

Correction des exercices sur les formes modulaires

CHAPITRE I

1. Énoncé du théorème de Deligne

Exercice 1

Soient $P = X^3 - 2 \in \mathbb{Z}[X]$ et $\alpha \in \mathbb{C}$ une racine de P . Le corps de décomposition K de P est de degré 6 de groupe de Galois isomorphe à \mathbb{S}_3 . Puisque \mathbb{S}_3 et $\mathrm{GL}_2(\mathbb{F}_2)$ sont isomorphes (*), on obtient par restriction une représentation $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_2)$ surjective non ramifiée en dehors de 2 et 3. En effet, on a $K = \mathbb{Q}(\alpha, \sqrt{-3})$ dont le discriminant est $-2^4 \cdot 3^7$ (il suffit de préciser que $\mathbb{Q}(\alpha)$ est non ramifié en dehors de 2 et 3, car le discriminant de P est $-108 = -2^2 \cdot 3^3$; en fait le discriminant de K est aussi -108 et 2, 3 sont totalement ramifiés dans $\mathbb{Q}(\alpha)$).

(*) Un isomorphisme $f : \mathbb{S}_3 \rightarrow \mathrm{GL}_2(\mathbb{F}_2)$ s'obtient en posant

$$f((1, 2)) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad f((1, 3)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad f((2, 3)) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$f((1, 2, 3)) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad f((1, 3, 2)) = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

En fait, \mathbb{S}_3 est engendré par les deux transpositions $(1, 2)$ et $(2, 3)$ de sorte qu'il suffit de préciser leurs images pour déterminer f (on a $(1, 2)(2, 3) = (1, 2, 3)$). Les éléments d'ordre 2 sont de trace nulle (leur polynôme minimal est $X^2 - 1$) et ceux d'ordre 3 sont de trace 1 (leur polynôme minimal est $X^2 + X + 1$ car il est de degré 2 et divise $X^3 - 1$).

Vérifions que la classe d'isomorphisme de cette représentation ne dépend pas de l'isomorphisme choisi entre $\mathrm{Gal}(K/\mathbb{Q})$ et $\mathrm{GL}_2(\mathbb{F}_2)$. Soient f et g deux tels isomorphismes et ρ, ρ' les représentations correspondantes. L'élément fg^{-1} est un automorphisme de $\mathrm{GL}_2(\mathbb{F}_2)$, donc est intérieur (tous les automorphismes de \mathbb{S}_3 sont intérieurs : on montre que $\mathrm{Aut}(\mathbb{S}_3)$ est d'ordre 6. Soient $f \in \mathrm{Aut}(\mathbb{S}_3)$ et σ_i les trois transpositions. Le groupe \mathbb{S}_3 est engendré par deux d'entre elles, disons σ_1 et σ_2 . Il y a trois possibilités pour $f(\sigma_1)$ et deux pour $f(\sigma_2)$, d'où l'assertion. Par ailleurs le centre de \mathbb{S}_3 est trivial, ce qui entraîne le résultat). Il existe donc $M \in \mathrm{GL}_2(\mathbb{F}_2)$ tel que $fg^{-1} = \alpha_M$, où $\alpha_M(P) = MPM^{-1}$ pour tout $P \in \mathrm{GL}_2(\mathbb{F}_2)$. Par ailleurs, on a $\rho = f \circ \mathrm{Res}$ et $\rho' = g \circ \mathrm{Res}$. On en déduit que $\rho = \alpha_M \circ g \circ \mathrm{Res} = \alpha_M \circ \rho'$. Ainsi, pour tout $\sigma \in G_{\mathbb{Q}}$, on a $\rho(\sigma) = M\rho'(\sigma)M^{-1}$, ce qui signifie que ρ et ρ' sont isomorphes.

Étant donné un nombre premier $p \neq 2, 3$, il est facile de déterminer la trace de $\rho(\mathrm{Frob}_p)$. En effet, il s'agit pour cela de calculer son ordre. Si \mathfrak{P} est un idéal premier de O_K (l'anneau d'entiers de K) au-dessus de p et si $\sigma_{\mathfrak{P}}$ est la substitution de Frobenius en \mathfrak{P} dans K/\mathbb{Q} , il s'agit donc de déterminer l'ordre de $\sigma_{\mathfrak{P}}$ dans $\mathrm{Gal}(K/\mathbb{Q})$. On utilise le

fait que $\sigma_{\mathfrak{P}}$ restreint à $\mathbb{Q}(\sqrt{-3})$ est la substitution de Frobenius de $\mathfrak{P} \cap A$ dans $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ où A est l'anneau d'entiers de ce corps quadratique, et cette substitution est triviale si et seulement si p est décomposé dans K . Par ailleurs les éléments d'ordre 3 dans $\text{Gal}(K/\mathbb{Q})$ fixent $\mathbb{Q}(\sqrt{-3})$. On en déduit que :

- 1) si p est inerte dans $\mathbb{Q}(\sqrt{-3})$, alors $\sigma_{\mathfrak{P}}$ ne fixe pas $\mathbb{Q}(\sqrt{-3})$ et $\sigma_{\mathfrak{P}}$ est alors d'ordre 2. On a donc dans ce cas $\text{Tr } \rho(\text{Frob}_p) = 0$.
- 2) Si p est décomposé dans $\mathbb{Q}(\sqrt{-3})$, on a deux cas à considérer selon que p est totalement décomposé dans K ou non. En fait :

Lemme. *Le nombre premier p est totalement décomposé dans K si et seulement si 2 est un cube dans \mathbb{F}_p et $\left(-\frac{3}{p}\right) = 1$ (cette dernière condition signifie $p \equiv 1 \pmod{3}$).*

Démonstration : On peut supposer $p \geq 5$ (2 et 3 sont ramifiés dans K de sorte que l'énoncé est vrai dans ce cas : on a $\left(-\frac{3}{2}\right) = -1$). Soit \mathfrak{p} un idéal premier de A au-dessus de p . Le polynôme P est séparable modulo \mathfrak{p} , donc \mathfrak{p} est (totalement) décomposé dans K si et seulement si P a une racine dans A/\mathfrak{p} . Si p est totalement décomposé dans K , on a $\left(-\frac{3}{p}\right) = 1$ et A/\mathfrak{p} est isomorphe à \mathbb{F}_p . Ainsi 2 est un cube dans \mathbb{F}_p . Inversement, si $\left(-\frac{3}{p}\right) = 1$, p est décomposé dans $\mathbb{Q}(\sqrt{-3})$ et P a une racine dans A/\mathfrak{p} , d'où le lemme.

Si p est totalement décomposé dans K , $\sigma_{\mathfrak{P}}$ est l'identité de K , i.e. $\sigma_{\mathfrak{P}}$ est dans le noyau de ρ , autrement dit, $\rho(\sigma_{\mathfrak{P}})$ est la matrice identité et en particulier on a $\text{Tr } \rho(\text{Frob}_p) = 0$. Supposons p totalement décomposé dans $\mathbb{Q}(\sqrt{-3})$ et pas dans K . Dans ce cas, $\sigma_{\mathfrak{P}}$ fixe $\mathbb{Q}(\sqrt{-3})$, ce qui entraîne que son ordre est 3. Par suite, $\text{Tr } \rho(\text{Frob}_p) = 1$.

On obtient donc l'énoncé suivant :

Proposition. *On a $\text{Tr } \rho(\text{Frob}_p) = 0$ si et seulement si on est dans l'un des deux cas suivants :*

- 1) on a $p \equiv 2 \pmod{3}$.
- 2) On a $p \equiv 1 \pmod{3}$ et 2 est un cube dans \mathbb{F}_p .

Sinon, on a $\text{Tr } \rho(\text{Frob}_p) = 1$.

Démonstration : Compte tenu de ce qui précède, il suffit de remarquer que l'on a $\left(-\frac{3}{p}\right) = \left(\frac{p}{3}\right)$.

2) Il suffit de considérer les représentations associées à P et au polynôme $X^3 - 3$. Cette dernière est non ramifiée en dehors de 3 et celle associée à P est ramifiée en 2.

Exercice 2

Il s'agit de montrer qu'il n'existe pas d'extensions de degré 3 de \mathbb{Q} non ramifiée en dehors de 2.

On remarque pour cela qu'il n'existe pas d'extensions de degré 3 de \mathbb{Q} dont la valeur absolue du discriminant D soit 4. Cela résulte de la formule de Samuel p. 70 (appliquée avec $n = 3$)

$$|D| \geq \left(\frac{3\pi}{4}\right)^{n-1} \times \frac{\pi}{3}.$$

Cela donne ici $|D| \geq 5,81$.

Supposons qu'il existe une extension K/\mathbb{Q} de degré 3 non ramifiée en dehors de 2.

a) Si K/\mathbb{Q} est galoisienne : on a nécessairement $2O_K = \mathfrak{P}^3$ où \mathfrak{P} est l'unique idéal premier de O_K au-dessus de 2. On en déduit que la différentielle $D_{K/\mathbb{Q}}$ est \mathfrak{P}^2 (car l'indice de ramification, qui est 3, est premier à la caractéristique résiduelle de \mathfrak{P}). Il en résulte que $|D_K| = 2^2 = 4$ (la norme de K sur \mathbb{Q} de \mathfrak{P} est 2). D'où une contradiction dans ce cas.

b) Si K/\mathbb{Q} est non galoisienne : sa clôture galoisienne L est de degré 6 sur \mathbb{Q} de groupe de Galois S_3 . Le corps quadratique H contenu dans L est $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ ou $\mathbb{Q}(\sqrt{-2})$. En effet, K/\mathbb{Q} étant non ramifiée en dehors de 2, il en est de même de l'extension L/\mathbb{Q} . Par ailleurs, l'anneau d'entiers de H est principal et l'extension L/H est non ramifiée à l'infini. C'est évident si $H = \mathbb{Q}(i)$ ou $\mathbb{Q}(\sqrt{-2})$; si $H = \mathbb{Q}(\sqrt{2})$, le discriminant de K est en fait deux fois un carré et est en particulier positif, ce qui entraîne (dans notre situation en degré 3) que K est totalement réel, et il en est de même de L . Il en résulte que l'extension L/H est totalement ramifiée au-dessus de 2 et l'indice de ramification de 2 dans L/\mathbb{Q} est donc 6 et celui dans K/\mathbb{Q} est 3. On a donc encore $2O_K = \mathfrak{P}^3$, d'où une contradiction comme ci-dessus et l'exercice.

Exercice 3

1) Le polynôme minimal de $\rho(c)$ est $X^2 - 1$. En effet, il divise ce polynôme et il est distinct de $X \pm 1$ car $\ell \neq 2$ et le déterminant de $\rho(c)$ est -1 [si $X + 1$ annulait $\rho(c)$, $\rho(c)$ serait la matrice moins l'identité]. Par suite, $\rho(c)$ a deux valeurs propres distinctes ± 1 , d'où l'assertion.

2) Soit $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_2)$ la représentation associée au polynôme $X^3 - 2$. Alors, $\rho(c)$ n'est pas conjuguée à l'identité, i.e. n'est pas l'identité, car c n'est pas dans le noyau de ρ . En effet, c ne fixe pas K car $\mathbb{Q}(\sqrt{-3})$ est contenu dans K . Cet argument vaut en remplaçant $X^3 - 2$ par un polynôme de degré 3 irréductible de $\mathbb{Q}[X]$ dont le discriminant est < 0 .

Exercice 4

1) Considérons une extension galoisienne finie L/\mathbb{Q} contenant les corps laissés fixes par les noyaux de $\det(\rho_{f,\ell})$ et de χ . Soit σ un élément de $\mathrm{Gal}(L/\mathbb{Q})$. D'après le théorème de densité de Chebotarev, il existe un idéal premier \mathfrak{P} de O_L au-dessus d'un nombre premier $p \neq \ell$ tel que $\sigma = \sigma_{\mathfrak{P}}$, où $\sigma_{\mathfrak{P}}$ est la substitution de Frobenius en \mathfrak{P} dans l'extension L/\mathbb{Q} . Il s'agit donc de vérifier que l'on a

$$\chi^{k-1}(\sigma_{\mathfrak{P}}) = \det(\rho_{f,\ell})(\sigma_{\mathfrak{P}}).$$

(On identifie ici χ et $\det(\rho_{f,\ell})$ à des homomorphismes de $\text{Gal}(L/\mathbb{Q})$ dans \mathbb{F}_ℓ^* .) On a l'égalité $\chi(\sigma_{\mathfrak{P}}) = p \bmod \ell$. En effet, soit ζ un générateur de μ_ℓ . On a ($\zeta \in L$)

$$\sigma_{\mathfrak{P}}(\zeta) \equiv \zeta^p \bmod \mathfrak{P}.$$

Par ailleurs, il existe j tel que $\sigma_{\mathfrak{P}}(\zeta) = \zeta^j$, d'où $\zeta^j \equiv \zeta^p \bmod \mathfrak{P}$. On obtient la congruence $1 - \zeta^{p-j} \equiv 0 \bmod \mathfrak{P}$. Cela entraîne $j \equiv p \bmod \ell$ car $1 - \zeta$ est un générateur de l'idéal premier de l'anneau d'entiers de $\mathbb{Q}(\mu_\ell)$ au-dessus de ℓ et $\ell \neq p$. Par suite, $\sigma_{\mathfrak{P}}(\zeta) = \zeta^p$, d'où l'assertion et l'égalité $\det(\rho_{f,\ell}) = \chi^{k-1}$.

2) On a $\det \rho_{f,\ell}(c) = (-1)^{k-1} = -1$ car k est pair.

2. Description de l'image de $\rho_{f,\ell}$

Exercice 5

1) Soit H_ℓ le sous-groupe de $\text{GL}_2(\mathbb{F}_\ell)$ formé des éléments dont le déterminant est une puissance $k-1$ -ième dans \mathbb{F}_ℓ^* . On a $\det \rho_{f,\ell} = \chi^{k-1}$, par suite G_ℓ est contenu dans H_ℓ . Par ailleurs, le caractère cyclotomique $\chi : G_\mathbb{Q} \rightarrow \mathbb{F}_\ell^*$ est surjectif car les racines primitives ℓ -ièmes de l'unité sont conjuguées sur \mathbb{Q} : si $a \in \mathbb{F}_\ell^*$ et si ζ est un générateur de μ_ℓ , il existe $\sigma \in G_\mathbb{Q}$ tel que $\sigma(\zeta) = \zeta^a$, et l'on a alors $\chi(\sigma) = a$. Si l'on a $b = a^{k-1} \in \mathbb{F}_\ell^{*k-1}$, il existe donc $\sigma \in G_\mathbb{Q}$ tel que $\det \rho_{f,\ell}(\sigma) = b$. On en déduit la suite exacte

$$1 \rightarrow \text{SL}_2(\mathbb{F}_\ell) \xrightarrow{i} G_\ell \xrightarrow{\det} \mathbb{F}_\ell^{*k-1} \rightarrow 1,$$

où i est le morphisme d'inclusion. Par ailleurs, on a aussi la suite exacte

$$1 \rightarrow \text{SL}_2(\mathbb{F}_\ell) \xrightarrow{i} H_\ell \xrightarrow{\det} \mathbb{F}_\ell^{*k-1} \rightarrow 1.$$

En effet, si $c \in \mathbb{F}_\ell^{*k-1}$, la matrice $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$ appartient à H_ℓ . Il en résulte que $H_\ell = G_\ell$ (cf. les ordres des deux groupes et le fait que G_ℓ soit contenu dans H_ℓ).

2) D'après la question précédente, on a $G_\ell = \text{GL}_2(\mathbb{F}_\ell)$ si et seulement si $\mathbb{F}_\ell^* = \mathbb{F}_\ell^{*k-1}$. En effet, si $G_\ell = \text{GL}_2(\mathbb{F}_\ell)$, alors le déterminant de toute matrice est une puissance $k-1$ -ième dans \mathbb{F}_ℓ , d'où $\mathbb{F}_\ell^* = \mathbb{F}_\ell^{*k-1}$ (car tel est le cas de la matrice $\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ où $a \in \mathbb{F}_\ell^*$). Inversement, supposons $\mathbb{F}_\ell^* = \mathbb{F}_\ell^{*k-1}$. Le sous-groupe de $\text{GL}_2(\mathbb{F}_\ell)$ formé des éléments dont le déterminant est dans \mathbb{F}_ℓ^{*k-1} est alors $\text{GL}_2(\mathbb{F}_\ell)$ tout entier, d'où l'assertion. Par ailleurs, on a $\mathbb{F}_\ell^* = \mathbb{F}_\ell^{*k-1}$ si et seulement si $k-1$ est premier à $\ell-1$. (On considère le morphisme de $\mathbb{F}_\ell^* \rightarrow \mathbb{F}_\ell^*$ qui à x associe x^{k-1} . Si $\mathbb{F}_\ell^* = \mathbb{F}_\ell^{*k-1}$, il est injectif. Or si $n \geq 2$ divise $k-1$ et $\ell-1$, il existe un élément x d'ordre n dans \mathbb{F}_ℓ^* et $x^{k-1} = 1$, ce qui contredit l'injectivité. Inversement, ce morphisme est injectif, donc est aussi surjectif). Par suite, sous l'hypothèse faite i.e. si $\text{SL}_2(\mathbb{F}_\ell)$ est contenu dans l'image de $\rho_{f,\ell}$, alors

$$G_\ell = \text{GL}_2(\mathbb{F}_\ell) \iff \text{pgcd}(k-1, \ell-1) = 1.$$

2.1. Sous-groupes de Cartan

Exercice 6

Soient $g \in \mathbb{GL}(V)$ et P son polynôme minimal. Soit d l'ordre de g . On a $g^d = 1$, de sorte que P divise $X^d - 1$. Si ℓ ne divise pas d , cela entraîne que P est séparable i.e. que g est semi-simple. Inversement, si g semi-simple, g est diagonalisable sur \mathbb{F}_{ℓ^2} , donc son ordre est premier à ℓ . [Dire que P est séparable signifie que les racines de P dans $\overline{\mathbb{F}_{\ell}}$ sont simples, autrement dit, que g est diagonalisable sur $\overline{\mathbb{F}_{\ell}}$.]

Exercice 7

1) Le commutant k de g est un sous- \mathbb{F}_{ℓ} -espace vectoriel de $\text{End}(V)$. On montre que k est de dimension 2 sur \mathbb{F}_{ℓ} . Puisque g n'est pas une homothétie, il existe une droite qui ne soit pas stable par g , autrement dit, il existe $x \in V$ tel que $(x, g(x))$ soit une base de V . Considérons l'application $k \rightarrow V$ qui à $f \in k$ associe $f(x)$. C'est une application linéaire injective : si $f(x) = 0$ l'égalité $f \circ g = g \circ f$ entraîne $f(g(x)) = 0$, par suite $f = 0$. On en déduit que la dimension de k sur \mathbb{F}_{ℓ} est au plus 2. Par ailleurs, $\mathbb{F}_{\ell}[g]$ est contenu dans k et la dimension de $\mathbb{F}_{\ell}[g]$ sur \mathbb{F}_{ℓ} est au moins 2. D'où $k = \mathbb{F}_{\ell}[g]$. [Si $a + bg = 0$ avec $a, b \in \mathbb{F}_{\ell}$, on a $a = b = 0$, car le polynôme minimal de g n'est pas de degré 1. Par suite, $(1, g)$ est libre sur \mathbb{F}_{ℓ} .] En fait la dimension de $\mathbb{F}_{\ell}[g]$ est le degré du polynôme minimal de g .

2) et 3) Le polynôme P est un générateur du noyau du morphisme de \mathbb{F}_{ℓ} -algèbres $\mathbb{F}_{\ell}[X] \rightarrow \mathbb{F}_{\ell}[g]$ qui à F associe $F(g)$. Il est surjectif. Par suite, on a un isomorphisme de $\mathbb{F}_{\ell}[X]/(P)$ sur $\mathbb{F}_{\ell}[g]$ qui n'est autre que k . D'où les assertions.

4) Le centralisateur C de g dans $\mathbb{GL}(V)$ est formé des éléments de k qui sont inversibles. Ainsi, l'ordre de C est $(\ell - 1)^2$ si P est réductible et $\ell^2 - 1$ sinon. Dans ce dernier cas, on a en fait $C = k^*$.

Exercice 8

1) Un élément semi-simple de $\mathbb{GL}(V) \simeq \mathbb{GL}_2(\mathbb{F}_2)$ est d'ordre impair, donc est d'ordre 1 ou 3. Par suite, un sous-groupe de Cartan déployé de $\mathbb{GL}(V)$ est le centralisateur d'un élément d'ordre 3 (car l'élément en question n'est pas une homothétie). Or l'ordre d'un sous-groupe de Cartan déployé de $\mathbb{GL}(V)$ est $(\ell - 1)^2 = 1$. D'où l'assertion.

3) Soit H le fixateur de $\{D, D'\}$ i.e. le sous-groupe de $\mathbb{GL}(V)$ formé des éléments s tels que $sD = D$ et $sD' = D'$. Il est d'ordre $(\ell - 1)^2$, donc il existe dans H un élément g qui n'est pas une homothétie. Cet élément est semi-simple car il d'ordre premier à ℓ . Le polynôme minimal de g est réductible et l'on a $H = C(g)$, où $C(g)$ est le centralisateur de g . En effet, l'ordre de $C(g)$ est celui de H et H est contenu dans $C(g)$; en effet, posons $D = \langle u \rangle$ et $D' = \langle u' \rangle$, de sorte que (u, u') est une base de V . Soit $h \in H$. On a $hgh^{-1}(u) = g(u)$ et $hgh^{-1}(u') = g(u')$, d'où $hgh^{-1} = g$ i.e. $hg = gh$, d'où l'assertion. On en déduit que H est un sous-groupe de Cartan déployé de $\mathbb{GL}(V)$.

3) Le groupe H est le centralisateur d'un élément g dont le polynôme minimal est de la forme $(X - a)(X - b)$ où $a \neq b$ sont dans \mathbb{F}_{ℓ}^* . Par suite, g a exactement deux droites

propres D_1 et D_2 [D_1 est par exemple l'ensemble des $x \in V$ tel que $g(x) = ax$]. Ces deux droites sont stables par tout élément de H (car pour tout $s \in H$ on a $sg = gs$). D'où l'assertion.

4) Soient H et H' deux sous-groupes de Cartan déployés de $\mathbb{GL}(V)$. Soient (D_1, D_2) et (D'_1, D'_2) les couples de droites propres associés à H et H' . Il existe $s \in \mathbb{GL}(V)$ tel que $sD_1 = D'_1$ et $sD_2 = D'_2$. Cela entraîne que $sHs^{-1} = H'$. En effet, sHs^{-1} est le fixateur de D'_1 et D'_2 qui n'est autre que H' [Si $\alpha D'_1 = D'_1$, on a $\alpha sD_1 = sD_1$, d'où $(s^{-1}\alpha s)D_1 = D_1$ et idem pour D'_2 . Par suite si α fixe $\{D'_1, D'_2\}$ i.e. si $\alpha \in H'$, alors $s^{-1}\alpha s$ appartient à H i.e. $\alpha \in sHs^{-1}$. L'inverse est clair.]

5) Il y en a exactement le nombre de paires de droites de V i.e. $C_{\ell+1}^2 = \ell(\ell+1)/2$ [l'application qui à un couple de droites distinctes de V associe le fixateur de ces deux droites est une bijection sur l'ensemble des sous-groupes de Cartan de $\mathbb{GL}(V)$].

Une autre façon de procéder est la suivante : on sait qu'il n'y a qu'une seule classe de conjugaison de sous-groupes de Cartan déployé. Soit H un tel sous-groupe. Leur nombre est donc le cardinal de la classe de conjugaison de H i.e. l'indice du normalisateur $N(H)$ de H dans $\mathbb{GL}(V)$. Si l'on sait que $N(H)$ est d'ordre $2(\ell-1)^2$, on en déduit que le nombre cherché est

$$\frac{|\mathbb{GL}(V)|}{2(\ell-1)^2} = \frac{\ell(\ell+1)}{2}.$$

Exercice 9

1) Un sous-groupe de Cartan non déployé possède cette propriété. Inversement, soit k une sous-algèbre de $\text{End}(V)$ qui soit un corps de cardinal ℓ^2 . Il s'agit de montrer qu'il existe un élément semi-simple $g \in \mathbb{GL}(V)$ qui n'est pas une homothétie tel que k soit le commutant de g . Il y a $\ell-1$ homothéties dans $\mathbb{GL}(V)$ et k est d'ordre ℓ^2-1 , donc il existe $g \in k^*$ qui n'est pas une homothétie. Montrons que k est le commutant de g . Le commutant de g dans $\text{End}(V)$ est $\mathbb{F}_\ell[g]$. Puisque k est abélien, k est contenu dans $\mathbb{F}_\ell[g]$ et par ailleurs $\mathbb{F}_p[g]$ est contenu dans k . D'où $k = \mathbb{F}_\ell[g]$ et l'assertion. L'ordre de g divise ℓ^2-1 , donc est premier à ℓ , autrement dit, g est semi-simple. D'où le résultat.

2) Soit $g \in \mathbb{GL}(V)$ ayant P pour polynôme minimal. Ce n'est pas une homothétie, donc il existe $x \in V$ tel que $(x, g(x))$ soit une base de V . Supposons $P = X^2 + aX + b \in \mathbb{F}_\ell[X]$. La matrice de g dans cette base est

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

Si maintenant g' est un autre élément de $\mathbb{GL}(V)$ ayant P pour polynôme minimal, il existe de même $y \in V$ tel que $(y, g'(y))$ soit une base de V . Dans ces deux bases g et g' sont représentés par la même matrice, donc g et g' sont conjugués dans $\mathbb{GL}(V)$. D'où l'assertion. [Soient B et B' ces bases et P_0 la matrice de passage de B à B' . On a

$$\text{Mat}(g, B') = P_0^{-1} \text{Mat}(g, B) P_0 = P_0^{-1} \text{Mat}(g', B') P_0.$$

On a donc $g = u^{-1}g'u$ où u est l'élément de $\mathbb{GL}(V)$ dont la matrice dans B' est P_0 .]

Autre preuve : P est de degré 2 donc est aussi le polynôme caractéristique χ de g . Le premier invariant de similitude est donc 1 (le produit des invariants de similitudes est χ). Ainsi deux tels éléments de $\mathbb{GL}(V)$ ont les mêmes invariants de similitudes donc sont conjugués.

3) Soient k_1 et k_2 deux sous-algèbres de $\text{End}(V)$ qui soient des corps à ℓ^2 éléments. Montrons que k_1 et k_2 sont conjugués dans $\text{End}(V)$ et donc que les groupes k_1^* et k_2^* sont des sous-groupes conjugués de $\mathbb{GL}(V)$. On considère pour cela un générateur γ de $\mathbb{F}_{\ell^2}^*$ et P son polynôme minimal sur \mathbb{F}_ℓ . Considérons un isomorphisme φ_1 de \mathbb{F}_ℓ -algèbres de \mathbb{F}_{ℓ^2} sur k_1 . Alors le polynôme minimal de $\varphi_1(\gamma) \in \text{End}(V)$ est P [$\varphi_1(\gamma)$ est annulé par P et P est irréductible sur \mathbb{F}_ℓ]. Il en est de même dans k_2 , autrement dit, il existe dans k_1 et k_2 deux éléments g_1 et g_2 dont les polynômes minimaux sont égaux à P . Puisque g_1 et g_2 le même polynôme minimal, ils sont conjugués dans $\mathbb{GL}(V)$. Si l'on a $ug_1u^{-1} = g_2$, parce que g_i est un générateurs de k_i^* , on a donc $uk_1u^{-1} = k_2$, d'où l'assertion. la question 1 entraîne alors le résultat.

4) Si l'on sait que le normalisateur d'un sous-groupe de Cartan non déployé est d'ordre $2(\ell^2 - 1)$, on déduit alors de la question 3 que le nombre cherché est

$$\frac{|\mathbb{GL}(V)|}{2(\ell^2 - 1)} = \frac{\ell(\ell - 1)}{2}.$$

[Soient G un groupe et H un sous-groupe de G . L'indice du normalisateur $N(H)$ de H dans G est le nombre de sous-groupes de G qui sont conjugués à H .]

Justification de l'assertion 2 p. 7 : tout élément de \mathbb{F}_{ℓ^2} s'écrit sous la forme $a + bt$ où $a, b \in \mathbb{F}_\ell$. La \mathbb{F}_ℓ -algèbre k est donc constituée des endomorphismes de V de la forme

$$a1_V + b\rho_t,$$

où ρ_t est l'endomorphisme de multiplication par t . La matrice d'un tel endomorphisme dans la base $(1, t)$ est précisément

$$\begin{pmatrix} a & b\alpha \\ b & a \end{pmatrix},$$

d'où l'assertion (cet endomorphisme est nul si et seulement si $a = b = 0$).

Exercice 10

Les groupes C_α et C_β sont conjugués dans $\mathbb{GL}(V)$: il existe $t \in \mathbb{F}_\ell$ tel que l'on ait $\alpha = t^2\beta$ (car $\alpha\beta$ est un carré dans \mathbb{F}_ℓ). Posons

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

On a alors $MC_\alpha M^{-1} = C_\beta$.

2.2. Normalisateurs des sous-groupes de Cartan

Exercice 11

1) Notons H l'ensemble des $s \in \mathbb{GL}(V)$ tels que $sD_1 = D_2$ et $sD_2 = D_1$. Il s'agit de montrer que $N - C = H$. D'abord H est contenu dans N . En effet, soit $s \in H$. Pour tout $g \in C$, on a

$$sgs^{-1}D_1 = sgD_2 = sD_2 = D_1 \quad \text{et} \quad sgs^{-1}D_2 = D_2.$$

On en déduit que $sgs^{-1} \in C$ i.e. que s normalise C , autrement dit, que $s \in N$. D'où l'assertion. En particulier, H est contenu dans $N - C$ car $D_1 \neq D_2$. Inversement, soit $s \in N - C$. Pour tout $g \in C$, on a

$$sgs^{-1}(sD_1) = sgD_1 = sD_1 \quad \text{et} \quad sgs^{-1}(sD_2) = sD_2.$$

Par ailleurs, puisque $sgs^{-1} \in C$, on a

$$sgs^{-1}(D_1) = D_1 \quad \text{et} \quad sgs^{-1}(D_2) = D_2.$$

Puisque s n'est pas dans C , s n'est pas une homothétie et sgs^{-1} non plus. Par suite, sgs^{-1} a exactement deux droites stables, d'où $sD_1 = D_1$ ou $sD_1 = D_2$ et $sD_2 = D_2$ ou $sD_2 = D_1$. Le fait que s ne soit pas dans C entraîne alors $sD_1 = D_2$ et $sD_2 = D_1$ i.e. s est dans H . D'où le résultat.

2) Soient $g, s \in N - C$. Ils sont en relation modulo C i.e. $g^{-1}s \in C$. En effet, on a

$$g^{-1}sD_1 = g^{-1}D_2 = D_1 \quad \text{et} \quad g^{-1}sD_2 = D_2.$$

Il y a donc deux classes de N modulo C , à savoir C et $N - C$ (le groupe N/C est d'ordre 2). D'où l'assertion.

Exercice 12

Commençons par la remarque suivante :

Soit k un sous-corps de $\text{End}(V)$ à ℓ^2 éléments. Soit $g \in k$ non nul. Le polynôme minimal de g sur \mathbb{F}_ℓ est le polynôme minimal de g comme endomorphisme de V (i.e. comme élément de $\mathbb{GL}(V)$).

Preuve : Si g est dans \mathbb{F}_ℓ , g est une homothétie et le polynôme minimal est de degré 1 égal à $X - g$ dans les deux cas (\mathbb{F}_ℓ s'identifie aux homothéties dans k i.e. dans $\text{End}(V)$: cf. l'assertion 2 p. 7. Dans l'énoncé cela est sous-entendu). Supposons g non dans \mathbb{F}_ℓ . Soit $P \in \mathbb{F}_\ell[X]$ le polynôme minimal de g sur \mathbb{F}_ℓ . On a $P(g) = 0$ et P annule donc l'endomorphisme g , d'où l'assertion (le polynôme minimal de $g \in \text{End}(V)$ divise P et il est de degré 2 car n'étant pas dans \mathbb{F}_ℓ , g n'est pas une homothétie).

1) Cette question résulte de la remarque ci-dessus car g et $F(g)$ sont conjugués sur \mathbb{F}_ℓ donc ont le même polynôme minimal sur \mathbb{F}_ℓ . Ils ont donc le même polynôme minimal P dans $\mathbb{GL}(V)$.

2) Le polynôme P est de degré 2. D'après la question 2 de l'exercice 9, g et $F(g)$ sont donc conjugués dans $\mathbb{GL}(V)$. (Notons que deux homothéties sont conjuguées si et seulement si elles sont égales, donc on utilise le fait que P soit de degré 2).

3) D'après la question 2, il existe $\gamma \in \mathbb{GL}(V)$ tel que $\gamma g \gamma^{-1} = F(g)$. En particulier, γ appartient à N . Pour tout élément $u \in k$, on a $\gamma u \gamma^{-1} = F(u)$. Le fait que ϕ soit un morphisme de groupes est immédiat. Son noyau est $C = k^*$ car k^* est son propre centralisateur [k^* est le centralisateur d'un élément semi-simple $x \in \mathbb{GL}(V)$. Un élément qui centralise k centralise en particulier x , donc est dans k , et par ailleurs, k est abélien]. Le morphisme ϕ est surjectif car $\text{Aut}(k)$ est de cardinal 2 formé de l'identité et de F , et l'on a $\phi(\gamma) = F$. Il en résulte que N/C est isomorphe à $\text{Aut}(k)$, donc est d'ordre 2 i.e. C est d'indice 2 dans N .

4) Par définition de la structure du k -espace vectoriel V , on a donc $u.x = u(x)$ pour tout $u \in k$ et $x \in V$. Le noyau de ϕ est C . Par suite, s est dans C si et seulement si on a $su = us$ pour tout $u \in k$. Cette condition signifie que pour tout $x \in V$, on a $su(x) = us(x)$, autrement dit, que $s(u.x) = u.s(x)$, d'où l'assertion.

5) Les éléments de $N - C$ sont donc les $s \in \mathbb{GL}(V)$ tel que $\phi(s) = F$. Autrement dit, ce sont les éléments $s \in \mathbb{GL}(V)$ tels que pour tout $u \in k$, on ait $sus^{-1} = F(u)$. On a $F(u) = u^p$. Par suite, $N - C$ est formé des éléments $s \in \mathbb{GL}(V)$ possédant la propriété suivante : pour tout $x \in V$ et tout $u \in k$, on a l'égalité $s(u.x) = u^p.s(x)$. Ce sont les éléments $s \in \mathbb{GL}(V)$ sont semi-linéaires pour la structure du k -espace vectoriel V .

6) Les matrices indiquées normalisent C_α et elles forment avec C_α un sous-groupe de $\mathbb{GL}(V)$ d'ordre $2|C_\alpha|$. Puisque $|N_\alpha| = 2|C_\alpha|$, cet ensemble est donc N_α . On vérifie en effet, que l'on a

$$\begin{pmatrix} a & b\alpha \\ b & a \end{pmatrix}^{-1} = \frac{1}{d} \begin{pmatrix} -a & b\alpha \\ -b & a \end{pmatrix} \quad \text{avec} \quad d = b^2\alpha - a^2,$$

$$\begin{pmatrix} a & -b\alpha \\ b & -a \end{pmatrix} \begin{pmatrix} u & \alpha v \\ v & u \end{pmatrix} \begin{pmatrix} a & -b\alpha \\ b & -a \end{pmatrix}^{-1} = \begin{pmatrix} u & -\alpha v \\ -v & u \end{pmatrix} \in C_\alpha.$$

Exercice 13

Soit g un élément de $N - C$. Ce n'est pas une homothétie car sinon g serait dans C . Il s'agit de montrer que g^2 est une homothétie. Supposons le contraire. L'élément g^2 appartient à C car C est d'indice 2 dans N . En particulier, g^2 est semi-simple. Le centralisateur $C(g^2)$ est donc un sous-groupe de Cartan de $\mathbb{GL}_2(\mathbb{F}_\ell)$. Puisque g^2 est dans C et que C est abélien, on en déduit que C est contenu dans $C(g^2)$. Par suite, $C = C(g^2)$ (car deux sous-groupes de Cartan distincts ne sont pas comparables (*)). Ainsi g (qui

centralise g^2) appartient à C . D'où une contradiction et l'assertion. Le polynôme minimal de g est donc de la forme $X^2 - a$ et sa trace est nulle, d'où l'exercice.

(*) : cela se justifie comme suit :

a) deux Cartan de même nature contenus l'un dans l'autre sont égaux car ils ont le même ordre.

b) Un Cartan déployé ne peut être contenu dans un Cartan non déployé. En effet, ce dernier est cyclique et pas un Cartan déployé qui est isomorphe à $\mathbb{F}_\ell^* \times \mathbb{F}_\ell^*$.

c) Un Cartan non déployé ne peut être contenu dans un Cartan déployé, car sinon $\ell^2 - 1$ devrait diviser $(\ell - 1)^2$ ce qui n'est pas.

2.3. L'image de $\rho_{f,\ell}$ si ℓ est exceptionnel

Exercice 14

1) D'après l'hypothèse faite, l'image de $\rho_{f,\ell}$ est d'ordre premier à ℓ donc tous ses éléments sont semi-simples. Or $\mathrm{SL}_2(\mathbb{F}_\ell)$ contient des éléments qui ne sont pas semi-simples. D'après l'exercice 6, tel est le cas de $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ qui est d'ordre ℓ (et dont le polynôme minimal est $(X - 1)^2$).

2) Si $\ell \geq 3$, l'image de $\rho_{f,\ell}$ est encore d'ordre premier à ℓ et le même argument que celui ci-dessus entraîne que ℓ est exceptionnel pour f .

Supposons $\ell = 2$. Dans ce cas, C est le sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_2)$. Montrons que 2 n'est pas exceptionnel pour f . Sinon, l'image de $\rho_{f,2}$ ne contient pas $\mathrm{SL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2)$ et est donc d'ordre $d = 1, 2$ ou 3 . On a $d \neq 3$ car l'image de $\rho_{f,2}$ n'est pas contenue dans C par hypothèse. Si $d = 2$, alors $\rho_{f,2}$ est réductible et dans ce cas, $\rho_{f,2}$ est triviale car elle est semi-simple. Par suite $d = 1$, ce qui contredit de nouveau l'hypothèse faite. D'où l'assertion.

3) On a nécessairement $\ell \geq 3$ (cf. l'ordre de l'image dans $\mathrm{PGL}_2(\mathbb{F}_\ell)$).

Supposons $\ell = 3$ et l'image de $G_\mathbb{Q}$ dans $\mathrm{PGL}_2(\mathbb{F}_3)$ isomorphe à S_4 . Il s'agit de montrer que 3 n'est pas exceptionnel pour f . Les groupes $\mathrm{PGL}_2(\mathbb{F}_3)$ et S_4 étant isomorphes, l'hypothèse faite signifie que le morphisme $G_\mathbb{Q} \rightarrow \mathrm{PGL}_2(\mathbb{F}_3)$ que l'on obtient en composant $\rho_{f,3}$ avec la surjection canonique est surjectif. Soit H l'image de $\rho_{f,3}$ dans $\mathrm{GL}_2(\mathbb{F}_3)$. Vérifions que $H = \mathrm{GL}_2(\mathbb{F}_3)$, ce qui prouvera en particulier que 3 n'est pas exceptionnel pour f . On a par hypothèse

$$H\mathbb{F}_3^* = \mathrm{GL}_2(\mathbb{F}_3).$$

Il en résulte que H est d'indice ≤ 2 dans $\mathrm{GL}_2(\mathbb{F}_3)$. En effet, il y a au plus deux classes à gauches de $\mathrm{GL}_2(\mathbb{F}_3)$ modulo H (H et $-H$). On en déduit que le sous-groupe dérivé de $\mathrm{GL}_2(\mathbb{F}_3)$, qui n'est autre que $\mathrm{SL}_2(\mathbb{F}_3)$, est contenu dans H . Supposons que H soit d'indice 2 dans $\mathrm{GL}_2(\mathbb{F}_3)$. On a alors $H = \mathrm{SL}_2(\mathbb{F}_3)$. Mais l'image de $\mathrm{SL}_2(\mathbb{F}_3)$ dans $\mathrm{PGL}_2(\mathbb{F}_3)$, qui est $\mathrm{PSL}_2(\mathbb{F}_3)$ n'est pas $\mathrm{PGL}_2(\mathbb{F}_3)$. D'où $H = \mathrm{GL}_2(\mathbb{F}_3)$ et l'assertion.

Supposons $\ell \geq 5$ et l'image de $G_{\mathbb{Q}}$ dans $\mathrm{PGL}_2(\mathbb{F}_{\ell})$ isomorphe à S_4 . Montrons que l'image H de $\rho_{f,\ell}$ ne contient pas $\mathrm{SL}_2(\mathbb{F}_{\ell})$ i.e. que ℓ est exceptionnel pour f . Sinon, l'image de H dans $\mathrm{PGL}_2(\mathbb{F}_{\ell})$, qui est $H\mathbb{F}_{\ell}^*/\mathbb{F}_{\ell}^*$, contiendrait $\mathrm{PSL}_2(\mathbb{F}_{\ell}) = \mathrm{SL}_2(\mathbb{F}_{\ell})/\{\pm 1\}$ [le noyau de la flèche $\mathrm{SL}_2(\mathbb{F}_{\ell}) \rightarrow H\mathbb{F}_{\ell}^*/\mathbb{F}_{\ell}^*$ est $\{\pm 1\}$]. Par ailleurs, l'ordre de $\mathrm{PSL}_2(\mathbb{F}_{\ell})$ est $\ell(\ell^2 - 1)/2$, qui est plus grand que 24. D'où l'assertion.

Exercice 15

1) Soit c la conjugaison complexe de $G_{\mathbb{Q}}$. On a $\det(\rho_{f,\ell}(c)) = -1$ donc c n'est pas plus ou moins l'identité car $\ell \geq 3$. Par ailleurs, on a $c^2 = 1$, donc le polynôme minimal de c est $X^2 - 1$ qui est réductible. Il en résulte que $\rho_{f,\ell}(c)$ n'appartient pas à un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_{\ell})$. On a en effet le résultat suivant :

Lemme. Soient V un plan vectoriel sur \mathbb{F}_{ℓ} et C un sous-groupe de Cartan non déployé de $\mathrm{GL}(V)$. Soit g un élément de C qui n'est pas une homothétie. Alors, le polynôme minimal de g est irréductible de degré 2.

Preuve : On peut supposer $V = \mathbb{F}_{\ell^2}$. Dans ce cas, g est un élément de \mathbb{F}_{ℓ^2} qui n'est pas dans \mathbb{F}_{ℓ} . Son polynôme minimal sur \mathbb{F}_{ℓ} est le polynôme de g comme endomorphisme de V . D'où le résultat.

2) Notons G l'image de $\rho_{f,\ell}$ et PG son image dans $\mathrm{PGL}_2(\mathbb{F}_{\ell})$. On considère les deux morphismes donnés par le déterminant, formant un carré commutatif

$$\phi_1 : G \rightarrow \mathbb{F}_{\ell}^* \rightarrow \mathbb{F}_{\ell}^*/\mathbb{F}_{\ell}^{*2} \quad \text{et} \quad \phi_2 : G \rightarrow PG \rightarrow \mathbb{F}_{\ell}^*/\mathbb{F}_{\ell}^{*2}.$$

L'entier k est pair et l'on a pour $p \neq \ell$,

$$\det(\rho_{f,\ell}(\mathrm{Frob}_p)) = p^{k-1} \pmod{\ell}.$$

En choisissant p non résidu quadratique modulo ℓ , on en déduit que ϕ_2 est surjectif. En particulier, PG a un sous-groupe d'indice 2, ce qui n'est pas le cas de \mathbb{A}_4 ni \mathbb{A}_5 , d'où l'exercice.

Exercice 16

1) (i) \implies (ii) : Par hypothèse, il existe deux caractères continus $\varphi, \psi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^*$ tels que $\rho_{f,\ell}$ soit représentable sous la forme

$$\begin{pmatrix} \varphi & 0 \\ 0 & \psi \end{pmatrix}.$$

Puisque $\rho_{f,\ell}$ est non ramifiée en dehors de ℓ , il en est de même de φ et ψ . Compte tenu du fait que le déterminant de $\rho_{f,\ell}$ est χ^{k-1} , tout revient donc à démontrer le lemme suivant :

Lemme. Soit $\varphi : G_{\mathbb{Q}} \rightarrow \mathbb{F}_{\ell}^*$ un homomorphisme de groupes continu non ramifié en dehors de ℓ . Alors, φ est une puissance du caractère cyclotomique.

Preuve : On peut supposer $\ell \geq 3$ car l'énoncé est évident si $\ell = 2$. Puisque φ est continu, son noyau est ouvert et correspond à une extension abélienne finie K de \mathbb{Q} . Son degré divise $\ell - 1$ et K/\mathbb{Q} est non ramifiée en dehors de ℓ . Par suite, K est contenu dans $\mathbb{Q}(\mu_{\ell})$ (*) et φ se factorise à travers $\text{Gal}(\mathbb{Q}(\mu_{\ell})/\mathbb{Q})$. Par ailleurs, le nombre d'homomorphismes de groupes $\text{Gal}(\mathbb{Q}(\mu_{\ell})/\mathbb{Q}) \rightarrow \mathbb{F}_{\ell}^*$ est $\ell - 1$. Si χ est le caractère cyclotomique, ce sont donc $1, \chi, \dots, \chi^{\ell-2}$. Ainsi φ est puissance de χ .

(*) Vérifions cette assertion : d'abord K est contenu dans $\mathbb{Q}(\mu_{\ell^\infty})$ pour des raisons de ramification (et de corps de classes). Par ailleurs $[K : \mathbb{Q}]$ divise $\ell - 1$ car $\text{Gal}(K/\mathbb{Q})$ est isomorphe à un sous-groupe de \mathbb{F}_{ℓ}^* . Supposons que K soit contenu dans $\mathbb{Q}(\mu_{\ell^n})$ pour un certain $n \geq 2$. Le degré de $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}$ est $\ell^{n-1}(\ell - 1)$ et celui de $\mathbb{Q}(\mu_{\ell^n})/\mathbb{Q}(\mu_{\ell})$ est ℓ^{n-1} . Soit L le composé de $\mathbb{Q}(\mu_{\ell})$ et de K . L'extension $L/\mathbb{Q}(\mu_{\ell})$ est galoisienne de groupe de Galois isomorphe à $\text{Gal}(K/K \cap \mathbb{Q}(\mu_{\ell}))$. Par suite, si $K \neq K \cap \mathbb{Q}(\mu_{\ell})$, alors ℓ divise le degré de K sur \mathbb{Q} , ce qui n'est pas. Ainsi on a $K = K \cap \mathbb{Q}(\mu_{\ell})$ autrement dit K est contenu dans $\mathbb{Q}(\mu_{\ell})$. D'où l'assertion.

(ii) \implies (iii) : cette implication résulte de la démonstration de l'exercice 4. En effet, soit K le sous-corps de $\overline{\mathbb{Q}}$ laissé fixe par le noyau de $\rho_{f,\ell}$. Soient p un nombre premier distinct de ℓ et \mathfrak{P} un idéal premier de l'anneau des entiers de K au-dessus de p . Soit $\sigma_{\mathfrak{P}}$ la substitution de Frobenius en \mathfrak{P} dans K/\mathbb{Q} (ou un des ses relèvements). On a par définition

$$\text{Tr } \rho_{f,\ell}(\sigma_{\mathfrak{P}}) = \text{Tr } \rho(\text{Frob}_p),$$

qui n'est autre que $a_p \bmod \ell$. Par ailleurs, on a $\chi(\sigma_{\mathfrak{P}}) = p \bmod \ell$, d'où l'implication.

(iii) \implies (i) : D'après le théorème d'unicité des représentations semi-simples, la représentation $\rho_{f,\ell}$ est isomorphe à celle donnée par

$$\begin{pmatrix} \chi^m & 0 \\ 0 & \chi^{k-1-m} \end{pmatrix}.$$

En effet, elles sont non ramifiées en dehors de ℓ et en considérant une extension galoisienne L/\mathbb{Q} contenant les corps laissés fixes par leurs noyaux, on constate que les polynômes caractéristiques des éléments de Frobenius sont les mêmes. En particulier, $\rho_{f,\ell}$ est réductible.

2) Considérons nombre premier ℓ impair et $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{F}_{\ell})$ une représentation non ramifiée en dehors de ℓ . On suppose que l'image de ρ est contenue dans le normalisateur N d'un sous-groupe de Cartan C sans l'être dans C . Soit K le corps laissé fixe par le noyau de ρ . Soient p un nombre premier autre que ℓ , \mathfrak{P} un idéal premier de O_K (l'anneau d'entiers de K) au-dessus de p et $\sigma_{\mathfrak{P}}$ la substitution de Frobenius dans K/\mathbb{Q} . Montrons l'énoncé suivant :

Lemme. *L'élément $\rho(\sigma_{\mathfrak{P}})$ appartient à $N - C$ si et seulement si $\left(\frac{p}{\ell}\right) = -1$.*

Démonstration : Considérons le morphisme de groupes

$$\phi : G_{\mathbb{Q}} \rightarrow N \rightarrow N/C,$$

déduit de ρ [on a $\phi(\sigma) = \rho(\sigma)C$]. L'hypothèse faite sur l'image de ρ entraîne que ϕ est surjectif. Il est non ramifié en dehors de ℓ et le corps L laissé fixe par noyau de ϕ est contenu dans K : le noyau de ρ est contenu dans celui de ϕ . En particulier, L/\mathbb{Q} est non ramifié en dehors de ℓ . Il en résulte que L est une extension quadratique de \mathbb{Q} non ramifiée en dehors de ℓ . On a donc $L = \mathbb{Q}(\sqrt{\pm\ell})$. La restriction de $\sigma_{\mathfrak{P}}$ à L est la substitution de Frobenius de $\mathfrak{P} \cap O_L$ sur p . Soit σ_p cette substitution dans $\text{Gal}(L/\mathbb{Q})$. Les conditions suivantes sont équivalentes :

- 1) $\rho(\sigma_{\mathfrak{P}})$ appartient à $N - C$.
- 2) $\sigma_{\mathfrak{P}}$ ne fixe pas L , i.e. $\sigma_{\mathfrak{P}}$ n'est pas dans le noyau de ϕ .
- 3) σ_p n'est pas l'identité de L .
- 4) p est inerte dans L .

L'équivalence des conditions 3 et 4 se justifie comme suit : l'élément $\sigma_{\mathfrak{P}}$ est un générateur du groupe de décomposition en p dans $\text{Gal}(L/\mathbb{Q})$ qui est de cardinal f (avec $2 = fg$ car p est non ramifié). Si p est inerte on a $g = 1$, $f = 2$ d'où $\sigma_p \neq 1$. Inversement, si $\sigma_p \neq 1$, on a $f \neq 1$, d'où $f = 2$ puis $g = 1$, autrement dit, p est inerte dans L .

Tout revient donc à montrer que p est inerte dans L si et seulement si $\left(\frac{p}{\ell}\right) = -1$. Distinguons pour cela deux cas.

Supposons $\ell \equiv 1 \pmod{4}$. On a alors $L = \mathbb{Q}(\sqrt{\ell})$ et p est inerte dans L si et seulement si $\left(\frac{p}{\ell}\right) = -1$: c'est vrai si $p = 2$ et si p est impair, on a $\left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right)$. [Rappelons que 2 est inerte dans L si et seulement si $\ell \equiv 5 \pmod{8}$].

Supposons $\ell \equiv 3 \pmod{4}$. On a alors $L = \mathbb{Q}(\sqrt{-\ell})$. On vérifie de nouveau l'assertion si $p = 2$ et si p est impair, on a $\left(\frac{p}{\ell}\right) = \left(\frac{-\ell}{p}\right)$.

Les éléments de $N - C$ étant de trace nulle, cela entraîne le résultat.

3) On suppose que l'image de $\rho_{f,\ell}$ dans $\text{PGL}_2(\mathbb{F}_{\ell})$ est isomorphe à \mathbb{S}_4 . Soit s un élément de l'image de $\rho_{f,\ell}$. Il s'agit de vérifier que

$$\frac{\text{Tr}(s)^2}{\det(s)} = 0, 1, 2, 4.$$

Les éléments de \mathbb{S}_4 sont d'ordre 1, 2, 3 ou 4. Par suite, d étant l'un de ces entiers, s^d est une homothétie. Si s est une homothétie, le rapport est 4. Supposons que s ne soit pas une

homothétie. Le polynôme minimal de s est alors de degré 2 et est de la forme $(X - \alpha)(X - \beta)$ avec α et β dans $\overline{\mathbb{F}_\ell}$. Si $\alpha = \beta$, s est représentable (sur $\overline{\mathbb{F}_\ell}$) par

$$\begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix},$$

et le rapport ci-dessus vaut encore 4. Si $\alpha \neq \beta$, on a $\alpha^d = \beta^d$ et il existe $\zeta \in \overline{\mathbb{F}_\ell}$ tel que $\alpha = \zeta\beta$ où $\zeta^d = 1$ et $\zeta \neq 1$. On a alors

$$r = \frac{\text{Tr}(s)^2}{\det(s)} = \zeta^{-1} + \zeta + 2.$$

Si $d = 2$, on a $\zeta = \pm 1$, d'où $r = 0$. Si $d = 3$, on a $\zeta^2 + \zeta + 1 = 0$, $\zeta^{-1} = \zeta^2$, d'où $r = 1$. Si $d = 4$, on a $\zeta^2 = -1$, et $\zeta^{-1} = \zeta^3 = -\zeta$, d'où $r = 2$ et l'assertion.

4. Les séries d'Eisenstein

Exercice 17

On peut utiliser le chapitre IV, car on y explicite les formes de Hecke. Les racines du polynôme cherchée sont $a_2(f_1)$ et $a_2(f_2)$. On a $a_2(f_1) = 540 + 12\alpha$ (α étant une racine de 144169). On trouve que c'est la polynôme

$$X^2 - 1080X - 20468736.$$

Exercice 18

Soit S une bande verticale comme indiquée dans l'énoncé. On démontre qu'il existe une constante $M > 0$ qui dépend seulement de A et δ telle que l'on ait

$$(1) \quad \frac{1}{|m + nz|^k} \leq \frac{M}{|m + ni|^k}$$

pour tout $z \in S$ et tout $(m, n) \neq (0, 0)$. Il suffit donc de prouver qu'il existe $K > 0$ dépendant seulement de A et δ telle que pour tout $z \in S$ on ait

$$(2) \quad |m + nz|^2 \geq K|m + ni|^2.$$

Notons ici que $|m + nz| \geq 1$ donc si (2) est vraie, on a en particulier $|m + nz|^k > |m + nz|^2$ et la condition (1). La condition (2) s'écrit, avec $z = x + iy$,

$$(3) \quad (m + nx)^2 + (ny)^2 > K(m^2 + n^2).$$

Si $n = 0$, (3) est réalisée avec par exemple $K = 1/2$. Si $n \neq 0$, posons $q = m/n$. La condition (3) est alors équivalente à l'inégalité

$$(4) \quad \frac{(q + x)^2 + y^2}{1 + q^2} > K.$$

On vérifie alors que la constante

$$K = \frac{\delta^2}{1 + (A + \delta)^2},$$

convient (toujours si $|x| \leq A$ et $y \geq \delta > 0$). En effet, si l'on a $|q| \leq A + \delta$, l'inégalité (4) est trivialement vérifiée. Supposons $|q| \geq A + \delta$. On alors

$$\left| \frac{x}{q} \right| \leq \frac{|x|}{A + \delta} \leq \frac{A}{A + \delta} < 1.$$

On en déduit les inégalités

$$\left| 1 + \frac{x}{q} \right| \geq 1 - \left| \frac{x}{q} \right| > 1 - \frac{A}{A + \delta} = \frac{\delta}{A + \delta},$$

d'où

$$|q + x| \geq \frac{|q|\delta}{A + \delta}.$$

Il en résulte que l'on a

$$\frac{(q + x)^2 + y^2}{1 + q^2} > \frac{\delta^2}{(A + \delta)^2} \times \frac{q^2}{1 + q^2}.$$

Puisque $|q| \geq A + \delta$, on a donc

$$\frac{q^2}{1 + q^2} \geq \frac{(A + \delta)^2}{1 + (A + \delta)^2},$$

ce qui conduit à la condition (4). D'où l'assertion. En particulier, la série $G_k(z)$ est normalement convergente sur tout compact de \mathfrak{H} , ce qui entraîne que G_k est une fonction holomorphe sur \mathfrak{H} .

CHAPITRE II

1. Congruences modulo 2^3 , 3^3 , 5^2 , 7 et 691

Exercice 1

On peut supposer que k est pair, car si k est impair, f et g sont nulles.

1) Il s'agit de vérifier les points suivants :

- 1) g est holomorphe sur \mathfrak{H} .
- 2) Pour tout $z \in \mathfrak{H}$, on a

$$g(z + 1) = g(z) \quad \text{et} \quad g\left(-\frac{1}{z}\right) = z^{k+2}g(z).$$

- 3) Le développement de Fourier de g à l'infini ne comporte que des termes de degrés positifs.

Rappelons à ce sujet la définition donnée dans [Se3] : une forme modulaire de poids k pour $\mathrm{SL}_2(\mathbb{Z})$ est une fonction holomorphe sur \mathfrak{H} , vérifiant les deux conditions suivantes :

- 1) $f\left(-\frac{1}{z}\right) = z^k f(z)$.
- 2) Il existe des $a_n \in \mathbb{C}$ tels que, si l'on pose $q = e^{2\pi iz}$, on ait

$$f(z) = a_0 + a_1 q + \cdots a_n q^n + \cdots,$$

la série étant absolument convergente pour $z \in \mathfrak{H}$, i.e. pour $|q| < 1$.

Notons que si $f \neq 0$, k est pair et ≥ 0 .

Il est évident que g est holomorphe sur \mathfrak{H} , périodique de période 1 (car tel est le cas de f et E_2) et que la condition 3 est satisfaite. Il s'agit donc de vérifier que l'on a

$$(1) \quad g\left(-\frac{1}{z}\right) = z^{k+2} g(z).$$

On a

$$f\left(-\frac{1}{z}\right)' = f'\left(-\frac{1}{z}\right) \frac{1}{z^2}.$$

Par ailleurs, on a

$$f\left(-\frac{1}{z}\right) = z^k f(z).$$

On en déduit que

$$z^2 \left(z^k f(z) \right)' = f'\left(-\frac{1}{z}\right),$$

autrement dit,

$$f'\left(-\frac{1}{z}\right) = k z^{k+1} f(z) + z^{k+2} f'(z).$$

On utilise alors l'égalité

$$g\left(-\frac{1}{z}\right) = \frac{1}{2\pi i} f'\left(-\frac{1}{z}\right) - \frac{k}{12} E_2\left(-\frac{1}{z}\right) f\left(-\frac{1}{z}\right).$$

Il en résulte que l'on a, en utilisant l'équation fonctionnelle de E_2 ,

$$\begin{aligned} g\left(-\frac{1}{z}\right) &= \frac{1}{2\pi i} \left(k z^{k+1} f(z) + z^{k+2} f'(z) \right) - \frac{k}{12} \left(z^2 E_2(z) + \frac{6z}{\pi i} \right) \left(z^k f(z) \right) \\ &= z^{k+1} \times 0 + z^{k+2} \left(\frac{1}{2\pi i} f'(z) - \frac{k}{12} E_2(z) f(z) \right) = z^{k+2} g(z). \end{aligned}$$

D'où l'égalité (1) et le résultat.

2) Soit $f = a_0 + a_1q + \dots$ le développement de Fourier de f (avec $q = e^{2\pi iz}$). On a

$$f'(z) = 2\pi i(a_1q + 2a_2q^2 + \dots).$$

Par suite, le premier terme du développement de Fourier de g , i.e. le terme de degré 0, est

$$-\frac{ka_0}{12},$$

ce qui entraîne l'assertion. D'où l'exercice.

Exercice 2

Démontrons l'égalité (1) de l'énoncé. On utilise l'exercice précédent. on a

$$E_4'(z) = 240(2\pi i) \sum_{n \geq 1} n\sigma_3(n)q^n.$$

Par ailleurs, E_4 appartient à M_4 et une base de M_6 est E_6 . D'après l'exercice 1, il existe donc $\lambda \in \mathbb{C}$ tel que

$$\frac{1}{2\pi i}E_4'(z) - \frac{1}{3}E_2E_4 = \lambda E_6.$$

On a ainsi

$$720 \sum_{n \geq 1} n\sigma_3(n)q^n - E_2E_4 = 3\lambda E_6.$$

On a $3\lambda = -1$ car le terme constant de E_6 est 1 et celui de $-E_2E_4$ est -1 . D'où l'égalité annoncée.

La preuve de la deuxième égalité est identique : on a

$$E_6'(z) = -504(2\pi i) \sum_{n \geq 1} n\sigma_5(n)q^n.$$

La fonction E_6 est dans M_6 et M_8 est engendré par E_4^2 . Il existe donc $\mu \in \mathbb{C}$ tel que

$$\frac{1}{2\pi i}E_6'(z) - \frac{1}{2}E_2E_6 = \mu E_4^2.$$

Cela entraîne

$$-1008 \sum_{n \geq 1} n\sigma_5(n)q^n - E_2E_6 = 2\mu E_4^2.$$

Le terme constant de E_4^2 et celui de E_2E_6 valent 1, d'où $2\mu = -1$ et le résultat.

Exercice 3

1) La dimension de M_8 est 1. Par suite, on a $E_4^2 = E_8$. On a

$$E_4^2 = 1 + 480 \sum_{n \geq 1} \sigma_3(n) q^n + (240)^2 \left(\sum_{n \geq 1} \sigma_3(n) q^n \right)^2,$$

$$\left(\sum_{n \geq 1} \sigma_3(n) q^n \right)^2 = \sum_{n \geq 1} \left(\sum_{k=1}^{n-1} \sigma_3(k) \sigma_3(n-k) \right) q^n = \sum_{n \geq 1} \left(\sum_{u+v=n, u, v \geq 1} \sigma_3(u) \sigma_3(v) \right) q^n.$$

Cela conduit à l'égalité (3) de l'énoncé en égalant le coefficient de Fourier de degré $n \geq 1$ des q -développements de E_4^2 et E_8 .

2) Soit n un entier ≥ 1 . On a

$$\begin{aligned} a_n &= 720 \sigma_3(n) + 3 \times 240^2 \sum_{u+v=n, u, v \geq 1} \sigma_3(u) \sigma_3(v) \\ &\quad + 240^3 \sum_{u+v+w=n, u, v, w \geq 1} \sigma_3(u) \sigma_3(v) \sigma_3(w). \\ b_n &= -1008 \sigma_5(n) + 504^2 \sum_{u+v=n, u, v \geq 1} \sigma_5(u) \sigma_5(v). \end{aligned}$$

On déduit de la question 1 que

$$a_n \equiv 720 \sigma_3(n) + 1440(\sigma_7(n) - \sigma_3(n)) \pmod{2^{12}},$$

en particulier, on a

$$a_n \equiv 208(2\sigma_7(n) - \sigma_3(n)) \pmod{2^9}.$$

D'où la congruence (4) de l'énoncé.

En ce qui concerne la congruence (5) : on a $d^5 \equiv d^3 \pmod{8}$ (pour tout d), d'où

$$\sum_{u+v=n, u, v \geq 1} \sigma_5(u) \sigma_5(v) \equiv \sum_{u+v=n, u, v \geq 1} \sigma_3(u) \sigma_3(v) \pmod{8}.$$

On en déduit que

$$\sum_{u+v=n, u, v \geq 1} \sigma_5(u) \sigma_5(v) \equiv \frac{\sigma_7(n) - \sigma_3(n)}{120} \pmod{8}.$$

Il en résulte que

$$b_n \equiv -1008 \sigma_5(n) + 504^2 \times \frac{\sigma_7(n) - \sigma_3(n)}{120} \pmod{2^9}.$$

On obtient ($504^2 \equiv 64 \pmod{2^9}$ et $64/120 = 8/15$)

$$b_n \equiv 16 \sigma_5(n) + \frac{8}{15} (\sigma_7(n) - \sigma_3(n)) \pmod{2^9}.$$

3) On utilise l'égalité

$$E_4^3 - E_6^2 = 1728 \sum_{n \geq 1} \tau(n) q^n \quad \text{i.e.} \quad a_n - b_n = 1728 \tau(n).$$

On déduit alors des congruences (4) et (5) de l'énoncé (après division par 8)

$$52 \sigma_7(n) - 26 \sigma_3(n) - \left(2\sigma_5(n) + \frac{\sigma_7(n) - \sigma_3(n)}{15} \right) \equiv 24\tau(n) \pmod{64},$$

puis en multipliant par 15 les deux membres de cette congruence

$$11\sigma_7(n) - 30\sigma_5(n) - 5\sigma_3(n) \equiv -24\tau(n) \pmod{64}.$$

D'où en ajoutant $24\sigma_1(n)$ aux deux membres

$$24((\sigma_1(n) - \tau(n))) \equiv 11\sigma_7(n) - 30\sigma_5(n) - 5\sigma_3(n) + 24\sigma_1(n) \pmod{64}.$$

Autrement dit,

$$24((\sigma_1(n) - \tau(n))) \equiv \sum_{d|n} (11d^7 - 30d^5 - 5d^3 + 24d) \pmod{64}.$$

1) Supposons n impair. Dans ce cas, les diviseurs d de n sont impairs, par suite on a $d^2 \equiv 1 \pmod{8}$ puis

$$11d^7 - 30d^5 - 5d^3 + 24d \equiv 0 \pmod{64}.$$

(on écrit que $11d^7 - 30d^5 - 5d^3 + 24d = d(d^2 - 1)(11d^4 - 19d^2 - 24)$ qui est divisible par 64 car $d^2 \equiv 1 \pmod{8}$). On obtient finalement

$$24((\sigma_1(n) - \tau(n))) \equiv 0 \pmod{64},$$

d'où la congruence (1).

2) Si n est pair : l'égalité

$$\tau(2)\tau(2^n) = \tau(2^{n+1}) + 2^{11}\tau(2^{n-1}),$$

entraîne que $\tau(2^n) \equiv 0 \pmod{8}$ pour tout $n \geq 1$ (récurrence). Le fait que τ soit une fonction multiplicative implique alors la congruence (2). D'où l'exercice.

Exercice 4

1) Posons

$$f = 2E_8'' - 9E_4'^2.$$

La fonction f est holomorphe sur \mathfrak{H} , périodique de période 1. Il s'agit de vérifier que l'on a

$$f\left(-\frac{1}{z}\right) = z^{12}f(z).$$

On a

$$\begin{aligned}\left(E_8\left(-\frac{1}{z}\right)\right)' &= E_8'\left(-\frac{1}{z}\right)\frac{1}{z^2}, \\ \left(E_8\left(-\frac{1}{z}\right)\right)'' &= \frac{1}{z^4}\left(E_8''\left(-\frac{1}{z}\right) - 2zE_8'\left(-\frac{1}{z}\right)\right),\end{aligned}$$

d'où l'on déduit que

$$(1) \quad E_8''\left(-\frac{1}{z}\right) = z^4\left(E_8\left(-\frac{1}{z}\right)\right)'' + 2z^3\left(E_8\left(-\frac{1}{z}\right)\right)'.$$

Puisque E_8 appartient à M_8 , on a

$$(2) \quad E_8\left(-\frac{1}{z}\right) = z^8E_8(z).$$

On écrit alors que

$$(3) \quad (z^8E_8(z))' = E_8'(z)z^8 + 8E_8(z)z^7,$$

$$(4) \quad (z^8E_8(z))'' = E_8''(z)z^8 + 16E_8'(z)z^7 + 56E_8(z)z^6.$$

On déduit alors des formules (1) à (4) que l'on a (en partant des formules (1) et (2))

$$(5) \quad E_8''\left(-\frac{1}{z}\right) = z^{12}E_8''(z) + 18E_8'(z)z^{11} + 72E_8(z)z^{10}.$$

Par ailleurs, on a par définition

$$E_4'^2\left(-\frac{1}{z}\right) = \left(E_4'\left(-\frac{1}{z}\right)\right)^2.$$

Puisque E_4 appartient à M_4 , on a

$$E_4\left(-\frac{1}{z}\right) = z^4E_4(z),$$

$$\left(E_4\left(-\frac{1}{z}\right)\right)' = E_4'\left(-\frac{1}{z}\right)\frac{1}{z^2}.$$

Il en résulte que

$$E_4'\left(-\frac{1}{z}\right) = 4z^5 E_4(z) + z^6 E_4'(z).$$

D'où

$$(6) \quad E_4'^2\left(-\frac{1}{z}\right) = 16z^{10} E_4^2(z) + z^{12} E_4'^2(z) + 8z^{11} E_4(z) E_4'(z).$$

On utilise alors l'égalité (M_8 est de dimension 1)

$$E_4^2 = E_8.$$

On obtient alors

$$(7) \quad E_4'^2\left(-\frac{1}{z}\right) = 16z^{10} E_8(z) + z^{12} E_4'^2(z) + 4z^{11} E_8'(z).$$

Les égalités (5) et (7) conduisent alors à

$$2E_8''\left(-\frac{1}{z}\right) - 9E_4'^2\left(-\frac{1}{z}\right) = z^{12} \left(2E_8''(z) - 9E_4'^2(z)\right),$$

autrement dit,

$$f\left(-\frac{1}{z}\right) = z^{12} f(z),$$

d'où l'assertion.

2) D'après la question 1, l'espace S_{12} étant de dimension 1, il existe $\lambda \in \mathbb{C}$ tel que

$$2E_8'' - 9E_4'^2 = \lambda \Delta.$$

On a

$$E_8''(z) = 480 \times (2\pi i)^2 \times \sum_{n \geq 1} n^2 \sigma_7(n) q^n.$$

On compare les termes de degré 1 des deux membres : celui de $9E_4'^2$ est nul. On a donc

$$\lambda = 2 \times 480 \times (2\pi i)^2 = 960 \times (2\pi i)^2.$$

On obtient ainsi

$$2 \times 480 \times (2\pi i)^2 \times \sum_{n \geq 1} n^2 \sigma_7(n) q^n - 9 \times 240^2 \times (2\pi i)^2 \times \left(\sum_{n \geq 1} n \sigma_3(n) q^n \right)^2 = 960 \times (2\pi i)^2 \times \Delta,$$

ce qui conduit à

$$\sum_{n \geq 1} n^2 \sigma_7(n) q^n - 540 \times \left(\sum_{n \geq 1} n \sigma_3(n) q^n \right)^2 = \Delta,$$

d'où le résultat.

3) La proposition résulte directement de l'égalité précédente en égalant les termes de degré n et en observant que 27 divise 540 ($= 20 \times 27$).

Exercice 5

1) L'espace M_{12} est de dimension 2 et (Δ, E_4^3) est un système libre (cf. les termes de degré 0 dans les développements de Fourier).

2) Rappelons que l'on a

$$E_{10} = 1 - 264 \sum_{n \geq 1} \sigma_9(n) q^n \in M_{10}.$$

D'après l'exercice 1, il existe donc $\lambda, \mu \in \mathbb{C}$ tel que

$$\frac{1}{2\pi i} E'_{10} - \frac{5}{6} E_2 E_{10} = \lambda \Delta + \mu E_4^3.$$

Autrement dit,

$$-264 \sum_{n \geq 1} n \sigma_9(n) q^n - \frac{5}{6} E_2 E_{10} = \lambda \Delta + \mu E_4^3.$$

En considérant les termes de degré 0 on voit que $\mu = -5/6$. En explicitant ceux de degré 1, on obtient

$$-264 - \frac{5}{6} (-24 - 264) = 720\mu + \lambda,$$

et l'on déduit $\lambda = 576$. On obtient ainsi l'égalité

$$-1584 \sum_{n \geq 1} n \sigma_9(n) q^n - 5 E_2 E_{10} = 3456 \Delta - 5 E_4^3 = 2(E_4^3 - E_6^2) - 5 E_4^3.$$

Puisque M_{10} est de dimension 1, on a $E_{10} = E_4 E_6$, d'où l'égalité annoncée.

3) Considérons un entier $n \geq 1$. On a (exercice 2)

$$E_4^2 - E_2 E_6 = 1008 \sum_{n \geq 1} n \sigma_5(n) q^n.$$

On a donc

$$5 E_4^3 - 5 E_2 E_4 E_6 = 5 E_4 \times 1008 \sum_{n \geq 1} n \sigma_5(n) q^n.$$

On a

$$5E_4 = 5 + 1200 \sum_{n \geq 1} \sigma_3(n) q^n.$$

Par suite le n -ème coefficient de Fourier de $5E_4^3 - 5E_2E_4E_6$ est congru modulo 25 à

$$5 \times 1008 \, n\sigma_5(n) \quad \text{i.e.} \quad 15 \, n\sigma_5(n).$$

Par ailleurs, on a $\sigma_9(n) \equiv \sigma_5(n) \pmod{5}$. Le n -ème coefficient de Fourier de $5E_4^3 - 5E_2E_4E_6$ est donc congru modulo 25 à $15n\sigma_9(n)$. Puisque l'on a $1728 \equiv 3 \pmod{25}$, on obtient

$$6\tau(n) \equiv -1584n\sigma_9(n) + 15n\sigma_9(n) \equiv 16n\sigma_9(n) + 15n\sigma_9(n) \equiv 6n\sigma_9(n) \pmod{25}.$$

D'où le résultat.

Exercice 6

Posons

$$E_2 = \sum_{n \geq 0} c_n q^n, \quad \text{et} \quad E_4 = \sum_{n \geq 0} d_n q^n.$$

1) On utilise la question 1 de l'exercice 3 : on en déduit que

$$\sigma_7(n) \equiv \sigma_3(n) + \sum_{k=1}^{n-1} \sigma_3(k)\sigma_3(n-k) \pmod{7}.$$

Par ailleurs, on a

$$\sigma_7(n) \equiv \sigma_1(n) \pmod{7} \quad \text{et} \quad a_n \equiv 4 \left(\sigma_3(n) + \sum_{k=1}^{n-1} \sigma_3(k)\sigma_3(n-k) \right) \pmod{7}.$$

Il résulte que $a_n \equiv 4\sigma_7(n) \pmod{7}$ puis que $a_n \equiv 4\sigma_1(n) \pmod{7}$, d'où l'assertion.

2) On a, en posant $a_0 = 1$ et $b_0 = 1$,

$$b_n = \sum_{k=0}^n a_k d_{n-k} \equiv \sum_{k=0}^n c_k d_{n-k} \pmod{7}.$$

[Le congruence se justifie comme suit : on a $a_k \equiv 4\sigma_1(k) \pmod{7}$ d'après la première question et $4\sigma_1(k) \equiv -24\sigma_1(k) = c_k \pmod{7}$, d'où $a_k \equiv c_k \pmod{7}$]. Par ailleurs, la dernière somme est le coefficient de degré n de E_2E_4 . On utilise l'égalité (1) de l'exercice 2 : pour tout $n \geq 1$ le n -ième coefficient de Fourier de E_6 est multiple de 7. On déduit pour tout $n \geq 1$ la congruence

$$b_n \equiv 720 \, n\sigma_3(n) \equiv 6 \, n\sigma_3(n) \pmod{7}.$$

3) On a l'égalité

$$E_4^3 - E_6^2 = 1728 \sum_{n \geq 1} \tau(n) q^n.$$

Il en résulte que pour tout $n \geq 1$, on a

$$1728 \tau(n) \equiv b_n \pmod{7}.$$

D'où $-\tau(n) \equiv -n\sigma_3(n) \pmod{7}$ et le résultat.

4) Tout revient à prouver le lemme suivant :

Lemme. Soient p un nombre premier impair et n un entier non carré modulo p . On a

$$\sigma_{(p-1)/2}(n) \equiv 0 \pmod{p}.$$

Démonstration : On a

$$\sigma_{(p-1)/2}(n) = \sum_{d|n} d^{(p-1)/2} \equiv \sum_{d|n} \left(\frac{d}{p}\right) \pmod{p}.$$

(Les diviseurs de n sont par hypothèse premiers à p). Par ailleurs, on a

$$\left(\frac{d}{p}\right) \left(\frac{n/d}{p}\right) = \left(\frac{n}{p}\right) = -1 \quad \text{i.e.} \quad \left(\frac{d}{p}\right) = -\left(\frac{n/d}{p}\right),$$

d'où le lemme.

Exercice 7

Rappelons que l'on a

$$E_6(z) = 1 - 504 \sum_{n \geq 1} \sigma_5(n) q^n \quad \text{et} \quad E_{12} = 1 + \frac{65520}{691} \sum_{n \geq 1} \sigma_{11}(n) q^n,$$

$$\Delta = \sum_{n \geq 1} \tau(n) q^n.$$

Puisque M_{12} est de dimension 2, de base (E_{12}, Δ) , il existe $a, b \in \mathbb{C}$ tels que

$$E_6^2 = aE_{12} + b\Delta.$$

Le terme de degré 0 de E_6^2 et E_{12} vaut 1, on a donc $a = 1$. Par ailleurs, on a

$$E_6^2 = 1 - 1008q + \dots$$

En identifiant les termes de degré 1, on obtient

$$-1008 = b + \frac{65520}{691}.$$

On en déduit

$$b = -\frac{762048}{691}.$$

Pour tout $n \geq 1$, en écrivant que $691E_6^2 = 691E_{12} + 691b\Delta$, on a donc

$$65520 \sigma_{11}(n) - 762048 \tau(n) \equiv 0 \pmod{691}.$$

On a

$$65520 \equiv 762048 \equiv 566 \pmod{691}.$$

Cela entraîne le résultat.

2. Formule du produit triple de Jacobi

Exercice 8

1) On applique le théorème d'associativité de [Go], tome 1, p. 139. On effectue une partition de \mathbb{Z} en les trois sous-ensembles :

$$I_1 = \{0\}, \quad I_2 = \{m|m \leq -1\}, \quad I_3 = \{m|m \geq 1\}.$$

D'après ce théorème (*loc. cit.*), il faut alors prouver que les séries

$$\sum_{m \in I_2} |q^{m^2} w^m|, \quad \sum_{m \in I_3} |q^{m^2} w^m|,$$

convergent en vrac (c'est l'assertion (i) du théorème d'associativité), autrement dit, par définition, qu'il existe $M > 0$ tel que pour toute partie finie F de I_j , on ait

$$\sum_{m \in F} |q^{m^2} w^m| \leq M.$$

(Un tel nombre réel M majore ainsi toutes les sommes partielles en vrac). Dans notre situation, il s'agit donc de montrer que ces séries sont absolument convergentes au sens classique (l'ensemble des indices est \mathbb{N} privé de 0). Vérifions qu'il en est bien ainsi pour la deuxième série (*loc. cit.*, p. 411). On a

$$|q^{m^2} w^m| = \exp\left(m^2 \log |q| + m \log |w|\right).$$

On regarde l'exposant : on a $\log |q| < 0$ d'où l'on déduit que

$$m^2 \log |q| + m \log |w| = m(m \log |q| + \log |w|) < -m \quad \text{si } m \text{ est assez grand.}$$

On a ainsi pour m assez grand

$$|q^{m^2} w^m| \leq \exp(-m),$$

qui est le terme général d'une série convergente (sa somme pour $n \geq 0$ est $\frac{e}{e-1}$). D'où l'assertion (théorème de comparaison). En ce qui concerne la première série, la démonstration est la même : on a dans ce cas $m \log |q| + \log |w| > 1$ si m est assez grand, d'où $m(m \log |q| + \log |w|) < m$ et la même conclusion.

2) Le terme général du produit est

$$(1 - q^{2n})(1 + q^{2n-1}w)(1 + q^{2n-1}w^{-1}) = 1 + f_n(q, w),$$

où

$$f_n(q, w) = q^{2n-1}(w + w^{-1}) - q^{4n-1}(w + w^{-1}) - q^{2n} + q^{4n-2} - q^{6n-2}.$$

Puisque $|q| < 1$ la série $\sum f_n(q, w)$ est absolument convergente (comme somme de séries absolument convergentes), d'où l'assertion. [Tout produit infini $\prod_{n \geq 1} (1 + u_n)$ est convergent si la série $\sum |u_n|$ est convergente : *loc. cit.* p. 396. Cet énoncé est aussi vrai s'il existe n tel que $u_n = -1$ car alors le produit est nul donc est convergent ; voir aussi à ce sujet la définition de Dieudonné p. 266].

3) Pour q fixé, $|q| < 1$, posons pour $w \in \mathbb{C}^*$

$$u_n(w) = f_n(q, w).$$

Sur un compact K de \mathbb{C}^* , il existe deux constantes > 0 N_K et M_K telles que pour tout $w \in K$, on ait $M_K \leq |w| \leq N_K$. Par suite, la série $\sum u_n(w)$ est normalement convergente sur K . L'assertion en résulte (th. Weierstrass sur les produits infinis normalement convergents [Go], tome 2, p. 320).

4) On examine les produit partiels d'indice n des deux produits $A(q, w)$ et $A(q, q^2w)$. Notons $P_n(w)$ celui de $A(q, w)$ et $Q_n(w)$ celui de $A(q, q^2w)$. On vérifie que l'on a

$$P_n(w) (1 + q^{2n+1}w) = qw Q_n(w) (1 + q^{2n-1}w^{-1}).$$

Puisque $|q| < 1$ la limite quand n tend vers $+\infty$ de $q^{2n+1}w$ et de $q^{2n-1}w^{-1}$ est nulle. En prenant la limite quand n tend vers $+\infty$ des deux membres de l'égalité précédente, on obtient le résultat.

5) L'égalité est vraie si $q = 0$: en effet, on a dans ce cas $A(0, w) = 1$, d'où par unicité du développement en série de Laurent, $a_n(q) = 0$ pour tout $n \neq 0$. Si $n = 0$, on a $a_0(q) = q^0 a_0(q)$ et $0^0 = 1$, d'où l'assertion. Supposons donc $q \neq 0$ auquel cas $q^2w \in \mathbb{C}^*$. On a donc

$$A(q, q^2w) = \sum_{n \in \mathbb{Z}} a_n(q) q^{2n} w^n.$$

On en déduit de la question 4 les égalités

$$(qw) \sum_{n \in \mathbb{Z}} a_n(q) q^{2n} w^n = \sum_{n \in \mathbb{Z}} a_n(q) q^{2n+1} w^{n+1} = \sum_{N \in \mathbb{Z}} a_{N-1}(q) q^{2N-1} w^N = \sum_{n \in \mathbb{Z}} a_n(q) w^n.$$

(on a posé $N = n + 1$). D'après l'unicité du développement en série de Laurent de la fonction $w \mapsto A(q, w)$, on a donc pour tout $n \in \mathbb{Z}$

$$a_n(q) = q^{2n-1} a_{n-1}(q).$$

Pour $n \geq 0$ on déduit alors l'égalité par récurrence. Si $n < 0$, on remarque que l'on a

$$A(q, w) = A(q, w^{-1}),$$

(d'après l'invariance des termes partiels par $w \mapsto w^{-1}$). Cela conduit à $a_n(q) = a_{-n}(q)$ et au résultat. On a alors

$$A(q, w) = a_0(q) \sum_{n \in \mathbb{Z}} q^{n^2} w^n = a_0(q) J(q, w),$$

d'où l'égalité.

6) Pour tout $n \in \mathbb{N}$ et $q \in B$, on a

$$|q^{n^2} w^n| = \exp\left(n^2 \log |q| + n \log |w|\right) \leq \exp\left(-n^2 \log 2 + n \log |w|\right),$$

le dernier terme étant celui d'une série numérique convergente (critère de Cauchy ou comparaison). Par suite, la série $\sum_{n \geq 0} q^{n^2} w^n$ est normalement convergente sur B . Il en est de même de la série $\sum_{n \geq 1} q^{n^2} w^{-n}$, d'où le fait que $q \mapsto J(q, w)$ soit continue sur B (comme somme de deux fonctions continues sur B).

Quant à la fonction

$$q \mapsto A(q, w),$$

elle est continue sur B car la série de fonctions $\sum f_n(q, w)$ est normalement convergente sur B ([Go], tome 1, p. 402). On en déduit que

$$\lim_{q \rightarrow 0} A(q, w) = A(0, w) = 1 \quad \text{et} \quad \lim_{q \rightarrow 0} J(q, w) = J(0, w) = 1.$$

Il résulte alors de la question 5 que la limite de $a_0(q)$ existe quand q tend vers 0 et que l'on a

$$\lim_{q \rightarrow 0} a_0(q) = 1.$$

7) La série $\sum q^{n^2} w^n$ étant convergente en vrac, le théorème d'associativité entraîne, avec $w = i$,

$$J(q, i) = 1 + \sum_{n \geq 1} q^{n^2} i^n + \sum_{n \geq 1} q^{n^2} i^{-n},$$

autrement dit,

$$J(q, i) = 1 + \sum_{n \geq 1} q^{n^2} (i^n + (-1)^n i^n).$$

En posant $n = 2k$, on obtient

$$J(q, i) = 1 + 2 \sum_{k \geq 1} (-1)^k q^{4k^2} = \sum_{k \in \mathbb{Z}} (-1)^k q^{4k^2} = J(q^4, -1).$$

[On considère les sommes partielles de la série : tous les termes d'indices impairs sont nuls. Posons $s_n(q) = q^{n^2} (i^n + (-1)^n i^n)$ et $S_n(q) = s_1(q) + \dots + s_n(q)$. On a l'égalité $S_{2k} = s_2(q) + \dots + s_{2k}(q)$ et la limite de S_{2k} quand k tend vers $+\infty$ est la somme de la série. Cela justifie la première égalité. La deuxième se justifie par le théorème d'associativité : on prend comme partition les ensembles $\{-k, k\}$ pour $k \geq 0$.]

Démontrons maintenant que l'on a

$$A(q, i) = A(q^4, -1).$$

On a

$$\prod_{n \geq 1} (1 - q^{2n}) = \prod_{n \geq 1} (1 - q^{4n})(1 - q^{4n-2}).$$

En effet, soit p_n le produit partiel d'indice n du premier produit. Le produit partiel p_{2n} d'indice $2n$ est le produit partiel q_n d'indice n du second produit. Puisque ces produits sont convergents, la limite de p_n , qui est le premier membre, est la limite de p_{2n} , qui est égale à la limite de q_n , qui n'est autre que le second membre. D'où l'égalité. Par ailleurs, on a

$$\prod_{n \geq 1} (1 + q^{2n-1}i)(1 - q^{2n-1}i) = \prod_{n \geq 1} (1 + q^{4n-2}),$$

de sorte que

$$A(q, i) = \prod_{n \geq 1} (1 - q^{2n})(1 + q^{4n-2}).$$

Les produits considérés ci-dessus étant convergents, on en déduit que (en considérant les produits partiels)

$$A(q, i) = \prod_{n \geq 1} (1 - q^{4n})(1 - q^{4n-2})(1 + q^{4n-2}) = \prod_{n \geq 1} (1 - q^{4n})(1 - q^{8n-4}).$$

Puisque l'on a (en considérant le produit partiel d'indice $2n$ du premier produit)

$$\prod_{n \geq 1} (1 - q^{4n}) = \prod_{n \geq 1} (1 - q^{8n})(1 - q^{8n-4}),$$

on obtient

$$A(q, i) = \prod_{n \geq 1} (1 - q^{8n})(1 - q^{8n-4})^2 = A(q^4, -1).$$

8) On déduit des questions 5 et 7 l'égalité

$$(a_0(q^4) - a_0(q))J(q, i) = 0.$$

Par ailleurs, on a $A(q, i) \neq 0$, car tous les termes du produit sont non nuls ([Go], tome 1, p. 396). Il en résulte que $J(q, i) \neq 0$ car $A(q, i) = a_0(q)J(q, i)$. D'où $a_0(q) = a_0(q^4)$. Pour tout $k \geq 1$, il en résulte que

$$a_0(q) = a_0(q^{4^k}).$$

Puisque (q^{4^k}) tend vers zéro quand k tend vers $+\infty$, on en déduit que

$$a_0(q) = \lim_{k \rightarrow +\infty} a_0(q^{4^k}) = 1,$$

D'où le théorème.

Exercice 9

On remplace dans la formule de Jacobi q par $q^{1/2}$ et w par $-wq^{1/2}$. On obtient l'égalité

$$\sum_{m \in \mathbb{Z}} (-w)^m q^{m(m+1)/2} = \prod_{n \geq 1} (1 - q^n)(1 - q^n w)(1 - q^{n-1} w^{-1}).$$

En considérant le produit partiel, on constate que

$$\prod_{n \geq 1} (1 - q^n)(1 - q^n w)(1 - q^{n-1} w^{-1}) = (1 - w^{-1}) \prod_{n \geq 1} (1 - q^n)(1 - q^n w)(1 - q^n w^{-1}).$$

On en déduit que

$$(1) \quad \frac{1}{w-1} \sum_{m \in \mathbb{Z}} (-w)^m q^{m(m+1)/2} = \frac{1}{w} \prod_{n \geq 1} (1 - q^n)(1 - q^n w)(1 - q^n w^{-1}).$$

Le produit converge normalement dans toute couronne $0 < r \leq |w| \leq R < +\infty$. Par suite ([Go], tome 1, p. 402 th. 15), lorsque w tend vers 1, le second membre tend vers le produit des limites i.e. vers $\prod (1 - q^n)^3$.

En ce qui concerne la série, on la considère comme une série entière de w . Posons pour tout $w \in \mathbb{C}^*$

$$f(w) = \sum_{m \in \mathbb{Z}} (-w)^m q^{m(m+1)/2}.$$

On a $f(1) = 0$ (on regroupe les termes d'indices m et $-m-1$ dans la série $f(1)$ qui se détruisent mutuellement) et f est une fonction holomorphe de w (une série entière est une

fonction holomorphe dans son disque de convergence ; il s'agit ici de la somme d'une série entière en w et d'une série entière en w^{-1} . En particulier, f est dérivable et l'on a

$$f'(w) = \sum_{m \in \mathbb{Z}} (-1)^m m w^{m-1} q^{m(m+1)/2}.$$

La limite du premier membre de (1) quand w tend vers 1 n'est autre que $f'(1)$ [c'est la dérivée de la série de Laurent au point 1]. D'où

$$\sum_{m \in \mathbb{Z}} (-1)^m m q^{m(m+1)/2} = \prod_{n \geq 1} (1 - q^n)^3.$$

Par ailleurs, on a, en groupant les termes d'indices m et $-m-1$,

$$\sum_{m \in \mathbb{Z}} (-1)^m m q^{m(m+1)/2} = \sum_{m \geq 0} (-1)^m (2m+1) q^{m(m+1)/2},$$

d'où l'exercice.

3. Congruences modulo 23

3.1. Sur l'anneau d'entiers du corps $\mathbb{Q}(\sqrt{-23})$

Exercice 10

1) Soit H le corps de classes de Hilbert de K . Le nombre de classes de K est 3. Par suite $[H : K] = 3$. Posons $L = K(\alpha)$. Le polynôme F est irréductible sur \mathbb{Q} , donc aussi sur K (sinon F aurait une racine dans K , ce qui n'est pas car $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$). Par suite, on a $[L : K] = 3$. Il s'agit alors de démontrer que l'extension L/K est non ramifiée. D'abord L/K est galoisienne. En effet, le discriminant de F est -23 et L est le corps de décomposition de F sur \mathbb{Q} . Par ailleurs, L/K est non ramifiée aux places à l'infini car K est imaginaire.

Soit \mathfrak{P} l'idéal premier de A au-dessus de 23. Le polynôme F est séparable modulo les idéaux premiers de A autres que \mathfrak{P} . Cela prouve que L/K est non ramifiée en dehors de \mathfrak{P} . [On peut aussi donner l'argument suivant : soit $D_{L/K}$ la différentielle de L/K . C'est un idéal de l'anneau des entiers B de L qui divise l'idéal de B engendré par $F'(\alpha)$. La norme de L sur K de $F'(\alpha) = 3\alpha^2 - 1$ est 23. D'où l'assertion.]

Il reste à vérifier que L/K est non ramifiée en \mathfrak{P} . On peut procéder de la façon suivante : supposons que L/K soit ramifiée en \mathfrak{P} . Puisque L/K est galoisienne, \mathfrak{P} doit être totalement ramifié dans L , en particulier il existe un unique idéal premier de B au-dessus de 23. Par ailleurs, l'anneau d'entiers de $\mathbb{Q}(\alpha)$ est $\mathbb{Z}[\alpha]$ (le discriminant de F est -23 qui est sans facteurs carrés) et la factorisation de F modulo 23 est $(X + 13)^2(X + 20) \in \mathbb{F}_{23}[X]$. Par suite, il existe deux idéaux premiers \mathfrak{p} et \mathfrak{q} dans $\mathbb{Z}[\alpha]$ au-dessus de 23 et l'on a $23\mathbb{Z}[\alpha] = \mathfrak{p}^2\mathfrak{q}$.

Cela conduit à une contradiction car il y a ainsi dans L au moins deux places au-dessus de 23. D'où l'assertion et le fait que $H = L$.

2) Supposons que p soit de la forme $x^2 + 23y^2$. On a alors $pA = (x + \omega y)(x - \omega y)$, ce qui entraîne que $(x + \omega y)A$ et $(x - \omega y)A$ sont les deux idéaux premiers de A au-dessus de p . Ils sont principaux, donc ils sont totalement décomposés dans H (théorème de réciprocité). En particulier, p est totalement décomposé dans H . [On peut aussi utiliser le lemme p. 20 directement].

Inversement, supposons p totalement décomposé dans H . Alors, p est totalement décomposé dans K et l'on a $\left(\frac{p}{23}\right) = 1$. On a $pA = \mathfrak{P}\mathfrak{P}'$ et $\mathfrak{P}, \mathfrak{P}'$ sont principaux car ils sont totalement décomposés dans H (théorème de réciprocité). D'après le lemme, p est donc de la forme $x^2 + 23y^2$. D'où le résultat.

3.2. Démonstration du théorème 2

Exercice 11

1) Il suffit de prouver le lemme suivant :

Lemme. Soient $F(X)$ un élément de $\mathbb{Z}[[X]]$ et p un nombre premier. Posons

$$F(X)^p = \sum_{n \geq 0} u_n X^n \quad \text{et} \quad F(X^p) = \sum_{n \geq 0} v_n X^n.$$

Alors, pour tout $n \geq 0$, on a $u_n \equiv v_n \pmod{p}$.

Démonstration : Posons

$$F(X) = \sum_{n \geq 0} t_n X^n.$$

Soit N un entier naturel. On a l'égalité

$$\left(\sum_{n \geq 0} t_n X^n \right)^p = \left(\sum_{j=0}^N t_j X^j + \sum_{j \geq N+1} t_j X^j \right)^p,$$

par suite, les coefficients u_k pour $k \leq N$ sont ceux du polynôme

$$H(X) := \left(\sum_{j=0}^N t_j X^j \right)^p,$$

tronqué au degré N . On a

$$H(X) = \sum_{j=0}^N t_j^p X^{jp} + pR(X) \in \mathbb{Z}[X].$$

Soit k un entier $\leq N$. Si $k = jp$, on a donc la congruence $u_k \equiv t_{k/p} \pmod{p}$ et si k n'est pas multiple de p on a $u_k \equiv 0 \pmod{p}$. Par ailleurs, on a

$$v_k = \begin{cases} 0 & \text{si } k \text{ n'est pas multiple de } p \\ t_{k/p} & \text{sinon.} \end{cases}$$

On a donc $u_k \equiv v_k \pmod{p}$, d'où le lemme.

On déduit de ce lemme que les coefficients qui interviennent dans les développements en séries entières de $\Phi(q^{23})$ et $\Phi(q)^{23}$ sont congrus modulo 23. Cela entraîne le résultat.

2) On a par définition

$$(a_0q + a_1q^2 + a_2q^3 + \cdots) (a_0 + a_1q^{23} + a_2q^{46} + \cdots) = \sum_{n \geq 1} c_n q^n.$$

Étant donnés un entier $p \geq 1$ et un entier $N \geq 0$, déterminons plus généralement le coefficient de degré N de la série formelle produit

$$(a_0X + a_1X^2 + a_2X^3 + \cdots) (a_0 + a_1X^p + a_2X^{2p} + \cdots)$$

en fonction des a_k . Posons pour tout $k \geq 0$

$$A_0 = 0, \quad A_k = a_{k-1} \quad (k \geq 1),$$

et pour tout $j \geq 0$

$$B_j = 0 \quad \text{si } j \not\equiv 0 \pmod{p}, \quad B_{pk} = a_k.$$

Il s'agit alors de déterminer le coefficient C_N de degré $N \geq 0$ de la série

$$(A_0 + A_1X + A_2X^2 + A_3X^3 + \cdots) (B_0 + B_1X + B_2X^2 + \cdots + B_pX^p + \cdots).$$

Par définition, on a

$$C_N = B_0A_N + B_1A_{N-1} + \cdots + B_pA_{N-p} + \cdots + B_{N-1}A_1 + B_NA_0.$$

On a $A_0 = 0$. Par suite, si h est le plus grand entier tel que

$$ph \leq N - 1 \quad \text{i.e.} \quad h = \left\lfloor \frac{N-1}{p} \right\rfloor$$

on obtient

$$C_N = B_0A_N + B_pA_{N-p} + \cdots + B_{ph}A_{N-ph}.$$

D'où l'égalité

$$(3) \quad C_N = a_0a_{N-1} + a_1a_{N-p-1} + a_2a_{N-2p-1} + \cdots + a_ha_{N-ph-1},$$

et le résultat avec $p = 23$ compte tenu du fait que $a_0 = 1$.

Exercice 12

On considère un entier $N \geq 1$. Vérifions que l'on a l'implication

$$(1) \quad \left(\frac{N}{23}\right) = -1 \implies a_{N-1} = 0.$$

Posons $N = 23k + r$ avec $0 \leq r < 23$. Supposons $a_{N-1} \neq 0$. Il existe alors un entier $m \geq 0$ tel que l'on ait

$$23k + r - 1 = \frac{1}{2}m(3m \pm 1).$$

On en déduit que $552k + 24r - 24 = 12(3m^2 \pm m)$, d'où

$$(6m \pm 1)^2 \equiv r \equiv N \pmod{23},$$

ce qui montre que N est un carré modulo 23, d'où (1). Compte tenu de la question 2 de l'exercice 11, l'implication (1) appliquée aux entiers $n, n - 23, \dots, n - 23h$ entraîne alors $c_n = 0$. D'où $\tau(n) \equiv 0 \pmod{23}$ d'après la question 1 de cet exercice.

Exercice 13

1) Vérifions que u et v sont congrus à ± 1 modulo 6. L'assertion est vraie si $p = 2$ ou $p = 3$ car on a alors respectivement $(u, v) = (5, 1)$ et $(u, v) = (7, 1)$. Supposons $p \geq 5$. Montrons que u et v sont impairs. Supposons pour cela que uv pair. Alors u et v sont pairs. Posons $u = 2a$ et $v = 2b$. On a $4a^2 + 23 \cdot 4b^2 = 24p$, d'où $a^2 + 23b^2 = 6p$. Nécessairement, ab est impair : si par exemple a est pair, b l'est aussi et $6p \equiv 0 \pmod{4}$, ce qui n'est pas si $p \neq 2$. On a donc $a^2 \equiv b^2 \equiv 1 \pmod{8}$, d'où $24p \equiv 0 \pmod{6}$, ce qui conduit de nouveau à une contradiction. Par suite, u et v sont impairs. Supposons que 3 divise uv . Alors, 3 divise u et v . L'égalité $u^2 + 23v^2 = 24p$ entraîne $p = 3$ et une contradiction. Les seuls congruences possibles de u et v modulo 6 sont dans ± 1 . D'où l'assertion. Il existe donc des entiers naturels m et n tels que $u = 6m \pm 1$ et $v = 6n \pm 1$. Soit $(m', n') \in \mathbb{N}^2$ un autre couple vérifiant ces égalités. On a alors, avec les mêmes signes que les précédents, $u = 6m' \pm 1$ et $v = 6n' \pm 1$, d'où $m = m'$ et $n = n'$.

2) Il existe des nombres premiers p et des entiers m et n tels que l'on ait les deux égalités

$$(6m + 1)^2 + 23(6n - 1)^2 = 24p \quad \text{et} \quad (6m - 1)^2 + 23(6n + 1)^2 = 24p.$$

Par exemple $p = 829$ avec $m = 23$ et $n = 1$. Ainsi on peut avoir deux couples distincts $(u, v) \in \mathbb{N}^2$ solutions de $u^2 + 23v^2 = 24p$ avec un même couple (m, n) correspondant.

3) Rappelons que l'on a, avec $a_0 = 1$,

$$(1) \quad c_p = a_0 a_{p-1} + a_1 a_{p-24} + \dots + a_h a_{p-1-23h},$$

où h est la partie entière de $(p-1)/23$. Soit T l'ensemble des entiers k tels que

$$0 \leq k \leq h \quad \text{et} \quad a_k a_{p-1-23k} \neq 0.$$

On construit une application $f : T \rightarrow S$ comme suit. Soit k un élément de T . Il existe un unique quadruplet $(m, n, \varepsilon_1, \varepsilon_2)$ tel que $(m, n) \in \mathbb{N}^2$, $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$ et que

$$k = \frac{1}{2}m(3m + \varepsilon_1) \quad \text{et} \quad p-1-23k = \frac{1}{2}n(3n + \varepsilon_2),$$

En posant

$$u = 6n + \varepsilon_2 \quad \text{et} \quad v = 6m + \varepsilon_1,$$

on vérifie que $u^2 + 23v^2 = 24p$: pour le vérifier, il suffit de considérer l'égalité

$$p-1-23\left(\frac{1}{2}m(3m + \varepsilon_1)\right) = \frac{1}{2}n(3n + \varepsilon_2),$$

et de multiplier ses deux membres par 24 pour obtenir l'assertion. On en déduit une application $f : T \rightarrow S$ telle $f(k) = (u, v)$. Inversement, considérons un couple $(u, v) \in S$. Il existe un unique couple $(m, n) \in \mathbb{N}^2$ tel que , avec $\varepsilon_i = \pm 1$, on ait

$$u = 6m + \varepsilon_1 \quad \text{et} \quad v = 6n + \varepsilon_2.$$

Posons

$$k = \frac{1}{2}n(3n + \varepsilon_2).$$

On vérifie que l'on a

$$p-1-23k = \frac{1}{2}m(3m + \varepsilon_1).$$

Pour cela, on peut calculer directement

$$24\left(p-1-23 \times \frac{1}{2}n(3n + \varepsilon_2)\right),$$

et en tenant compte du fait que $u^2 + 23v^2 = 24p$, on obtient $36m^2 + 12m\varepsilon_1$, qui en divisant par 24, donne le résultat. En particulier $(p-1)/23 - k > 0$, d'où $k \leq h$ et l'on a $a_k a_{p-1-23k} \neq 0$. On obtient ainsi une application $g : S \rightarrow T$ telle que $g((u, v)) = k$. Il est immédiat que f et g sont inverses l'une de l'autre.

Par ailleurs, pour chaque $k \in T$, on a $a_k a_{p-1-23k} = (-1)^{\psi((u, v))}$, où $f(k) = (u, v)$. D'où le résultat.

Exercice 14

1) On a $p \geq 5$ et l'égalité des idéaux de A :

$$pA = (x - \omega y)(x + \omega y).$$

Les idéaux $\mathfrak{P} := (x + \omega y)A$ et $\mathfrak{P}' := (x - \omega y)A$ sont donc les deux idéaux premiers de A au-dessus de p . Par ailleurs, une égalité de la forme $(x - \omega y)A = (x' \pm \omega y')A$ entraîne $x = \pm x'$ et $y = \pm y'$ car les unités de A sont ± 1 . D'où l'unicité d'un tel couple $(x, y) \in \mathbb{N}^2$.

2) Si (u, v) est l'un des deux couples (fonctions de x et y) intervenant dans l'énoncé, on vérifie d'abord que $(u, v) \in S$.

Inversement, considérons un élément $(u, v) \in S$. On a les égalités $p = x^2 + 23y^2$ et $u^2 + 23v^2 = 24p$, d'où $24(x^2 + 23y^2) = u^2 + 23v^2$. Par suite, on a

$$(1) \quad (1 + \omega)(1 - \omega)(x - \omega y)(x + \omega y) = (u - v\omega)(u + v\omega).$$

Prouvons le lemme suivant :

Lemme. *Les deux signes étant indépendants, on a l'égalité des idéaux de A*

$$(u + v\omega)A = (x \pm \omega y)A \quad (1 \pm \omega)A.$$

Démonstration : Posons $I = (u + v\omega)A$ et $I' = (u - v\omega)A$. On a l'égalité

$$(1 + \omega)A \quad (1 - \omega)A \quad \mathfrak{P} \quad \mathfrak{P}' = II'.$$

Rappelons les égalités (2) du paragraphe 3.1 :

$$(1 + \omega)A = \mathfrak{P}_2^2 \mathfrak{P}_2' \mathfrak{P}_3' \quad \text{et} \quad (1 - \omega)A = \mathfrak{P}_2'^2 \mathfrak{P}_2 \mathfrak{P}_3.$$

Les idéaux I et I' sont conjugués par Galois et il en est de même de \mathfrak{P} et \mathfrak{P}' . Par suite, \mathfrak{P} ou \mathfrak{P}' divise I . Supposons par exemple que \mathfrak{P} divise I , auquel cas, \mathfrak{P}' divise I' . Il existe donc deux idéaux J et J' de A tels que l'on ait

$$J\mathfrak{P} = I \quad \text{et} \quad J'\mathfrak{P}' = I'.$$

On a ainsi les égalités

$$(1 + \omega)A(1 - \omega)A = (\mathfrak{P}_2 \mathfrak{P}_2')^3 \mathfrak{P}_3 \mathfrak{P}_3' = JJ'.$$

Il s'agit alors de démontrer que J est l'un des idéaux $(1 + \omega)A$ ou $(1 - \omega)A$. On est dans l'un des cas suivants :

(1) on a $v_{\mathfrak{P}_2}(J) = 3$, auquel cas, on a

$$J = \mathfrak{P}_2^3 \mathfrak{P}_3 \quad \text{ou bien} \quad J = \mathfrak{P}_2^3 \mathfrak{P}_3'.$$

(2) on a $v_{\mathfrak{P}_2}(J) = 2$. Dans ce cas, \mathfrak{P}'_2 doit diviser J et l'on a

$$J = \mathfrak{P}_2^2 \mathfrak{P}'_2 \mathfrak{P}_3 \quad \text{ou bien} \quad J = \mathfrak{P}_2^2 \mathfrak{P}'_2 \mathfrak{P}'_3.$$

(3) on a $v_{\mathfrak{P}_2}(J) = 1$ ou $v_{\mathfrak{P}_2}(J) = 0$, et dans ce cas, on a respectivement $v_{\mathfrak{P}_2}(J') = 2$ et $v_{\mathfrak{P}_2}(J') = 3$ et l'on se ramène aux deux cas précédents.

Supposons que l'on soit dans le premier cas, par exemple que l'on ait $J = \mathfrak{P}_2^3 \mathfrak{P}_3$. L'idéal J est principal et parce que le nombre de classes de K est 3, il en est de même de \mathfrak{P}_2^3 . Par suite \mathfrak{P}_3 l'est aussi, ce qui conduit à une contradiction. Le cas 1 ne peut donc se produire.

Supposons que l'on ait $J = \mathfrak{P}_2^2 \mathfrak{P}'_2 \mathfrak{P}_3$. On écrit que l'on a $J = \mathfrak{P}_2^3 \mathfrak{P}_2^{-1} \mathfrak{P}'_2 \mathfrak{P}_3$. Puisque $\mathfrak{P}_2^{-1} \mathfrak{P}_3$ est principal, cela entraîne que \mathfrak{P}'_2 l'est aussi, d'où de nouveau une contradiction.

Dans les deux premiers cas, on obtient finalement comme possibilité, $J = \mathfrak{P}_2^2 \mathfrak{P}'_2 \mathfrak{P}'_3$ i.e. $J = (1 + \omega)A$. Si l'on est dans le cas (3), on en déduit alors que l'on a $J' = (1 + \omega)A$, ce qui prouve notre assertion. D'où le lemme. [On notera que si \mathfrak{P} divise I' la démonstration ne change pas car on se ramène de nouveau à montrer que J est l'un des idéaux $(1 + \omega)A$ et $(1 - \omega)A$.]

Les unités de A étant ± 1 , on déduit du lemme que l'on a

$$\pm(u + v\omega) = (x \pm y\omega)(1 \pm \omega).$$

ce qui entraîne que (u, v) est l'un des couples annoncés. D'où le résultat.

3) Soit (u, v) un élément de S . Il s'agit de déterminer la parité de $\psi((u, v))$. Soient $(m, n) \in \mathbb{N}^2$ et $\varepsilon_i = \pm 1$ tels que

$$u = 6m + \varepsilon_1 \quad \text{et} \quad v = 6n + \varepsilon_2.$$

En distinguant les cas où $x \geq 23y$ et $x < 23y$, ainsi que les cas où $x \geq y$ ou $x < y$, on constate directement que l'on a

$$u + v \equiv 0 \pmod{24} \quad \text{ou bien} \quad u - v \equiv 0 \pmod{24}.$$

Supposons $u - v$ divisible par 24. On a alors

$$6(m - n) + \varepsilon_1 - \varepsilon_2 \equiv 0 \pmod{24}.$$

En particulier, $\varepsilon_1 \equiv \varepsilon_2 \pmod{6}$, d'où $\varepsilon_1 = \varepsilon_2$ et le fait que $\psi((u, v)) = m + n$ soit pair dans ce cas. De même, si $u + v$ est divisible par 24, on a

$$6(m + n) + \varepsilon_1 + \varepsilon_2 \equiv 0 \pmod{24},$$

d'où (par réduction modulo 6), $\varepsilon_1 = -\varepsilon_2$ et $m + n$ est pair. D'après la question 3 de l'exercice 13, on déduit alors que $c_p = 2$ puis que $\tau(p) \equiv 2 \pmod{p}$. D'où le résultat.

Exercice 15

1) Les classes de \mathfrak{P}_2 et \mathfrak{P}_3 sont égales et il en est de même des classes de \mathfrak{P}'_2 et \mathfrak{P}'_3 . On en déduit que

$$\mathfrak{P}_2 \sim \mathfrak{P}_3 \sim \mathfrak{P} \quad \text{et} \quad \mathfrak{P}'_2 \sim \mathfrak{P}'_3 \sim \mathfrak{P}'.$$

La classe de l'idéal $\mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}$ est donc la classe de \mathfrak{P}^3 qui est donc triviale. D'où l'assertion.

2) D'après la question précédente, il existe des entiers relatifs u et v de même parité tels que

$$(1) \quad \mathfrak{P}_2\mathfrak{P}_3\mathfrak{P} = \left(\frac{u + v\omega}{2} \right).$$

On a (en prenant les normes)

$$24p = u^2 + 23v^2.$$

Par suite, l'ensemble S n'est pas vide.

3) Supposons qu'il existe deux couples (u, v) et (u', v') dans S . Les entiers u, v sont de même parité, donc $(u + v\omega)/2$ est dans A . Il en est de même de $(u' + v'\omega)/2$. La norme sur \mathbb{Q} de ces deux éléments est $6p$. Vérifions que si $a \in A$ est un élément de norme $6p$, alors

$$(2) \quad aA = \mathfrak{P}_2\mathfrak{P}_3\mathfrak{P} \quad \text{ou bien} \quad aA = \mathfrak{P}'_2\mathfrak{P}'_3\mathfrak{P}'.$$

Dans la décomposition de aA en produit d'idéaux premiers n'intervient que des idéaux au-dessus de 2, 3 et p avec une valuation 1. Les idéaux de A au-dessus de 2, 3 et p sont respectivement $\mathfrak{P}_2, \mathfrak{P}'_2, \mathfrak{P}_3, \mathfrak{P}'_3$ et $\mathfrak{P}, \mathfrak{P}'$. On utilise alors la remarque suivante : dans un groupe abélien d'ordre 3, trois éléments non nuls de somme nulle sont égaux. Cela entraîne la condition (2). On déduit alors de la condition 2 que les idéaux

$$\left(\frac{u + v\omega}{2} \right)A \quad \text{et} \quad \left(\frac{u' + v'\omega}{2} \right)A,$$

sont égaux ou conjugués (car ils sont de norme $6p$). Compte tenu du fait u, v, u' et v' sont des entiers naturels, cela entraîne $u = u', v = v'$. D'où le résultat.

4) Soit (u, v) l'élément de S . Quitte à changer v en $-v$, on peut supposer, d'après l'alinéa précédent, que l'on a

$$\left(\frac{u + v\omega}{2} \right)A = \mathfrak{P}_2\mathfrak{P}_3\mathfrak{P}.$$

L'égalité

$$6 = 2 \left(\frac{3 + 3\omega}{2} \right) + 3(1 - \omega)$$

entraîne

$$\mathfrak{P}_2\mathfrak{P}_3 = \left(\frac{3+3\omega}{2}, 1-\omega\right).$$

On a donc

$$\left(\frac{3+3\omega}{2}, 1-\omega\right)\mathfrak{P} = \left(\frac{u+v\omega}{2}\right).$$

Puisque p appartient à \mathfrak{P} , en exprimant le fait que

$$p\left(\frac{3+3\omega}{2}\right) \quad \text{et} \quad p(1-\omega)$$

appartiennent à l'idéal engendré par $(u+v\omega)/2$, on en déduit l'existence d'entier r, s, r', s' tel que l'on ait dans A les égalités

$$p\left(\frac{3+3\omega}{2}\right) = \left(\frac{r+s\omega}{2}\right)\left(\frac{u+v\omega}{2}\right) \quad \text{et} \quad p(1-\omega) = \left(\frac{r'-s'\omega}{2}\right)\left(\frac{u+v\omega}{2}\right).$$

On multiplie les deux membres de ces égalités par $(u-v\omega)/2$. On obtient alors compte tenu de l'égalité $u^2 + 23v^2 = 24p$:

$$(1+\omega)(u-v\omega) = 4(r+s\omega) \quad \text{et} \quad (1-\omega)(u-v\omega) = 6(r'-s'\omega).$$

5) D'après les égalités précédentes, on a

$$(3) \quad u-v = 4s \quad \text{et} \quad u+v = 6s'.$$

Soient $(m, n) \in \mathbb{N}^2$ et $\varepsilon_i = \pm 1$ tels que

$$u = 6m + \varepsilon_1 \quad \text{et} \quad v = 6n + \varepsilon_2.$$

La condition (3) entraîne

$$6(m-n) + \varepsilon_1 - \varepsilon_2 \equiv 0 \pmod{4} \quad \text{et} \quad 6(m+n) + \varepsilon_1 + \varepsilon_2 \equiv 0 \pmod{6}.$$

On déduit de la deuxième égalité que $\varepsilon_1 + \varepsilon_2 \equiv 0 \pmod{6}$, autrement dit, que $\varepsilon_1 = -\varepsilon_2$. D'après la première égalité on a alors $6(m-n) \pm 2 \equiv 0 \pmod{4}$, ce qui entraîne que $\psi((u, v)) = m+n$ est impair. Par suite, on a $c_p = -1$, puis $\tau(p) \equiv -1 \pmod{23}$. D'où l'exercice.

Notons que si

$$\left(\frac{u+v\omega}{2}\right)A = \mathfrak{P}'_2\mathfrak{P}'_3\mathfrak{P}',$$

alors, en conjuguant par Galois, on a

$$\left(\frac{u-v\omega}{2}\right)A = \mathfrak{P}_2\mathfrak{P}_3\mathfrak{P},$$

et l'on obtient alors comme condition : $u-v \equiv 0 \pmod{6}$ et $u+v \equiv 0 \pmod{4}$, ce qui entraîne la même conclusion.

CHAPITRE III

2. La représentation modulo 23

Exercice 1

1) Les vecteurs $e_1 = (1, -1, 0)$ et $e_2 = (1, 0, -1)$ forment une base de H . Si σ est la transposition $(1, 2)$, on a $\sigma(e_1) = (-1, 1, 0)$ et $\sigma(e_2) = (0, 1, -1)$. On a ainsi $\sigma(e_1) = -e_1$ et $\sigma(e_2) = e_2 - e_1$. On a ainsi

$$r((1, 2)) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Si τ est le cycle $(1, 2, 3)$, on a $\tau(e_1) = (-1, 0, 1) = -e_2$ et $\tau(e_2) = (0, -1, 1) = e_1 - e_2$. On obtient dans ce cas

$$r((1, 2, 3)) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

On vérifie alors que l'on a

$$r((1, 3, 2)) = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad r((1, 3)) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad r((2, 3)) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

D'où la représentation r . On notera que son image est contenue dans $\mathrm{GL}_2(\mathbb{Z})$.

2) Le fait que r soit injective est évident. Vérifions que r est irréductible. Supposons qu'il existe une droite de H stable par l'action de \mathbb{S}_3 : notons $u = ae_1 + be_2$ une base de cette droite. Si $\sigma = (1, 2)$, on a

$$r(\sigma)(u) = -ae_1 + b(e_2 - e_1) = -(a + b)e_1 + be_2.$$

Il existe $\lambda \in \mathbb{C}$ tel que $r(\sigma)(u) = \lambda u$, d'où $\lambda = 1$ et $2a = -b$ et la droite stable doit être celle engendrée par $e_1 - 2e_2$ (on a $b \neq 0$ car la droite engendrée par e_1 n'est pas stable). Si $\tau = (1, 2, 3)$, on a $r(\tau)(e_1 - 2e_2) = e_2 - 2e_1$ qui n'appartient pas à la droite engendrée par $e_1 - 2e_2$. D'où l'assertion.

On peut aussi utiliser le critère de Serre (th. 5, p. 29) : le caractère de r est par définition :

$$\theta(s) = \mathrm{Tr}(r(s)) \quad \text{pour tout } s \in \mathbb{S}_3.$$

On a donc $\theta(s) = 2$ si s est l'identité, $\theta(s) = 0$ si s est d'ordre 2 et $\theta(s) = -1$ si s est d'ordre 3. On a

$$(\theta|\theta) = \frac{1}{6} \sum_{t \in \mathbb{S}_3} \theta(t) \overline{\theta(t)}.$$

On trouve donc

$$(\theta|\theta) = \frac{1}{6}(4 + 1 + 1) = 1.$$

À isomorphisme près, r est l'unique représentation linéaire irréductible de degré 2 de \mathbb{S}_3 . Il y a en fait trois représentations irréductibles de \mathbb{S}_3 (c'est le nombres de classes de conjugaison de \mathbb{S}_3) : deux de degré 1, données par la représentation unité et la signature, et une de degré 2.

Exercice 2

1) Si ρ_{23} était réductible, les valeurs propres des éléments de l'image de ρ_{23} devraient appartenir à \mathbb{F}_{23} . Or le polynôme caractéristique de $\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ est $X^2 + X + 1$ qui n'a pas de racines dans \mathbb{F}_{23} (car son discriminant -3 n'est pas un carré dans \mathbb{F}_{23} : on peut le vérifier par la loi de réciprocité quadratique). Par ailleurs, le sous-corps de $\overline{\mathbb{Q}}$ laissé fixe par son noyau, est le corps H qui est non ramifié en dehors de 23. D'où l'assertion.

2) Pour tout $\sigma \in G_{\mathbb{Q}}$, $\chi(\sigma)$ est l'élément de \mathbb{F}_{23}^* tel que

$$\sigma(\zeta) = \zeta^{\chi(\sigma)},$$

où ζ est une racine primitive de l'unité d'ordre 23. Le caractère χ^{11} est d'ordre 2. Vérifions que l'on a $\chi^{11}(\sigma) = 1$ si σ fixe K et $\chi^{11}(\sigma) = -1$ sinon. En effet, $\text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ est isomorphe à \mathbb{F}_{23}^* via la flèche $\sigma \mapsto \chi(\sigma)$. Par ailleurs, le sous-groupe $\text{Gal}(\mathbb{Q}(\zeta)/K)$ étant d'indice 2 il est isomorphe par cette flèche au sous-groupe des carrés de \mathbb{F}_{23}^* . Par suite, σ fixe K si et seulement si $\chi(\sigma) \in \mathbb{F}_{23}^*$ est un carré, autrement dit, si et seulement si $\chi^{11}(\sigma) = 1$. Vérifions maintenant que l'on a

$$\det \rho = \chi^{11}.$$

Soit $\sigma \in G_{\mathbb{Q}}$. Supposons que σ fixe K . Dans ce cas, σ est d'ordre 1 ou 3 dans $\text{Gal}(H/\mathbb{Q})$, et ρ étant injective, il en est de même de $\rho(\sigma)$. D'après l'exercice 1, on constate alors que $\det \rho(\sigma) = 1$. Puisque l'on a aussi $\chi^{11}(\sigma) = 1$, On obtient ainsi $\det \rho(\sigma) = \chi^{11}(\sigma)$. Supposons que σ ne fixe pas K . L'élément $\rho(\sigma)$ est alors d'ordre 2 et son déterminant est -1 . On obtient de nouveau $\det \rho(\sigma) = \chi^{11}(\sigma)$, d'où l'assertion.

3) Notons I_{23} un tel sous-groupe d'inertie. L'ordre de l'image de I_{23} est 2. En effet, 23 est ramifié dans K et H est le corps de classes de Hilbert de K [on peut aussi dire que dans l'anneau d'entiers de $\mathbb{Q}(\alpha)$, où $\alpha^3 - \alpha - 1 = 0$, on a $(23) = \mathfrak{p}^2 \mathfrak{p}'$ (cela résulte de l'égamité $X^3 - X - 1 = (X - 3)(X + 13)^2$ dans $\mathbb{F}_{23}[X]$). Par ailleurs, on a $6 = efg$, de sorte que e divise 6 et 2 divise e . Puisque 23 n'est pas totalement ramifié dans $\mathbb{Q}(\alpha)$, on a donc $e = 2$]. Il y a ainsi trois idéaux premiers de l'anneau d'entiers de H au-dessus de 23. Soit \mathfrak{P} l'une d'entre elles. Un élément $\sigma \in I_{23}$ est déterminé par sa restriction à H et il suffit donc de décrire la restriction de ρ au sous-groupe d'inertie $I_{\mathfrak{P}}$ de $\text{Gal}(H/\mathbb{Q})$ en \mathfrak{P} . Le sous-groupe $I_{\mathfrak{P}}$ est d'ordre 2 : pour tout $\sigma \in I_{\mathfrak{P}}$, on a $\rho(\sigma) = 1$ ou bien $\rho(\sigma)$ est d'ordre 2. Considérons un élément $\sigma \in I_{\mathfrak{P}}$ tel que $\rho(\sigma) \neq 1$. D'après l'exercice 1, on a $\rho(\sigma) \neq -1$. Par suite, le polynôme minimal de $\rho(\sigma)$ est $X^2 - 1$. Il existe donc une matrice $M \in \text{GL}_2(\mathbb{F}_{23})$ tel que

$$M\rho(\sigma)M^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Puisque $\rho(I_{\mathfrak{P}})$ est d'ordre 2, on a donc **pour tout** $\sigma \in I_{\mathfrak{P}}$,

$$M\rho(\sigma)M^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{ou bien} \quad M\rho(\sigma)M^{-1} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Par ailleurs, si $\rho(\sigma) \neq 1$, puisque $\rho(\sigma)$ est d'ordre 2, σ ne fixe pas K et l'on a donc $\chi^{11}(\sigma) = -1$. On en déduit que la restriction de ρ à $I_{\mathfrak{P}}$ (ou à I_{23}), est représentable sous la forme

$$\begin{pmatrix} \chi^{11} & 0 \\ 0 & 1 \end{pmatrix}.$$

Exercice 3

1) De l'égalité $\det \rho = \chi^{11}$ on déduit que l'on a $\det \rho(\text{Frob}_p) = p^{11} \bmod. 23$ i.e.

$$\det \rho(\text{Frob}_p) = \left(\frac{p}{23} \right) \bmod. 23.$$

Supposons que l'on ait $\left(\frac{p}{23} \right) = -1$. Par suite, on a dans ce cas $\det \rho(\text{Frob}_p) = -1$. D'après l'exercice 1, $\rho(\text{Frob}_p)$ est donc d'ordre 2 et sa trace est nulle.

Supposons que p soit de la forme $x^2 + 23y^2$. D'après l'exercice 10, p est totalement décomposé dans H . Il en résulte que $\rho(\text{Frob}_p) = 1$ i.e. que $\rho(\text{Frob}_p)$ est la la matrice identité. En particulier, sa trace est 2.

Supposons $\left(\frac{p}{23} \right) = 1$ et que p ne soit pas de la forme $x^2 + 23y^2$. On a dans ce cas $\det \rho(\text{Frob}_p) = 1$ et p n'est pas totalement décomposé dans H , autrement dit, on a $\rho(\text{Frob}_p) \neq 1$. Il en résulte que $\rho(\text{Frob}_p)$ est d'ordre 3 et sa trace est -1 .

Le théorème 2 entraîne alors le résultat.

2) C'est une conséquence de la question précédente.

3) L'image de ρ est isomorphe à \mathbb{S}_3 d'après l'exercice 1. Puisque 6 ne divise pas 2×22^2 , qui est l'ordre du normalisateur d'un sous-groupe de Cartan déployé, et que ρ est irréductible, on obtient le résultat.

COMPLÉMENTS

Exercice 1 (sous-groupes de $\mathbb{GL}(V)$ d'ordre divisible par ℓ)

Soit H un sous-groupe de $\mathbb{GL}(V)$ d'ordre divisible par ℓ . Alors, il existe une droite de V stable par tous les éléments de H ou bien $\mathbb{SL}(V)$ est contenu dans H .

Il existe un élément $g \in H$ d'ordre ℓ . Il est représentable sous la forme

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

En effet, on a $g^\ell = 1$ donc le polynôme minimal de g divise $X^\ell - 1 = (X - 1)^\ell$. Ce n'est pas $X - 1$ car g n'est pas l'identité, c'est donc $(X - 1)^2$. D'où la forme de Jordan ci-dessus (ou bien on utilise la question 2 de l'exercice 9, ce qui prouve directement qu'il existe une unique classe de conjugaison d'éléments d'ordre ℓ). En particulier, g a une unique droite fixe (il ne peut avoir deux droites stables car son ordre serait premier à ℓ : une matrice représentant g serait diagonale). On distingue alors deux cas :

1) tous les éléments d'ordre ℓ de H ont une même droite stable D . Dans ce cas, D est stable par tous les éléments de H . En effet, soit h un élément quelconque de H . L'élément hgh^{-1} est d'ordre ℓ et laisse stable $h(D)$. D'où $h(D) = D$.

2) Supposons qu'il existe deux éléments x et y d'ordre ℓ de H ayant deux droites D_x et D_y fixes distinctes. Soit (e_1, e_2) une base de V telle que $e_1 \in D_x$ et $e_2 \in D_y$. Alors dans cette base, la matrice de x est

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

De même, dans cette base, la matrice de y est

$$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}.$$

Quitte à élever x et y à des puissances convenables, on peut supposer $a = b = 1$. Or les deux matrices ci-dessus engendrent $\mathbb{SL}(V)$. D'où le résultat.

Exercice 2

Supposons $\ell \geq 3$. Soit $g \in \mathbb{GL}(V)$ un élément semi-simple qui n'est pas une homothétie. Alors, il existe un unique sous-groupe de Cartan qui contient g .

Soit C le centralisateur de g dans $\mathbb{GL}(V)$. Supposons qu'il existe deux sous-groupes de Cartan C_1 et C_2 de $\mathbb{GL}(V)$ qui contiennent g . Puisque C_1 et C_2 sont abéliens, ils centralisent g et donc C contient C_1 et C_2 . Il en résulte que $C = C_1$, $C = C_2$, d'où $C_1 = C_2$: on utilise les assertions suivantes :

a) deux Cartan de même nature contenus l'un dans l'autre sont égaux car ils ont le même ordre.

b) Un Cartan déployé ne peut être contenu dans un Cartan non déployé. En effet, ce dernier est cyclique et pas un Cartan déployé qui est isomorphe à $\mathbb{F}_\ell^* \times \mathbb{F}_\ell^*$.

c) Un Cartan non déployé ne peut être contenu dans un Cartan déployé, car sinon $\ell^2 - 1$ devrait diviser $(\ell - 1)^2$ ce qui n'est pas.

D'où l'exercice.

Exercice 3

Les cas 2 et 3 du théorème 3 sont disjoints.

Soit G_ℓ l'image de $\rho_{f,\ell}$. Supposons G_ℓ contenue dans le normalisateur N d'un sous-groupe de Cartan sans être contenu dans C . Posons

$$H = G_\ell \cap C.$$

Vérifions que $[G_\ell : H] = 2$. On considère pour cela le morphisme $G_\ell \rightarrow N \rightarrow N/C$. Son noyau est H de sorte que G_ℓ/H est d'ordre ≤ 2 . Puisque G_ℓ n'est pas contenu dans C , on a donc l'assertion. Soit $\pi : \mathrm{GL}_2(\mathbb{F}_\ell) \rightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$ la surjection canonique. On a

$$[\pi(G_\ell) : \pi(H)] \leq 2.$$

En effet, considérons le morphisme $\psi : G_\ell \rightarrow \pi(G_\ell)/\pi(H)$. Son noyau contient H . Par suite, on a un morphisme surjectif $G_\ell/H \rightarrow \pi(G_\ell)/\pi(H)$, ce qui entraîne l'assertion. Par hypothèse, $\pi(G_\ell)$ est isomorphe à S_4 . Or le groupe $\pi(H)$ est abélien et S_4 n'a pas de sous-groupe d'indice ≤ 2 abélien. D'où l'exercice.

Définition. La représentation régulière d'une K -algèbre A est le morphisme K de groupes $K \rightarrow \mathrm{End}_K(A)$ qui à x associe l'endomorphisme de multiplication par x .