TD5 : Modules sur un anneau principal ; Discriminant

Diego Izquierdo

Les exercices 8, 14, 18 et 22 ont été traités pendant la séance.

Exercice 1 (révision) : Facteurs invariants
Trouver les facteurs invariants du $\mathbb{Z}$-module :

$$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}.$$

Exercice 2 (révision) : Examen 2012

1. Soient $n \geq 1$ un entier et u_1, ..., u_n des éléments de $\mathbb{Z}^n$ linéairement indépendants dans l'espace vectoriel $\mathbb{Q}^n$. Soit M le sous-groupe de $\mathbb{Z}^n$ engendré par $u_1, ..., u_n$. Montrer que l'indice de M dans $\mathbb{Z}^n$ est égal à la valeur absolue du déterminant des vecteurs $u_1, ..., u_n$ dans la base canonique.
2. Soit M sous-groupe de $\mathbb{Z}^3$ engendré par $u_1 = (2, 1, 1)$, $u_2 = (1, 2, 1)$ et $u_3 = (1, 1, 2)$. Calculer $\mathbb{Z}^3/M$.
3. Plus généralement, soit $(u_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n}$ la matrice telle que $u_{i,j} = 2$ si $i = j$ et $u_{i,j} = 1$ sinon, et notons u_1, ..., u_n les vecteurs colonne de cette matrice. Soit M le sous-groupe de $\mathbb{Z}^n$ engendré par $u_1, ..., u_n$. Calculer $\mathbb{Z}^n/M$.

Exercice 3 (révision) : Bases adaptées

1. Donner une base adaptée pour le sous-$\mathbb{Z}$-module M de $\mathbb{Z}^4$ engendré par $(2, -1, 0, 0)$, $(-1, 2, -1, -1)$, $(0, -1, 2, 0)$ et $(0, -1, 0, 2)$. Calculer le quotient $\mathbb{Z}^4/M$.
2. Même question pour le sous-$\mathbb{Z}$-module M de $\mathbb{Z}^3$ engendré par $(4, 8, 16)$, $(1, 5, 10)$, $(6, 2, 4)$ et $(5, 8, 6)$.
3. Même question pour le sous-module de $\mathbb{Z}^3$ défini par $5x+7y+35z = 0$.
4. Même question pour le sous-module de $\mathbb{Z}^3$ défini par $x + 2y + 3z \equiv 0 \mod 4$.
5. Même question pour le sous-$\mathbb{C}[[X]]$-module de $\mathbb{C}[[X]]^2$ engendré par $((1 - X)^{-1}, (1 - X^2)^{-1})$ et $((1 + X)^{-1}, (1 + X^2)^{-1})$.
6. Exhiber deux sous-$\mathbb{Z}$-modules M et N de $\mathbb{Z}^2$ de rang 2 tels qu'il n'existe pas une base (e_1, e_2) de $\mathbb{Z}^2$ pour laquelle on peut trouver des entiers a, b, c, d tels que (ae_1, be_2) est une base de M et (ce_1, de_2) est une base de N.

Exercice 4 : $\mathbb{Z}[i]$-modules finis

1. Combien existe-t'il de $\mathbb{Z}[i]$-modules de cardinal 3 à isomorphisme près ? de cardinal 5 ? de cardinal 9 ?

> **Indications :** L'anneau $\mathbb{Z}[i]$ est principal. Donc un $\mathbb{Z}[i]$-module fini M s'écrit sous la forme :
>
> $$M \cong \bigoplus_{r=1}^{n} \mathbb{Z}[i]/(z_r)$$
>
> où $z_r \in \mathbb{Z}[i]$ pour chaque r et $z_1|z_2|...|z_n$. En utilisant la question 1 de l'exercice 2, on voit immédiatement que $|M| = |z_1...z_r|^2$. Il n'existe donc aucun $\mathbb{Z}[i]$-module de cardinal 3, il existe deux $\mathbb{Z}[i]$-modules de cardinal 5 (à savoir $\mathbb{Z}[i]/(2+i)$ et $\mathbb{Z}[i]/(2-i)$) et un $\mathbb{Z}[i]$-module de cardinal 9 (à savoir $\mathbb{Z}[i]/(3)$).

2. *(plus difficile)* Combien existe-t'il de $\mathbb{Z}[i]$-modules de cardinal $5^3 \cdot 6^4$ à isomorphisme près ?

> **Indications :** Un $\mathbb{Z}[i]$-module fini M s'écrit sous la forme :
>
> $$M \cong \bigoplus_{r=1}^{n} \bigoplus_{s=1}^{m} (\mathbb{Z}[i]/(z_r^s))^{a_{r,s}},$$
>
> où $z_1, ..., z_n$ sont des irréductibles deux à deux non associés et $a_{r,s} \geq 0$. On a $|M| = \prod_r |z_r|^{2sa_{r,s}}$. A unité près, la liste des irréductibles dans $\mathbb{Z}[i]$ est la suivante :
> - il y a un irréductible π_2 de norme $|\pi_2|^2 = 2$;
> - pour chaque premier $p \equiv 1 \mod 4$, il y a deux irréductibles π_p et π'_p de norme p ;
> - pour chaque premier $p \equiv 3 \mod 4$, il y a irréductible π_p de norme p^2.
>
> Il n'y a pas d'autres irréductibles. Comme $5^3 \cdot 6^4 = 2^4 \times 3^4 \times 5^3$, en comptant, on voit alors que la réponse est $5 \times 2 \times (4+4+2) = 100$.

Exercice 5 (à préparer) : Retour sur le théorème des deux carrés

Soit p un nombre premier congru à 1 modulo 4. Montrer qu'il est possible de munir $\mathbb{Z}/p\mathbb{Z}$ d'une structure de $\mathbb{Z}[i]$-module. En déduire qu'il deux entiers a et b tels que $p = a^2 + b^2$.

Exercice 6 : Une caractérisation des anneaux principaux

Soit A un anneau commutatif unitaire intègre et noethérien. Montrer que A est principal si, et seulement si, tout module de type fini sans torsion sur A est libre.

Indications : Le sens direct découle du théorème de classification des modules de type fini sur un anneau principal. Supposons que tout module de type fini sans torsion sur A est libre. Soit I un idéal non nul de A. Comme A est noethérien, il existe $a_1, ..., a_n \in A$ tels que $I = (a_1, ..., a_r)$. On en déduit que I est un A-module de type fini. Il est sans torsion car A est intègre. Donc il est libre par hypothèse. S'il était de rang au moins 2, il existerait $x, y \in I$ deux éléments A-libres : mais $yx - xy = 0$ est une relation de liaison entre ces deux éléments, absurde ! Donc I est de rang 1, ce qui signifie qu'il est principal.

Exercice 7 : Matrices à coefficients dans des anneaux euclidiens

Soit A un anneau euclidien. Soit $M \in \mathcal{M}_{m,n}(A)$.

1. Montrer qu'il existe $P \in \mathcal{M}_m(A)$ et $Q \in \mathcal{M}_n(A)$ produits de matrices élémentaires telles que PMQ est de la forme :

$$\begin{pmatrix} d_1 & 0 & 0 & ... & 0 & ... & 0 \\ 0 & d_2 & 0 & ... & 0 & ... & 0 \\ 0 & 0 & d_3 & ... & 0 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & ... & \vdots \\ 0 & 0 & 0 & ... & d_r & ... & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & ... & \vdots \\ 0 & 0 & 0 & ... & 0 & ... & 0 \end{pmatrix}$$

où $d_1, ..., d_r$ sont des éléments de A tels que $d_1|d_2|d_3|...|d_r$.

2. Montrer que, si $M \in GL_n(A)$, alors il existe $P \in \mathcal{M}_n(A)$ produit de matrices élémentaires telle que :

$$PM = \begin{pmatrix} 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 1 & 0 \\ 0 & 0 & ... & 0 & \det(M) \end{pmatrix}.$$

En déduire que le sous-groupe de $GL_n(A)$ engendré par les matrices élémentaires est $SL_n(A)$.

Exercice 8 (à préparer) : Partiel 2014

Soit A un groupe abélien. Pour $n \in \mathbb{N}^*$, on note $S(A, n)$ l'ensemble des sous-groupes de A d'indice n.

1. Soit $X \in S(A, n)$. Montrer que $nA \subseteq X$.

2. Montrer qu'il existe une bijection entre $S(A, n)$ et $S(A/nA, n)$.

3. Soient $m \in \mathbb{N}^*$ et $N \in \mathbb{N}^*$. Montrer que, si $m \wedge n = 1$, alors il existe une bijection entre $S((\mathbb{Z}/mn\mathbb{Z})^N, mn)$ et $S((\mathbb{Z}/m\mathbb{Z})^N, m) \times S((\mathbb{Z}/n\mathbb{Z})^N, n)$.

4. Montrer que $S(\mathbb{Z}^2, 2)$ possède 3 éléments, que l'on explicitera.

5. Faire la liste des éléments de $S(\mathbb{Z}^2, n)$. Pour ce faire, on pourra faire la liste des $X \in S(\mathbb{Z}^2, n)$ tels que $X \cap (\mathbb{Z} \oplus 0) = a\mathbb{Z} \oplus 0 \subseteq \mathbb{Z}^2$ pour chaque diviseur positif a de n. En déduire que $|S(\mathbb{Z}^2, n)| = \sum_{a|n} a$, puis expliciter les séries génératrices $\sum_{r\geq 0} |S(\mathbb{Z}^2, p^r)|T^r$ et $\sum_{n\geq 1} |S(\mathbb{Z}^2, n)|n^{-s}$.

6. Faire la liste des éléments de $S(\mathbb{Z}^3, n)$. En déduire que $|S(\mathbb{Z}^3, n)| = \sum_{ab|n} a^2 b$, puis expliciter les séries génératrices $\sum_{r\geq 0} |S(\mathbb{Z}^3, p^r)|T^r$ et $\sum_{n\geq 1} |S(\mathbb{Z}^3, n)|n^{-s}$.

Exercice 9 : Arbre de Bruhat-Tits

Soit p un nombre premier. On note V_0 le $\mathbb{Z}$-module $\mathbb{Z}^2 = \mathbb{Z} \oplus \mathbb{Z}$. Soit $\mathcal{V}_1$ l'ensemble des sous-$\mathbb{Z}$-modules d'indice p dans V_0.

1. Montrer que $\mathcal{V}_1$ a exactement $p + 1$ éléments.

> **Indications :** Cela découle de la question 5 de l'exercice 8.

Soient V_1 un élément de $\mathcal{V}_1$ et $\mathcal{V}_2$ l'ensemble de ses sous-modules d'indice p.

2. Montrer que $\mathcal{V}_2$ a exactement $p+1$ éléments et qu'il contient un unique sous-module homothétique à V_0.

> **Indications :** On remarque que V_1 est un sous-module de $\mathbb{Z}^2$. On en déduit qu'il est de type fini (car $\mathbb{Z}$ est noethérien) et sans torsion. Il existe donc $n \geq 0$ tel que $V_1 \cong \mathbb{Z}^n$. Comme V_1 est d'indice fini dans $\mathbb{Z}^2$, il est de rang 2. Donc $V_1 \cong \mathbb{Z}^2$ et, d'après la question 1., $\mathcal{V}_2$ a $p + 1$ éléments. Soit $V_2 \in \mathcal{V}_2$ homothétique à V_0. Soit $m \in \mathbb{N}$ tel que $V_2 = mV_0$. Alors on a $[V_0 : V_2] = m^2 = [V_0 : V_1][V_1 : V_2] = p^2$. Donc $V_2 = pV_0$, et $\mathcal{V}_2$ contient bien un unique sous-module homothétique à V_0.

On munit l'ensemble (de sommets)

$$\mathcal{T}_p = \{\text{sous-}\mathbb{Z}\text{-modules de } \mathbb{Z}^2 \text{ d'indice une puissance de } p\}/(\text{homothétie})$$

de la structure de graphe suivante : une arête relie v à v' s'il existe des représentants V et V' de v et v' respectivement tels que V est un sous-module d'indice p de V'.

3. Montrer que l'on a une arête $v \to v'$ si et seulement si il existe une arête $v' \to v$.

> **Indications :** Considérons $v \to v'$ une arête. Soient V et V' des représentants de v et v' tels que V est un sous-module d'indice p de V'. On remarque alors que $pV' \subseteq V$ et $[V : pV'] = \frac{[V':pV']}{[V':V]} = p$. Donc $v' \to v$ est une arête.

Les questions suivantes établissent alors que la structure de graphe conférée à $\mathcal{T}_p$ est en fait un arbre non orienté. Soient v et v' deux sommets de $\mathcal{T}_p$.

4. Montrer qu'il existe des représentants $V_{(0)}$ et $V_{(n)}$ de v et v' respectivement ainsi que des $V_{(i)}$ pour $1 \leq i \leq n-1$ vérifiant $V_{(0)} \supseteq V_{(1)} \supseteq \cdots \supseteq V_{(n)}$ et tels que $V_{(i+1)}$ est d'indice p dans $V_{(i)}$ pour tout i.

Indications : Soient $V_{(0)}$ et W des représentants de v et v'. Soit $m \geq 0$ tel que $V_{(0)}$ est d'indice p^m dans V_0. Soit $V' = p^m W$. On remarque immédiatement que $V' \subseteq V_{(0)}$. Si $V' = V_{(0)}$, il n'y a rien à démontrer. Supposons donc que $V_{(0)} \neq V'$. D'après le théorème de classification des groupes abéliens finis, $V_{(0)}/V'$ s'écrit sous la forme :

$$V_{(0)}/V' \cong \bigoplus_{i=1}^{k} \mathbb{Z}/p^{r_i}\mathbb{Z}.$$

Ce groupe contient bien un sous-groupe d'indice p. Donc $V_{(0)}$ contient un sous-module $V_{(1)}$ d'indice p contenant V'. De même, on montre que, si $V_{(1)} \neq V'$, alors $V_{(1)}$ contient un sous-module $V_{(2)}$ d'indice p contenant V'. Et on continue ainsi : en procédant par récurrence, on trouve donc des $V_{(i)}$ pour $1 \leq i \leq n$ vérifiant $V_{(0)} \supseteq V_{(1)} \supseteq \cdots \supseteq V_{(n)}$, $V_{(n)} = V'$ et tels que $V_{(i+1)}$ est d'indice p dans $V_{(i)}$ pour tout i.

Remarque : On peut aussi faire appel au théorème de la base adaptée : il montre qu'il existe une base (e_1, e_2) de $V_{(0)}$ et des entiers $a, b > 0$ tels que $V' = p^a\mathbb{Z}e_1 \oplus p^b\mathbb{Z}e_2$. On a alors :

$$V_{(0)} \supseteq p\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \supseteq p^2\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \supseteq ... \supseteq p^a\mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \supseteq p^a\mathbb{Z}e_1 \oplus p\mathbb{Z}e_2 \supseteq ... \supseteq V'.$$

Soient $v_0, v_1, \ldots, v_{n-1}, v_n = v_0$ des sommets où chaque v_i est relié à v_{i+1} par une arête.

5. Montrer que l'on a $n = 0$ ou bien ($n \geq 2$ et il existe $1 \leq i \leq n-1$ avec $v_{i+1} = v_{i-1}$).

Indications : Supposons $n > 0$. Pour v et w deux sommets, on note $d(v, w)$ la longueur du plus court chemin de v à w. Soit r entre 1 et n tel que $d(v_0, v_r) = \max_i d(v_0, v_i)$. Grâce au théorème de la base adaptée, il existe des représentants V_0 et V_r de v_0 et v_r ainsi qu'une base (e_1, e_2) de V_0 tels que $V_r = \mathbb{Z}e_1 \oplus p^a\mathbb{Z}e_2$ pour un certain $a > 0$. Grâce à la question précédente, on remarque que $d(v_0, v_r) = a$. Par ailleurs, les sommets reliés à V_r sont $\mathbb{Z}e_1 \oplus p^{a-1}\mathbb{Z}e_2$, et les $V_{k,a} = (e_1 + bp^a e_2)\mathbb{Z} \oplus p^{a+1}\mathbb{Z}e_2$ avec $b \in \{0, ..., p-1\}$. Or, si $v_{k,a}$ est le sommet correspondant à $V_{k,a}$, on a $d(v_0, v_{k,a}) = a+1$. Par conséquent, v_{r-1} et v_{r+1} sont représentés par $\mathbb{Z}e_1 \oplus p^{a-1}\mathbb{Z}e_2$: on a bien $v_{r-1} = v_{r+1}$.

Exercice 10 : Groupes abéliens finis

Soient A et B deux groupes abéliens finis tels que $|A[n]| = |B[n]|$ pour tout $n > 0$. Montrer que A et B sont isomorphes.

Indications : Pour chaque groupe abélien fini Z, on note $f_Z : n \mapsto |_nZ|$. On peut supposer que A et B sont de torsion p-primaire pour un certain nombre premier p.
Procédons par récurrence forte sur l'ordre de A. Si $|A| = 1$, le résultat est évident. Supposons maintenant que le lemme soit démontré lorsque l'ordre de A est au plus a pour un certain entier a. Soit A un groupe abélien fini d'ordre $a+1$. On écrit alors $A = \bigoplus_{i=1}^{r}(\mathbb{Z}/p^{\alpha_i}\mathbb{Z})^{m_i}$ et $B = \bigoplus_{i=1}^{r'}(\mathbb{Z}/p^{\alpha'_i}\mathbb{Z})^{m'_i}$, avec :

- $r, r', \in \mathbb{N}$,
- $m_1, ..., m_r, m'_1, ..., m'_{r'} \in \mathbb{N}^*$,
- $\alpha_1, ..., \alpha_r, \alpha'_1, ..., \alpha'_{r'} \in \mathbb{N}^*$,
- $\alpha_1 < ... < \alpha_r$ et $\alpha'_1 < ... < \alpha'_{r'}$.

On remarque que $f_A(n) = p^{\sum_{i=1}^{r} m_i \min\{v_p(n),\alpha_i\}}$ et $f_B(n) = p^{\sum_{i=1}^{r'} m'_i \min\{v_p(n),\alpha'_i\}}$.
Si $\alpha_1 < \alpha'_1$, alors :

$$\log_p f_A(p^{\alpha_1}) = (\sum_{i=1}^{r} m_i)\alpha_1 = (\sum_{i=1}^{r'} m'_i)\alpha_1 = \log_p f_B(p^{\alpha_1}),$$

$$\log_p f_A(p^{\alpha_1+1}) = m_1\alpha_1 + (\sum_{i=2}^{r} m_i)(\alpha_1+1) = (\sum_{i=1}^{r'} m'_i)(\alpha_1+1) = \log_p f_B(p^{\alpha_1+1}),$$

et donc $m_1 = 0$, ce qui est absurde. Par symétrie, on en déduit que $\alpha_1 = \alpha'_1$. Or, par hypothèse de récurrence, $(\mathbb{Z}/p^{\alpha_1}\mathbb{Z})^{m_1-1} \oplus \bigoplus_{i=2}^{r}(\mathbb{Z}/p^{\alpha_i}\mathbb{Z})^{m_i} \cong (\mathbb{Z}/p^{\alpha'_1}\mathbb{Z})^{m'_1-1} \oplus \bigoplus_{i=2}^{r'}(\mathbb{Z}/p^{\alpha'_i}\mathbb{Z})^{m'_i}$, donc $A \cong B$, ce qui achève la récurrence.

Exercice 11 (difficile) : Groupes abéliens de type cofini

0. *(Quesion préliminaire)* Soit M un groupe abélien. Soit N un sous-groupe de M. On suppose N divisible (ie tel que, pour tout entier $n > 0$, la multiplication par n sur N est surjective). Montrer que M est isomorphe à $N \oplus M/N$.

Soit A un groupe abélien de torsion tel que, pour tout entier naturel non nul n, le sous-groupe de n-torsion $A[n]$ est fini. On dit alors que A est de torsion de type cofini. Nous cherchons à comprendre la structure de A.

1. Fixons un nombre premier p et supposons que A est de torsion p-primaire.
   (a) Montrer que A possède un plus grand sous-groupe divisible A_{div} (au sens de l'inclusion).
   (b) Montrer qu'il existe $r \geq 0$ tel que $A_{div} \cong (\mathbb{Q}/\mathbb{Z})\{p\}^r$.
   (c) Soit $\overline{A} = A/A_{div}$. Montrer que $\overline{A}$ est fini.
   (d) En déduire qu'il existe des entiers naturels non nuls $n_1, ..., n_k$ tels que $A \cong (\mathbb{Q}/\mathbb{Z})\{p\}^r \oplus \bigoplus_{i=1}^{k} \mathbb{Z}/p^{n_i}\mathbb{Z}$.

2. Déduire de la question précédente la structure des groupes abéliens de torsion de type cofini.

Soit maintenant B un groupe abélien de type cofini, c'est-à-dire un groupe abélien tel que, pour tout entier naturel non nul n, les groupes $B[n]$ et B/n

sont finis. On note $h_n(B) = \frac{|B[n]|}{|B/n|}$ et on cherche maintenant à comprendre la fonction $n \mapsto h_n(B)$.

3. (a) Considérons $0 \to B \to C \to D \to 0$ une suite exacte de groupes abéliens. Montrer que, si deux parmi les trois groupes B, C, D sont de type cofini, alors le troisième l'est aussi et pour tout $n > 0$, on a :

$$h_n(C) = h_n(B)h_n(D).$$

(b) Soit $n > 0$ un entier. Considérons la décomposition de n en produit de facteurs premiers $n = p_1^{b_1}...p_s^{b_s}$. Montrer que $h_n(B) = \prod_{i=1}^{s} h_{p_i^{b_i}}(B)$.

4. (a) Soit A un groupe fini. Montrer que $h_n(A) = 1$ pour tout $n > 0$.

(b) Soit A un groupe de torsion de type cofini. Montrer que A est un groupe de type cofini et qu'il existe une famille d'entiers naturels $(r_p)_{p\in\mathbb{P}}$ (où $\mathbb{P}$ est l'ensemble des nombres premiers) telle que, pour tout entier $n > 0$, on a :

$$h_n(A) = \prod_{p\in\mathbb{P}} p^{r_p v_p(n)}.$$

Ici, $v_p(n)$ désigne la valuation p-adique de n.

5. Fixons un nombre premier ℓ. Montrer qu'il existe un groupe de torsion de type cofini A, un entier naturel m, un groupe abélien C, un groupe abélien D sur lequel la multiplication par ℓ est un automorphisme et des suites exactes :

$$0 \to A \to B \to C \to 0$$
$$0 \to \mathbb{Z}^m \to C \to D \to 0.$$

6. En déduire qu'il existe une famille d'entiers relatifs $(r_p)_{p\in\mathbb{P}}$ (où $\mathbb{P}$ est l'ensemble des nombres premiers) telle que, pour tout entier $n > 0$:

$$h_n(B) = \prod_{p\in\mathbb{P}} p^{r_p v_p(n)}.$$

Exercice 12 : Polynôme caractéristique et similitude

Soient K un corps, $n \geq 1$ un entier et $P \in K[X]$ un polynôme unitaire de degré n. On note p la fonction partition, qui à un entier $i \geq 1$ associe le nombre de façons distinctes de représenter i comme somme d'entiers.

1. Exprimer, en fonction de la décomposition en facteurs irréductibles de P, le nombre de classes de similitude de matrices de $\mathcal{M}_n(K)$ ayant P pour polynôme caractéristique.

Indications : Pour chaque entier naturel r, soit $\mathcal{P}(r)$ l'ensemble des partitions de i. On écrit la décomposition en facteurs irréductibles de P : $P = P_1^{r_1}...P_s^{r_s}$. L'ensemble des classes de similitude de matrices de $\mathcal{M}_n(K)$ ayant P pour polynôme caractéristique est en bijection avec l'ensemble E constitué des familles de polynômes unitaires $(Q_1, ..., Q_t)$ de degré non nul telles que $Q_1|Q_2|...|Q_t$ et $Q_1...Q_t = P$. La fonction

$$E \to \prod_{i=1}^{s} \mathcal{P}(r_i)$$
$$(Q_1, ..., Q_t) \mapsto (\{v_{P_i}(Q_{j+1}/Q_j) | 1 \leq j \leq t-1\})_{1 \leq i \leq s}$$

est une bijection. Donc le nombre recherché est $p(r_1)...p(r_s)$.

2. Expliciter le résultat pour $P = X^2(X-1)^3(X+1)$.

Indications : Si K n'est pas de caractéristique 2, le nombre recherché est $2 \times 3 \times 1 = 6$. Si K est de caractéristique 2, le nombre recherché est $2 \times 5 = 10$.

3. Combien y a-t'il de classes de similitude dans $\mathcal{M}_3(\mathbb{Z}/2\mathbb{Z})$?

Indications : Sur $\mathbb{Z}/2\mathbb{Z}$, il y a :
- deux polynômes de degré 3 de la forme P^3 avec P irréductible ;
- deux polynômes de degré 3 de la forme P^2Q avec P est Q irréductibles ;
- deux polynômes de degré 3 de la forme P_1P_2 avec P_1 et P_2 irréductibles, P_1 de degré 1, P_2 de degré 2 ;
- deux polynômes irréductibles de degré 3.

En utilisant la question 1., cela montre qu'il y a 14 classes de similitude.

Exercice 13 : Endomorphismes de polynôme minimal donné

Soient K un corps et $P \in K[X]$ un polynôme non constant. Soit Σ l'ensemble des entiers naturels n tels qu'il existe un K-espace vectoriel V de dimension n muni d'un endomorphisme linéaire u de polynôme minimal égal à P. Montrer qu'il existe $N \in \mathbb{N}$ et $d \in \mathbb{N}^*$ tels que $\Sigma \cap [N, +\infty[= d\mathbb{N} \cap [N, +\infty[$. Que vaut d ?

Indications : On écrit P comme produit de facteurs irréductibles : $P = P_1^{r_1}...P_k^{r_k}$. Soit V un tel espace vectoriel. On peut le voir comme un $K[X]$-module sur lequel X agit par u. Il est alors isomorphe à : $V \cong \prod_{i=1}^{s} K[X]/(Q_i)$ avec pour certains $Q_1, ..., Q_s$ unitaires non constants tels que $Q_1|...|Q_s$ et $Q_s = P$. Par conséquent, $\dim V \in \deg P + \sum_{i=1}^{k} \deg P_i\mathbb{N}$. Réciproquement, soit $n \in \deg P + \sum_{i=1}^{k} \deg P_i\mathbb{N}$. On écrit $n = \deg P + \sum_{i=1}^{k} n_i \deg P_i$. En prenant $V = \prod_{i=1}^{k} K[X]/(P_i) \times K[X]/(P)$ et $u : V \to V, v \mapsto Xv$, on voit que $n \in \Sigma$. Donc :

$$\Sigma = \deg P + \sum_{i=1}^{k} \deg P_i\mathbb{N},$$

ce qui achève la preuve pour $d = \deg P_1 \wedge ... \deg P_k$.

Exercice 14 (à préparer) : Examen 2011

Soit K un corps. Pour chaque polynôme unitaire $P \in K[X]$, on note $C(P)$

la matrice compagnon associée. Si P et Q sont deux polynômes unitaires, déterminer les invariants de similitude de la matrice :

$$\begin{pmatrix} C(P) & 0 \\ 0 & C(Q) \end{pmatrix}.$$

Indications : Soient $V = K^{\deg P + \deg Q}$ et $u \in \mathrm{End}(V)$ défini par la matrice de l'énoncé. En voyant V comme $K[X]$-module (en faisant agir X par u), on a un isomorphisme :

$$V \cong K[X]/(P) \oplus K[X]/(Q).$$

On écrit les décompositions de P et Q comme produits d'irréductibles : $P = R_1^{a_1}...R_s^{a_s}$ et $Q = R_1^{b_1}...R_s^{b_s}$, avec a_i et b_i éventuellement nuls. A l'aide du lemme chinois :

$$\begin{aligned} V &\cong \bigoplus_{i=1}^{s} (K[X]/(R_i^{a_i}) \oplus K[X]/(R_i^{b_i})) \\ &\cong K[X]/(\prod_{i=1}^{s} R_i^{\min\{a_i,b_i\}}) \oplus K[X]/(\prod_{i=1}^{s} R_i^{\max\{a_i,b_i\}}) \\ &\cong K[X]/(P \wedge Q) \oplus K[X]/(P \vee Q). \end{aligned}$$

Les facteurs de similitude sont donc $P \wedge Q$ et $P \vee Q$.

Exercice 15 : Commutant

Soient K un corps infini et V un K-espace vectoriel non nul de dimension finie. Pour u un endomorphisme de V, on note $\mathcal{C}(u) = \{v \in \mathrm{End}_K(V) \mid uv = vu\}$ et $\mathcal{P}(u) = \{P(u) \mid P \in K[X]\}$.

1. Soit $u \in \mathrm{End}_K(V)$. Montrer que $\mathcal{P}(u) = \bigcap_{v \in \mathcal{C}(u)} \mathcal{C}(v)$.

Indications : L'inclusion $\mathcal{P}(u) \subseteq \bigcap_{v \in \mathcal{C}(u)} \mathcal{C}(v)$ est évidente.
Soit maintenant $f \in \bigcap_{v \in \mathcal{C}(u)} \mathcal{C}(v)$. On peut voir V comme un $K[X]$-module où X agit par u. On écrit $V = \bigoplus_{r=1}^{n} K[X]/(P_r)$ avec $P_1|P_2|...|P_n$. Comme f est un morphisme de $K[X]$-modules qui commute avec les projections sur $K[X]/(P_r)$ pour chaque r, les sous-espaces $K[X]/(P_r)$ de V sont stables par f. Il existe donc des polynômes $Q_1, ..., Q_n$ tels que

$$f : (R_1, ..., R_n) \in \bigoplus_{r=1}^{n} K[X]/(P_r) \mapsto (Q_1R_1, ..., Q_nR_n) \in \bigoplus_{r=1}^{n} K[X]/(P_r).$$

De plus, pour chaque r, la projection $K[X]/(P_{r+1}) \to K[X]/(P_r)$ induit un morphisme de $K[X]$-modules $V \to V$. Comme f doit commuter avec ce morphisme de $K[X]$-modules, on en déduit que $Q_{r+1} \equiv Q_r \mod P_r$. Par conséquent, $f = Q_n(u) \in \mathcal{P}(u)$.

2. Soit $u \in \mathrm{End}_K(V)$. Montrer que les propriétés suivantes sont équivalentes :

(i) u est cyclique ;

(ii) le polynôme minimal de u est égal (au signe près) au polynôme caractéristique ;
(iii) $\mathcal{C}(u) = \mathcal{P}(u)$;
(iv) V n'a qu'un nombre fini de sous-espace stables par u.

Indications : On peut voir V comme un $K[X]$-module où X agit par u.
L'implication $(i) \Rightarrow (ii)$ est évidente.
Supposons (ii) et montrons (i), (iii) et (iv). On écrit $V = \bigoplus_{r=1}^{n} K[X]/(P_r)$ avec $P_1|P_2|...|P_n$. Le polynôme minimal de u est alors P_n et le polynôme caractéristique $P_1...P_n$. On en déduit que $n = 1$ et $V = K[X]/(P_1)$. Donc u est cyclique (ce qui prouve (i)). Soit maintenant $f \in \mathcal{C}(u)$. Alors f est un morphisme de $K[X]$-modules. Soit $P \in K[X]$ dont la classe module P_1 est $f(1)$. On remarque alors que, pour tout $Q \in K[X]/(P_1)$, on a $f(Q) = PQ$ et donc $f = P(u) \in \mathcal{C}(u)$ (ce qui prouve (iii)). Se donner un sous-espace stable de u, c'est se donner un sous-$K[X]$-module de $K[X]/(P_1)$, c'est-à-dire se donner un diviseur de P_1 (constante multiplicative près). Cela montre (iv) puisque P_1 a un nombre fini de diviseurs à constante multiplicative près. Par conséquent, on a montré que (ii) implique (i), (iii) et (iv).
Supposons (iii). On écrit $V = \bigoplus_{r=1}^{n} K[X]/(P_r)$ avec $P_1|P_2|...|P_n$. Soit π la projection $V \to \bigoplus_{r=1}^{n-1} K[X]/(P_r)$. C'est un morphisme $K[X]$-modules. Par (iii), on déduit que c'est la multiplication par un élément Q de $K[X]$. Comme π est nul sur $K[X]/(P_n)$, on a $P_n|Q$. Mais alors $\pi = 0$, et $n = 1$. Donc u est cylique et (iii) implique (i).
Supposons (iv). On écrit $V = \bigoplus_{r=1}^{n} K[X]/(P_r)$ avec $P_1|P_2|...|P_n$. Supposons $n \geq 2$. Soit $x \in K$ tel que $P_2(x) \neq 0$. On remarque alors que les sous-$K[X]$-modules engendrés par $(c, X - x, 0, ..., 0)$ dans V pour $c \in K$ sont deux à deux distincts : absurde! Donc $n = 1$ et (iv) implique (i).
Remarque : L'infinitude de K n'intervient que pour les implications $(iv) \Rightarrow (i)$, $(iv) \Rightarrow (ii)$ et $(iv) \Rightarrow (iii)$.

Pour les deux exercices qui suivent, on rappelle que les racines du polynôme $x^3 + px + q = 0$ sont les :

$$\zeta \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \zeta^2 \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

pour ζ parcourant les racines cubiques de l'unité.

Exercice 16 : Résolution d'équations

1. Exhiber une solution réelle de l'équation $x^3 - 3x^2 - 6x - 4 = 0$.

Indications : En posant $y = x - 1$, on a $y^3 - 9y - 12 = 0$. Une solution de cette équation est $y = \sqrt[3]{3} + \sqrt[3]{9}$ et donc $x = 1 + \sqrt[3]{3} + \sqrt[3]{9}$ est solution de l'équation proposée.

2. Même question pour $x^6 + 3x^5 - 3x^4 + 2x^3 - 3x^2 + 3x + 1 = 0$.

Indications : En posant $z = x + x^{-1}$, on a $z^3 - 3z^2 - 6z - 4 = 0$. Donc $x = \frac{z + \sqrt{z^2 - 4}}{2}$ avec $z = 1 + \sqrt[3]{3} + \sqrt[3]{9}$ est une solution réelle de l'équation proposée.

Exercice 17 : Calculs de nombres algébriques

1. Calculer les parties réelle et imaginaire d'une racine cubique de :

$$z = 3\sqrt{3} + i\sqrt{5}.$$

> **Indications :** Considérons l'équation $x^3 - 6\sqrt[3]{4}x - 6\sqrt{3} = 0$ (*). Ses solutions sont les doubles des parties réelles des racines cubiques de z. On pose $y = \frac{\sqrt[3]{4}}{\sqrt{3}}x$. On remarque alors que y est solution de $y^3 - 8y - 8 = 0$. Mais on voit aisément que -2 est solution de cette dernière équation. Par conséquent, $x = -2\frac{\sqrt{3}}{\sqrt[3]{4}}$ est solution de (*). On en déduit que z possède une racine racine cubique de partie réelle $-\frac{\sqrt{3}}{\sqrt[3]{4}}$. La partie imaginaire est alors $-\sqrt{32 - \frac{3}{2\sqrt[3]{2}}}$.

2. Soit j une racine cubique primitive de l'unité. Montrer qu'il existe des rationnels a, x, y, que l'on déterminera, tels que :

$$\cos\left(\frac{2\pi}{7}\right) = a + \sqrt[3]{x + yj} + \sqrt[3]{x + yj^2}.$$

> **Indications :** Le complexe ζ_7 est solution de $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = 0$. Par conséquent, $y = 2\cos\left(\frac{2\pi}{7}\right) = \zeta_7 + \zeta_7^{-1}$ vérifie $y^3 + y^2 - 2y - 1 = 0$. En posant $z = y + \frac{1}{3}$, on a $z^3 - \frac{7}{3}z - \frac{7}{27} = 0$. On obtient donc la formule :
>
> $$\cos\left(\frac{2\pi}{7}\right) = -\frac{1}{6} + \frac{1}{2}\sqrt[3]{\frac{35}{54} - \frac{7}{9}\rho} + \frac{1}{2}\sqrt[3]{\frac{35}{54} - \frac{7}{9}\rho^2}.$$

Exercice 18 : Calcul de discriminant - Examen 2014

Soient a et b deux éléments de $\mathbb{C}$. Soit $n \geq 2$. Calculer le discriminant du polynôme $X^n + aX + b$.

Exercice 19 : Discriminant d'un polynôme cyclotomique

Soient p un nombre premier et n un entier naturel non nul. Calculer le discriminant de $\phi_{p^n} = \sum_{k=0}^{p-1} X^{kp^{n-1}}$ au signe près.

Indications : Soit $\zeta \in \mathbb{C}$ une racine primitive p^n-ième de l'unité. Les racines de ϕ_{p^n} sont alors les ζ^k avec $1 \leq k \leq p^n$ non multiple de p. Le discriminant de ϕ_{p^n} est alors :

$$\Delta = \pm \prod_{\substack{k=1 \\ p \nmid k}}^{p^n} \phi'_{p^n}(\zeta^k).$$

En dérivant $(X^{p^{n-1}} - 1)\phi_{p^n} = X^{p^n} - 1$, on obtient :

$$(X^{p^{n-1}} - 1)\phi'_{p^n} + p^{n-1}X^{p^{n-1}-1}\phi_{p^n} = p^n X^{p^n-1}.$$

Par conséquent, on a $(\zeta^{kp^{n-1}} - 1)\phi'_{p^n}(\zeta^k) = p^n\zeta^{k(p^n-1)}$ pour $1 \leq k \leq p^n$ non multiple de p. En multipliant toutes ces relations, on obtient :

$$\phi_p(1)^{p^{n-1}}\Delta = \pm p^{np^{n-1}(p-1)}.$$

Par conséquent, $\Delta = \pm p^{np^{n-1}(p-1)-p^{n-1}}$.

Exercice 20 : Résultant et discriminant

Soit A un anneau commutatif. Pour $n \in \mathbb{N}$, on note $A_n[X]$ le A-module des polynômes de degré strictement plus petit que n. On appellera base canonique de $A_n[X]$ la base $(X^{n-1}, X^{n-2}, ..., 1)$. Pour $(P, Q) \in A[X] \times A[X]$ avec $\deg P = n$ et $\deg Q = m$, on note $\mathrm{Res}(P, Q)$ le déterminant dans les bases canoniques de l'application A-linéaire $A_m[X] \times A_n[X] \to A_{m+n}[X]$ qui envoie (U, V) sur $PU + QV$.

1. Écrire $\mathrm{Res}(P, Q)$ comme déterminant d'une matrice.

2. Comparer $\mathrm{Res}(P, Q)$ et $\mathrm{Res}(Q, P)$.

3. On suppose que P est un polynôme unitaire.

(a) Montrer que $\mathrm{Res}(P, Q)$ est égal au déterminant de la multiplication par Q sur l'anneau $A[X]/(P)$ dans la base $(X^{n-1}, X^{n-2}, ..., 1)$.

(b) Considérons $Q_1 \in A[X]$ et $Q_2 \in A[X]$ de degrés respectifs m_1 et m_2. Calculer $\mathrm{Res}(P, Q_1Q_2)$ en fonction de $\mathrm{Res}(P, Q_1)$ et $\mathrm{Res}(P, Q_2)$.

(c) Exprimer $\mathrm{Res}(P, (X-\lambda_1)...(X-\lambda_m))$ en fonction de $P(\lambda_1)...P(\lambda_m)$.

(d) En déduire une formule explicite pour $\Delta^2 = \prod_{i<j}(X_i - X_j)^2 \in \mathbb{Z}[X_1, ..., X_n]$ en fonction des polynômes symétriques élémentaires.

Exercice 21 : Fractions rationnelles fixées par le groupe alterné

Soit K un corps de caractéristique différente de 2. Montrer que, pour $n \geq 2$, le sous-corps de $K(x_1, ..., x_n)$ fixé par $\mathcal{A}_n$ est :

$$K(x_1, ..., x_n)^{\mathcal{A}_n} = \{f + g\Delta | f, g \in K(x_1, ..., x_n)^{\mathcal{S}_n}\},$$

où $\Delta = \prod_{i<j}(x_i - x_j)$.

Indications : Pour $\sigma \in \mathcal{S}_n$, $f \in K(x_1,...,x_n)^{\mathcal{S}_n}$ et $g \in K(x_1,...,x_n)^{\mathcal{S}_n}$, on a $\sigma \cdot (f + \Delta g) = f + \epsilon(\sigma)\Delta g$, et donc $f + g\Delta \in K(x_1,...,x_n)^{\mathcal{A}_n}$. Réciproquement, soit $h \in K(x_1,...,x_n)^{\mathcal{A}_n}$. Soit $\tau \in \mathcal{S}_n$ une transposition. Posons $f = \frac{h+\tau\cdot h}{2}$ et $g = \frac{h-\tau\cdot h}{2\Delta}$. On a alors $h = f + g\Delta$ et on vérifie immédiatement que f et g sont dans $K(x_1,...,x_n)^{\mathcal{S}_n}$.

Exercice 22 : Fractions rationnelles fixées par un groupe cyclique

1. Soit $n > 0$ un entier. Soit G un sous-groupe cyclique de $GL_n(\mathbb{C})$. On fait agir naturellement G sur $\mathbb{C}(x_1,...,x_n)$. Montrer que le corps $\mathbb{C}(x_1,...,x_n)^G$ est isomorphe à $\mathbb{C}(y_1,...,y_n)$.

Indications : Soit M un générateur de G. Soit m l'ordre de G.
L'action de M sur $\mathbb{C}(x_1,...,x_n)$ est définie de la manière suivante : si $F(x_1,...,x_n) \in \mathbb{C}(x_1,...,x_n)$, alors $M \star F(x_1,...,x_n) = F(y_1,...,y_n)$ où :

$$\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = M \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

On note ζ une racine primitive m-ième de l'unité. Comme G est cyclique, il existe $P \in GL_n(\mathbb{C})$ et des entiers $a_1,...,a_n$ tels que $PMP^{-1} = Diag(\zeta^{a_1},...,\zeta^{a_n})$. On pose :

$$\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Comme P est inversible, on a $K(x_1,...,x_n) = K(z_1,...,z_n)$ et on définit un isomorphisme de corps $K(x_1,...,x_n) \to K(z_1,...,z_n)$ en envoyant x_i sur z_i. On remarque que :

$$\begin{pmatrix} M \star z_1 \\ \vdots \\ M \star z_n \end{pmatrix} = PM \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = Diag(\zeta^{a_1},...,\zeta^{a_n})P \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \zeta^{a_1} z_1 \\ \vdots \\ \zeta^{a_n} z_n \end{pmatrix}.$$

Soit maintenant $A = \mathbb{C}[z_1,...,z_n,z_1^{-1},...,z_n^{-1}] \subseteq \mathbb{C}(z_1,...,z_n)$. Pour $b = (b_1,...,b_n) \in \mathbb{Z}^n$, on note $z^b = z_1^{b_1}...z_n^{b_n}$. Soit $P = \sum_{b\in\mathbb{Z}^n} \lambda_b z^b \in A$. On a alors :

$$M \star P = \sum_{b\in\mathbb{Z}^n} \lambda_b \zeta^{a_1 b_1 + ... a_n b_n} z^b.$$

Par conséquent, P est fixé par M si, et seulement si, $\lambda_b = 0$ dès que m ne divise pas $a_1b_1 + ... + a_nb_n$. Autrement dit,

$$A^G = \mathbb{C}[(z^b)_{b\in B}]$$

où B est noyau de $\mathbb{Z}^n \to \mathbb{Z}/m\mathbb{Z}, (b_1, ..., b_n) \mapsto a_1b_1 + ... + a_nb_n$. On remarque alors que B est un groupe abélien libre de rang n. On se donne donc une base $b^{(1)}, ..., b^{(n)}$ de B. Comme la famille $b^{(1)}, ..., b^{(n)}$ engendre B, on a :

$$A^G = \mathbb{C}[z^{b^{(1)}}, ..., z^{b^{(n)}}, z^{-b^{(1)}}, ..., z^{-b^{(1)}}].$$

Comme la famille $b^{(1)}, ..., b^{(n)}$ est libre, on définit un isomorphisme d'anneaux $A \to A^G$ en envoyant z_i sur $z^{b^{(i)}}$ et z_i^{-1} sur $z^{-b^{(i)}}$. Ce dernier s'étend en un isomorphisme entre $\mathbb{C}(z_1, ..., z_n)$ et $Frac(A^G)$. Or, si P et Q sont des éléments non nuls de A et $P/Q \in \mathbb{C}(z_1, ..., z_n)^G$, alors en écrivant :

$$\frac{P}{Q} = \frac{P\prod_{i=1}^{m-1}(M^i \star Q)}{\prod_{i=0}^{m-1}(M^i \star Q)},$$

on voit que $P/Q \in Frac(A^G)$. Par conséquent, $Frac(A^G) = \mathbb{C}(x_1, ..., x_n)^G$ et $\mathbb{C}(x_1, ..., x_n)^G$ est isomorphe à $\mathbb{C}(z_1, ..., z_n)$.

2. Exhiber un isomorphisme explicite entre les corps $\{F \in \mathbb{C}(x_1, ..., x_n) \mid F(x_1, x_2, ..., x_n) = F(x_2, x_3, ..., x_n, x_1)\}$ et $\mathbb{C}(y_1, ..., y_n)$.

Indications : Soit G le sous-groupe de $GL_n(\mathbb{C})$ en engendré par la matrice $M = (m_{ij})$ telle que $m_{ij} = 1$ si $i \equiv j + 1 \mod n$, $m_{ij} = 0$ sinon. On cherche $\mathbb{C}(x_1, ..., x_n)^G$.
Soit ζ une racine primitive n-ième de l'unité. Pour $0 \leq k \leq m - 1$, posons :

$$y_k = \sum_{i=1}^{m} \zeta^{ik} x_k.$$

On vérifie immédiatement que :

$$M \star y_k = \zeta^{-k} y_k.$$

En tenant compte de la question 1, on s'intéresse au noyau de

$$\mathbb{Z}^n \to \mathbb{Z}/n\mathbb{Z}, (b_0, ..., b_{n-1}) \mapsto b_1 + 2b_2 + 3b_3 + ... + n - 1b_{n-1}.$$

Si $(e_0, ..., e_{n-1})$ est la base canonique de $\mathbb{Z}^n$, une base de ce noyau est donnée par e_0, ne_1, et les $e_k - ke_1$ pour $k \geq 2$. Cela montre que l'on a un isomorphisme entre $\mathbb{C}(z_0, ..., z_{n-1})$ et $\mathbb{C}(x_1, ..., x_n)^G$ envoyant z_0 sur y_0, z_1 sur y_1^n et z_k sur $y_k y_1^{-k}$ pour $k \geq 2$.

Exercice 23 : Formules de Newton

Soit K un corps. Soient $\sigma_1, ..., \sigma_n$ les polynômes symétriques élémentaires de $K[X_1, ..., X_n]$. Pour $k > n$, on pose $\sigma_k = 0$. On note $S_i = X_1^i + ... + X_n^i$ pour $i > 0$. Montrer que, pour $k > 1$, on a $S_k = (-1)^{k+1}k\sigma_k + \sum_{i=1}^{k-1}(-1)^{k+1-i}\sigma_{k-i}S_i$.

Indications :

- Supposons d'abord $k \geq n$. Pour chaque j entre 1 et n, on a :

$$X_j^n + \sum_{i=1}^{n} (-1)^i \sigma_i X_j^{n-i} = 0.$$

On a alors aussi, pour $1 \leq j \leq n$:

$$X_j^k + \sum_{i=1}^{n} (-1)^i \sigma_i X_j^{k-i} = 0.$$

En ajoutant ces relations, on obtient :

$$S_k = (-1)^{k+1} k\sigma_k + \sum_{i=1}^{k-1} (-1)^{k+1-i} \sigma_{k-i} S_i$$

pour $k \geq n$.

- Supposons maintenant que $k < n$. Pour chaque entier $i \geq 2$, on note $R_i = \sum_{sym} X_1^i X_2 ... X_{k-i+1}$. On remarque alors que, pour $1 < i < k$, on a $R_i + R_{i+1} = S_i \sigma_{k-i}$. De plus, $R_k = S_k$, et $S_1 \sigma_{k-1} = k\sigma_k + R_2$. On obtient donc :

$$\begin{aligned}(-1)^{k+1} k\sigma_k + \sum_{i=1}^{k-1} (-1)^{k+1-i} \sigma_{k-i} S_i & \\ &= (-1)^{k+1} k\sigma_k + (-1)^k (k\sigma_k + R_2) + \sum_{i=2}^{k-1} (-1)^{k+1-i} (R_i + R_{i+1}) \\ &= S_k.\end{aligned}$$

Nous traiterons peut-être l'exercice 24 la semaine prochaine...