \pi B$ . Donc  $p\mathbb{Z} \subseteq \pi B \cap \mathbb{Z}$ . Comme  $N(\pi) \neq 1$ ,  $\pi$  n'est pas inversible dans  $B$  et :

$$p\mathbb{Z} \subseteq \pi B \cap \mathbb{Z} \subsetneq \mathbb{Z}$$

d'où :  $p\mathbb{Z} = \pi B \cap \mathbb{Z}$  car  $p\mathbb{Z}$  est un idéal maximal de  $\mathbb{Z}$ .

Donc on a un morphisme injectif d'anneaux :

$$\mathbb{Z}/p\mathbb{Z} \rightarrow B/\pi B \quad k \bmod p \mapsto k \bmod \pi B .$$

Or,  $|B/\pi B| = |N(\pi)| = p$  donc ce morphisme est un isomorphisme.

Soit  $b \in B$ . Il existe donc  $a_0 \in \mathbb{Z} \subseteq \mathbb{Z}[z]$ ,  $b_1 \in B$  tels que  $b = a_0 + \pi b_1$ .  
Donc  $B = \mathbb{Z}[z] + \pi B$ .

De même, il existe  $a_1 \in \mathbb{Z}$ ,  $b_2 \in B$  tels que :

$$\begin{aligned} b_1 &= a_1 + \pi b_2 \\ \Rightarrow b &= a_0 + \pi a_1 + \pi^2 b_2 \\ \Rightarrow b &\in \mathbb{Z}[z] + \pi^2 B \end{aligned}$$

car  $\pi = 1 - z \in \mathbb{Z}[z]$ . Par récurrence, on en déduit facilement que :

$$B = \mathbb{Z}[z] + \pi^m B$$

pour tout  $m$ .

On a :

$$\begin{aligned} N(\pi) &= \prod_{\substack{i=1 \\ i \wedge p=1}}^{p^r-1} (1 - z^i) = p \\ &= \pi^{\varphi(p^r)} \prod_{\substack{i=1 \\ i \wedge p=1}}^{p^r-1} \frac{1 - z^i}{1 - z} . \end{aligned}$$

Or  $N\left(\frac{1-z^i}{1-z}\right) = 1$  et comme  $\frac{1-z^i}{1-z} = 1 + \dots + z^{i-1} \in B$ ,  $\frac{1-z^i}{1-z}$  est inversible dans  $B$ . Donc  $\pi^{\varphi(p^r)} = pu$  pour un certain  $u \in B^\times$ .

On a donc pour tout  $m$ ,  $\mathbb{Z}[z] + p^m B = \mathbb{Z}[z] + \pi^{\varphi(p^r)m} B = B$ .

En particulier pour  $m = N$  :

$$\mathbb{Z}[z] + p^N B = \mathbb{Z}[z] = B .$$

Soient  $K, L$  deux extensions de  $\mathbb{Q}$  de degrés respectifs  $m, n$  contenues dans  $\mathbb{C}$ . On suppose que l'extension  $KL$  est de degré  $mn$  sur  $\mathbb{Q}$ .

Notons  $\mathcal{P}_K$  l'ensemble des  $\mathbb{Q}$ -plongements de  $K$  dans  $\mathbb{C}$ . On définit de même  $\mathcal{P}_L$  et  $\mathcal{P}_{KL}$ .

L'application :

$$\begin{aligned} \mathcal{P}_{KL} &\rightarrow \mathcal{P}_K \times \mathcal{P}_L \\ s &\mapsto (s|_K, s|_L) \end{aligned}$$

est injective puisque  $K, L$  engendrent  $KL$ . Or comme on est en caractéristique nulle, on a :

$$|\mathcal{P}_{KL}| = [KL : \mathbb{Q}] = mn = [K : \mathbb{Q}][L : \mathbb{Q}] = |\mathcal{P}_K| |\mathcal{P}_L| .$$

Donc l'application ci-dessus est aussi surjective, autrement dit, pour tous plongements  $s_1, s_2$  de  $K$  et de  $L$  dans  $\mathbb{C}$ , il existe un plongement (unique)  $s$  de  $KL$  dans  $\mathbb{C}$  tel que  $s|_K = s_1, s|_L = s_2$ .

Soient  $R, S, T$  les anneaux des entiers algébriques (sur  $\mathbb{Z}$ ) des corps  $K, L, KL$ . On notera  $RS$  le sous-anneau de  $T$  engendré par  $R, S$ .

Soient  $r_1, \dots, r_m$  une  $\mathbb{Z}$ -base de  $R$  et  $s_1, \dots, s_n$  une  $\mathbb{Z}$ -base de  $S$ .

La famille  $\{r_i s_j : 1 \leq i \leq m, 1 \leq j \leq n\}$  engendre le  $\mathbb{Q}$ -espace vectoriel  $KL$ . Comme  $KL$  est de dimension  $mn$ , cette famille est donc une base.

Si  $a \in T$ , alors il existe des entiers  $c_{i,j}, q \in \mathbb{Z}$  tels que :

$$a = \sum_{i,j} \frac{c_{i,j}}{q} r_i s_j .$$

Quitte à simplifier les fractions on peut supposer que  $q$  est premier avec l'ensemble des  $c_{i,j}$ .

Notons  $\sigma_1, \dots, \sigma_n$  les  $\mathbb{Q}$ -plongements de  $L$  dans  $\mathbb{C}$ .

Comme on l'a déjà vu précédemment, chaque  $\sigma_i$  peut se prolonger en un unique  $\mathbb{Q}$ -plongement de  $KL$  dans  $\mathbb{C}$  qui est l'identité sur  $K$ . On note encore  $\sigma_i$  un tel prolongement.

On a donc :

$$\sigma_i(a) = \sum_{j=1}^n d_j \sigma_i(s_j)$$

pour tout  $i$  où :  $d_j := \sum_{k=1}^m \frac{c_{k,j}}{q} r_k$ .

Donc :

$$\begin{pmatrix} \sigma_1(a) \\ \vdots \\ \sigma_n(a) \end{pmatrix} = A^{-1} \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix}$$

où  $A$  est la matrice  $(\sigma_i(s_j))_{1 \leq i, j \leq n} \in \mathcal{M}_n(S)$ . Cette matrice est bien inversible car

$$\det A^2 = \text{Disc}(S) .$$

Puisque  $A^{-1} = \frac{1}{\det A} {}^t \tilde{A}$ , on a :

$$d_1, \dots, d_n \in \frac{1}{\det A} S \subseteq \frac{1}{\text{Disc}(S)} S$$

en particulier :

$$\sum_{k=1}^m \text{Disc}(S) \frac{c_{k,j}}{q} r_k$$

est entier sur  $\mathbb{Z}$  pour tout  $j$  (et c'est aussi un élément de  $K$ ). Donc :

$$\sum_{k=1}^m \text{Disc}(S) \frac{c_{k,j}}{q} r_k \in R$$

pour tout  $j$ .

Puisque les  $r_k$  forment une  $\mathbb{Z}$ -base de  $R$ , on a forcément :

$$\text{Disc}(S) \frac{c_{k,j}}{q} \in \mathbb{Z}$$

pour tous  $k, j$ . Donc  $q | \text{Disc}(S)$  puisque  $q$  est premier avec l'ensemble des  $c_{k,j}$ .

De même on peut montrer que  $q$  divise  $\text{Disc}(R)$ . Donc :

$$RS \subseteq T \subseteq d^{-1}T$$

où  $d$  est le pgcd des discriminants de  $R$  et  $S$ .

**Application :** On montre par récurrence sur  $n \geq 1$  que l'anneau des entiers  $B_n$  du corps cyclotomique  $\mathbb{Q}(z_n)$  ( $z_n$  est une racine primitive  $n$ -ième de l'unité) est  $B_n = \mathbb{Z}[z_n]$ .

C'est facile pour  $n = 1$ . Supposons  $n > 1$ . Soit  $p$  un diviseur premier de  $n$  et  $p^r$  la puissance maximale de  $p$  qui divise  $n$ . Soit  $1 \leq n' < n$  tel que :

$$n = p^r n' .$$

Comme  $p^r$  et  $n'$  sont premiers entre eux,  $\mathbb{Q}(z_{n'})\mathbb{Q}(z_{p^r}) = \mathbb{Q}(z_n)$  et  $[\mathbb{Q}(z_n) : \mathbb{Q}] = \varphi(n) = \varphi(n')\varphi(p^r) = [\mathbb{Q}(z_{n'}) : \mathbb{Q}][\mathbb{Q}(z_{p^r}) : \mathbb{Q}]$ .

Par hypothèse de récurrence :  $B_{n'} = \mathbb{Z}[z_{n'}]$ . D'après ce qu'on a montré au début, on a aussi :  $B_{p^r} = \mathbb{Z}[z_{p^r}]$ .

Or, le discriminant de  $\mathbb{Z}[z_{n'}] = B_{n'}$  est le discriminant du polynôme  $\Phi_{n'}$  et le discriminant de  $\mathbb{Z}[z_{p^r}] = B_{p^r}$  est le discriminant du polynôme  $\Phi_{p^r}$ . Ces deux discriminants sont donc premiers entre eux (*cf.* la formule du discriminant d'un polynôme cyclotomique). Donc on a :

$$B_{n'}B_{p^r} = B_n$$

$$\Leftrightarrow \mathbb{Z}[z_{n'}]\mathbb{Z}[z_{p^r}] = B_n .$$

Pour conclure, on vérifie facilement que  $\mathbb{Z}[z_{n'}]\mathbb{Z}[z_{p^r}] = \mathbb{Z}[z_n]$ .  
*q.e.d.*