Université Paul Sabatier — Novembre 2014

Devoir L3 — **Algèbre**

Dans tout ce qui suit, un nombre premier impair p est fixé. On suppose choisie une fois pour toutes une racine p-ème de l'unité $\zeta \neq 1$. On pose $\lambda = 1 - \zeta$.

On rappelle que le polynôme cyclotomique associé à p est :

$$\Phi_p = 1 + X + X^2 + \cdots + X^{p-1} \, .$$

1) L'inclusion $\mathbf{Q} \subset \mathbf{C}$ définit un morphisme d'anneaux $\mathbf{Q} \to \mathbf{C}$, et la propriété niverselle de l'anneau des polynômes $\mathbf{Q}[X]$ implique qu'il existe un unique morphisme d'anneaux

$$f : \mathbf{Q}[X] \to \mathbf{C}$$

tel que $f(x) = x$, et tel que $f(X) = \zeta$. Posons

$$\mathbf{Q}[\zeta] = \{a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \,|\, (a_0, \ldots, a_{p-1}) \in \mathbf{Q}^{p-1}\} \, .$$

Montrons que $\mathbf{Q}[\zeta] = \mathrm{Im}(f)$. On a clairement l'inclusion

$$\mathbf{Q}[\zeta] \subset \mathrm{Im}(f) \, .$$

En effet, si $(a_0, \ldots, a_{p-2}) \in \mathbf{Q}^{p-1}$, on a

$$f(a_0 + a_1X + \cdots + a_{p-2}X^{p-2}) = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \, .$$

Soit $P \in \mathbf{Q}[X]$. On peut effectuer la division euclidienne de P par Φ_p, et donc écrire $P = Q\Phi_p + R$ avec $Q, R \in \mathbf{Q}[X]$ et R de degré $< p - 1$. Comme

$$(X - 1)\Phi_p = X^p - 1 \, ,$$

et vu que l'anneau des nombres complexes $\mathbf{C}$ est intègre (puisqu'un corps), on doit avoir $\Phi_p(\zeta) = 0$. Il s'en suit que

$$P(\zeta) = Q(\zeta)\Phi_p(\zeta) + R(\zeta) \, .$$

Autrement dit $f(P) = f(R)$. Or il est clair que $f(R) \in \mathbf{Q}[\zeta]$. L'ensemble $\mathbf{Q}[\zeta]$ est donc un sous-anneau de $\mathbf{C}$ en tant qu'image d'un morphisme d'anneaux à valeurs dans $\mathbf{C}$.

2) On vient de voir que $\mathbf{Q}[\zeta]$ est l'image du morphisme d'anneaux f construit ci-dessus. Il résulte donc du premier théorème d'isomorphie de Noether que f induit canoniquement un isomorphisme

$$\mathbf{Q}[X]/\ker(f) \simeq \mathbf{Q}[\zeta] \, .$$

Or le morphisme f a pour noyau l'idéal engendré par Φ_p. En effet, on a déjà vu ci-dessus que $\Phi_p(\zeta) = 0$, ce qui signifie que $f(\Phi_p) = 0$ et donc que $\Phi_p \in \ker(f)$, d'où on déduit l'inclusion $(\Phi_p) \subset \ker(f)$. Réciproquement, considérons $P \in \ker(f)$. Comme $P(\zeta) = 0$, le polynôme $X - \zeta$ divise P dans $\mathbf{C}[X]$. Par conséquent P et Φ_p ne sont pas premiers entre eux dans $\mathbf{C}[X]$. Cela implique qu'ils ne sont pas premiers entre eux dans $\mathbf{Q}[X]$. En effet, si P et Φ_p étaient premiers entre eux, le théorème de Bézout (dans le contexte de l'anneaux principal $\mathbf{Q}[X]$) impliquerait que $UP + \Phi_p V = 1$ avec $U, V \in \mathbf{Q}[X]$. On aurait donc la même relation dans $\mathbf{C}[X]$, ce qui signifierait que 1 est dans l'idéal engendré par P et par Φ_p, et donc impliquerait que $X - \zeta$ est inversible dans $\mathbf{C}[X]$, d'où une contradiction. Les polynômes P et Φ_p ont donc un facteur irréductible commun. Comme il est connu que le polynôme cyclotomique Φ_p est irréductible, cela implique que Φ_p doit diviser P. On a ainsi établi l'égalité $\ker(f) = (\Phi_p)$, et donc l'existence d'un isomorphisme canonique

$$\mathbf{Q}[X]/(\Phi_p) \simeq \mathbf{Q}[\zeta]$$

qui envoie la classe de X sur ζ.

3) Comme au numéro 1), on voit qu'il existe un unique morphisme d'anneaux $g : \mathbf{Z}[X] \to \mathbf{C}$ qui envoie X sur ζ (c'est la restriction du morphisme f ci-dessus au sous-anneau $\mathbf{Z}[X]$ de $\mathbf{Q}[X]$). Comme le polynôme Φ_p est à coefficients entiers et unitaire, on peut faire la division euclidienne par Φ_p dans $\mathbf{Z}[X]$: pour tout polynôme $P \in \mathbf{Z}[X]$, il existe un unique couple $(Q, R) \in \mathbf{Z}[X]^2$ tel que $P = Q\Phi_p + R$ avec R de degré $< p - 1$. Les arguments du numéro 1) restent donc valables en remplaçant $\mathbf{Q}$ par $\mathbf{Z}$. En particulier, l'ensemble $\mathbf{Z}[\zeta]$ est un sous-anneau de $\mathbf{C}$ en tant qu'image d'un morphisme d'anneaux à valeurs dans $\mathbf{C}$. Pour prouver que g induit canoniquement un isomorphisme

$$\mathbf{Z}[X]/(\Phi_p) \simeq \mathbf{Z}[\zeta]$$

qui envoie la classe de X sur ζ, on procède comme au numéro 2) : en vertu de ce qui précède et du premier théorème d'isomorphie de Noether, il suffit de prouver que $\ker(g) = (\Phi_p)$ (où, cette fois, (Φ_p) désigne l'idéal de $\mathbf{Z}[X]$ engendré par Φ_p). L'inclusion $(\Phi_p) \subset \ker(g)$ est évidente (c'est une reformulation de la relation $\Phi_p(\zeta) = 0$). Soit $P \in \mathbf{Z}[X]$ tel que $P(\zeta) = 0$. Alors, en vertu des arguments expliqués au numéro 2), P est divisible par Φ_p dans $\mathbf{Q}[X]$. Cela signifie que le reste de la division euclidienne de P par Φ_p est nul. Or la division euclidienne par Φ_p peut être faite dans $\mathbf{Z}[X]$. Cela signifie que $P = Q\Phi_p$ avec $Q \in \mathbf{Z}[X]$, et prouve donc que $\ker(g) = (\Phi_p)$.

4) Il y a au plus un morphisme d'anneaux $\mathbf{Q}[\zeta] \to \mathbf{Q}[\zeta]$ qui envoie ζ sur ζ^i. En effet, considérons deux tels morphismes π et π'. Alors aussi bien $\pi \circ f$ que $\pi' \circ f$ peut être caractérisé comme l'unique morphisme d'anneaux $\mathbf{Q}[X] \to \mathbf{Q}[\zeta]$ qui envoie X sur ζ^i. En particulier, $\pi \circ f = \pi' \circ f$, et vu que f est surjectif, cela implique que $\pi = \pi'$.

L'identification

$$(X - 1)\Phi_p = X^p - 1$$

implique que les racines de Φ_p dans le corps algébriqument clos $\mathbf{C}$ sont précisément les racines p-èmes de l'unité qui sont distinctes de 1. Comme p est un nombre premier, celles-ci sont les éléments de l'ensemble

$$\{\zeta^i \,|\, 1 \leqslant i \leqslant p-1\}$$

Pour $1 \leqslant i \leqslant p-1$, le morphisme d'anneaux

$$f_i : \mathbf{Q}[X] \to \mathbf{C}$$

défini par $f_i(X) = \zeta^i$ induit un isomorphisme

$$\mathbf{Q}[X]/(\Phi_p) \to \mathrm{Im}(f_i) = \mathbf{Q}[\zeta^i] = \mathbf{Q}[\zeta]$$

(les arguments du numéro 2) sont valables en remplaçant ζ par ζ^i puisque ζ n'est jamais qu'une racine p-ème de l'unité non tiviale quelconque). En composant avec l'inverse de l'isomorphisme établi au numéro 2), on obtient de la sorte un isomorphisme d'anneaux :

$$\pi_i : \mathbf{Q}[\zeta] \to \mathbf{Q}[\zeta]\,.$$

Par construction, ce dernier envoie ζ sur ζ^i.

Avec les mêmes arguments (mais en remplaçant les références au numéro 2) par des références au numéro 3), on voit que, pour tout entier i tel que $\zeta^i \neq 1$, il existe un unique morphisme d'anneaux

$$\mathbf{Z}[\zeta] \to \mathbf{Z}[\zeta]$$

qui envoie ζ sur ζ^i. Autrement dit, le morphisme π_i induit un isomorphisme de $\mathbf{Z}[\zeta]$ sur lui-même.

4 bis) Considérons un morphisme d'anneaux

$$\varphi : \mathbf{Q}[\zeta] \to \mathbf{Q}[\zeta]\,.$$

Le morphisme $\varphi \circ f$ a pour noyau un idéal de $\mathbf{Q}[X]$, et comme tout anneau de polynômes sur un corps est principal, il existe un unique polynôme unitaire $P \in \mathbf{Q}[X]$ tel que

$$\ker(\varphi \circ f) = (P)\,.$$

On a $f(P) = 0$ et donc $(P) \subset (\Phi_p)$. D'autre part, le premier théorème d'isomorphie de Noether implique que l'on a un unique isomorphisme

$$\mathbf{Q}[X]/(P) \simeq \mathrm{Im}(\varphi \circ f)$$

qui envoie la classe de X sur $\varphi(\zeta)$. En particulier, l'anneau quotient $\mathbf{Q}[X]/(P)$ étant isomorphe à un sous-anneau de $\mathbf{C}$, il est intègre, et donc l'idéal (P) est premier, ce qui implique que P est un élément irréductible de $\mathbf{Q}[X]$. Comme Φ_p divise P et comme P est unitaire, cela implique que $P = \Phi_p$. Autrement dit, le morphisme φ doit être injectif. On a donc $1 \neq \varphi(\zeta)$. Comme

$$1 = \varphi(1) = \varphi(\zeta^p) = \varphi(\zeta)^p\,,$$

on en déduit que $\varphi(\zeta) = \zeta^i$ pour un certain i, $1 \leqslant i \leqslant p-1$. Autrement dit, $\varphi \circ f$ est l'unique morphisme qui envoie X sur ζ^i, et il résulte donc du numéro 4) que $\varphi = \pi_i$.

Le corps $\mathbf{F}_p = \mathbf{Z}/(p)$ a pour éléments inversibles les classes modulo p des entiers $1, \dots, p-1$. Ceux-ci forment un groupe $\mathbf{F}_p^*$ à $p-1$ éléments (ce groupe est cyclique, car on peut montrer que les éléments inversibles d'un corps finis forment toujours un groupe cyclique pour la multiplication). On définit une application bijective

$$\begin{aligned} \mathbf{F}_p^* &\to \mathrm{Aut}(\mathbf{Q}[\zeta]) \\ i &\mapsto \pi_i \end{aligned}$$

On vérifie aussitôt que cette aplication est compatible aux structures de groupes, car $(\zeta^i)^j = \zeta^{ij}$.

5) Il y a exactement $p-1$ racines p-èmes de l'unité distinctes de 1, et celles-ci sont les racines de Φ_p, lequel est un polynôme de degré $p-1$. Il s'en suit que la décomposition de Φ_p en produit de facteurs irréductibles dans $\mathbf{C}[X]$ est

$$\Phi_p = \prod_{i=1}^{p-1} (X - \zeta^i)\,.$$

En évaluant en $X = 1$, on obtient que

$$p = \Phi_p(1) = \prod_{i=1}^{p-1} (1 - \zeta^i)\,.$$

6) Il existe un unique morphisme d'anneaux

$$u : \mathbf{F}_p \to \mathbf{Z}[\zeta]/(\lambda)\,.$$

En effet, il résulte de la formule prouvée au numéro 5) que p est divisible par λ dans $\mathbf{Z}[\zeta]$ et donc que la classe de p est nulle modulo λ. L'unique morphisme d'anneaux $\mathbf{Z} \to \mathbf{Z}[\zeta]$ induit le morphisme escompté. Comme la classe de ζ modulo λ est égale à 1, on voit que cette application u est surjective. Vu qu'il s'agit d'un morphisme d'anneaux dont le domaine est un corps, cette application u ne peut qu'être qu'injective, et donc bijective.

7) Pour $1 \leqslant i \leqslant p-1$, posons $\varepsilon_i = \frac{1-\zeta^i}{1-\zeta}$. On a

$$1 - \zeta^i = (1-\zeta)(1 + \zeta + \cdots + \zeta^{i-1})$$

d'où

$$\varepsilon_i = 1 + \zeta + \cdots + \zeta^{i-1} \in \mathbf{Z}[\zeta]\,.$$

De même, si j est un inverse de i modulo p, on a aussi

$$1 - \zeta = (1 - \zeta^i)(1 + \zeta^i + \cdots + \zeta^{i(j-1)})$$

d'où

$$\varepsilon_i^{-1} = 1 + \zeta^i + \cdots + \zeta^{i(j-1)} \in_Z Z[\zeta]\,.$$

En particulier, ε_i est inversible dans $\mathbf{Z}[\zeta]$. Posons $\varepsilon = \varepsilon_1 \cdots \varepsilon_{p-1}$. On a alors,en vertu de la formule prouvée au numéro 5) :

$$p = \varepsilon\lambda^{p-1}\,.$$

On note

$$N : \mathbf{Q}[\zeta] \to \mathbf{Q}$$

l'application définie comme suit. Pour $x \in \mathbf{Q}[\zeta]$, la multiplication par x définit une application $\mathbf{Q}$-linéaire

$$\begin{aligned} m_x : \mathbf{Q}[\zeta] &\to \mathbf{Q}[\zeta] \\ y &\mapsto xy \end{aligned}$$

et on pose

$$N(x) = \det(m_x)\,.$$

On remarque immédiatement que $N(x) = 0$ si et seulement si $x = 0$ (car $N(x) = 0$ si et seulement si m_x n'est pas bijective, ce qui équivaut à la condition $x = 0$). et que $N(xy) = N(x)N(y)$ pour tous $x, y \in \mathbf{Q}[\zeta]$ (car le déterminant est compatible à la composition des applications linéaires).

8) Soit x un élément de $\mathbf{Z}[\zeta]$. Montrons que x est inversible dans $\mathbf{Z}[\zeta]$ si et seulement si $|N(x)| = 1$. En effet, si x est inversible, alors il existe $y \in \mathbf{Z}[\zeta]$ tel que $xy = 1$ d'où

$$1 = N(1) = N(xy) = N(x)N(y)\,.$$

En particulier, $N(x)$ est inversible dans $\mathbf{Z}$, et donc $N(x) = \pm 1$. Pour la réciproque, on a utilise le fait suivant : l'isomorphisme canonique $\mathbf{Q}[X]/(\Phi_p) \simeq \mathbf{Q}[\zeta]$ établi au numéro 2) implique que $\mathbf{Q}[\zeta]$ est un $\mathbf{Q}$-espace vectoriel de dimension $p-1$, avec pour base l'ensemble $\mathcal{B} = \{1, \zeta, \ldots, \zeta^{p-2}\}$ (puisque Φ_p est de degré $p-1$). Si A désigne la matrice représentant m_x dans cette base, ses coordonnées sont des nombres entiers : la i-ème colonne de A est l'écriture de $x\zeta^i$ dans la base $\mathcal{B}$. Si en outre $N(x) = \pm 1$, alors la multiplicaton par $\frac{1}{x}$ a pour matrice représentative dans cette même base la co-matrice de A (au signe près). En particulier, les coordonnées de la matrice représentant $m_{\frac{1}{x}}$ dans la base $\mathcal{B}$ sont des nombres entiers. On en déduit que la multiplication par $\frac{1}{x}$ envoie le sous-anneau $\mathbf{Z}[\zeta]$ dans lui-même. En particulier, x est inversible dans $\mathbf{Z}[\zeta]$.