Fiche VIII, exo. 1 : Soient $p_1 < ... < p_t$ des nombres premiers tels que : t est impair ≥ 3 et $p_1 + p_2 > p_t$. On pose $n := p_1...p_t$et $p := p_t$

Alors grâce à la formule d'inversion de Möbius, on a :

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

Or, les diviseurs de n sont $1, p_1, .., p_t$ et les produits :

$$p_{i_1}...p_{i_k} \ : \ 2 \leq k \leq t \, , \, 1 \leq i_1 < ... < i_k \leq t \ .$$

Or, si $d = p_{i_1}...p_{i_k}$ avec $k \geq 2$, alors $d \geq p_1p_2 > p_1 + p_2 > p$ et donc $X^d = 0 \bmod X^{p+1}$.

Donc dans l'anneau $\mathbb{Q}[X]/(X^{p+1})$, on a :

$$\Phi_n(X) = (X-1)^{\mu(n)}(X^{p_1} - 1)^{\mu(n/p_1)}...(X^{p_t} - 1)^{\mu(n/p_t)}(-1)^e$$

où $e = \sum_{\substack{2 \leq k \leq t \\ 1 \leq i_1 < ... < i_k \leq t}} \mu(n/p_{i_1}...p_{i_k})$.

Or, comme t est impair, $\mu(n) = -1$, $\mu(n/p_i) = 1$ et :

$$\begin{aligned} e &= \sum_{\substack{2 \leq k \leq t \\ 1 \leq i_1 < ... < i_k \leq t}} (-1)^{k+1} \\ &= -\sum_{2 \leq k \leq t} \binom{n}{k} (-1)^k \\ &= -((1-1)^t - 1 + 1) = 0 \ . \end{aligned}$$

donc :

$$\begin{aligned} \Phi_n(X) &= (X^{p_1} - 1)...(X^{p_t} - 1)(X-1)^{-1} \bmod X^{p+1} \\ &= (1 - X^{p_1})...(1 - X^{p_t})(1-X)^{-1} \bmod X^{p+1} \\ &= (1 - X^{p_1} ... - X^{p_t})(1 + X + ... + X^p) \bmod X^{p+1} \end{aligned}$$

car $p_1 + p_2 \geq p + 1$ et $(1-X)^{-1} = 1 + ... + X^p \bmod X^{p+1}$.

Si on développe on trouve les coefficients c_{p-2} et c_p devant X^{p-2} et X^p de $\Phi_n(X)$:

$$c_{p-2} = 2 - t \text{ et } c_p = 1 - t \ . \tag{1}$$

Si $m > 2$, alors $\varphi(m)$ est pair. Donc $\Phi_m(-X)$ est de degré pair et donc unitaire.

Si m est impair ≥ 3, alors

$$-e^{2i\pi/2m} = e^{2i\pi/2m + i\pi}$$

$$= e^{2i(\frac{m+1}{2})\pi/m} \ .$$

Comme $\frac{m+1}{2}$ et m sont premiers entre eux, $e^{2i(\frac{m+1}{2})\pi/m}$ est une racine de Φ_m. Donc $\Phi_m(-e^{2i\pi/2m}) = 0$.

Par conséquent, $\Phi_m(-X)$ est un multiple dde $\Phi_{2m}(X)$ dans $\mathbb{Q}[X]$, car $\Phi_{2m}(X)$ est le polynôme minimal sur $\mathbb{Q}$ de $e^{2i\pi/2m}$. Comme de plus $\Phi_m(-X)$ et $\Phi_{2m}(X)$ sont unitaires de même degré $\varphi(m) = \varphi(2m)$, on a $\Phi_m(-X) = \Phi_{2m}(X)$.

Donc si $n = p_1...p_t$ avec $p_1, ..., p_t =: p$ comme au début et $p_1 \geq 3$, alors n est impair, $\Phi_n(-X) = \Phi_{2n}(X)$ et donc les coefficients de $\Phi_{2n}(X)$ devant X^{p-2} et X^p sont respectivement :

$$t - 2 \text{ et } t - 1 \ . \tag{2}$$

Ainsi tout entier non nul (tout entier non nul est de la forme $\pm(t-1)$ ou $\pm(t-2)$ pour un t impair ≥ 3) peut apparaître comme coefficient d'un polynôme cyclotomique pour peu que la propriété suivante soit vérifiée :

($\mathscr{P}$) : *pour tout t impair ≥ 3, il existe des nombres premiers $3 \leq p_1 < ... < p_t$ tels que $p_1 + p_2 > p_t$.*

Il se trouve que ($\mathscr{P}$) est vraie.

En effet, supposons par l'absurde que ($\mathscr{P}$) est fausse pour un certain $t \geq 3$ impair. Si $k \geq 2$ et si $2^{k-1} < p_1 < ... < p_t \leq 2^k$ sont des nombres premiers, alors :

$$p_1 + p_2 \leq p_t \leq 2^k < 2p_1$$

$$\Rightarrow p_2 < p_1$$

impossibile ! Donc on aurait moins de t nombres premiers entre 2^{k-1} et 2^k. En particulier si on note $\pi(j)$ le nombre de nombre premiers entre 1 et j, on a :

$$\pi(2^k) \leq 1 + \sum_{r=2}^{k} t = (k-1)t + 1$$

$$\leq kt \ .$$

Mais alors : $\pi(2^k) \leq kt$ pour tout $k \geq 2$. Cela est impossible car d'après le théorème de répartition des nombres premiers ou théorème fondamental de l'analyse :

$$\pi(n) \sim n/\log n$$

quand n tend vers l'infini (*cf.* par exemple *Hlawka, Schoissengeier, Taschner, Geometric and analytic number theory, Springer universitext, 1991, th. 3, ch.5*).

Fiche VIII, exo. 4 :

Soit $t \in \mathbb{Q}\pi$. On suppose que $\cos t \in \mathbb{Q}$. Le polynôme $X^2 - 2\cos t X + 1 = (X - e^{it})(X - e^{-it})$ est à coefficients rationnels et annule e^{it}. Donc e^{it} est de degré 1 ou 2 sur $\mathbb{Q}$. Or $t = 2p\pi/q$ pour certains entiers p, q premiers entre eux. Donc e^{it} est une racine primitive $q-$ième de l'unité et par conséquent e^{it} est de degré $\varphi(q)$ sur $\mathbb{Q}$. On a donc : $\varphi(q) = 1$ ou 2.

Or si $q = p_1^{\alpha_1}...p_r^{\alpha_r}$ est la décomposition de q en produits de nombres premiers $p_1 < ... < p_r$ avec $\alpha_1, ..., \alpha_r \geq 1$. Alors :

$$\varphi(q) = p_1^{\alpha_1 - 1}(p_1 - 1)...p_r^{\alpha_r - 1}(p_r - 1)$$

donc $\varphi(q) = 1, 2 \Rightarrow p_r \leq 3$ et donc $q = 1, 2, 3, 4$ ou 6.

ainsi : $\cos t = (\cos 2\pi p/q) = 0, \pm 1$ ou $\pm 1/2$.

Si $\sin t \in \mathbb{Q}$, alors $\sin t = \cos(\pi/2 - t)$ et comme $\pi/2 - t \in \mathbb{Q}\pi$, on a aussi $\sin t = 0, \pm 1$ ou $\pm 1/2$.

Si $\tan t \in \mathbb{Q}$, alors $\cos(2t) = \frac{2}{\tan^2 t + 1} - 1 \in \mathbb{Q}$.

Donc :

$$\tan^2 t = 0,\ \frac{1}{1 \pm 1} - 1,\ \text{ou}\ \frac{1}{1 \pm 1/2} - 1$$
$$\Rightarrow \tan t = 0 \text{ ou } \pm 1$$

les autre solutions ne sont pas rationnelles.

Fiche IX exo.7 : Calcul de $\Phi_{15}(X)$:

$$\Phi_{15}(X) = \frac{(X^{15} - 1)(X - 1)}{(X^5 - 1)(X^3 - 1)}$$
$$= \frac{X^{10} + X^5 + 1}{X^2 + X + 1}$$
$$= X^8 - X^7 + X^5 - X^4 + X^3 - X + 1\ .$$

Soit ζ une racine primitive $n-$ième de l'unité. Alors $\zeta + \zeta^{-1} \in \mathbb{Q}(\zeta) \cap \mathbb{R}$. De plus ζ est racine du polynôme $X^2 - (\zeta + \zeta^{-1})X + 1$. Donc ζ est de degré 1 ou 2 sur $\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq \mathbb{Q}(\zeta) \cap \mathbb{R}$.

Si $n > 2$, alors $\zeta \notin \mathbb{R}$ donc ζ est de degré 2 sur $\mathbb{Q}(\zeta + \zeta^{-1})$. Comme

$$\mathbb{Q}(\zeta + \zeta^{-1}) \subseteq \mathbb{Q}(\zeta + \zeta^{-1}) \cap \mathbb{R} \subseteq \mathbb{Q}(\zeta)$$

on a forcément $\mathbb{Q}(\zeta + \zeta^{-1}) = \mathbb{Q}(\zeta) \cap \mathbb{R}$.

De plus, $\zeta + \zeta^{-1}$ est de degré $\varphi(n)/2$ sur $\mathbb{Q}$.

Si par exemple $\zeta = e^{2i\pi/15}$, $\zeta+\zeta^{-1} = 2\cos(2\pi/15)$. Soit $P(X)$ le polynôme minimal de $\zeta + \zeta^{-1}$ sur $\mathbb{Q}$. Alors $P(X)$ est de degré $\varphi(n)/2$. La fraction rationnelle :

$$X^{\varphi(n)/2}P(X + X^{-1})$$

est en fait un polynôme rationnel unitaire de degré $\varphi(n)$ qui annule ζ. C'est donc forcément $\Phi_n(X)$:

$$\Phi_n(X) = X^{\varphi(n)/2}P(X + X^{-1}) \ .$$

Soit $Q(X) := X^4 - X^3 - 4X^2 + 4X + 1$. On vérifie que $X^4Q(X + X^{-1}) = \Phi_{15}(X)$. On a donc :

$$X^4P(X + X^{-1}) = X^4Q(X + X^{-1})$$

$$\Leftrightarrow Q = P \ .$$

Fiche VII, exo. 4 :

Soit A un anneau factoriel (par exemple $A = \mathbb{Z}$ ou $k[t]$). Si $f = a_0 + ... + a_dX^d \in A[X]$, on pose $c(f) :=$ le *contenu* de A : c'est le pgcd des coefficients $a_0, ..., a_d$. C'est un élément de A défini à multiplication par un élément de $A^\times$ près. On note K le corps des fractions de A.

Lemme 0.1

$$(i) \ \ f \text{ est irréductible dans } A[X] \ ;$$

$$\Leftrightarrow$$

$$(ii) \ \ f \text{ est irréductible dans } K[X] \text{ et } c(f) = 1 \ .$$

démo : Soient $f, g \in A[X]$. Alors $c(fg) = c(f)c(g)$. En effet, soit $\gamma := c(f)c(g)$. On a :

$$c(fg) = c\left(\gamma \frac{f}{c(f)} \frac{g}{c(g)}\right) = \gamma c\left(\frac{f}{c(f)} \frac{g}{c(g)}\right)$$

il suffit donc de vérifier que $c\left(\frac{f}{c(f)} \frac{g}{c(g)}\right) = 1$. Pour cela, on peut supposer que $c(f) = c(g) = 1$. Montrons que $c(fg) = 1$. On raisonne par l'absurde : si $c(fg) \neq 1$, alors il existe un élément irréductible p de A (si $A = \mathbb{Z}$: un nombre premier, si $A = k[X]$, un polynôme irréductible) qui divise $c(fg)$ *i.e.* qui divise tous les coefficients de fg. Mais alors dans l'anneau $A/(p)[X]$, si on note $\overline{f}$ et $\overline{g}$ les classes de $f, g \bmod p$, on a :

$$\overline{f}\overline{g} = 0 \ .$$

Or, si p est irréductible, l'idéal (p) est premier donc l'anneau $A/(p)$ est intégre et donc l'anneau $A/(p)[X]$ aussi. par conséquent $\overline{f}$ ou $\overline{g} = 0$ *i.e.* f ou g a tous ses coefficients divisibles par p ce qui est impossible vu que $c(f) = c(g) = 1$.

Supposons que $f \in A[X]$ est irréductible dans $A[X]$. En particulier, f n'est divisible par aucun élément irréductible de A. Donc $c(f) = 1$. Supposons que $f = pq$ avec $p, q \in K[X]$. Alors, il existe $a, b \in A$ non nuls tels que $ap, bq \in A[X]$. On a alors :

$$abf = (ap)(bq)$$

$$\Rightarrow ab = c(ap)c(bq)$$

$$\Rightarrow f = pq = \frac{ap}{c(ap)}\frac{bq}{c(bq)}$$

et donc comme f est irréductible dans $A[X]$, $\frac{ap}{c(ap)}$ ou $\frac{bq}{c(bq)}$ est inversible dans $A[X]$. D'où p ou q inversible dans $K[X]$. On a donc bien f irréductible sur K. Réciproquement, si $f \in A[X]$ est irréductible sur K et si $c(f) = 1$, alors si $f = pq$ avec $p, q \in A[X]$ alors p ou q est inversible dans $K[X]$. Donc p ou q est constant. Par exemple si p est constant, alors $p \in A$ et $p|c(f)$. Or $c(f) = 1$ donc $p \in A^\times$.

Soit k un corps. Soit $f \in k(T)$ une fraction rationnelle non constante. Soient $P, Q \in k[T]$ deux polynômes premiers entre eux tels que $f = P/Q$. Montrons que

$$[k(T) : k(f)] = \max\{\deg P, \deg Q\} \ .$$

En effet, le polynôme :

$$F(X) := fQ(X) - P(X) \in k(f)[X]$$

est un polynôme non nul qui annule T.

Donc, comme $k(T) = k(f)(T)$, T est de degré $\leq \deg F$ sur $k(f)$. En particulier l'extension $k(f) \subseteq k(T)$ est algébrique. Le degré de F est $\max \deg P, \deg Q$.

Démontrons que $F(X)$ est irréductible sur $k(f)$. On remarque que

$$k[Y] \to k[f] \ , \ Y \mapsto f$$

est un isomorphisme d'algèbres (car f est non constante). Cet isomorphisme se prolonge en un isomorphisme de corps : $k(f) \simeq k(Y)$. Il s'agit donc de montrer que $\widetilde{F}(X) := YQ(X) - P(X)$ est irréductible sur $k(Y)$. Il suffit de montrer que le polynôme $\widetilde{F}$ est irréductible sur $k[Y]$ *i.e.* dans $k[Y][X] = k[X, Y] = k[X][Y]$. Or, vu comme polynôme en la variable Y et à coefficients dans $k[X]$, le polynôme $\widetilde{F}(X, Y)$ est de degré 1 donc irréductible dans

$k(X)[Y]$ et son contenu est $c(\widetilde{F}) = 1$ car ses « coefficients » sont $P(X)$ et $Q(X)$ qui sont premiers entre eux. Donc $\widetilde{F}$ est irréductible dans $k[X,Y]$ donc dans $k(Y)[X]$. Ainsi, F est irréductible sur $k(f)$.

Soit $k = \mathbb{F}_q$ le corps fini à q éléments. Alors on sait que $q = p^r$ pour un certain nombre premier p et un certain $r \geq 1$.

On a $|\mathrm{PGL}_2(k)| = \frac{|\mathrm{GL}_2(k)|}{|k^\times|} = \frac{(q^2-1)(q^2-q)}{q-1} = q^3 - q$.

Si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(k)$, on pose $h_g(t) := \frac{at+b}{ct+d}$.

On remarque que si $g' = g \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$, alors $h_{g'} = h_g$.

Donc on peut définir sans ambiguïté h_g pour une classe $g \in \mathrm{PGL}_2(k)$.

On remarque que :

$$h_g(h'_g(t)) = h_{gg'}(t)$$

pour tous $g, g' \in \mathrm{PGL}_2(k)$. En particulier :

$$h_g(h_{g^{-1}}(t)) = t \ .$$

De plus, si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(k)$, on a $k(h_g(t)) = k(t)$ En effet, $k(h_g(t)) \subseteq k(t)$ et

$$[k(t) : k(h_g(t))] = \max\{\deg(at+b), \deg(ct+d)\} = 1 \ .$$

Réciproquement, si $f \in k(t)$ est telle que $k(t) = k(f)$, alors f est non constante et le numérateur et le dénominateur de f sont de degré ≤ 1. Donc il exite $g \in \mathrm{PGL}_2(k)$ tel que $f = h_g$.

Soit :

$$\Phi : \mathrm{PGL}_2(k) \to \mathrm{Aut}_k(k(t)) \ , \ g \mapsto \sigma_{g^{-1}}$$

où pour tout $g \in \mathrm{PGL}_2(k)$, $\sigma_g : k(t) \to k(t)$ est l'automorphisme qui laisse fixes les éléments de k et qui envoie t sur $h_g(t)$.

L'application Φ est un isomorphisme de groupes. D'après ce qui précède, il ne reste plus qu'à montrer l'injectivité. Or, si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{PGL}_2(k)$ vérifie $\sigma_g = \mathrm{Id}_{k(t)}$, alors $\sigma_g(t) = h_g(t) = t$ d'où :

$$\frac{at+b}{ct+d} = t$$

$$\Leftrightarrow at + b = ct^2 + dt$$

$$\Leftrightarrow a = d \text{ et } b = c = 0$$

et g est une homothétie (*i.e.* $g = 1$ dans $\mathrm{PGL}_2(k)$).

Comme k est un corps, on sait (grâce à la méthode du pivot de Gauss) que $\mathrm{GL}_2(k)$ est engendré par les matrices :

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$$

pour $a \in k^\times, b, c \in k$.

Or, on a :

$$\begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ .$$

donc le groupe $\mathrm{GL}_2(k)$ est engendré par les matrices :

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$b \in k, a \in k^\times$

Les automorphismes correspondants de $k(t)$ sont (respectivement) les changements de variables :

$$t \mapsto t + b \, , \, t \mapsto at \, , \, t \mapsto t^{-1} \ .$$

Ces automorphismes engendrent donc le groupe $\mathrm{Aut}_k(k(t))$.

Donc si on pose $G := \mathrm{Aut}_k(k(t))$, on a :

$$[k(t) : k(t)^G] = |G| = q^3 - q \ .$$

Or, $f := \frac{(t^{q^2} - t)^{q+1}}{(t^q - t)^{q^2+1}}$ est invariante par les changements de variables $t \mapsto t+b$, $t \mapsto at$ et $t \mapsto t^{-1}$ comme de simples calculs le démontrent. Donc $f \in k(t)^G$.

Or,

$$\begin{aligned} t^{q^2} - t &= t^{q^2} - t^q + t^q - t \\ &= (t^q - t)^q + t^q - t \\ &= (t^q - t)((t^q - t)^{q-1} + 1) \end{aligned}$$

donc on a :

$$f = \frac{(t^q - t)^{q+1}((t^q - t)^{q-1} + 1)^{q+1}}{(t^q - t)^{q+1}}$$
$$= \frac{((t^q - t)^{q-1} + 1)^{q+1}}{(t^q - t)^{q^2-q}} \ .$$

La fraction est sous-forme irréductible donc :

$$[k(t) : k(f)] = \max\{(q+1)(q^2 - q), q(q^2 - q)\} = q^3 - q \ .$$

On a donc :

$$k(f) \subseteq k(t)^G \subseteq k(t)$$

et :

$$k(t) : k(t)^G] = [k(t) : k(f)] = q^3 - q$$

ce qui entraîne que :

$$k(f) = k(t)^G \ .$$