INTRODUCTION AU PROBLÈME DE NOETHER

G.BERHUY

Table des matières

Dans tout ce qui suit, F désignera un corps. Le point de départ de cet article est le théorème de structure des polynômes symétriques, qui peut s'énoncer comme suit.

pour tout $P \in F[X_1, \ldots, X_n]$, les propriétés suivantes sont équivalentes :

(1) on a $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n)$ pour tout $\sigma \in \mathfrak{S}_n$.

(2) il existe un unique $Q \in F[T_1, \ldots, T_n]$ tel que $P = Q(\sigma_1, \ldots, \sigma_n)$, où $\sigma_1, \ldots, \sigma_n$ sont les polynômes symétriques élémentaires en $X_1, \ldots, X_n$.

On peut démontrer que le résultat est vrai si l'on remplace $F[X_1, \ldots, X_n]$ par $F(X_1, \ldots, X_n)$.

Une question naturelle est de savoir si ces résultats sont encore vrais lorsque l'on remplace $\mathfrak{S}_n$ par un de ses sous-groupes.

Le but de cet article est d'étudier succinctement cette question. Avant de l'aborder, nous allons en premier lieu faire quelques rappels sur les polynômes et fractions rationnelles.

1. Rappels et compléments sur les polynômes et les fractions rationnelles

Définition 1.1. Une *F-algèbre* est un couple $(\mathscr{A}, \mu)$, où $\mathscr{A}$ et $\mu : \mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A}$ est une application F-bilinéaire, appelé *loi produit*.

Si $a_1, a_2 \in \mathscr{A}$, l'élément $\mu(a_1, a_2)$ est simplement noté $a_1 a_2$.

Une F-algèbre $\mathscr{A}$ est dite associative/commutative/unitaire si sa loi produit l'est.

Date: 21 septembre 2022.

Un *morphisme d'algèbres* $f : \mathscr{A} \longrightarrow \mathscr{A}'$ est une application F-linéaire telle que

$$f(a_1a_2) = f(a_1)f(a_2) \text{ pour tous } a_1, a_2 \in \mathscr{A}.$$

On définit de manière évidente la notion d'isomorphisme et d'automorphisme de F-algèbre.

Exemples 1.2.

(1) Pour tout $n \geq 0$, $F[X_1, \ldots, X_n]$ est une F-algèbre associative, commutative et unitaire.

(2) Soit L/F une extension de corps. Alors, L est une F-algèbre associative, commutative et unitaire pour les lois évidentes.

(3) Pour tout $n \geq 1$, $\mathrm{M}_n(F)$ est une F-algèbre associative et unitaire, non commutative dès que $n \geq 2$.

Convention. Dans tout ce qui suit, toutes les F-algèbres seront implicitement supposées associatives et unitaires.

Nous allons maintenant nous intéresser aux morphismes de F-algèbres de source $F[X_1, \ldots, X_n]$ ou $F(X_1, \ldots, X_n)$. On commence par le cas des polynômes.

Proposition 1.3. *Soit $\mathscr{A}$ une F-algèbre commutative, et soit $\mathbf{a} = (a_1, \ldots, a_n) \in \mathscr{A}^n$. Alors, il existe un unique morphisme de F-algèbres $ev_{\mathbf{a}} : F[X_1, \ldots, X_n] \longrightarrow \mathscr{A}$, appelé morphisme d'évaluation en $\mathbf{a}$, tel que*

$$ev_{\mathbf{a}}(X_i) = a_i \quad \textit{pour tout } i \in [\![1, n]\!].$$

Il est défini par

$$ev_{\mathbf{a}}\Big(\sum_{m_1,\ldots,m_n} \lambda_{m_1,\ldots,m_n} X_1^{m_1} \cdots X_n^{m_n}\Big) = \sum_{m_1,\ldots,m_n} \lambda_{m_1,\ldots,m_n} a_1^{m_1} \cdots a_n^{m_n}.$$

De plus, tout morphisme de F-algèbres $F[X_1, \ldots, X_n] \longrightarrow \mathscr{A}$ est de la forme $ev_{\mathbf{a}}$, pour un unique $\mathbf{a} \in \mathscr{A}^n$.

Démonstration. Le fait que $ev_{\mathbf{a}}$ soit un morphisme de F-algèbres qui envoie X_i sur a_i est un calcul facile laissé au lecteur.

Si maintenant $f : F[X_1, \ldots, X_n] \longrightarrow \mathscr{A}$ est un morphisme de F-algèbres, on a nécessairement

$$ev_{\mathbf{a}}\Big(\sum_{m_1,\ldots,m_n} \lambda_{m_1,\ldots,m_n} X_1^{m_1} \cdots X_n^{m_n}\Big) = \sum_{m_1,\ldots,m_n} \lambda_{m_1,\ldots,m_n} f(X_n)_1^{m_1} \cdots f(X_n)^{m_n}$$

pour tout $P = \sum_{m_1,\ldots,m_n} \lambda_{m_1,\ldots,m_n} X_1^{m_1} \cdots X_n^{m_n} \in F[X_1, \ldots, X_n]$. On a donc $f = ev_{\mathbf{a}}$, avec $\mathbf{a} = (f(X_1), \ldots, f(X_n))$.

En particulier, si f est un morphisme de F-algèbres tel que $f(X_i) = a_i$ pour tout $i \in [\![1, n]\!]$, l'égalité précédente montre que $f = ev_{\mathbf{a}}$.

Enfin, si $f = ev_{\mathbf{a_1}} = ev_{\mathbf{a_2}}$, en calculant l'image de chaque X_i, on obtient immédiatement $\mathbf{a_1} = \mathbf{a_2}$. □

Notation. Si $P \in F[X_1, \ldots, X_n]$, on note $P(a_1, \ldots, a_n)$, voire $P(\mathbf{a})$, l'image de P par le morphisme $ev_{\mathbf{a}}$.

Lorsque $n = 1$ et $\mathbf{a}$ est un élément de $\mathscr{A}$, le morphisme $ev_{\mathbf{a}}$ est injectif si $\mathbf{a}$ est transcendant sur F. Lorsque $n \geq 1$, l'injectivité du morphisme d'évaluation conduit à la notion d'éléments algébriquement indépendants sur F.

Définition 1.4. Soit $\mathscr{A}$ une F-algèbre commutative. On dit que des éléments $a_1, \ldots, a_n \in \mathscr{A}$ sont *algébriquement indépendants sur* F si pour tout $P \in F[X_1, \ldots, X_n]$, on a

$$P(a_1, \ldots, a_n) = 0 \Longrightarrow P = 0.$$

On s'intéresse maintenant au cas des fractions rationnelles, même si nous n'en aurons besoin que de façon anecdotique. Pour simplifier l'exposition, nous nous bornerons aux morphismes à valeurs dans un corps. On a alors la proposition suivante.

Proposition 1.5. *Soit L/F une extension de corps, et soit $\mathbf{a} = (a_1, \ldots, a_n) \in L^n$, où $a_1, \ldots, a_n$ sont algébriquement indépendants sur F. Alors, il existe un unique morphisme de F-algèbres $ev'_{\mathbf{a}} : F(X_1, \ldots, X_n) \longrightarrow L$, appelé morphisme d'évaluation en $\mathbf{a}$, tel que*

$$ev'_{\mathbf{a}}(X_i) = a_i \quad \textit{pour tout } i \in [\![1, n]\!] .$$

Il est défini par

$$ev'_{\mathbf{a}}(\frac{P}{Q}) = P(\mathbf{a})Q(\mathbf{a})^{-1} (= P(a_1, \ldots, a_n)Q(a_1, \ldots, a_n)^{-1}).$$

De plus, tout morphisme de F-algèbres $F[X_1, \ldots, X_n] \longrightarrow L$ est de la forme $ev'_{\mathbf{a}}$, pour un unique $\mathbf{a} = (a_1, \ldots, a_n) \in L^n$, où $a_1, \ldots, a_n$ sont algébriquement indépendants sur F.

Démonstration. Soit $\mathbf{a} = (a_1, \ldots, a_n) \in L^n$, où $a_1, \ldots, a_n$ sont algébriquement indépendants sur F. Le morphisme d'évaluation $ev_{\mathbf{a}} : F[X_1, \ldots, X_n] \longrightarrow L$ est donc injectif. Ainsi, si $Q \in F[X_1, \ldots, X_n]$ est non nul, alors $Q(a_1, \ldots, a_n) \in L$ est non nul, donc inversible dans L.

Si $f = \dfrac{P}{Q} \in F(X_1, \ldots, X_n)$, on vérifie alors que la quantité $P(\mathbf{a})Q(\mathbf{a})^{-1}$ ne dépend pas de la représentation de f choisie, et que l'application $ev'_{\mathbf{a}} : F(X_1, \ldots, X_n) \longrightarrow L$ est un morphisme de F-algèbres qui envoie X_i sur a_i.

Notons maintenant qu'un morphisme de F-algèbres $\rho : F(X_1, \ldots, X_n) \longrightarrow \mathscr{A}$ est non trivial. Comme $F(X_1, \ldots, X_n)$ est un corps, ce morphisme est nécessairement injectif.

La restriction de ce morphisme à $F[X_1, \ldots, X_n]$ est donc un morphisme injectif $F[X_1, \ldots, X_n] \longrightarrow L$, donc de la forme $ev_{\mathbf{a}}$, où les coordonnées de $\mathbf{a}$ sont algébriquement indépendantes sur F. En particulier, un polynôme Q non nul est envoyé sur un élément non nul de L, donc inversible. Mais alors, on a

$$\rho(\frac{P}{Q}) = \rho(P)\rho(Q)^{-1} = P(\mathbf{a})Q(\mathbf{a})^{-1},$$

si bien que $\rho = ev'_{\mathbf{a}}$. L'unicité de $\mathbf{a}$ se démontre comme dans le cas des polynômes.

Enfin, si $\rho = ev_{\mathbf{a}'}$ est un morphisme de F-algèbres envoyant X_i sur a_i, on a nécessairement $\mathbf{a}' = \mathbf{a}$, comme on le voit en regardant les images des X_i, d'où l'unicité d'un morphisme possédant cette propriété. □

2. Polynômes et fractions rationnelles invariantes sous l'action d'un groupe fini

Comme déjà mentionné, le point de départ de tout ce qui suit est le théorème de structure des polynômes symétriques, dont on rappelle maintenant l'énoncé.

Soit F un corps[1], et soit $n \geq 1$ un entier. Un polynôme $P \in F[X_1, \ldots, X_n]$ est dit *symétrique* si l'on a

$$P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n) \text{ pour tout } \sigma \in \mathfrak{S}_n.$$

Le théorème de structure des polynômes symétriques symétriques s'énonce alors comme suit : pour tout polynôme $P \in F[X_1, \ldots, X_n]$ symétrique, il existe un unique polynôme $Q \in F[T_1, \ldots, T_n]$ tel que $P = Q(\sigma_1, \ldots, \sigma_n)$, où $\sigma_1, \ldots, \sigma_n$ sont les polynômes symétriques élémentaires en $X_1, \ldots, X_n$.

Notons qu'un polynôme symétrique n'est rien d'autre qu'un point fixe de $F[X_1, \ldots, X_n]$ sous l'action de $\mathfrak{S}_n$ définie par

$$\begin{aligned} \mathfrak{S}_n \times F[X_1, \ldots, X_n] &\longrightarrow F[X_1, \ldots, X_n] \\ (\sigma, P) &\longmapsto \sigma \cdot P = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}). \end{aligned}$$

D'autre part, l'unicité de Q est de manière évidente équivalente à la propriété suivante : pour tout $Q \in F[T_1, \ldots, T_n]$, on a

$$Q(\sigma_1, \ldots, \sigma_n) = 0 \Longrightarrow Q = 0.$$

Autrement dit, les polynômes $\sigma_1, \ldots, \sigma_n$ sont algébriquement indépendants sur F.

Le théorème précédent peut alors se réinterpréter comme suit : il existe des éléments $\sigma_1, \ldots, \sigma_n \in F[X_1, \ldots, X_n]^{\mathfrak{S}_n}$ vérifiant les deux conditions suivantes :

1) on a $F[X_1, \ldots, X_n]^{\mathfrak{S}_n} = F[\sigma_1, \ldots, \sigma_n]$

2) les polynômes $\sigma_1, \ldots, \sigma_n$ sont algébriquement indépendants sur F.

Une autre reformulation possible est la suivante : on a un isomorphisme de F-algèbres

$$F[T_1, \ldots, T_n] \simeq F[X_1, \ldots, X_n]^{\mathfrak{S}_n},$$

l'isomorphisme étant induit par l'évaluation $T_i \rightsquigarrow \sigma_i$.

On a d'ailleurs une parfaite équivalence entre ces deux points de vue, comme le montre le lemme suivant.

1. Le résultat mentionné est aussi valable si on remplace F par un anneau commutatif, mais nous n'en aurons pas besoin ici.

Lemme 2.1. *Soit $\mathscr{A}$ une F-algèbre commutative, et soit $r \geq 0$ un entier. Les propriétés suivantes sont équivalentes :*

(i) il existe des éléments $a_1, \ldots, a_r \in \mathscr{A}$ algébriquement indépendants sur F tels que $\mathscr{A} = F[a_1, \ldots, a_r]$.

(ii) il existe un isomorphisme de F-algèbres $F[T_1, \ldots, T_r] \simeq \mathscr{A}$.

Démonstration. Tout morphisme de F-algèbres $F[T_1, \ldots, T_r] \longrightarrow \mathscr{A}$ est un morphisme d'évaluation en certains éléments $a_1, \ldots, a_r \in \mathscr{A}$ déterminés de manière unique (cf. Proposition 1.3).

L'équivalence de (i) et (ii) est alors claire, la surjectivité de l'évaluation $T_i \rightsquigarrow a_i$ étant équivalente à (i) et son injectivité étant équivalente à (ii) induit un isomorphisme de F-algèbres $F[T_1, \ldots, T_r] \simeq \mathscr{A}$. □

On peut donc légitimement se poser la question de savoir si le résultat est encore vrai si l'on remplace $\mathfrak{S}_n$ par un sous-groupe G.

Autrement dit, soit G un sous-groupe de $\mathfrak{S}_n$, agissant sur $F[X_1, \ldots, X_n]$ par

$$\begin{aligned} G \times F[X_1, \ldots, X_n] &\longrightarrow F[X_1, \ldots, X_n] \\ (\sigma, P) &\longmapsto \sigma \cdot P = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}). \end{aligned}$$

Existe-t-il un isomorphisme de F-algèbres $F[X_1, \ldots, X_n]^G \simeq F[T_1, \ldots, T_r]$, pour un certain entier $r \geq 0$? [2]

La réponse est négative, comme le montre déjà le cas du groupe de Klein.

Exemple 2.2. Soit $G = \{\mathrm{Id}, s, t, st\} \subset \mathfrak{S}_4$, où $s = (1\,2)(3\,4)$ et $t = (1\,3)(2\,4)$

Posons

$$U_1 = X_1 + X_2 + X_3 + X_4,\ U_2 = X_1 - X_2 + X_3 - X_4,$$
$$U_3 = X_1 + X_2 - X_3 - X_4,\ U_4 = X_1 - X_2 - X_3 - X_4.$$

Notons que

$$X_1 = \frac{U_1 + U_2 + U_3 + U_4}{4},\ X_2 = \frac{U_1 - U_2 + U_3 - U_4}{4},$$
$$X_3 = \frac{U_1 + U_2 - U_3 - U_4}{4},\ X_4 = \frac{U_1 - U_2 - U_3 - U_4}{4}.$$

Il est alors clair que $F[X_1, X_2, X_3, X_4] = F[U_1, U_2, U_3, U_4]$, et que $U_1, \ldots, U_4$ sont algébriquement indépendants sur F.

On vérifie alors $U_2U_3U_4, U_2^2, U_3^2, U_4^2 \in \mathscr{A} = F[X_1, \ldots, X_4]^G$. Montrons que ces quatre éléments sont des éléments irréductibles de $\mathscr{A}$, deux à deux non associés.

Comme $\mathscr{A}$ est un sous-anneau de $F[X_1, \ldots, X_4]$, $\mathscr{A}^\times$est un sous-groupe de $F[X_1, \ldots, X_4]^\times = F^\times$. Comme les éléments de $F^\times$ sont clairement fixes sous l'action de G, on a $\mathscr{A}^\times = F^\times$. Il est alors immédiat que $U_2U_3U_4, U_2^2, U_3^2, U_4^2$ sont deux à deux non associés.

2. On peut en fait démontrer que, si c'est le cas, on a nécessairement $r = n$, mais encore une fois, nous n'aurons pas besoin de ce résultat.

Pour vérifier qu'ils sont irréductibles, notons tout d'abord qu'ils sont non nuls et non inversibles. Montrons maintenant que $U_2U_3U_4$ est irréductible. Si $f \in \mathscr{A}$ est un diviseur de $U_2U_3U_4$ dans $\mathscr{A}$, c'est aussi un diviseur dans $F[X_1, \dots, X_4] = F[U_1, \dots, U_4]$.

Comme $U_1, \dots, U_4$ sont algébriquement indépendants, les diviseurs en question sont, à une constante multiplicative non nulle près :

$$1, U_2, U_3, U_4, U_2U_3, U_2U_4, U_3U_4, U_2U_3U_4.$$

Dans cette liste, seuls 1 et $U_2U_3U_4$ sont fixes sous l'action de G. Cela entraîne aisément l'irréductibilité de $U_2U_3U_4$.

On procède de même pour U_2^2, U_3^2, U_4^2. Mais alors, l'égalité

$$(U_2U_3U_4)^2 = U_2^2U_3^2U_4^2$$

montre que $(U_2U_3U_4)^2$ possède deux décompositions en irréductibles distinctes, et donc que l'anneau $\mathscr{A}$ n'est pas factoriel. En particulier, $\mathscr{A}$ ne peut être isomorphe à une algèbre de polynômes sur F.

On peut donc essayer de chercher une question un peu plus raisonnable. Au lieu de se préoccuper de polynômes, on peut s'intéresser aux fractions rationnelles.

Avant de continuer, on a besoin d'une définition.

Définition 2.3. Soit $\mathscr{A}$ une F-algèbre. Une action d'un groupe G sur $\mathscr{A}$ est une action *par automorphismes de F-algèbre* si pour tout $g \in G$, tous $a, a_1, a_2 \in \mathscr{A}$ et tout $\lambda \in F$, on a :

(1) $g{\cdot}1_{\mathscr{A}} = 1_{\mathscr{A}}$

(2) $g{\cdot}(a_1 + a_2) = g{\cdot}a_1 + g{\cdot}a_2)$

(3) $g{\cdot}(\lambda a) = \lambda(g{\cdot}a)$

(4) $g{\cdot}(a_1a_2) = (g{\cdot}a_1)(g{\cdot}a_2)$.

Autrement dit, une action d'un groupe G sur $\mathscr{A}$ est une action *par automorphismes de F-algèbre* si pour tout $g \in G$, la permutation

$$\begin{aligned} \mathscr{A} &\longrightarrow \mathscr{A} \\ a &\longmapsto g{\cdot}a \end{aligned}$$

est un automorphisme de F-algèbre, ou encore si le morphisme de groupes associé à l'action est en fait un morphisme $G \longrightarrow \mathrm{Aut}_{F-alg}(\mathscr{A})$.

Exemple 2.4. L'action d'un sous-groupe G de $\mathfrak{S}_n$ sur $F[X_1, \dots, X_n]$ décrite précédemment est une action par automorphisme de F-algèbre.

On a alors le lemme suivant.

Lemme 2.5. *Soit G un groupe agissant sur $F[X_1, \dots, X_n]$ par automorphismes de F-algèbre*[3].

3. Attention ! L'action considérée ici n'est pas nécessairement celle étudiée jusqu'à présent.

Alors, l'application

$$G \times F(X_1, \dots, X_n) \longrightarrow F(X_1, \dots, X_n)$$
$$(g, \frac{P}{Q}) \longmapsto g{\cdot}\frac{P}{Q} = \frac{g{\cdot}P}{g{\cdot}Q}$$

est bien définie, et est une action de G sur $F(X_1, \dots, X_n)$ par automorphismes de F-algèbre.

Si de plus G est fini, on a

$$F(X_1, \dots, X_n)^G = \{\frac{P}{Q} \mid P \in F[X_1, \dots, X_n]^G, Q \in F[X_1, \dots, X_n]^G \setminus \{0\}\}.$$

Démonstration. Si $\dfrac{P_1}{Q_1} = \dfrac{P_2}{Q_2}$, on a $P_1Q_2 = Q_1P_2$. Puisque g agit par automorphismes, en appliquant l'action de g à cette égalité, on obtient $(g{\cdot}P_1)(g{\cdot}Q_2) = (g{\cdot}Q_1)(g{\cdot}P_2)$, et ainsi

$$\frac{g{\cdot}P_1}{g{\cdot}Q_1} = \frac{g{\cdot}P_2}{g{\cdot}Q_2}.$$

Cela montre que l'application de l'énoncé est bien définie. Le fait que cela définit une action par automorphismes de F-algèbre découle alors des définitions, et de vérifications un peu longues mais faciles.

Supposons maintenant que G soit fini, et montrons l'égalité annoncée. L'inclusion « $\supset$ » étant claire au vu des définitions, montrons l'autre inclusion. Soit $f = \dfrac{P}{Q} \in F(X_1, \dots, X_n)^G$.

Posons $S = \displaystyle\prod_{g \in G} (g{\cdot}Q)$. On a alors $f = \dfrac{R}{S}$, pour un certain $R \in F[X_1, \dots, X_n]$.

Remarquons que, par construction, $S \in F[X_1, \dots, X_n]^G$. Montrons que $R \in F[X_1, \dots, X_n]^G$. Pour cela, soit $g \in G$. On a alors

$$g{\cdot}f = \frac{g{\cdot}R}{g{\cdot}S} = \frac{g{\cdot}R}{S} = f = \frac{R}{S},$$

d'où $g{\cdot}R = R$. Ceci étant vrai pour tout $g \in G$, on a bien $R \in F[X_1, \dots, X_n]^G$, d'où le résultat. □

La seconde partie de ce lemme montre en particulier que $F(X_1, \dots, X_n)^{\mathfrak{S}_n} = F(\sigma_1, \dots, \sigma_n)$. De plus, l'évaluation $T_i \rightsquigarrow \sigma_i$ induit un isomorphisme de F-algèbres

$$F(T_1, \dots, T_n) \simeq F(X_1, \dots, X_n)^{\mathfrak{S}_n}.$$

Comme précédemment, on a l'équivalence suivante, dont la démonstration est semblable en tous points à celle du lemme 2.1, mais cette fois en s'appuyant sur les résultats de la proposition 1.5.

Lemme 2.6. *Soit L/F une extension de corps, et soit $r \geq 0$ un entier. Les propriétés suivantes sont équivalentes :*

(i) il existe des éléments $a_1, \dots, a_r \in L$ algébriquement indépendants sur F tels que $L = F(a_1, \dots, a_r)$.

(ii) il existe un isomorphisme de F-algèbres $F(T_1, \dots, T_r) \simeq L$.

Une question peut-être plus raisonnable serait donc la suivante.

Soit G un sous-groupe de $\mathfrak{S}_n$, agissant sur $F[X_1,\dots,X_n]$ par

$$\begin{aligned} G\times F[X_1,\dots,X_n] &\longrightarrow F[X_1,\dots,X_n]\\ (\sigma,P) &\longmapsto \sigma\cdot P = P(X_{\sigma(1)},\dots,X_{\sigma(n)}). \end{aligned}$$

Considérons alors l'action de G induite sur $F(X_1,\dots,X_n)$.

Problème de Noether. Existe-t-il un isomorphisme de F-algèbres

$$F(X_1,\dots,X_n)^G \simeq F(T_1,\dots,T_r),$$

pour un certain entier $r\geq 0$? [4]

Remarquons que si $F[X_1,\dots,X_n]^G \simeq F[T_1,\dots,T_r]$, on a $F(X_1,\dots,X_n)^G \simeq F(T_1,\dots,T_n)$ (il suffit de considérer des éléments $a_1,\dots,a_r$ algébriquement indépendants sur F tels que $F[X_1,\dots,X_n]^G = F[a_1,\dots,a_r]$ et de considérer l'évaluation $T_i \rightsquigarrow a_i$).

En revanche, la réciproque est fausse. Par exemple, on démontrera plus loin que, dans la situation de l'exemple 2.2, on a

$$F(X_1,\dots,X_4)^G = F(U_1,U_2^2,U_3^2,U_2U_3U_4)$$

et que $U_1,U_2^2,U_3^2,U_2U_3U_4$ sont algébriquement indépendants sur F.

Il est beaucoup plus difficile de donner des exemples de groupe G pour lequel le problème de Noether possède une réponse négative sans utiliser des outils sophistiqués. Mentionnons sans démonstration que lorsque $F=\mathbb{Q}$, $G=\mathbb{Z}/8\mathbb{Z}$ fournit un contre-exemple. En revanche, nous verrons que si $F=\mathbb{C}$, le problème de Noether admet une réponse positive pour tout groupe abélien fini. La réponse au problème de Noether dépend donc très fortement du corps F, ce qui rend cette question très délicate.

Nous allons maintenant donner quelques généralisations naturelles de cette question, qui sont considérées dans la littérature.

Une première généralisation facile est la suivante. On considère un groupe fini abstrait G, et on considère l'algèbre de polynômes $F[X_g, g\in G]$. Le groupe $\mathfrak{S}(G)$ agit sur $F[X_g,g\in G]$ par

$$\sigma\cdot P(X_g,g\in G) = P(X_{\sigma(g)},g\in G).$$

D'après le théorème de Cayley, G est isomorphe au sous-groupe $\{\sigma_g \mid g\in G\}$ de $\mathfrak{S}(G)$, où σ_g est la multiplication à gauche par g dans G. On fait alors agir G via ce sous-groupe. Autrement dit, on fait agir G sur $F[X_g\in G]$ par

$$g\cdot P(X_h,h\in G) = P(X_{gh},h\in H).$$

Cette action, ainsi que celle étudiée précédemment, peuvent être vues dans un contexte plus général. Avant d'expliquer lequel, on a besoin d'un lemme calculatoire.

4. Encore une fois, on peut en fait démontrer que, si c'est le cas, on a nécessairement $r=n$.

Si $M = (a_{ij}) \in \mathrm{M}_n(F)$, et si $P \in F[X_1, \ldots, X_n]$, on pose

$$M * P(X_1, \ldots, X_n) = P(\sum_k a_{k1}X_k, \ldots, \sum_k a_{kn}X_k).$$

On a alors le résultat suivant.

Lemme 2.7. *Pour tous $M, N \in \mathrm{M}_n(F)$, et tout $P \in F[X_1, \ldots, X_n]$, on a :*

(1) $I_n * P = P$

(2) $M * (N * P) = MN * P$.

Démonstration. Le premier point est clair. Montrons le second point. Si $M = (a_{ij})$ and $N = (b_{ij})$, on a $MN = (\sum_k a_{ik}b_{kj})$. Posons $Q = N * P = P(\sum_k b_{k1}X_k, \ldots, \sum_k b_{kn}X_k)$.

On a alors

$$M*(N*P) = Q(\sum_\ell a_{\ell 1}X_\ell, \ldots, \sum_\ell a_{\ell n}X_\ell) = P(\sum_k b_{k1}(\sum_\ell a_{\ell k}X_\ell), \ldots, \sum_k b_{kn}(\sum_\ell a_{\ell k}X_\ell)).$$

On a donc

$$M * (N * P) = P(\sum_\ell (\sum_k a_{\ell k}b_{k1})X_\ell), \ldots, \sum_\ell (\sum_k a_{\ell k}b_{kn})X_\ell) = MN * P.$$

□

Remarque 2.8. Par définition, on a l'égalité

$$\begin{pmatrix} M * X_1 \\ \vdots \\ M * X_n \end{pmatrix} = M^t \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

On peut alors définir toute une famille d'action par automorphisme.

Lemme 2.9. *Soit G un groupe, et soit $\rho : G \longrightarrow \mathrm{GL}_n(F)$ un morphisme de groupes. Alors, l'application*

$$\begin{aligned} G \times F[X_1, \ldots, X_n] &\longrightarrow F[X_1, \ldots, X_n] \\ (g, P) &\longmapsto g{\cdot}P = \rho(g)^{-t} * P \end{aligned}$$

définit une action de G sur $F[X_1, \ldots, X_n]$ par automorphisme de F-algèbre.

Démonstration. Ce sont de simples calculs. □

Exemples 2.10.

(1) Pour tout $\sigma \in \mathfrak{S}_n$, on pose $M_\sigma = (\delta_{i\sigma(j)})$. Pour tout sous-groupe G de $\mathfrak{S}_n$, l'application

$$\begin{aligned} \rho\colon G &\longrightarrow \mathrm{GL}_n(F) \\ \sigma &\longmapsto M_\sigma \end{aligned}$$

est alors un morphisme de groupes.

En particulier, $M_\sigma^{-t} = M_{\sigma^{-1}}^t = (\delta_{j\sigma^{-1}(i)})$. On a alors $\sum_k \delta_{j\sigma^{-1}(k)}X_k = X_{\sigma(j)}$, et pour tout $P \in F[X_1, \ldots, X_n]$, on a donc $\sigma{\cdot}P = P(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$.

(2) Soit G un groupe d'ordre n. On indexe les éléments de $\mathrm{M}_n(F)$ par les éléments de G. Pour tout $g \in G$, on pose $\rho'(g) = (\delta_{h,gk})_{h,k\in G}$. L'application $\rho' : G \longrightarrow \mathrm{GL}_n(F)$ est alors un morphisme de groupes. C'est en fait le morphisme obtenu en composant le morphisme de Cayley $G \longrightarrow \mathfrak{S}(G)$ et le morphisme ρ du point précédent.

Il est alors facile de constater que pour tout $g \in G$ et tout $P \in F[X_h, h \in G]$, on a $g{\cdot}P = P(X_{gh}, h \in G)$.

On peut maintenant utiliser la famille d'actions par automorphisme définie dans le lemme 2.9 pour généraliser les questions précédentes.

Soit $\rho : G \longrightarrow \mathrm{GL}_n(F)$ un morphisme de groupes. On considère les actions de G induites sur $F[X_1, \ldots, X_n]$ et $F(X_1, \ldots, X_n)$.

(i) La F-algèbre $F[X_1, \ldots, X_n]^G$ est-elle isomorphe à une algèbre de polynômes sur F ?

(ii) **Problème de Noether généralisé.** La F-algèbre $F(X_1, \ldots, X_n)^G$ est-elle isomorphe à une algèbres de fractions rationnelles sur F ?

Comme on a l'a déjà constaté, la réponse à la question (i) est déjà négative pour le groupe de Klein (et positive pour (ii)), mais avec cette version généralisée, on peut donner un contre-exemple avec $G = \mathbb{Z}/2\mathbb{Z}$.

Exemple 2.11. Soit F un corps de caractéristique différente de 2. Soit $\rho : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{GL}_2(F)$ l'unique morphisme de groupes envoyant $\overline{1}$ sur $-I_2$. L'action correspondante sur $F[X_1, X_2]$ est donnée par

$$\overline{m}{\cdot}P = P((-1)^m X_1, (-1)^m X_2).$$

Il est facile de voir [5] que $F[X_1, X_2]^{\mathbb{Z}/2\mathbb{Z}} = \mathrm{Vect}_F(X_1^m X_2^n, m \equiv n\ [2])$. Remarquons que si $m \equiv n\ [2]$, on a $m = n + 2k$ ou $n = m + 2k, k \geq 0$, selon que $m \geq n$ ou $n \geq m$. Dans le premier cas, on a $X_1^m X_2^n = (X_1X_2)^n (X_1^2)^k$ et $X_1^m X_2^n = (X_1X_2)^m (X_2^2)^k$ dans le second.

On en déduit rapidement l'égalité $F[X_1, X_2]^{\mathbb{Z}/2\mathbb{Z}} = F[X_1^2, X_1X_2, X_2^2]$. Comme dans l'exemple 2.2, on montre que X_1^2, X_1X_2 et X_2^2 sont irréductibles, non associés deux à deux et que $F[X_1^2, X_1X_2, X_2^2]$ ne peut être isomorphe à une algèbre de polynômes sur F.

En revanche, la réponse au problème de Noether dans ce cas est encore positive.

En effet, le lemme 2.5 montre que $F(X_1, X_2)^{\mathbb{Z}/2\mathbb{Z}} = F(X_1^2, X_1X_2, X_2^2)$. Comme $X_1^2 = \dfrac{(X_1X_2)^2}{X_2^2}$, on a $F(X_1, X_2)^{\mathbb{Z}/2\mathbb{Z}} = F(X_1X_2, X_2^2)$.

Puisque X_1X_2 et X_2^2 sont algébriquement indépendants sur F, on a bien $F(X_1, X_2)^{\mathbb{Z}/2\mathbb{Z}} \simeq F(T_1, T_2)$.

On peut se demander pourquoi définir l'action de G sur $F[X_1, \ldots, X_n]$ de manière si compliquée, au lieu de simplement poser $g{\cdot}P = \rho(g) * P$.

5. Cela utilise le fait que $-1 \neq 1$ dans F, d'où l'hypothèse de caractéristique sur F.

L'action proposée est en fait la plus naturelle. Pour l'expliquer, nous allons réinterpréter les actions de G sur $F[X_1, \ldots, X_n]$ et $F(X_1, \ldots, X_n)$ dans le contexte de la théorie des représentations.

Introduisons quelques notations utiles.

Notations.

(i) Soit $\mathcal{A}$ une F-algèbre **commutative**, et soit S une partie de $\mathscr{A}$. On note

$$F[S] = \{P(\mathbf{s}) \mid n \geq 0, \mathbf{s} \in S^n, P \in F[X_1, \ldots, X_n]\}.$$

C'est en fait la sous-algèbre de $\mathscr{A}$ engendrée par S.

(ii) Soit L/F une extension de corps, et soit S une partie de L. On note

$$F(S) = \{P(\mathbf{s})Q(\mathbf{s})^{-1} \mid n \geq 0, \mathbf{s} \in S^n,\ P, Q \in F(X_1, \ldots, X_n), Q(\mathbf{s}) \neq 0\}.$$

C'est la sous-extension de L/F engendrée par S.

On peut maintenant définir la notion de fonction polynomiales sur un espace vectoriel.

Définition 2.12. Soit V un F-espace vectoriel de dimension finie $n \geq 1$.

Une *fonction monomiale sur* V est une fonction $V \longrightarrow F$ de la forme $c\varphi_1 \cdots \varphi_r$, où $r \geq 0$, $c \in F^\times$ et $\varphi_1, \ldots, \varphi_r \in V^*$. Une *fonction polynomiale sur* V est une somme finie (éventuellement vide) de fonctions monomiales sur V.

L'ensemble des fonctions polynomiales sur V est une sous-algèbre commutative de l'algèbre $\mathscr{F}(V, F)$ des fonctions de V dans F.

C'est en fait la sous-algèbre $F[V^*]$ de $\mathscr{F}(V, F)$ engendrée par les éléments de V^*.

Explicitons un peu plus la définition. Soit $(e_1, \ldots, e_n)$ une F-base de V, et soit $(e_1^*, \ldots, e_n^*)$ la base duale de V^*. Toute forme linéaire sur V étant combinaison linéaire de $e_1^*, \ldots, e_n^*$, on constate facilement qu'une fonction polynomiale sur V est une combinaison linéaire de fonctions de la forme $(e_1^*)^{m_1} \cdots (e_n^*)^{m_n}, m_i \geq 0$.

Autrement dit, une fonction polynomiale $f : V \longrightarrow F$ s'écrit sous la forme

$$f = \sum_{m_1, \ldots, m_n \geq 0} \lambda_{m_1, \ldots, m_n} (e_1^*)^{m_1} \cdots (e_n^*)^{m_n}, \lambda_{m_1, \ldots, m_n} \in F.$$

On a alors $f(\sum_{i=1}^{n} x_i e_i) = \sum_{m_1, \ldots, m_n \geq 0} \lambda_{m_1, \ldots, m_n} x_1^{m_1} \cdots x_n^{m_n}$ pour tout $x_i \in F$, ce qui justifie le nom de fonction polynomiale.

Notons que l'on a un morphisme d'évaluation $\begin{array}{ccc} F[X_1, \ldots, X_n] & \longrightarrow & F[V^*] \\ P & \longmapsto & P(e_1^*, \ldots, e_n^*) \end{array}$ qui est surjectif, d'après ce qui précède.

En général, ce morphisme n'est pas injectif, comme on le voit déjà dans le cas $F = \mathbb{F}_2$, puisque le polynôme $X^2 - X$ s'évalue en la fonction nulle.

En revanche, si F est infini, tout se passe bien.

Lemme 2.13. *Soit V un F-espace vectoriel de dimension $n \geq 1$, et soit $(e_1, \ldots, e_n)$ une base de V. Si F est infini, le morphisme d'évaluation*

$$\begin{aligned} F[X_1, \ldots, X_n] &\longrightarrow F[V^*] \\ P &\longmapsto P(e_1^*, \ldots, e_n^*) \end{aligned}$$

est un isomorphisme de F-algèbres.

Démonstration. Il reste à démontrer l'injectivité du morphisme d'évaluation. Cela revient à démontrer le fait suivant : si F est un corps infini, alors pour tout $P \in F[X_1, \ldots, X_n]$, on a

$$P(x_1, \ldots, x_n) = 0 \text{ pour tous } x_1, \ldots, x_n \in F \Longrightarrow P = 0.$$

C'est un résultat bien connu pour $n = 1$ (un polynôme en une indéterminée ayant une infinité de racines est nécessairement nul), et le cas général découle d'une récurrence finie. □

Nous pouvons maintenant expliquer d'où vient l'action définie dans le lemme 2.9. Pour commencer, remarquons qu'un morphisme de groupes $G \longrightarrow \mathrm{GL}_n(F)$ correspond à une action linéaire de G sur F^n. Nous allons donc utiliser ce point de vue.

Supposons que G agisse linéairement sur V. Alors, G agit linéairement sur $\mathscr{F}(V, F)$ par

$$(g \cdot f)(v) = f(g^{-1} \cdot v) \text{ pour tout } v \in V.$$

Notons que si $\varphi \in V^*$, on a aussi $g \cdot \varphi \in V^*$ pour tout $g \in G$. Il s'ensuit que cette action de G sur $\mathscr{F}(V, F)$ se restreint en une action linéaire sur V^* et en une action par automorphismes d'algèbre sur $F[V^*]$.

Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base de V, et soit $\mathscr{B}^* = (e_1^*, \ldots, e_n^*)$ la base duale de V^*.

Si on écrit les éléments de V dans la base $\mathscr{B}$ l'action de G sur V correspond à un morphisme $\rho : G \longrightarrow \mathrm{GL}_n(F)$. Le morphisme $\rho^* : G \longrightarrow \mathrm{GL}_n(F)$ correspondant à l'action induite sur V^* est alors défini par

$$\rho^*(g) = \rho(g)^{-t} \text{ pour tout } g \in G.$$

Autrement dit, si $\rho(g)^{-t} = (a'_{ij})$, alors $g \cdot e_j^* = \sum_k a'_{kj} e_k^*$.

Si $f = P(e_1^*, \ldots, e_n^*) \in F[V^*]$, on a donc

$$g \cdot f = P(g \cdot e_1^*, \ldots, g \cdot e_n^*) = P(\sum_k a'_{k1} e_k^*, \ldots, \sum_k a'_{kn} e_k^*),$$

la deuxième égalité provenant du fait que G agit par automorphismes d'algèbre.

En transportant l'action de G sur $F[V^*]$ en une action de G sur $F[X_1, \ldots, X_n]$ via l'isomorphisme du lemme 2.13, on obtient alors l'action définie dans le lemme 2.9.

3. Le théorème de Fischer : aspect théorique

Nous allons maintenant étudier le problème de Noether pour les groupes abéliens finis lorsque le corps de base contient suffisamment de racines de l'unité. Plus précisément, nous allons montrer le théorème suivant.

Rappelons que si G est un groupe fini, l'exposant de G est le plus petit entier $e \geq 1$ tel que $g^e = 1_G$ pour tout $g \in G$.

Si $n \geq 1$ est un entier, on note $\mu_n(\overline{F})$ l'ensemble des racines n-ièmes de l'unité d'une clôture algébrique $\overline{F}$ de F. Autrement dit

$$\mu_n(\overline{F}) = \{x \in \overline{F} \mid x^n = 1\}.$$

C'est un groupe cyclique d'ordre n lorsque $\mathrm{car}(F) \nmid n$.

Théorème 3.1 (Fischer). *Soit G un groupe abélien fini d'exposant e, et soit F un corps tel que $\mathrm{car}(F) \nmid e$ et $\mu_e(\overline{F}) \subset F$.*

Alors, pour tout morphisme $\rho : G \longrightarrow \mathrm{GL}_n(F)$, on a un isomorphisme d'algèbres

$$F(X_1, \ldots, X_n)^G \simeq F(T_1, \ldots, T_n).$$

Autrement dit, il existe des fractions rationnelles $f_1, \ldots, f_n \in F(X_1, \ldots, X_n)^G$ algébriquement indépendantes sur F telles que $F(X_1, \ldots, X_n)^G = F(f_1, \ldots, f_n)$.

Remarque 3.2. Ce théorème n'est plus vrai si on remplace $F(X_1, \ldots, X_n)$ par $F[X_1, \ldots, X_n]$, comme le montre déjà l'exemple 2.11.

Nous allons maintenant nous employer à démontrer le théorème de Fischer. Dans ctte partie, nous fournirons une démonstration théorique de ce résultat, mais nous verrons dans la partie suivante une méthode explicite pour tout calculer.

Dans la suite, on fixe un groupe abélien fini G d'exposant e, et un morphisme $\rho : G \longrightarrow \mathrm{GL}_n(F)$, où F vérifie $\mathrm{car}(F) \nmid e$ et $\mu_e(\overline{F}) \subset F$.

On commence par faire un changement de variables qui sera plus adapté pour nos calculs.

Lemme 3.3.

(1) *Il existe une matrice $R \in \mathrm{GL}_n(F)$ et des morphismes de groupes $\omega_i : G \longrightarrow \mu_e(\overline{F})$ tels que*

$$R^{-1}\rho(g)R = \begin{pmatrix} \omega_1(g) & & \\ & \ddots & \\ & & \omega_n(g) \end{pmatrix} \quad \textit{pour tout } g \in G.$$

(2) *Soit $R \in \mathrm{GL}_n(F)$ une matrice vérifiant la propriété précédent. Si $R^{-1} = (a'_{ij})$, on pose*

$$U_j = \sum_k a'_{jk} X_k \quad \textit{pour tout } j \in [\![1, n]\!].$$

Alors, $F[X_1,\dots,X_n] = F[U_1,\dots,U_n]$ *et* $U_1,\dots,U_n$ *sont algébriquement indépendants sur* F*. De plus,*

$$g{\cdot}U_i = \omega_i(g)^{-1}U_i \text{ pour tout } g\in G, \text{ et tout } i\in[\![1,n]\!].$$

Démonstration. Soit $g\in G$. Puisque $g^e = 1_G$, on a $\rho(g)^e = \rho(g^e) = I_n$. Les hypothèses sur F entraînent que le polynôme $X^e-1\in F[X]$ est scindé sur F à racines simples, et $\rho(g)$ est donc diagonalisable, et ses valeurs propres sont des racines e-ièmes de l'unité. Puisque G est abélien, les matrices $\rho(g), g\in G$, sont donc codiagonalisables. [6]

Il existe donc $R\in \mathrm{GL}_n(F)$ tel que

$$R^{-1}\rho(g)R = \begin{pmatrix}\omega_1(g) & & \\ & \ddots & \\ & & \omega_n(g)\end{pmatrix} \quad \text{pour tout } g\in G,$$

où $\omega_1(g),\dots,\omega_n(g)\in\mu_e(\overline{F})$.

Puisque ρ est un morphisme de groupes, les applications $\omega_i : G\longrightarrow \mu_e(\overline{F})$ sont des morphismes de groupes, comme on le voit grâce à un simple calcul. Ceci démontre le point (1).

Démontrons (2). Par définition de $U_1,\dots,U_n$, on a $\begin{pmatrix}U_1\\ \vdots\\ U_n\end{pmatrix} = R^{-1}\begin{pmatrix}X_1\\ \vdots\\ X_n\end{pmatrix}$.

Puisque $g{\cdot}U_i = \sum_j a'_{ij}g{\cdot}X_j$, on a donc $\begin{pmatrix}g{\cdot}U_1\\ \vdots\\ g{\cdot}U_n\end{pmatrix} = R^{-1}\begin{pmatrix}g{\cdot}X_1\\ \vdots\\ g{\cdot}X_n\end{pmatrix}$.

D'après la remarque 2.8 et la définition de l'action de G sur $F[X_1,\dots,X_n]$, on a $\begin{pmatrix}g{\cdot}X_1\\ \vdots\\ g{\cdot}X_n\end{pmatrix} = (\rho(g)^{-t})^t\begin{pmatrix}X_1\\ \vdots\\ X_n\end{pmatrix} = \rho(g)^{-1}\begin{pmatrix}X_1\\ \vdots\\ X_n\end{pmatrix}$. On a donc

$$\begin{pmatrix}g{\cdot}U_1\\ \vdots\\ g{\cdot}U_n\end{pmatrix} = R^{-1}\rho(g)^{-1}\begin{pmatrix}X_1\\ \vdots\\ X_n\end{pmatrix} = R^{-1}\rho(g)^{-1}R\begin{pmatrix}U_1\\ \vdots\\ U_n\end{pmatrix} = \begin{pmatrix}\omega_1(g) & & \\ & \ddots & \\ & & \omega_n(g)\end{pmatrix}^{-1}\begin{pmatrix}U_1\\ \vdots\\ U_n\end{pmatrix}.$$

Ainsi, on obtient

$$g{\cdot}U_i = \omega_i(g)^{-1}U_i \text{ pour tout } g\in G, \text{ et tout } i\in[\![1,n]\!].$$

Notons maintenant que par définition des U_i, on a $P(U_1,\dots,U_n) = R^{-t}*P(X_1,\dots,X_n)$ pour tout $P\in F[X_1,\dots,X_n]$.

Comme $P = R^t*(R^{-t}*P) = R^t*P(U_1,\dots,U_n)$, on en déduit $F[U_1,\dots,U_n] = F[X_1,\dots,X_n]$.

6. Ceci reflète le fait que les représentations irréductibles d'un groupe abélien sont toutes de degré 1.

D'autre part, si $Q \in F[T_1, \dots, T_n]$ vérifie $Q(U_1, \dots, U_n) = 0$, on a donc $R^{-t} * Q = 0$, puis $Q = R^t * (R^{-t} * Q) = 0$. Ainsi, $U_1, \dots, U_n$ sont algébriquement indépendants sur F. □

Nous pouvons maintenant décrire une première famille de générateurs de l'algèbre des polynômes et fractions rationnelles G-invariantes.

Avant d'énoncer le résultat, on introduit une notation.

Si $T_1, \dots, T_n$ sont des indéterminées sur F, et si $\mathbf{m} = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \in \mathbb{N}^n$, on pose

$$T^{\mathbf{m}} = T_1^{m_1} \cdots T_n^{m_n} \in F[T_1, \dots, T_n].$$

De même, si $\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \in \mathbb{Z}^n$, on pose

$$T^{\boldsymbol{\gamma}} = T_1^{\gamma_1} \cdots T_n^{\gamma_n} \in F(T_1, \dots, T_n).$$

On a alors le lemme suivant.

Lemme 3.4. *Soient*

$$\mathscr{M} = \{\mathbf{m} = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \in \mathbb{N}^n \mid \omega_1(g)^{m_1} \cdots \omega_n(g)^{m_n} = 1 \text{ pour tout } g \in G\}$$

et

$$\Gamma = \{\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \in \mathbb{Z}^n \mid \omega_1(g)^{\gamma_1} \cdots \omega_n(g)^{\gamma_n} = 1 \text{ pour tout } g \in G\}.$$

Alors, on a les égalités suivantes :

(1) $F[X_1, \dots, X_n]^G = \mathrm{Vect}_F(U^{\mathbf{m}}, \mathbf{m} \in \mathscr{M}) = F[U^{\mathbf{m}}, \mathbf{m} \in \mathscr{M}]$.

(2) $F(X_1, \dots, X_n)^G = F(U^{\mathbf{m}}, \mathbf{m} \in \mathscr{M}) = F(U^{\boldsymbol{\gamma}}, \boldsymbol{\gamma} \in \Gamma)$.

Démonstration. Gardons les notations du lemme précédent. D'après ce même lemme, on a $F[X_1, \dots, X_n] = F[U_1, \dots, U_n]$, où les U_i sont algébriquement indépendants sur F. Autrement dit, tout polynôme $P \in F[X_1, \dots, X_n]$ s'écrit de manière unique sous la forme

$$P = \sum_{\mathbf{m}} \lambda_{\mathbf{m}} U^{\mathbf{m}}, \ \lambda_{\mathbf{m}} \in F.$$

On a alors

$$g \cdot P = \sum_{\mathbf{m}} \lambda_{\mathbf{m}} \omega_1(g)^{-m_1} \cdots \omega_n(g)^{-m_n} U^{\mathbf{m}} \text{ pour tout } g \in G.$$

L'égalité précédente montre que l'on a $P \in F[X_1, \dots, X_n]^G$ si, et seulement si, $\lambda_{\mathbf{m}} \omega_1(g)^{-m_1} \cdots \omega_n(g)^{-m_n} = \lambda_{\mathbf{m}}$ pour tout $g \in G$ et tout $\mathbf{m} \in \mathbb{N}^n$.

On en déduit alors facilement l'égalité

$$F[X_1,\dots,X_n]^G = \mathrm{Vect}_F(U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}),$$

puis

$$F[X_1,\dots,X_n]^G = F[U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}].$$

En effet, l'inclusion $\mathrm{Vect}_F(U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}), \subset F[U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}]$ est évidente, et l'autre inclusion provient du fait qu'un produit fini de monômes de la forme $U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}$, est encore un monôme de cette forme, car $\mathscr{M}$ est stable par addition.

Le lemme 2.5 implique alors l'égalité

$$F(X_1,\dots,X_n)^G = F(U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}).$$

Montrons (2). Encore une fois, l'inclusion

$$F(X_1,\dots,X_n)^G = F(U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}) \subset F(U^{\boldsymbol{\gamma}}, \boldsymbol{\gamma}\in\Gamma)$$

est évidente.

Pour établir l'autre inclusion, il suffit de voir que $U^{\boldsymbol{\gamma}} \in F(U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M})$ pour tout $\boldsymbol{\gamma}\in\Gamma$.

Or, on a $e\mathbb{Z}^n \subset \Gamma$ par définition de l'exposant. Soit alors $k\in\mathbb{N}$ tel que $m_i' = ke+\gamma_i \geq 0$ pour tout $i\in[\![1,n]\!]$.

Alors, $\begin{pmatrix} ke \\ \vdots \\ ke \end{pmatrix}$ et $\mathbf{m}'$ sont des éléments de $\mathscr{M}$, et on a

$$U^{\boldsymbol{\gamma}} = \frac{U_1^{m_1'}\cdots U_n^{m_n'}}{U_1^{ke}\cdots U_n^{ke}} \in F(U^{\mathbf{m}}, \mathbf{m}\in\mathscr{M}),$$

d'où la conclusion souhaitée. □

On peut se demander ce que l'on a gagné en remplaçant $\mathscr{M}$ par Γ, puisque, a priori, on a rajouté des générateurs inutiles. Avant de répondre à cette question, introduisons quelques définitions commodes.

Définition 3.5. Soit $\mathscr{E}$ un groupe abélien, que l'on notera additivement. Une famille finie $(v_1,\dots,v_n)$ de $\mathscr{E}$ est dite $\mathbb{Z}$-*libre* si pour tous $m_1,\dots,m_n\in\mathbb{Z},$, on a

$$m_1{\cdot}v_1+\cdots+m_r{\cdot}v_r = 0 \Longrightarrow m_1=\cdots=m_r=0.$$

Elle est dite $\mathbb{Z}$-*génératrice* si $\langle v_1,\dots,v_n\rangle = \mathscr{E}$, c'est-à-dire si tout élément v de $\mathscr{E}$ s'écrit sous la forme

$$v = m_1{\cdot}v_1+\cdots+m_r{\cdot}v_r,\ m_i\in\mathbb{Z}.$$

On dit que $(v_1,\dots,v_n)$ est une $\mathbb{Z}$-*base* de $\mathscr{E}$ si elle est à la fois $\mathbb{Z}$-libre et $\mathbb{Z}$-génératrice, ce qui revient à dire que tout élément $v\in\mathscr{E}$ s'écrit de manière unique sous la forme

$$v = a_1{\cdot}v_1+\cdots+a_n{\cdot}v_n,\ a_i\in\mathbb{Z}.$$

Enfin, on dit que $\mathscr{E}$ est un groupe abélien *libre de rang fini* s'il possède au moins une $\mathbb{Z}$-base.

Exemple 3.6. Le groupe abélien $\mathbb{Z}^n$ est abélien libre de rang fini, pour tout $n \geq 1$. En effet, les vecteurs

$$\varepsilon_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \varepsilon_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

forment une $\mathbb{Z}$-base de $\mathbb{Z}^n$, appelée *base canonique*.

Remarques 3.7.

(1) Il est facile de voir qu'un groupe $\mathscr{E}$ abélien est libre de rang fini s'il existe $n \geq 0$ tel que $\mathscr{E} \simeq \mathbb{Z}^n$.

En particulier, tout groupe abélien n'est pas nécessairement libre de rang fini, comme le montre déjà l'exemple d'un groupe abélien fini non trivial.

(2) On peut démontrer également que toutes les $\mathbb{Z}$-bases d'un groupe abélien $\mathscr{E}$ libre de rang fini ont même cardinal. Ce cardinal commun est alors appelé le *rang* de $\mathscr{E}$.

Ce résultat n'est pas complètement évident, mais on peut le démontrer facilement dans le cas des sous-groupes de $\mathbb{Z}^n$.

En effet, soit $\mathscr{E}$ un groupe abélien libre de rang fini. On suppose que $\mathscr{E}$ est un sous-groupe de $\mathbb{Z}^n$. On a donc des inclusions

$$\mathscr{E} \subset \mathbb{Z}^n \subset \mathbb{Q}^n.$$

Il est facile de voir qu'une $\mathbb{Z}$-base de $\mathscr{E}$ est une famille $\mathbb{Q}$-libre de $\mathbb{Q}^n$ (il suffit de chasser les dénominateurs dans une relation de dépendance $\mathbb{Q}$-linéaire). En particulier, une $\mathbb{Z}$-base de $\mathscr{E}$ est une $\mathbb{Q}$-base du $\mathbb{Q}$-sous-espace vectoriel de $\mathbb{Q}^n$ engendré par les éléments de $\mathscr{E}$. On utilise alors le fait que deux bases d'un même espace vectoriel de dimension finie ont même cardinal pour conclure.

On a alors la proposition suivante.

Proposition 3.8. *Soit $n \geq 0$ un entier. Alors, tout sous-groupe de $\mathbb{Z}^n$ est libre de rang $\leq n$.*

Démonstration. On procède par récurrence sur n. Pour $n = 0$, on obtient le groupe trivial, et tout sous-groupe est trivial de rang nul (une base étant la famille vide). Supposons avoir démontré le résultat pour tous les sous-groupes de $\mathbb{Z}^n$, pour un entier $n \geq 0$, et soit Γ un sous-groupe de $\mathbb{Z}^{n+1}$. Soit Γ' le sous-groupe de Γ formés des éléments dont la dernière composante est nulle. Ce sous-groupe est clairement isomorphe au sous-groupe de $\mathbb{Z}^n$ obtenu en oubliant la dernière composante, donc admet une base $e_1, \ldots, e_r$ de cardinal $r \leq n$, par hypothèse de récurrence. D'autre part, l'image de Γ par la projection $\mathbb{Z}^{n+1} \longrightarrow \mathbb{Z}$ sur la dernière composante est un sous-groupe de $\mathbb{Z}$, donc de la forme $d\mathbb{Z}, d \geq 0$. Si $d = 0$, cela signifie que $\Gamma = \Gamma'$, et on a fini d'après ce qui précède. Sinon, choisissons $e_{r+1} \in \Gamma$ dont la dernière composante est d. Nous allons démontrer que $(e_1, \ldots, e_{r+1})$ est une $\mathbb{Z}$-base de Γ. Comme elle est de cardinal $r + 1 \leq n + 1$, ceci achèvera la récurrence.

Montrons tout d'abord que cette famille est libre. Soient $m_1, \dots, m_r \in \mathbb{Z}$ tels que

$$m_1 e_1 + \cdots + m_r e_r + m_{r+1} e_{r+1} = 0.$$

Alors, $m_{r+1} e_{r+1} = -(m_1 e_1 + \cdots + m_r e_r) \in \Gamma'$. La dernière coordonnée de $m_{r+1} e_{r+1}$ est donc nulle, i.e.$m_{r+1} d = 0$, soit $m_{r+1} = 0$ puisque $d \geq 1$. On a donc $m_1 e_1 + \cdots + m_r e_r = 0$, ce qui entraîne que $m_1 = \cdots = m_r = 0$, puisque $(e_1, \dots, e_r)$ est une $\mathbb{Z}$-base de Γ', donc une famille $\mathbb{Z}$-libre.

Montrons maintenant que cette famille est $\mathbb{Z}$-génératrice.

Si $\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix}$, alors $\gamma_n = d\gamma'_n, \gamma'_n \in \mathbb{Z}$. On a alors $\boldsymbol{\gamma} - \gamma'_n e_{r+1} \in \Gamma'$. Ainsi, $\boldsymbol{\gamma} - \gamma'_n e_{r+1}$ est une combinaison $\mathbb{Z}$-linéaire de $e_1, \dots, e_r$, et $\boldsymbol{\gamma} = (\boldsymbol{\gamma} - \gamma'_n e_{r+1}) + \gamma'_n e_{r+1}$ est une combinaison $\mathbb{Z}$-linéaire de $e_1, \dots, e_{r+1}$, ce qu'il fallait démontrer. Cela achève la démonstration. □

On peut alors démontrer le résultat suivant, qui permet de conclure.

Proposition 3.9. *Soit $(\boldsymbol{\gamma}^{(1)}, \dots, \boldsymbol{\gamma}^{(n)})$ une $\mathbb{Z}$-base de Γ. Alors :*

(1) $F(X_1, \dots, X_n)^G = F(U^{\boldsymbol{\gamma}^{(j)}},\ j \in [\![1, n]\!])$;

(2) *Les fractions rationnelles $U^{\boldsymbol{\gamma}^{(j)}},\ j \in [\![1, n]\!]$, sont algébriquement indépendantes sur F.*

Démonstration. On sait déjà que $F(X_1, \dots, X_n)^G = F(U^{\boldsymbol{\gamma}}, \boldsymbol{\gamma} \in \Gamma)$. Pour démontrer le point (1), il suffit donc de constater l'égalité

$$F(U^{\boldsymbol{\gamma}}, \boldsymbol{\gamma} \in \Gamma) = F(U^{\boldsymbol{\gamma}^{(j)}},\ j \in [\![1, n]\!]).$$

L'inclusion $\ll \supset \gg$ est évidente. Démontrons l'inclusion manquante. Soit $\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \in \Gamma$. Il existe donc $a_1, \dots, a_n \in \mathbb{Z}$ tels que

$$\boldsymbol{\gamma} = a_1 \boldsymbol{\gamma}^{(1)} + \cdots + a_n \boldsymbol{\gamma}^{(n)}.$$

On a alors

$$U^{\boldsymbol{\gamma}} = \prod_{j=1}^{n} (U^{\boldsymbol{\gamma}^{(j)}})^{a_j} \in F(U^{\boldsymbol{\gamma}^{(j)}},\ j \in [\![1, n]\!]).$$

Cela suffit à conclure. Montrons le point (2).

Soit $P = \sum_{\mathbf{m}} \lambda_{\mathbf{m}} T^{\mathbf{m}} \in F[T_1, \dots, T_n]$ tel que

$$P(U^{\boldsymbol{\gamma}^{(1)}}, \dots, U^{\boldsymbol{\gamma}^{(n)}}) = 0.$$

On a donc

$$\sum_{\mathbf{m}} \lambda_{\mathbf{m}} U^{\sum_{j=1}^{n} m_j \boldsymbol{\gamma}^{(j)}} = 0.$$

Soit $\mathbf{u} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$, et soit $k \geq 1$ un entier tel que $k\mathbf{u} + \sum_{j=1}^{n} m_j \boldsymbol{\gamma}^{(j)} \in \mathbb{N}^n$. En multipliant l'égalité précédente par $(U_1 \cdots U_n)^k$, on obtient

$$\sum_{\mathbf{m}} \lambda_{\mathbf{m}} U^{k\mathbf{u}+\sum_{j=1}^{n} m_j \boldsymbol{\gamma}^{(j)}} = 0 \in F[U_1, \ldots, U_n].$$

Montrons que les n-uplets $k\mathbf{u} + \sum_{j=1}^{n} m_j \boldsymbol{\gamma}^{(j)}$, lorsque $\mathbf{m}$ parcourt $\mathbb{N}^n$, sont distincts deux à deux.

Supposons que

$$k\mathbf{u} + \sum_{j=1}^{n} m_j \boldsymbol{\gamma}^{(j)} = k\mathbf{u} + \sum_{j=1}^{n} m'_j \boldsymbol{\gamma}^{(j)}.$$

On a donc $\sum_{j=1}^{n} (m_j - m'_j) \boldsymbol{\gamma}^{(j)} = 0$ pour tout $i \in [\![1, n]\!]$. Comme $(\boldsymbol{\gamma}^{(1)}, \ldots, \boldsymbol{\gamma}^{(n)})$ est une $\mathbb{Z}$-base, on en déduit que $m_j = m'_j$ pour tout $j \in [\![1, n]\!]$, ce qu'il fallait montrer.

L'égalité

$$\sum_{\mathbf{m}} \lambda_{\mathbf{m}} U^{k\mathbf{u}+\sum_{j=1}^{n} m_j \boldsymbol{\gamma}^{(j)}} = 0 \in F[U_1, \ldots, U_n]$$

fait donc intervenir des monômes deux à deux distincts. On en déduit que tous les coefficients correspondants sont nuls, i.e. $\lambda_{\mathbf{m}} = 0$ pour tout $\mathbf{m} \in \mathbb{N}^n$. Ainsi, $P = 0$, et on a fini. □

4. Le théorème de Fischer : aspect pratique

Nous allons maintenant nous intéresser à l'aspect calculatoire du théorème de Fischer. Le but de cette partie est de donner une méthode pratique pour calculer des fractions rationnelles G-invariantes algébriques indépendantes engendrant $F(X_1, \ldots, X_n)^G$.

La démonstration du théorème de Fischer donnée dans la partie précédente nous fournit a priori un moyen de tout calculer à deux exceptions près :

(a) il faut réussir à exhiber une matrice R satisfaisant les conditions du lemme 3.3

(b) il faut pouvoir trouver une $\mathbb{Z}$-base du groupe Γ défini dans le lemme 3.4.

Intéressons-nous tout d'abord au calcul d'une matrice R convenable, c'est-à-dire au calcul d'une base de diagonalisation commune des matrices $\rho(g), g \in G$.

Le point (1) du lemme 3.3 nous fournit l'existence d'une base $(v_1, \ldots, v_n)$ de F^n telle que

$$\rho(g)(e_i) = \omega_i(g) e_i \quad \text{pour tout } g \in G, \text{ et tout } i \in [\![1, n]\!],$$

où $\omega_i : G \longrightarrow \mu_e(\overline{F})$ est un morphisme de groupes.

La première étape est de décrire ces morphismes. Pour éviter de rallonger l'exposition, on suppose que l'on a déjà à disposition une décomposition $G = \langle g_1\rangle \odot \cdots \odot \langle g_r\rangle$ en sous-groupes cycliques, d'ordres $d_1, \ldots, d_r$ respectivement (avec $2 \leq d_1 \mid \cdots \mid d_r$ si l'on souhaite avoir un r minimal).

Tout élément $g \in G$ s'écrit alors de manière unique sous la forme

$$g = g_1' \cdots g_r',\ g_i' \in \langle g_i\rangle.$$

Chaque g_i' s'écrit $g_i' = g_i^{m_i}, m_i \in \mathbb{Z}$, où m_i est unique modulo d_i.

On a alors le lemme suivant.

Lemme 4.1. *Pour chaque $i \in [\![1, r]\!]$, fixons $z_i \in \mu_{d_i}(\overline{F})$. Alors, il existe un unique morphisme de groupes $\omega_{z_1,\ldots,z_n} : G \longrightarrow \mu_e(\overline{F})$ tel que*

$$\omega_{z_1,\ldots,z_n}(g_i) = z_i \quad \textit{pour tout } i \in [\![1, r]\!]\,.$$

Il est défini par

$$\omega_{z_1,\ldots,z_n}(g_1^{m_1} \cdots g_r^{m_r}) = z_1^{m_1} \cdots z_r^{m_r},\ m_i \in \mathbb{Z}.$$

De plus, tout morphisme $\omega : G \longrightarrow \mu_e(\overline{F})$ est de la forme $\omega_{z_1,\ldots,z_n}$, où $z_1, \ldots, z_n$ sont uniques.

Démonstration. Notons que l'on a $d_i \mid e$, puisque $g_i^e = 1_G$, et donc que l'on a bien $z_i \in \mu_e(\overline{F})$. On remarque que $\omega_{z_1,\ldots,z_n}(g_1^{m_1} \cdots g_r^{m_r})$ est bien une racine e-ième de l'unité, qui ne dépend pas du choix des m_i, puisque $z_i^{d_i} = 1$. Il est alors facile de voir que $\omega_{z_1,\ldots,z_n}$ est un morphisme de groupes.

Soit maintenant $\omega : G \longrightarrow \mu_e(\overline{F})$ un morphisme de groupes. Notons que

$$\omega(g_i)^{d_i} = \omega(g_i^{d_i}) = \omega(1_G) = 1.$$

On a donc nécessairement $\omega(g_i) \in \mu_{d_i}(\overline{F})$. Si l'on pose $z_i = \omega(g_i)$, on a donc

$$\omega(g_1^{m_1} \cdots g_r^{m_r}) = z_1^{m_1} \cdots z_r^{m_r} \quad \text{pour tous } m_1, \ldots, m_r \in \mathbb{Z},$$

et ainsi $\omega = \omega_{z_1,\ldots,z_r}$.

Si maintenant $\omega = \omega_{z_1',\ldots,z_r'}$, alors en évaluant les images en chaque g_i, on obtient $z_i' = \omega(g_i)$, d'où la partie unicité. □

On en déduit un résultat qui nous sera fort utile un peu plus loin.

Corollaire 4.2. *Soit G un groupe abélien fini d'exposant e, et soient $\omega, \omega' : G \longrightarrow \mu_e(\overline{F})$ deux morphismes de groupes. Alors, on a*

$$\frac{1}{|G|}\sum_{g\in G} \omega(g)^{-1}\omega'(g) = \begin{cases} 1 & \textit{si } \omega = \omega' \\ 0 & \textit{sinon.} \end{cases}$$

Démonstration. Le cas $\omega = \omega'$ étant clair, on peut supposer que $\omega \neq \omega'$.

Gardons les notations du lemme précédent. D'après ce même lemme, on a $\omega = \omega_{z_1,\ldots,z_r}$ et $\omega' = \omega_{z_1',\ldots,z'r}$, avec $z_i, z_i' \in \mu_{d_i}(\overline{F})$. On a donc $z_j \neq z_j'$ pour un certain $j \in [\![1, r]\!]$

Notons qu'un élément $g \in G$ s'écrit de manière unique

$$g = g_1^{k_1} \cdots g_r^{k_r}, k_i \in [\![0, d_i - 1]\!]\,.$$

On a alors

$$\frac{1}{|G|}\sum_{g\in G}\omega(g)^{-1}\omega'(g) = \frac{1}{|G|}(\sum_{k_1=0}^{d_1-1}(z_1^{-1}z_1')^{k_1})\cdots(\sum_{k_r=0}^{d_r-1}(z_r^{-1}z_r')^{k_r}).$$

Or, si z est une racine d-ième de l'unité différente de 1, on a

$$\sum_{k=0}^{d-1} z^k = \frac{1-z^d}{1-z} = 0.$$

Par hypothèse, le j-ème facteur de l'expression précédente est donc nul, puisque $z_j^{-1}z_j' \neq 1$. Cela achève la démonstration. □

Reprenons nos considérations. Si $\omega : G \longrightarrow \mu_e(\overline{F})$ est un morphisme de groupes, on pose

$$V_\omega = \bigcap_{g\in G} \mathrm{Ker}(\rho(g) - \omega(g)\mathrm{Id}) = \{v \in F^n \mid \rho(g)v = \omega(g)v \ \text{ pour tout } g \in G\}.$$

Le lemme 3.3 nous dit alors que l'on a une décomposition en somme directe

$$F^n = \bigoplus_\omega V_\omega,$$

où ω décrit l'ensemble des morphismes $G \longrightarrow \mu_e(\overline{F})$. Notons que V_ω peut très bien être le sous-espace nul. Pour éviter cela, on peut bien sûr limiter la somme aux seuls morphismes aux seuls morphismes ω_i qui apparaissent dans le lemme 3.3, mais cela suppose de factoriser les polynômes caractéristiques des matrices $\rho(g), g \in G$ (ou au moins des $\rho(g_k)$).

Tout le jeu consiste maintenant à calculer une base de V_ω pour chaque ω à partir de la seule connaissance de ρ. La solution est donnée par la proposition suivante.

Proposition 4.3. *Pour tout morphisme $\omega : G \longrightarrow \mu_e(\overline{F})$, on pose*

$$P_\omega = \frac{1}{|G|}\sum_{g\in G}\omega(g)^{-1}\rho(g).$$

Alors, P_ω est la matrice dans la base canonique de la projection sur V_ω parallèlement à $\bigoplus_{\omega'\neq\omega} V_{\omega'}$.

Démonstration. Soit $\omega' : G \longrightarrow \mu_e(\overline{F})$ un morphisme de groupes, et soit $v \in V_{\omega'}$. On doit démontrer que $P_\omega v = v$ si $\omega = \omega'$ et que $P_\omega v = 0$ si $\omega \neq \omega'$.

Par définition de $V_{\omega'}$, on a

$$P_\omega v = \frac{1}{|G|}\sum_{g\in G}\omega(g)^{-1}\omega'(g)v.$$

On utilise alors le lemme précédent pour conclure. □

Autrement dit, pour calculer une base de diagonalisation simultanée, il suffit de procéder aux étapes suivantes :

(1) On calcule tous les morphismes $\omega : G \longrightarrow \mu_e(\overline{F})$. Notons que cela suppose connue une décomposition de G en somme directe de sous-groupes cycliques.

(2) Pour chaque morphisme ω, on calcule la matrice P_ω. Une famille de colonnes de P_ω linéairement indépendantes fournit une base de V_ω (notons que si $P_\omega = 0$, on obtient la famille vide).

(3) On recolle les bases obtenues pour obtenir la base voulue.

Remarque 4.4. Le lecteur familier avec la théorie des représentations aura remarqué que le corollaire 4.2 n'est rien d'autre que le fait que les caractères irréductibles forment une famille orthonormée pour un produit scalaire adéquat sur l'espace des fonctions centrales, et que d'autre part, les sous-espaces V_ω sont les composantes isotypiques liées à la représentation $\rho : G \longrightarrow \mathrm{GL}_n(F)$.

Il reste maintenant à comprendre comment calculer une base du groupe Γ.

On commence par un résultat d'algèbre linéaire. On note $\mathrm{GL}_n(\mathbb{Z})$ le groupe des inversibles de l'anneau $\mathrm{M}_n(\mathbb{Z})$. Rappelons à toutes fins utiles que

$$\mathrm{GL}_n(\mathbb{Z}) = \{P \in \mathrm{M}_n(\mathbb{Z}) \mid \det(P) = \pm 1\},$$

même si nous n'en aurons pas besoin.

Soit $\ell \geq 2$ un entier. Si $r, s \in [\![1, \ell]\!]$, on note E_{rs} la matrice de $\mathrm{M}_\ell(A)$ qui admet un seul coefficient non nul égal 1 à l'intersection de la ligne r et de la colonne s.

Si $i, j \in [\![1, \ell]\!]$, avec $i \neq j$, on pose

$$S_{i,j}^{(\ell)} = E_{ij} + E_{ji} + \sum_{k \neq i,j} E_{kk} \in \mathrm{M}_\ell(A).$$

Autrement dit, $S_{i,j}^{(\ell)}$ est la matrice

$$\begin{array}{c} \\ i \longrightarrow \\ \\ \\ \\ j \longrightarrow \\ \\ \end{array} \begin{array}{c} \begin{array}{cccccccc} & & & i & & & j & \\ & & & \downarrow & & & \downarrow & \\ \end{array} \\ \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & & & 1 & \\ & & & & 1 & & & \\ & & & & & \ddots & & \\ & & & & & & 1 & \\ & & & 1 & & & 0 & \\ & & & & & & & 1 \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix} \end{array} \in \mathrm{M}_\ell(A)$$

Cette matrice est inversible, d'inverse

$$(S_{i,j}^{(\ell)})^{-1} = S_{i,j}^{(\ell)}.$$

Si $C \in \mathrm{M}_{m \times n}(A)$, l'opération

$$C \longmapsto S_{i,j}^{(m)} C$$

revient à échanger les lignes i et j de C, tandis que l'opération

$$C \longmapsto CS_{i,j}^{(n)}$$

revient à échanger les colonnes i et j de C. Une matrice de ce type est appelée une *matrice de transposition*.

Si $i, j \in [\![1, \ell]\!]$, avec $i \neq j$, et $a \in A$, on pose

$$T_{i,j}^{(\ell)}(a) = I_\ell + aE_{ij} \in \mathrm{M}_\ell(A).$$

Autrement dit, $T_{i,j}^{(\ell)}(a)$ est la matrice

$$\begin{array}{c} \\ i \longrightarrow \end{array} \begin{array}{c} \begin{array}{c} \\ j \\ \downarrow \end{array} \\ \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & \ddots & a & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \end{array} \in \mathrm{M}_\ell(A).$$

Cette matrice est inversible, d'inverse

$$\left(T_{i,j}^{(\ell)}(a)\right)^{-1} = T_{i,j}^{(\ell)}(-a).$$

Si $C \in \mathrm{M}_{m\times n}(A)$, l'opération

$$C \longmapsto T_{i,j}^{(m)}(a)C$$

revient à faire l'opération

$$L_i \longleftarrow L_i + aL_j,$$

où $L_1, \ldots, L_m$ sont les lignes de C, tandis que l'opération

$$C \longmapsto CT_{i,j}^{(n)}(a)$$

revient à faire l'opération

$$C_j \longleftarrow C_j + aC_i,$$

où $C_1, \ldots, C_n$ sont les colonnes de C. Une matrice de ce type est appelée une *matrice de transvection*.

On peut alors démontrer le lemme suivant.

Lemme 4.5. *Soit $C \in \mathrm{M}_{m\times n}(\mathbb{Z})$. Alors, il existe $U \in \mathrm{GL}_m(\mathbb{Z})$ et $V \in \mathrm{GL}_n(\mathbb{Z})$, et des entiers $\delta_1, \ldots, \delta_r \in \mathbb{Z} \setminus \{0\}$ tels que*

$$UCV = \begin{pmatrix} \delta_1 & & & & & \\ & \ddots & & & & \\ & & \delta_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

Démonstration. On va en fait démontrer que l'on peut arriver à la forme voulue en utilisant des opérations sur les lignes et les colonnes des deux types précédents. On peut toujours supposer que C est non nulle, sinon on a fini.

Il suffit d'appliquer l'algorithme suivant.

Algorithme.

(1) Puisque $C = (a_{ij})$ est non nulle, il existe un élément $a_{i_0j_0}$ non nul, que l'on ramène en position $(1,1)$ en multipliant C à gauche et à droite par des matrices de transposition convenables. En pratique, on essaye de prendre $a_{i_0j_0}$ tel que $|a_{i_0j_0}|$ soit minimale.

(2) On note encore par C la matrice obtenue, et on regarde l'ensemble des éléments de la première ligne et de la première colonne de C. Si tous ces éléments sont divisibles par a_{11}, on passe à l'étape (3).

Sinon, on repère un élément b non divisible par a_{11}. On effectue la division euclidienne de b par a_{11} : $b = qa_{11} + b_1$. Une opération appropriée sur les colonnes ou sur les lignes remplace b par b_1. En effectuant les divisions successives de l'algorithme d'Euclide, on finit par remplacer b par un pgcd d de a_{11} et de b. Remarquons que par construction, d est un diviseur strict de a_{11}. On ramène ensuite d en position $(1,1)$. Cela nous donne un élément un nouvel élément que l'on note $a_{11}^{(1)}$.

Si tous les éléments de la première ligne et de la première colonne sont divisibles par $a_{11}^{(1)}$, on passe à l'étape (3). Sinon on recommence le procédé pour remplacer $a_{11}^{(1)}$ par un diviseur strict $a_{11}^{(2)}$. Le procédé s'arrête nécessairement, puisqu'un élément n'a qu'un nombre fini de diviseurs stricts à association près. On obtient ainsi nécessairement un coefficient ± 1 au bout d'un nombre fini d'étapes, qui a les propriétés voulues. On obtient une nouvelle matrice, notée encore C par abus, dont l'élément a en position $(1,1)$ divise tous les éléments de la première ligne et de la première colonne. Remarquons aussi que a est diviseur strict de a_{11} dans le cas où C n'était pas de la forme voulue au début de l'étape.

(3) On ramène C à une matrice de la forme

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & C' & \\ 0 & & & \end{pmatrix},$$

en faisant des opérations sur les lignes et les colonnes.

En appliquant récursivement l'algorithme aux sous-matrices obtenues, on obtient l'existence de deux matrices $U \in \mathrm{GL}_m(\mathbb{Z})$ et $V \in \mathrm{GL}_n(\mathbb{Z})$ telles que UCV est de la forme voulue. □

On peut maintenant construire une $\mathbb{Z}$-base de Γ.

Proposition 4.6. *Soit $\mathscr{G} = \{g'_1, \dots, g'_m\}$ une partie génératrice de G.*[7] *Pour tout $i \in [\![1, m]\!]$, et pour tout $j \in [\![1, n]\!]$, soit $a_{ij} \in \mathbb{Z}$ tel que $\omega_j(g'_i) = \zeta_e^{a_{ij}}$, où ζ_e*

7. On peut simplement prendre $\mathscr{G} = G$, par exemple.

est une racine primitive e-ième de l'unité. Enfin, soit $C = (a_{ij}) \in \mathrm{M}_{m\times n}(\mathbb{Z})$, *et soient* $U \in \mathrm{GL}_m(\mathbb{Z}), V \in \mathrm{GL}_n(\mathbb{Z}), \delta_1, \dots, \delta_r \in \mathbb{Z} \setminus \{0\}$ *tels que*

$$UCV = \begin{pmatrix} \delta_1 & & & & & \\ & \ddots & & & & \\ & & \delta_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix},$$

et posons $e_k = \dfrac{e}{\mathrm{pgcd}(\delta_k, e)}$ *pour tout* $k \in [\![1, r]\!]$. *Soient* $C_1, \dots, C_n$ *les colonnes de* V. *Alors, les vecteurs*

$$\boldsymbol{\gamma}^{(1)} = e_1 C_1, \dots, \boldsymbol{\gamma}^{(r)} = e_r C_r, \boldsymbol{\gamma}^{(r+1)} = C_{r+1}, \dots, \boldsymbol{\gamma}^{(n)} = C_n$$

forment une $\mathbb{Z}$*-base de* Γ.

Démonstration. Rappelons que

$$\Gamma = \{\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \in \mathbb{Z}^n \mid \omega_1(g)^{\gamma_1} \cdots \omega_n(g)^{\gamma_n} = 1 \text{ pour tout } g \in G\}.$$

Puisque $\omega_1, \dots, \omega_n$ sont des morphismes de groupes et que $\mathscr{G}$ est une partie génératrice de G, il est facile de voir que

$$\Gamma = \{\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \in \mathbb{Z}^n \mid \omega_1(g_i')^{\gamma_1} \cdots \omega_n(g_i')^{\gamma_n} = 1 \text{ pour tout } i \in [\![1, m]\!]\}.$$

Comme ζ_e est d'ordre e, et en gardant les notations de l'énoncé, on a ainsi

$$\Gamma = \{\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \in \mathbb{Z}^n \mid \sum_{j=1} a_{ij}\gamma_j \equiv 0 \ [e] \text{ pour tout } i \in [\![1, m]\!]\},$$

ce qui se récrit

$$\Gamma = \{\boldsymbol{\gamma} \in \mathbb{Z}^n \mid C\,\boldsymbol{\gamma} \equiv 0 \ [e]\}.$$

Si $\boldsymbol{\gamma} \in \mathbb{Z}^n$, on pose $\boldsymbol{\gamma}' = V^{-1}\gamma$. On a alors

$$C\,\boldsymbol{\gamma} \equiv 0 \ [e] \iff UC\,\boldsymbol{\gamma} \equiv 0 \ [e] \iff UCV\,\boldsymbol{\gamma}' \equiv 0 \ [e].$$

Si $\boldsymbol{\gamma}' = \begin{pmatrix} \gamma_1' \\ \vdots \\ \gamma_n' \end{pmatrix}$, cette dernière condition équivaut à

$$\delta_k \gamma_k' \equiv 0 \ [e] \text{ pour tout } k \in [\![1, r]\!].$$

Soit $\Delta_k = \operatorname{pgcd}(\delta_k, e)$. On peut alors écrire $\delta_k = \Delta_k u_k$ et $e = \Delta_k e_k$, où u_k et e_k sont premiers entre eux. En particulier, u_k est inversible modulo e_k. On a alors

$$\delta_k \gamma'_k \equiv 0\ [e] \iff u_k \gamma'_k \equiv 0\ [e_k] \iff \gamma'_k \equiv 0\ [e_k],$$

la dernière équivalence découlant du fait que u_k est inversible modulo e_k.

Par conséquent, on obtient

$$\delta_k \gamma'_k \equiv 0\ [e] \text{ pour tout } k \in [\![1, r]\!] \iff \boldsymbol{\gamma}' = \begin{pmatrix} c_1 e_1 \\ \vdots \\ c_r e_r \\ c_{r+1} \\ \vdots \\ c_n \end{pmatrix}, c_1, \ldots, c_n \in \mathbb{Z}.$$

Cette dernière condition se réinterprète en disant que $\boldsymbol{\gamma}'$ est une combinaison $\mathbb{Z}$-linéaire de $e_1\varepsilon_1, \ldots, e_r\varepsilon_r, \varepsilon_{r+1}, \ldots, \varepsilon_n$. Il est aisé de voir que ces n vecteurs sont $\mathbb{Z}$-linéairement indépendants (ils sont sont déjà sur $\mathbb{Q}$!).

Par conséquent, $\boldsymbol{\gamma} \in \Gamma$ si, et seulement si, $\boldsymbol{\gamma}' = V^{-1}\boldsymbol{\gamma}$ s'écrit de manière unique comme combinaison $\mathbb{Z}$-linéaire de $e_1\varepsilon_1, \ldots, e_r\varepsilon_r, \varepsilon_{r+1}, \ldots, \varepsilon_n$. Comme $V \in \mathrm{GL}_n(\mathbb{Z})$, on en déduit que $\boldsymbol{\gamma} \in \Gamma$ si, et seulement si, $\boldsymbol{\gamma}$ s'écrit de manière unique comme combinaison $\mathbb{Z}$-linéaire de $e_1 V\varepsilon_1, \ldots, e_r V\varepsilon_r, V\varepsilon_{r+1}, \ldots, V\varepsilon_n$, ce qu'il fallait démontrer. □

Nous allons maintenant donner un algorithme qui, à partir d'un morphisme $\rho : G \longrightarrow \mathrm{GL}_n(F)$, permet de calculer des fractions rationnelles $f_1, \ldots, f_n$ algébriquement indépendantes sur F telles que $F(X_1, \ldots, X_n)^G = F(f_1, \ldots, f_n)$.

Algorithme.

Étape 1. On calcule tout d'abord une matrice $R \in \mathrm{GL}_n(F)$ vérifiant

$$R^{-1}\rho(g)R = \begin{pmatrix} \omega_1(g) & & \\ & \ddots & \\ & & \omega_n(g) \end{pmatrix} \text{ pour tout } g \in G,$$

où $\omega_1, \ldots, \omega_n : G \longrightarrow \mu_e(\overline{F})$ sont des morphismes de groupes (pas nécessairement distincts).

Pour cela, on peut procéder comme suit.

(i) On calcule tous les morphismes de groupes $G \longrightarrow \mu_e(\overline{F})$. Si $G = \langle g_1 \rangle \odot \cdots \odot \langle g_r \rangle$, avec $o(g_i) = d_i$, ce sont les morphismes $\omega_{z_1,\ldots,z_r}$, avec $z_i \in \mu_{d_i}(\overline{F})$, définis par

$$\omega_{z_1,\ldots,z_r}(g_1^{m_1} \cdots g_r^{m_r}) = z_1^{m_1} \cdots z_r^{m_r}.$$

(ii) Pour chaque morphisme $\omega : G \longrightarrow \mu_e(\overline{F})$, on calcule la matrice

$$P_\omega = \frac{1}{|G|} \sum_{g \in G} \omega(g)^{-1} \rho(g),$$

et on extrait un système de colonnes de P_ω linéairement indépendantes. On recolle le tout pour obtenir une matrice inversible $R \in \mathrm{GL}_n(F)$, qui vérifie alors les propriétés souhaitées.

Étape 2. On pose

$$\Gamma = \{\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_n \end{pmatrix} \in \mathbb{Z}^n \mid \omega_1(g)^{\gamma_1} \cdots \omega_n(g)^{\gamma_n} = 1 \text{ pour tout } g \in G\},$$

où les ω_i sont les morphismes définis dans l'étape 1, et on calcule une $\mathbb{Z}$-base $\boldsymbol{\gamma}^{(1)}, \ldots, \boldsymbol{\gamma}^{(n)}$ de Γ.

Pour ce faire, on peut effectuer les étapes suivantes.

(i) On choisit une partie génératrice $\mathscr{G} = \{g'_1, \ldots, g'_m\}$ de G (par exemple, on peut prendre les générateurs utilisés dans l'étape 1 (i), ou prendre G lui-même).

Pour tout $i \in [\![1, m]\!]$, et pour tout $j \in [\![1, n]\!]$, soit $a_{ij} \in \mathbb{Z}$ tel que $\omega_j(g'_i) = \zeta_e^{a_{ij}}$, où ζ_e est une racine primitive e-ième de l'unité, et on définit $C = (a_{ij}) \in \mathrm{M}_{m\times n}(\mathbb{Z})$.

(ii) En utilisant des opérations sur les lignes et les colonnes de C, on calcule $U \in \mathrm{GL}_m(\mathbb{Z}), V \in \mathrm{GL}_n(\mathbb{Z}), \delta_1, \ldots, \delta_r \in \mathbb{Z} \setminus \{0\}$ tels que

$$UCV = \begin{pmatrix} \delta_1 & & & & & \\ & \ddots & & & & \\ & & \delta_r & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

Notons que l'on n'a pas besoin de calculer U ; seule la matrice V est importante. Celle-ci se calcule en faisant le produit de matrices de transvection et de permutation correspondant aux opérations sur les colonnes. On a donc intérêt à faire au maximum des opérations sur les lignes.

Posons $e_k = \dfrac{e}{\mathrm{pgcd}(\delta_k, e)}$ pour tout $k \in [\![1, r]\!]$. Si $C_1, \ldots, C_n$ sont les colonnes de V, alors les vecteurs

$$\boldsymbol{\gamma}^{(1)} = e_1 C_1, \ldots, \boldsymbol{\gamma}^{(r)} = e_r C_r, \boldsymbol{\gamma}^{(r+1)} = C_{r+1}, \ldots, \boldsymbol{\gamma}^{(n)} = C_n$$

forment une $\mathbb{Z}$-base de Γ.

Étape 3. On achève le calcul de $f_1, \ldots, f_n$.

(i) On considère la matrice R obtenue dans l'étape 1, et on calcule $R^{-1} = (a'_{ij})$.

(ii) Soit $(\boldsymbol{\gamma}^{(1)}, \ldots, \boldsymbol{\gamma}^{(n)})$ une $\mathbb{Z}$-base de Γ, et posons

$$U_j = \sum_k a'_{jk} X_k \quad \text{pour tout } j \in [\![1, n]\!].$$

Alors, les fractions rationnelles $f_j = U^{\gamma^{(j)}},\ j \in [\![1,n]\!]$, sont algébriquement indépendantes sur F, et $F(X_1,\dots,X_n)^G = F(f_1,\dots,f_n)$.

Exemple 4.7. Reprenons le cas du groupe de Klein $G = \{\mathrm{Id}, s, t, st\} \subset \mathfrak{S}_4$, où $s = (1\ 2)(3\ 4)$ et $t = (1\ 3)(2\ 4)$, agissant sur $F[X_1,\dots,X_4]$ par

$$\sigma\cdot P = P(X_{\sigma(1)},\dots,X_{\sigma(4)}).$$

D'après l'exemple 2.10 (1), cette action est celle induite par la représentation $\rho : G \longrightarrow \mathrm{M}_4(F)$ définie par

$$\rho(\sigma) = M_\sigma \quad \text{pour tout } \sigma \in G.$$

On a donc

$$\rho(s) = M_s = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},\ \rho(t) = M_t = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},\ \rho(st) = M_{st} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Comme $G = \langle s\rangle \odot \langle t\rangle$, et G est d'exposant 2, les morphismes $G \longrightarrow \mu_2(\overline{F})$ sont les quatre morphismes $\omega_1,\dots,\omega_4$ caractérisés par

$$\begin{array}{llll} \omega_1(s) = 1 & \omega_2(s) = 1 & \omega_3(s) = -1 & \omega_4(s) = -1 \\ \omega_1(t) = 1 & \omega_2(t) = -1 & \omega_3(t) = 1 & \omega_4(t) = -1. \end{array}$$

On a donc

$$P_{\omega_1} = \frac{1}{4}(I_4 + Ms + M_t + M_{st}) = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

$$P_{\omega_2} = \frac{1}{4}(I_4 - M_s + M_t - M_{st}) = \frac{1}{4}\begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix}$$

$$P_{\omega_3} = \frac{1}{4}(I_4 + M_s - M_t - M_{st}) = \frac{1}{4}\begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$$

$$P_{\omega_4} = \frac{1}{4}(I_4 - M_s - M_t + M_{st}) = \frac{1}{4}\begin{pmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

On peut donc prendre

$$R = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Puisque $R^{-1} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$, on a donc

$$U_1 = X_1 + X_2 + X_3 + X_4,\ U_2 = X_1 - X_2 + X_3 - X_4,$$
$$U_3 = X_1 + X_2 - X_3 - X_4,\ U_4 = X_1 - X_2 - X_3 - X_4.$$

Ce calcul explique donc le choix des U_i dans l'exemple 2.2.

En regardant l'action de G sur les U_i, on constate que

$$\sigma \cdot U_i = \omega_i(\sigma)^{-1} U_i \ \text{ pour tout } \sigma \in G,$$

où les ω_i sont définis plus haut.

On a donc

$$\Gamma = \{\boldsymbol{\gamma} \in \mathbb{Z}^4 \mid \omega_1(\sigma)^{\gamma_1} \cdots \omega_4(\sigma)^{\gamma_4} = 1 \ \text{ pour tout } \sigma \in G\}.$$

Or, s et t sont des générateurs de G, et on a

$$\begin{aligned} \omega_1(s)^{\gamma_1} \cdots \omega_4(s)^{\gamma_4} &= (-1)^{\gamma_2+\gamma_4} \\ \omega_1(t)^{\gamma_1} \cdots \omega_4(t)^{\gamma_4} &= (-1)^{\gamma_3+\gamma_4}. \end{aligned}$$

On en déduit facilement que $\boldsymbol{\gamma} \in \Gamma$ si, et seulement si, $\boldsymbol{\gamma}$ est de la forme

$$\boldsymbol{\gamma} = \begin{pmatrix} \gamma_1 \\ \gamma_4 + 2k \\ \gamma_4 + 2\ell \\ \gamma_4 \end{pmatrix},\ k, \ell, \gamma_1, \gamma_4 \in \mathbb{Z}.$$

La famille de vecteurs

$$\boldsymbol{\gamma}^{(1)} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ \boldsymbol{\gamma}^{(2)} = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 0 \end{pmatrix},\ \boldsymbol{\gamma}^{(3)} = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \end{pmatrix},\ \boldsymbol{\gamma}^{(4)} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

est une famille $\mathbb{Z}$-génératrice de Γ. Il est facile de voir qu'elle est aussi $\mathbb{Z}$-libre. C'est donc une $\mathbb{Z}$-base de Γ.

Finalement, on obtient que les fractions rationnelles $U_1, U_2^2, U_3^2, U_2U_3U_4$ sont algébriquement indépendantes, et que

$$F(X_1, X_2, X_3, X_4)^G = F(U_1, U_2^2, U_3^2, U_2U_3U_4),$$

comme annoncé précédemment.

Pour finir, nous allons maintenant donner un exemple où l'on met en œuvre la méthode proposée pour calculer une base de Γ.

Exemple 4.8. Soit F un corps vérifiant $\mathrm{car}(F) \neq 3$ et contenant une racine 9-ième de l'unité, que l'on notera ζ_9. On pose

$$s = \begin{pmatrix} \zeta_9^3 & 0 \\ 0 & \zeta_9^3 \end{pmatrix},\ t = \begin{pmatrix} \zeta_9^5 & 0 \\ 0 & \zeta_9^3 \end{pmatrix}.$$

Soit $G = \langle s, t \rangle$. On vérifie que s est d'ordre 3, t est d'ordre 9 et que $G = \langle s \rangle \odot \langle t \rangle$, si bien que $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. En particulier, G est d'exposant 9.

Enfin, on considère $\rho : G \longrightarrow \mathrm{GL}_2(F)$ le morphisme d'inclusion, ainsi que l'action de G associée sur $F(X_1, X_2)$.

Soient $\omega_1, \omega_2 : G \longrightarrow \mu_9(\overline{F})$ les morphismes définis de manière unique par

$$\begin{array}{ll} \omega_1(s) = \zeta_9^3 & \omega_2(s) = \zeta_9^3 \\ \omega_1(t) = \zeta_9^5 & \omega_2(t) = \zeta_9^3. \end{array}$$

Par définition de l'action associée à ρ, on a

$$g{\cdot}X_i = \omega_i(g)^{-1} X_i.$$

Posons $C = \begin{pmatrix} 3 & 3 \\ 5 & 3 \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$. Nous allons maintenant utiliser des opérations élémentaires sur les lignes et les colonnes pour transformer C en une matrice diagonale. Nous calculerons la matrice V correspondant aux opérations sur les colonnes de proche en proche, en initialisant à $V = I_2$, puis en multipliant à droite par la matrice correspondant à chaque opération élémentaire successive.

Si $M_1, M_2 \in \mathrm{M}_2(\mathbb{Z})$, on notera $M_1 \sim M_2$ lorsque l'on peut passer de M_1 à M_2 par une succession d'opérations élémentaires.

On commence par effectuer l'opération $L_2 \longleftarrow L_2 - L_1$. On a donc

$$C \sim \begin{pmatrix} 3 & 3 \\ 2 & 0 \end{pmatrix}.$$

On échange ensuite les colonnes, si bien que

$$C \sim \begin{pmatrix} 3 & 3 \\ 0 & 2 \end{pmatrix},$$

et on fait $V \longleftarrow V \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Enfin, on effectue $C_2 \longleftarrow C_2 - 3C_1$. Ainsi,

$$C \sim \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix},$$

et on fait $V \longleftarrow V \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

Finalement, on a

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

Avec les notations de l'algorithme, on a donc

$$e_1 = \frac{9}{\mathrm{pgcd}(3, e)} = 3, \ e_2 = \frac{9}{\mathrm{pgcd}(2, e)} = 9,$$

et les vecteurs

$$\boldsymbol{\gamma}^{(1)} = 3 \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \ \boldsymbol{\gamma}^{(2)} = 9 \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 9 \\ -9 \end{pmatrix}$$

forment une $\mathbb{Z}$-base de Γ. Ainsi, X_2^3 et $X_1^9 X_2^{-9}$ sont algébriquement indépendantes sur F, et on a

$$F(X_1, X_2) = F(X_2^3, X_1^9 X_2^{-9}).$$