Calcul du discriminant du polynôme cyclotomique :

Soit $n \geq 2$. Soit Δ le discriminant de $\Phi_n(X)$, le $n-$ième polynôme cyclotomique. On connaît déjà le signe de Δ : c'est $(-1)^{\varphi(n)/2}$ car $\Phi_n(X)$ n'a que des racines complexes conjuguées (*cf.* la fiche X).

Calculons $|\Delta|$:

$$|\Delta| = \prod_{\epsilon} |\Phi_n'(\epsilon)|$$

où ϵ décrit les racines primitives $n-$ièmes de l'unité.

Or, d'après la formule d'inversion de Möbius :

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}$$

$$= (X^n - 1) \prod_{\substack{d|n \\ d<n}} (X^d - 1)^{\mu(n/d)}$$

où $\mu(n/d) = \begin{cases} (-1)^r \text{ si } n/d = p_1...p_r \text{ avec } p_1 < ... < p_r \text{ premiers} \\ 0 \text{ sinon} \end{cases}$.

Donc :

$$\Phi_n'(X) = nX^{n-1} \prod_{\substack{d|n \\ d<n}} (X^d - 1)^{\mu(n/d)} \bmod (X^n - 1)$$

$$\Rightarrow \Phi_n'(\epsilon) = n\epsilon^{n-1} \prod_{\substack{d|n \\ d<n}} (\epsilon^d - 1)^{\mu(n/d)}$$

pour toute racine primitive $n-$ième de l'unité ϵ.

Ainsi :

$$|\Delta| = n^{\varphi(n)} \prod_{\substack{d|n \\ d<n}} \prod_{\epsilon} |\epsilon^d - 1|^{\mu(n/d)}$$

or, lorsque ϵ est une racine primitive $n-$ième de l'unité, ϵ^d est une racine primitive $(n/d)-$ième de l'unité. Plus précisément, si on note Π_k l'ensemble des racines primitives $k-$ièmes de l'unité, le morphisme :

$$\Pi_n \to \Pi_{n/d} \quad \epsilon \mapsto \epsilon^d$$

est surjectif.

En effet, posons $k := n/d$; on peut identifier Π_n à $(\mathbb{Z}/n\mathbb{Z})^\times$ et Π_k à $(\mathbb{Z}/k\mathbb{Z})^\times$ et le morphisme ci-dessus au morphisme de groupes :

$$(\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/k\mathbb{Z})^\times \quad x \bmod n \mapsto x \bmod k \ .$$

Ce morphisme est surjectif ! C'est facile si $n = p^r$ pour un certain nombre premier p. Pour le cas général : $n = p_1^{r_1}...p_t^{r_t}$ pour des nombres premiers distincts p_i, $k = p_1^{s_1}...p_t^{s_t}$ avec $s_i \leq r_i$ et on utilise le théorème des isomorphismes chinois :

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq (\mathbb{Z}/p_1^{r_1})^\times \times ... \times (\mathbb{Z}/p_s^{r_s})$$

... on obtient un produit cartésien de morphismes surjectifs.

Donc le morphisme (de groupes (on munit Π_n, Π_k des structures de groupes de $(\mathbb{Z}/n\mathbb{Z})^\times, (\mathbb{Z}/k\mathbb{Z})^\times)$) :

$$\Pi_n \to \Pi_k \quad \epsilon \mapsto \epsilon^d$$

est surjectif de noyau de cardinal :

$$|\text{noyau}| = \frac{|\Pi_n|}{|\Pi_k|}$$

$$= \varphi(n)/\varphi(k) = \varphi(n)/\varphi(n/d) \ .$$

Par conséquent :

$$\prod_{\epsilon} |\epsilon^d - 1| = \prod_{\epsilon'} |\epsilon' - 1|^{\varphi(n)/\varphi(n/d)}$$

où ϵ' décrit les racine primitives $(n/d)-$ièmes de l'unité.

Donc :

$$\prod_{\epsilon} |\epsilon^d - 1| = \prod_{\epsilon'} |\epsilon' - 1|^{\varphi(n)/\varphi(n/d)} = \Phi_{n/d}(1)^{\varphi(n)/\varphi(n/d)} \ .$$

Or pour un entier m, $\Phi_m(1) = \begin{cases} p \text{ si } m = p^r,\ r \geq 1,\ p \text{ premier} \\ 1 \text{ sinon} \end{cases}$. En effet d'une part :

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

et d'autre part, si $n = p_1^{a_1}...p_r^{a_r}$, avec des nombres premiers p_i deux à deux distincts :

$$n = \frac{X^n - 1}{X - 1}|_{X=1} = \prod_{\substack{d|n \\ d>1}} \Phi_d(1)$$

$$= \prod_i p_i^{a_i} \prod_d \Phi_d(1)$$

où d décrit les diviseurs de n qui ne sont pas une puissance d'un nombre premier. Ainsi $\Phi_d(1) = \pm 1$ si d n'est pas une puissance d'un nombre premier et donc dans ce cas $\Phi_d(1) = 1$ (par la formule d'inversion de Möbius il est facile de voir que $\Phi_d(1) \geq 0$).

Pour résumer :

$$|\Delta| = n^{\varphi(n)} \prod_{p \text{ premier}} \prod_{a>0} \prod_{\substack{d|n \\ n/d=p^a}} (p^{\varphi(n)/\varphi(p^a)})^{\mu(p^a)}$$

$$= n^{\varphi(n)} \prod_{\substack{p|n \\ p \text{ premier}}} p^{-\varphi(n)/(p-1)} \ .$$

Conclusion le discriminant du polynôme cyclotomique $\Phi_n(X)$ est donné par la formule :

$$\Delta = (-1)^{\varphi(n)/2} \frac{n^{\varphi(n)}}{\prod_{\substack{p|n \\ p\text{premier}}} p^{\varphi(n)/(p-1)}} \ .$$

Anneau des entiers d'une extension 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 :

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

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 $\underline{e} := (e_1, ..., e_n)$ une $\mathbb{Z}-$base de B (où $n = p^r$). Soit P la matrice de passage de $(e_1, ..., e_n)$ dans $\underline{z} := (1, ..., z^{n-1})$ (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 $\underline{f} := (f_1, ..., f_n)$ de B, $d_1, ..., d_n$ des entiers tels que :

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

est une base de J. Alors :

$$B/J \simeq \mathbb{Z}/d_1 \times .... \times \mathbb{Z}/d_n$$

$$\Rightarrow |B/J| = d_1 ... d_n \ .$$

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

On considère la forme bilinéaire :

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

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

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

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

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

Donc :

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

Or, $\mathrm{Disc}(1, ..., z^{n-1})$ est aussi le discriminant du polynôme cyclotomique $\Phi_n(X) = \Phi_{p^r}(X)$. C'est donc un puissance de p. Donc B/J est 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 $N(\pi) \neq 1$, π n'est pas inversible dans B et :

$$p\mathbb{Z} \subseteq \pi B \cap \mathbb{Z} \underset{\neq}{\subset} \mathbb{Z}$$

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 :

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

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 $b = b_0 + \pi b_1$. Donc $B = \mathbb{Z}[z] + \pi B$.

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

$$b_1 = a_1 + \pi b_2$$

$$\Rightarrow b = a_0 + \pi a_1 + \pi^2 b_2$$

$$\Rightarrow b \in \mathbb{Z}[z] + \pi^2 B$$

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 :

$$N(\pi) = \prod_{\substack{i=1 \\ i \wedge p = 1}}^{p^r - 1} (1 - z^i) = p$$

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

Or $N\left(\frac{1-z^i}{1-z}\right) = 1$ et comme $\frac{1-z^i}{1-z} = 1 + ... + z^{i-1} \in B$, $\frac{1-z^i}{1-z}$ 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 $\mathscr{P}_K$ l'ensemble des $\mathbb{Q}-$plongements de K dans $\mathbb{C}$. On définit de même $\mathscr{P}_L$ et $\mathscr{P}_{KL}$.

L'application :

$$\mathscr{P}_{KL} \to \mathscr{P}_K \times \mathscr{P}_L$$

$$s \mapsto (s|_K \, , s|_L \,)$$

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

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

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 $r_1, ..., r_m$ une $\mathbb{Z}-$base de R et $s_1, ..., s_n$ 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 $\sigma_1, ..., \sigma_n$ les $\mathbb{Q}-$plongements de L dans $\mathbb{C}$.

Comme on l'a déjà vu précédemment, chaque σ_i peut se prolonger en un unique $\mathbb{Q}-$plongement de KL dans $\mathbb{C}$ qui est l'identité sur K. On note encore σ_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 $(\sigma_i(s_j))_{1\leq i,j\leq n} \in \mathscr{M}_n(S)$. Cette matrice est bien inversible car

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

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

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

en particulier :

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

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

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

pour tout j.

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

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

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

De même on peut montrer que q divise $\mathrm{Disc}(R)$. 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 polynômee $\Phi_{n'}$ et le discriminant de $\mathbb{Z}[z_{p^r}] = B_{p^r}$ est le discriminant du polynômee Φ_{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.