Fiche 8, exo. 5 :

Soit G un groupe cyclique d'ordre n. Soit H un sous-groupe d'ordre d. Alors $d|n$. Le groupe G/H est d'ordre n/d. Donc si g est un générateur de G, $g^{n/d} \in H$. Or, $g^{n/d}$ est d'ordre d donc $H = \langle g^{n/d} \rangle$. Donc pour tout d qui divise n, il existe un seul sous-groupe de G d'ordre d.

Soit p premier. Le groupe $G := (\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$. Si $f|p-1$, on note H_f le sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ d'ordre f.

Si $f|p-1$, alors on pose pour tout entier l :

$$(f,l) := \sum_{h \in H_f} \zeta^{lh} \ .$$

On a :

$$(f,l) \in \mathbb{Q}(\zeta)^{H_f} \ .$$

Soient $l_1, ..., l_e$ un système de représentants de G/H_f. L'orbite de (f,l_1) pour l'action de G est formée des (f,l_i). Les (f,l_i) sont deux à deux distincts car $\zeta, ..., \zeta^{p-1}$ sont indépendants (en effet, $\Phi_p(X) = 1 + ... + X^{p-1}$ est le polynôme minimal de ζ). Le polynôme :

$$(X - (f,l_1))...(X - (f,l_e))$$

a ses coefficients dans $\mathbb{Q}$ et c'est le polynôme minimal de (f,l_i) sur $\mathbb{Q}$ pour tout i.

Comme $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)^{H_f}] = f$, on a aussi :

$$[\mathbb{Q}(\zeta)^{H_f} : \mathbb{Q}] = e$$

donc : $\mathbb{Q}(\zeta)^{H_f} = \mathbb{Q}((f,l_i))$ pour tout i.

On a :

$$(f,l)(f,m) = \sum_{h,h' \in H_f} \zeta^{lh+mh'}$$

$$= \sum_{h' \in H_f} \sum_{h \in H_f} \zeta^{lh+mh'}$$

$$= \sum_{h' \in H_f} \sum_{h'' \in H_f} \zeta^{lh'h''+mh'}$$

car pour tout $h' \in H_f$, $h'H_f = H_f$.

Donc :

$$(f,l)(f,m) = \sum_{h',h'' \in H_f} (\zeta^{lh''+m})^{h'}$$

$$= \sum_{h'' \in H_f} (f, lh" + m) \ .$$

Applications : On a : $\langle 3 \rangle = (\mathbb{Z}/17\mathbb{Z})^\times$.

Si $f = 8$, $H_f = \langle 3^2 \rangle = \{-8, -4, -2, -1, 8, 4, 2, 1\}$ (on prend ces valeurs modulo 17).

On a donc :

$$(\mathbb{Z}/17\mathbb{Z})^\times = H_8 \cup 3H_8$$

et :

$$(8,1) = \sum_{a \in H_8} \zeta^a$$

$$= \zeta + \zeta^{-1} + \zeta^2 + \zeta^{-2} + \zeta^{-4} + \zeta^4 + \zeta^8 + \zeta^{-8}$$

$$(8,3) = \sum_{a \in 3H_8} \zeta^a$$

$$= \zeta^3 + \zeta^{-3} + \zeta^6 + \zeta^{-6} + \zeta^{-5} + \zeta^5 + \zeta^7 + \zeta^{-7}$$

en particulier :

$$(8,1) + (8,3) = \sum_{a \in \mathbb{Z}/17\mathbb{Z}} \zeta^a - 1 = -1 \ .$$

On a aussi :

$$(8,1)(8,3) = \sum_{h \in H_8} (8, h+3)$$

$$= (8,2) + (8,4) + (8,1) + (8,5) + (8,-1) + (8,7) + (8,-6) + (8,-5)$$

or, $(8,2) = (8,4) = (8,1) = (8,-1)$ et $(8,5) = (8,-5) = (8,7) = (8,6) = (8,3)$.

Donc : $(8,1)(8,3) = -4$; et $(8,1), (8,3)$ sont les racines de :

$$X^2 + X - 4 \ .$$

D'où : $(8,1) = \frac{-1 \pm \sqrt{17}}{2}$.

Or, $(8,1) = 2\cos(2\pi/17) + 2\cos(4\pi/17) + 2\cos(8\pi/17) + 2\cos(16\pi/17) > 2\cos(16\pi/17) > -2$.

Comme $\frac{-1-\sqrt{17}}{2} < -2$, on a forcément :

$$(8,1) = \frac{-1 + \sqrt{17}}{2} \ .$$

De même on trouve les valeurs :

$$(4,1), (4,2), (4,3), (2,1), (2,3)$$

avec $\cos(2\pi/17) = 1/2$ $(2,1)$.

Fiche X, exo. 1 (résultant) :

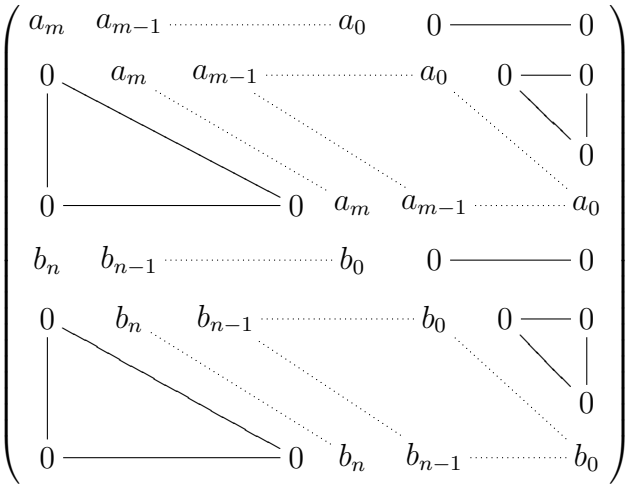
Soit A un anneau factoriel. Soient :

$$f = f_m X^m + ... + f_0$$

$$g = g_n X^n + ... + g_0$$

deux polynômes dans $A[X]$.

On note $S(f,g)$ la matrice :



Si f, g ont un facteur commun non constant $h \in A[X]$, on a :

$$(g/h)f = (f/h)g$$

et $F := f/h, G := g/h$ vérifient : $\deg F < \deg f$, $\deg G < \deg g$.

Réciproquement, s'il existe F, G non nuls dans $A[X]$ tels que : $\deg F < \deg f$, $\deg G < \deg g$ et $Fg = Gf =: Q$. Quitte à diviser F, G par leur pgcd, on peut supposer que F, G sont premiers entre eux. Alors considérons la décomposition en facteur irréductibles de f :

$$f = a_1^{m_1} ... a_r^{m_r} f_1^{n_1} ... f_r^{n_r}$$

où les $a_i \in A$, $f_i \in A[X]$ sont des irréductibles premiers entre eux deux à deux et $m_i, n_i \geq 1$.

Pour des raisons de degrés, il existe i tel que $f_i^{n_i}$ ne divise pas F. Comme $f_i^{n_i} | fG = Fg$, f_i divise g car f_i est irréductible. On a donc un facteur non constant commun à f et g.

Si $F = F_0 + ..; + F_{m-1} X^{m-1}$, $G = G_0 + ... + G_{n-1} X^{n-1}$, alors :

$$Fg = Gf \Leftrightarrow LS(f,g) = 0$$

où $L := (F_0, ..., F_{m-1}, -G_0, ..., -G_{n-1}) \in A^{m+n}$. . Si F ou $G \neq 0$, alors $L \neq 0$. Donc si on note S' la transposée de la comatrice de S, on a :

$$0 = LSS' = L\text{dét}\, S \Rightarrow \text{dét}\, S = 0$$

car l'anneau A est intègre.

Réciproquement si $\text{dét}\, S = 0$, il existe un vecteur ligne $L \in K^{m+n}$ non nul tel que $LS = 0$ où K est le corps des fractions de A. Quitte à multiplier par un élément non nul de A, on peut supposer $L \in A^{m+n}$. On en déduit qu'il existe F, G non nuls de degrés respectifs $< m$, $< n$ tels que $Fg = Gf$.

On pose $R := \text{dét}\, S$.

Si S' est la comatrice de $S(f, g)$, S' a ses coefficients dans A et :

$$S'S = \text{dét}\, SI_{m+n} = R(f, g)I_{m+n}$$

Soit $(a_0, ..., a_{n-1}, b_0, ..., b_{m-1})$ la première ligne de S'. On s'aperçoit que :

$$hf + kg = R$$

avec $h := a_0 + ... + a_{n-1}X^{n-1}$ et $k := b_0 + ... + b_{m-1}X^{m-1}$.

c) Soient

$$f = f_m(X - x_1)...(X - x_m)$$
$$g = g_n(X - y_1)...(X - y_n) \ .$$

Considérons les x_i, y_j, f_m, g_n comme des indéterminées. On obtient un résultant $R(f, g) \in \mathbb{Z}[f_m, g_n][x_1, ..., x_m; y_1, ..., y_n]$.

Notons $s_1, ...s_m$ les fonctions symétriques élémentaires en les x_i et $s'_1, ..., s'_n$ les fonctions symétriques élémentaires en les y_j. On a :

$$f = f_m X^m - f_m s_1 X^{m-1} + ... + (-1)^m f_m s_m$$

$$g = g_n X^n - g_n s'_1 + ...(-1)^n g_n s'_n \ .$$

Le résultant $R(f, g)$ est donc un polynôme symétrique en les x_i et en les y_j. Fixons i, j. Dans l'anneau

$$\mathbb{Z}[f_m, g_n][x_1, ..., x_m; y_1, ..., y_n]/(x_i - y_j) \simeq \mathbb{Z}[f_m, g_n][x_1, ..., x_m; y_1, ..., \hat{y_j}, ..., y_n]$$

on a : $R(f, g) = 0 \bmod (x_i - y_j)$ car f et g ont pour facteur commun : $X - x_i = X - y_j \bmod (x_i - y_j)$.

Donc $R(f, g)$ est divisible par $(x_i - y_j)$ pour tous i, j.

Soit $Q \in \mathbb{Z}[f_m, g_n][x_1, ..., x_m; y_1, ..., y_n]$ tel que $R(f, g) = \prod_{i,j}(x_i - y_j)Q$.

Comme $R(f, g)$ et $\prod_{i,j}(x_i - y_j)$ sont symétriques en les x_i et en les y_j, Q aussi. Donc Q est un polynôme en les $s_1, ..., s_m; s'_1, ..., s'_n$. Or, R est de degré

$\leq n$ en chaque s_i et de degré $\leq m$ en chaque $s'j$. D'un autre côté, $\prod_{i,j}(x_i - y_j)$ est de degré n en chaque s_i et de degré m en chaque s'_j car :

$$\prod_{i,j}(x_i - y_j) = \frac{\prod_j f(y_j)}{f_m^n} = \pm\frac{\prod_i g(x_i)}{g_n^m} \ .$$

donc $Q \in \mathbb{Z}[f_m, g_n]$. Or vu la forme du déterminant R, R est homogène de degré n en f_m et de degré m en g_n. Donc $R = f_m^n g_n^m \prod_{i,j}(x_i - y_j)q$ pour un $q \in \mathbb{Z}$.

Sur la diagonale de la matrice qui permet de définir le résultant on trouve $\underbrace{f_m, ...f_m}_{n}, \underbrace{(-1)^n f_m s'_n, ..., (-1)^n f_m s'_n}_{m}$. et donc en comparant les coefficients dominants en s'_n de R et $\prod_{i,j}(x_i - y_j)$, on obtient $q = 1$ *i.e.* :

$$R = f_m^n g_n^m \prod_{i,j}(x_i - y_j) \ .$$