Résolvantes & partitions

Stéphane VINATIER

1. LA RÉSOLVANTE DE LAGRANGE

On considère un polynôme unitaire du 3e degré à cœfficients dans un corps K (par exemple $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \ldots$) :

$$f(t) = t^3 + at^2 + bt + c \ .$$

On cherche les formules donnant en fonction des cœfficients a, b, c les solutions t_1, t_2, t_3 de l'équation $f(t) = 0$, c'est-à-dire les *racines* du polynôme f. On sait que, pour tout t :

$$t^3 + at^2 + bt + c = (t - t_1)(t - t_2)(t - t_3) = t^3 - \sigma_1 t^2 + \sigma_2 t - \sigma_3 \ ,$$

où

$$\sigma_1 = t_1 + t_2 + t_3 \ , \quad \sigma_2 = t_1t_2 + t_2t_3 + t_3t_1 \ , \quad \sigma_3 = t_1t_2t_3$$

sont les *fonctions symétriques élémentaires* des racines t_1, t_2, t_3, qui vérifient donc les relations cœfficients-racines :

$$a = -\sigma_1 \ , \quad b = \sigma_2 \ , \quad c = -\sigma_3 \ .$$

1.1. **Fonctions symétriques des racines.** On sait par un théorème général que *toute expression polynômiale en les racines t_1, t_2, t_3 qui est invariante par les permutations de ces racines peut s'écrire sous la forme d'un polynôme en σ_1, σ_2, σ_3*. Par exemple :

(i) $\tau_2 = t_1^2 + t_2^2 + t_3^2 = \sigma_1^2 - 2\sigma_2$;

(ii) $\tau_3 = t_1^3 + t_2^3 + t_3^3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, en utilisant la formule :

$$(\alpha+\beta+\gamma)^3 = \alpha^3 + \beta^3 + \gamma^3 + 6\alpha\beta\gamma + 3\big(\alpha^2(\beta+\gamma) + \beta^2(\alpha+\gamma) + \gamma^2(\alpha+\beta)\big) \ ;$$

(iii) le discriminant du polynôme f, défini par :

$$\mathrm{disc}(f) = \big((t_1 - t_2)(t_2 - t_3)(t_3 - t_1)\big)^2 \ ,$$

dont on ne détermine pas ici l'expression générale en fonction de σ_1, σ_2, σ_3. On pourra cependant vérifier que, dans le cas $\sigma_1 = 0$, on a

$$\mathrm{disc}(t^3 + pt + q) = -4p^3 - 27q^2 \ .$$

Notons aussi que la formule analogue pour le polynôme t^2+bt+c permet de retrouver que son discriminant vaut b^2-4c.

1.2. **L'apport de Lagrange.** Dans un mémoire publié en 1770, Lagrange analyse les travaux antérieurs sur la résolution des équations polynômiales et détermine le principe sous-jacent aux diverses méthodes : *certaines expressions des racines sont solutions d'une équation dont le degré est inférieur à celui de l'équation de départ et dont les cœfficients sont invariants par permutation des racines*. Ces « expressions des racines » sont appelées les *résolvantes de Lagrange*.

Dans le cas de l'équation de degré 3, on considère

$$y=t_1+jt_2+j^2t_3 \quad \text{et} \quad z=t_1+j^2t_2+jt_3 \ ,$$

où $j=\exp\left(\frac{2i\pi}{3}\right)$ est une *racine primitive cubique de l'unité*, c'est-à-dire $j^3-1=0$ (et $j\neq 1$) donc

$$1+j+j^2=0 \ .$$

Alors les nombres y^3 et z^3 sont invariants par les permutations qui sont des 3-*cycles*, à savoir $t_1\mapsto t_2\mapsto t_3\mapsto t_1$, noté $(1\,2\,3)$, et $t_1\mapsto t_3\mapsto t_2\mapsto t_1$, noté $(1\,3\,2)$. Par contre les *transpositions* $t_1\mapsto t_2\mapsto t_1$, noté $(1\,2)$, *etc.* (il s'agit donc des 2-cycles) échangent y^3 et z^3. Il s'ensuit que y^3+z^3 et y^3z^3 sont invariants par toutes les permutations des racines (qui sont l'identité, les transpositions et les 3-cycles) et donc s'expriment en fonction de σ_1, σ_2, σ_3, c'est-à-dire en fonction des cœfficients a, b, c de l'équation de départ.

Calculons ces expressions :

$$\begin{aligned}
y^3z^3 &= \big((t_1+jt_2+j^2t_3)(t_1+j^2t_2+jt_3)\big)^3\\
&= \big(t_1^2+t_2^2+t_3^2+t_1t_2(j^2+j)+t_2t_3(j+j^2)+t_3t_1(j^2+j)\big)^3\\
&= \big(t_1^2+t_2^2+t_3^2-(t_1t_2+t_2t_3+t_3t_1)\big)^3 \qquad \text{car } j+j^2=-1\\
&= \big(\tau_2-\sigma_2\big)^3\\
&= \big(\sigma_1^2-3\sigma_2\big)^3\\
&= \sigma_1^6-9\sigma_1^4\sigma_2+27\sigma_1^2\sigma_2^2-27\sigma_2^3
\end{aligned}$$

$$\begin{aligned}
y^3+z^3 &= (t_1+jt_2+j^2t_3)^3+(t_1+j^2t_2+jt_3)^3\\
&= 2(t_1^3+t_2^3+t_3^3)+12t_1t_2t_3-3\big(t_1^2(t_2+t_3)+t_2^2(t_3+t_1)+t_3^2(t_1+t_2)\big)
\end{aligned}$$

or

$$t_1^2(t_2+t_3)+t_2^2(t_3+t_1)+t_3^2(t_1+t_2)=(t_1^2+t_2^2+t_3^2)(t_1+t_2+t_3)-(t_1^3+t_2^3+t_3^3)$$

d'où

$$y^3+z^3=2\tau_3+12\sigma_3-3\sigma_1\tau_2+3\tau_3=2\sigma_1^3-9\sigma_1\sigma_2+27\sigma_3 \ .$$

Les résolvantes y^3 et z^3 sont donc les racines du polynôme :

$$x^2-(2\sigma_1^3-9\sigma_1\sigma_2+27\sigma_3)x+(\sigma_1^6-9\sigma_1^4\sigma_2+27\sigma_1^2\sigma_2^2-27\sigma_2^3) \ .$$

Puisqu'il s'agit d'un polynôme du 2e degré, on peut les calculer (dans **C**) ; en prenant *une* racine cubique de y^3, on obtient une valeur possible pour y (les autres s'obtiennent en la multipliant par j et par j^2) ; on utilise la relation $yz = \sigma_1^2 - 3\sigma_2$ pour en déduire z. Enfin on détermine t_1, t_2 et t_3 en notant que

$$\left\{\begin{array}{rcl} \sigma_1 & = & t_1+t_2+t_3 \\ y & = & t_1+jt_2+j^2t_3 \\ z & = & t_1+j^2t_2+jt_3 \end{array}\right.$$

entraîne

$$\left\{\begin{array}{rcl} 3t_1 & = & \sigma_1+y+z \\ 3t_2 & = & \sigma_1+j^2y+jz \\ 3t_3 & = & \sigma_1+jy+j^2z \ . \end{array}\right.$$

1.3. **Les formules.** Plutôt que d'écrire les formules dans le cas général, on remarque qu'il est possible de se ramener au cas où $\sigma_1 = 0$. En effet, notre équation

$$t^3+at^2+bt+c=0$$

équivaut à

$$(t+\tfrac{a}{3})^3+(b-\tfrac{a^2}{3})t+(c-\tfrac{a^3}{27})=0 \ ,$$

soit, en posant $u = t+\frac{a}{3}$:

$$u^3+(b-\tfrac{a^2}{3})u+(c-\tfrac{ab}{3}+\tfrac{2a^3}{27})=0 \ ,$$

ce qui nous ramène à chercher les solutions u_1, u_2, u_3 d'une équation de la forme :

$$u^3+pu+q=0$$

(on en déduira facilement les racines de l'équation d'origine puisque $t_1 = u_1 - \frac{a}{3}$, *etc.*). En utilisant le travail fait précédemment (et les relations cœfficients-racines), on obtient que les résolvantes $(y')^3$ et $(z')^3$ associées à la nouvelle équation sont racines de

$$x^2+27qx-27p^3=0 \ ,$$

dont le discriminant est $\Delta = 27^2q^2+4\cdot 27p^3$ (donc $\Delta = -27\cdot\mathrm{disc}(u^3+pu+q)$), si bien que l'une des deux résolvantes, disons $(y')^3$ vaut

$$(y')^3 = -27\left(\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}\right) \ .$$

On choisit *une* racine cubique de ce nombre, que l'on note

$$y' = -3\cdot\sqrt[3]{\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} \ ;$$

comme $y'z' = -3p$, on en déduit

$$z' = \frac{p}{\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}} \ .$$

Enfin on obtient les racines par le procédé expliqué ci-dessus :

$$\begin{aligned}
u_1 &= -\sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \frac{p}{3 \cdot \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}} \\
u_2 &= -j^2 \cdot \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \frac{j\,p}{3 \cdot \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}} \\
u_3 &= -j \cdot \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \frac{j^2 p}{3 \cdot \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}}
\end{aligned}$$

Noter que les différents choix effectués lors de la résolution n'affectent pas l'*ensemble* $\{u_1, u_2, u_3\}$ des racines, mais seulement l'ordre dans lequel elles apparaissent. Si on le souhaite, on peut remplacer p et q par leurs expressions en a, b et c et enlever $\frac{a}{3}$ à chaque racine pour obtenir les formules donnant les solutions de l'équation générale de degré 3 !

1.4. **Degré 4.** Soient x_1, x_2, x_3 et x_4 les 4 racines d'un polynôme de degré 4. On pose

$$y_1 = (x_1 + x_2)(x_3 + x_4) \ .$$

Cette expression est invariante par les permutations de $\{1,2,3,4\}$ suivantes : (12), (34), $(12)(34)$, $(13)(24)$, $(14)(23)$, (1324), (1423) et bien sûr l'identité. Ses « valeurs » (le terme est de Lagrange) possibles quand on permute les racines sont :

$$y_2 = (x_1 + x_3)(x_2 + x_4) \quad \text{et} \quad y_3 = (x_1 + x_4)(x_2 + x_3) \ .$$

En effet, il n'y a que trois possibilités pour la racine qui accompagne x_1 et son choix détermine les deux racines qui composent l'autre facteur.

L'ensemble des valeurs s'appelle l'*orbite* de la résolvante y_1 ; l'ensemble des permutations qui la laissent invariante s'appelle son *stabilisateur*. On note que le produit des cardinaux de ces deux ensembles (3×8) est égal au nombre total de permutations des 4 racines ($4!$), ce qui nous fournit un exemple d'application d'un résultat élémentaire en théorie des groupes, laquelle s'est justement développée à partir des travaux de Lagrange.

Le *polynôme résolvant* est

$$\mathrm{P}(y) = (y - y_1)(y - y_2)(y - y_3) \ .$$

Ses cœfficients sont symétriques en y_1, y_2, y_3, donc invariants par toutes les permutations de x_1, x_2, x_3 et x_4. En conséquence, les cœfficients de $P(y)$ s'expriment à partir de ceux de l'équation de départ (que l'on suppose donnés). Puisque $P(y)$ est un polynôme de degré 3, on sait calculer ses racines en fonction de ses cœfficients (formules ci-dessus !), donc on peut écrire y_1, y_2 et y_3 à l'aide des cœfficients de l'équation de départ.

Pour en déduire x_1, x_2, x_3 et x_4, on note que l'on peut se ramener au cas où leur somme $x_1+x_2+x_3+x_4$ est nulle (par le même procédé qu'en degré 3). On voit qu'alors $y_1=-(x_1+x_2)^2$ donc

$$x_1+x_2=\sqrt{-y_1}\ ,$$

pour un choix de racine carrée de $-y_1$. On fait de même avec les autres « valeurs », on obtient un système linéaire de 4 équations pour nos 4 inconnues, dont la résolution donne les formules souhaitées. Qu'il ne reste qu'à écrire...

1.5. **Note historique et références bibliographiques.** Les formules pour l'équation de degré 2 sont connues depuis l'Antiquité ; en degrés 3 et 4, elles le sont depuis le XVI$^{\text{e}}$ siècle (Del Ferro, Cardan, Tartigliano, Ferrari...).

La détermination du principe de résolution, ainsi que certains cas particuliers en degré 5, sont dus à Lagrange (1770). Le cas général en degré ≥ 5 (c'est-à-dire la non résolubilité par radicaux de l'*équation générale*) a été établi par Ruffino en 1802 (preuve incomplète) et par Abel en 1826, tous deux se basant sur les travaux de Lagrange (on montre que pour l'équation générale de degré ≥ 5, le polynôme résolvant est de degré toujours supérieur ou égal à celui de l'équation de départ).

Enfin, l'aboutissement de ces idées a été obtenu par Galois, dont la théorie permet d'associer à tout polynôme un groupe de permutations de ses racines qui contient de façon assez claire toute l'information souhaitée, en particulier sur la possibilité d'exprimer ses racines par radicaux. Le transfert de l'information vers un groupe de permutation a bien sûr incité à développer la théorie des groupes, qui reste aujourd'hui encore un sujet de recherche très riche.

Le contenu de cette première section est tiré en grande partie de quelques pages (§1.8) de l'ouvrage de DIXON et MORTIMER, *Permutation groups*, GTM 163, Springer (1996). Pour une présentation historique plus détaillée et en français, on peut consulter la *Notice Historique* des *Eléments de Mathématiques, XI, Algèbre*, chap. IV (Polynômes et fractions rationnelles) de BOURBAKI.

2. RÉSOLVANTE GÉNÉRALISÉE ET PERMUTATIONS DE PARTITIONS

On fixe un nombre premier $p\geq 3$ et t_0, $t_1,\dots,t_{p-1}$ des nombres *conjugués* sur $\mathbf{Q}$, c'est-à-dire racines d'un même polynôme à cœfficients dans $\mathbf{Q}$, *irréductible* (non factorisable) sur $\mathbf{Q}$.

On note ζ une racine primitive p-ième de l'unité ($\zeta^p=1$ mais $\zeta^k\neq 1$ pour $0<k<p$). C'est une solution de $X^p-1=0$; or $X^p-1=(X-1)(1+X+\cdots+X^{p-1})$,

d'où

$$\zeta+\zeta^2+\cdots+\zeta^{p-1}=-1\ .$$

Noter que ζ^k avec $0<k<p$ est aussi une racine primitive p-ième de l'unité.

Comme lorsque $p=3$, on définit des « résolvantes » en posant

$$\begin{cases} y_1 &= t_0+\zeta t_1+\zeta^2 t_2+\cdots+\zeta^{p-1}t_{p-1}\\ y_2 &= t_0+\zeta^2 t_1+(\zeta^2)^2 t_2+\cdots+(\zeta^2)^{p-1}t_{p-1}\\ &\vdots\\ y_{p-1} &= t_0+\zeta^{p-1}t_1+\zeta^{2p-2}t_2+\cdots+\zeta^{(p-1)^2}t_{p-1}\end{cases}$$

soit, pour $1\le k\le p-1$,

$$y_k=\sum_{i=0}^{p-1}\zeta^{ik}t_i\ .$$

Comme pour $p=3$, on souhaite calculer

$$y_1^p+y_2^p+\cdots+y_{p-1}^p=\sum_{k=1}^{p-1}\Big(\sum_{i=0}^{p-1}\zeta^{ik}t_i\Big)^p\ .$$

Pour $p\ge 5$, cette expression n'est pas invariante par toutes les permutations des racines, notamment par les transpositions ; elle ne peut donc pas *a priori* s'écrire sous forme de polynôme en les fonctions symétriques élémentaires des racines. L'idée ici n'est plus de tenter de résoudre une équation polynômiale de degré p, mais d'utiliser d'autres propriétés arithmétiques des résolvantes. On peut en effet montrer que l'exposant de p qui divise une somme d'expressions similaires à celle ci-dessus détermine l'invariance de certains modules liés à des polynômes irréductibles sous l'action de leurs groupes de Galois.

2.1. **Formule du multinôme de Newton.** On doit développer une puissance d'une somme de p termes. Soient n un entier naturel et $a_0, a_1,\ldots, a_{p-1}$ des nombres quelconques, alors :

$$\Big(\sum_{i=0}^{p-1}a_i\Big)^n=\sum_{\underline{\ell}}\frac{n!}{\ell_0!\ell_1!\cdots\ell_{p-1}!}\prod_{i=0}^{p-1}a_i^{\ell_i}\ ,$$

où $\underline{\ell}=(\ell_0,\ell_1,\ldots,\ell_{p-1})$ décrit toutes les *combinaisons* de n à p parts (éventuellement nulles[1]), c'est-à-dire $\ell_i\ge 0$ pour tout i et $\ell_0+\ell_1+\cdots+\ell_{p-1}=n$. Noter qu'en remplaçant p par 2, on retrouve la formule tout à fait classique du *binôme de Newton*.

Montrons la formule du multinôme, on a :

$$\Big(\sum_{i=0}^{p-1}a_i\Big)^n=\Big(\sum_{i=0}^{p-1}a_i\Big)\times\Big(\sum_{i=0}^{p-1}a_i\Big)\times\cdots\times\Big(\sum_{i=0}^{p-1}a_i\Big)\qquad (n\text{ fois})\ ,$$

[1] L'usage dans ce domaine est de ne pas compter les parts nulles, cependant il est naturel de le faire ici puisqu'elles interviennent comme exposants dans la formule.

donc lorsqu'on développe, le nombre total de facteurs dans chaque terme est toujours n. Par ailleurs il est clair que chaque a_i apparaît un nombre positif ou nul de fois. Une combinaison $\underline{\ell} = (\ell_0, \ell_1, \ldots, \ell_{p-1})$ de n étant fixée, combien de fois le terme correspondant $\prod_{i=0}^{p-1} a_i^{\ell_i}$ apparaît-il ? Si l'on convient dans un premier temps de distinguer les a_i avec le même indice i qui proviennent de parenthèses différentes (autrement dit la multiplication n'est plus supposée commutative), alors choisir ℓ_0 parenthèses dans lesquelles on prend a_0, et de même pour tout i, revient à ordonner les n nombres (considérés distincts) $a_0, \ldots, a_0$ (ℓ_0 fois), $a_1, \ldots, a_1$ (ℓ_1 fois), *etc.*, et ceci peut se faire de $n!$ manières.

Si l'on tient maintenant compte du fait que notre loi $\times$ est commutative, on voit que l'ordre qu'on a mis sur les a_0 est superflu, ce qui donne $\ell_0!$ fois trop de façons de compter les termes $\prod_{i=0}^{p-1} a_i^{\ell_i}$; il en va de même pour chaque indice i, d'où le résultat.

On peut remarquer, comme l'on fait certaines personnes qui assistaient à l'exposé dont ces notes sont tirées, que ceci est équivalent au décompte du nombre d'anagrammes que l'on peut écrire à partir d'un mot de n lettres comportant ℓ_0 fois une première lettre, ℓ_1 une deuxième, *etc.*, par exemple le mot *ananas* : $n = 6$, $\ell_0 = 3$, $\ell_1 = 2$, $\ell_3 = 1$, d'où $\frac{6!}{3!\cdot 2!} = 60$ anagrammes[(2)].

2.2. **Avec des permutations.** La formule de Newton étant maintenant bien établie, nous allons la compliquer un peu. L'idée sous-jacente à ce qui va suivre est que le cœfficient multinômial

$$\frac{n!}{\ell_0! \cdots \ell_{p-1}!} = \binom{n}{\ell_0, \ldots, \ell_{p-1}}$$

ne dépend pas de l'ordre des parts ℓ_i de la combinaison $\underline{\ell}$. Comme le but final est de trouver le plus grand exposant de p qui divise une somme d'expressions similaires à $y_1^p + \cdots + y_{p-1}^p$, il semble qu'on ait intérêt à factoriser ces expressions autant que possible. Pour cela, au lieu d'indicer la somme par les combinaisons de n à p parts (éventuellement nulles), on va le faire par les *partitions* de n à p parts (éventuellement nulles), c'est-à-dire qu'on impose que les ℓ_i soient rangés par ordre décroissant :

$$\ell_0 \geq \ell_1 \geq \cdots \geq \ell_{p-1} \geq 0 \quad \text{et} \quad \ell_0 + \ell_1 + \cdots + \ell_{p-1} = n \ .$$

Pour retrouver tout de même tous les termes $\prod_{i=0}^{p-1} a_i^{\ell_i}$ qu'on avait précédemment, il suffira de faire agir une permutation sur les parts ℓ_i. On note $\mathfrak{S}_p$ le groupe de toutes les permutations de l'ensemble $\{0, 1, \ldots, p-1\}$ et, pour $\sigma \in \mathfrak{S}_p$, on pose

$$\sigma(\ell_0, \ldots, \ell_{p-1}) = (\ell_{\sigma(0)}, \ldots, \ell_{\sigma(p-1)}) \ .$$

---

(2) Combien d'anagrammes pour le mot « anagramme » ?

Si $\underline{\ell}$ est une partition, $\sigma(\underline{\ell})$ va décrire toutes les combinaisons qui ont les mêmes parts que $\underline{\ell}$, rangées dans n'importe quel ordre, quand σ décrit $\mathfrak{S}_p$. Chaque combinaison pourra être obtenue plusieurs fois. En particulier, on voit facilement que le nombre de permutations $\sigma \in \mathfrak{S}_p$ qui laissent $\underline{\ell}$ invariante est égal à $e_0(\underline{\ell})! \times e_1(\underline{\ell})! \times \cdots \times e_n(\underline{\ell})!$, où

$$e_k(\underline{\ell}) = \text{nombre de parts de } \underline{\ell} \text{ égales à } k\ , \qquad 0 \leq k \leq n\ .$$

(En particulier, $e_n(\underline{\ell})$ vaut 0 ou 1, donc $e_n(\underline{\ell})!$ vaut toujours 1.) En effet, il y a $e_0(\underline{\ell})!$ façons de permuter les parts égales à 0 entre elles, $e_1(\underline{\ell})!$ façons de permuter les parts égales à 1 entre elles, *etc.* On note $\underline{e}(\underline{\ell})$ la combinaison

$$\underline{e}(\underline{\ell}) = (e_0(\underline{\ell}), e_1(\underline{\ell}), \ldots, e_n(\underline{\ell}))$$

et, si $\underline{m} = (m_0, m_1, \ldots, m_r)$, on note

$$\underline{m}! = m_0! \times m_1! \times \cdots \times m_r!\ .$$

Chaque combinaison apparaissant $\underline{e}(\underline{\ell})!$ fois lorsqu'on fait agir $\mathfrak{S}_p$ sur une partition $\underline{\ell}$, on doit diviser la somme obtenue par ce nombre. On peut maintenant réécrire la formule de Newton :

$$\Big(\sum_{i=0}^{p-1} a_i\Big)^n = \sum_{\underline{\ell}} \frac{n!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!} \Big(\sum_{\sigma \in \mathfrak{S}_p} \prod_{i=0}^{p-1} a_i^{\ell_{\sigma(i)}}\Big)\ ,$$

où $\underline{\ell} = (\ell_0, \ell_1, \ldots, \ell_{p-1})$ décrit toutes les partitions de n à p parts (éventuellement nulles).

Avant d'appliquer cette formule à notre calcul, notons deux propriétés de la combinaison $\underline{e}(\underline{\ell})$:

(i) $\sum_{k=0}^{n} e_k(\underline{\ell}) =$ nombre total de parts de $\underline{\ell} = p$, donc $\underline{e}(\underline{\ell})$ est une combinaison de p ;

(ii) $\sum_{k=0}^{n} k e_k(\underline{\ell}) = (0+\cdots+0)+(1+\cdots+1)+\cdots+(n+\cdots+n)$, où 0 apparaît $e_0(\underline{\ell})$ fois, 1 apparaît $e_1(\underline{\ell})$ fois, ..., n apparaît $e_n(\underline{\ell}) = 0$ ou 1 fois, d'où

$$\sum_{k=0}^{n} k e_k(\underline{\ell}) = \sum_{k=0}^{p-1} \ell_k = n\ ,$$

autrement dit $(0, e_1(\underline{\ell}), 2e_2(\underline{\ell}), \ldots, ne_n(\underline{\ell}))$ est une combinaison de n.

2.3. **Application au calcul de la résolvante.** Ici $n = p$. On obtient :

$$y_1^p + \cdots + y_{p-1}^p = \sum_{k=1}^{p-1} \sum_{\underline{\ell}, \sigma} \frac{p!}{\underline{\ell}!\,\underline{e}(\underline{\ell})!} \prod_{i=0}^{p-1} \left(\zeta^{ik} t_i\right)^{\ell_{\sigma(i)}},$$

où $\underline{\ell} = (\ell_0, \ell_1, \ldots, \ell_{p-1})$ décrit toutes les partitions de p à p parts (éventuellement nulles), et σ décrit toutes les permutations de $\mathfrak{S}_p$. Or

$$\prod_{i=0}^{p-1} \left(\zeta^{ik} t_i\right)^{\ell_{\sigma(i)}} = \prod_{i=0}^{p-1} \zeta^{ik\ell_{\sigma(i)}} \cdot \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} = \zeta^{k\sum_{i=0}^{p-1} i\ell_{\sigma(i)}} \cdot \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \ ,$$

d'où

$$y_1^p + \cdots + y_{p-1}^p = \sum_{\underline{\ell},\sigma} \frac{p!}{\underline{\ell}!\, \underline{e}(\underline{\ell})!} \Big(\prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}}\Big) \Big(\sum_{k=1}^{p-1} \zeta^{k\sum_{i=0}^{p-1} i\ell_{\sigma(i)}}\Big) \ .$$

Comme

$$\sum_{k=1}^{p-1} \zeta^{ak} = \begin{cases} p-1 & \text{si } p \mid a \quad \text{(car alors } \zeta^a = 1\text{)} \\ -1 & \text{sinon} \quad \text{(car alors } \zeta^a \text{ racine primitive de 1),} \end{cases}$$

on obtient :

$$\begin{aligned} y_1^p + \cdots + y_{p-1}^p &= (p-1) \sum_{(\underline{\ell},\sigma)} \frac{p!}{\underline{\ell}!\, \underline{e}(\underline{\ell})!} \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} - p \sum_{(\underline{\ell},\sigma)^*} \frac{p!}{\underline{\ell}!\, \underline{e}(\underline{\ell})!} \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \\ &= (p-1)(t_0 + \cdots + t_{p-1})^p - p \sum_{(\underline{\ell},\sigma)^*} \frac{p!}{\underline{\ell}!\, \underline{e}(\underline{\ell})!} \prod_{i=0}^{p-1} t_i^{\ell_{\sigma(i)}} \ , \end{aligned}$$

où la deuxième somme de chaque égalité porte sur les couples $(\underline{\ell}, \sigma)$ tels que p ne divise pas $\sum_{i=0}^{p-1} i\ell_{\sigma(i)}$.

Le calcul dans lequel $y_1^p + \cdots + y_{p-1}^p$ apparaît fait intervenir $1 + p + \cdots + p^{m-1}$ expressions similaires (m est un entier fixé), plus une fois l'expression $(t_0 + \cdots + t_{p-1})^p$, qui apparaît donc au total $1 + (p-1)(1 + p + \cdots + p^{m-1}) = p^m$ fois, ce qui est la puissance de p que l'on cherche à faire apparaître. La décomposition de $y_1^p + \cdots + y_{p-1}^p$ ci-dessus semble donc aller dans le bon sens, d'autant que la deuxième somme a p en facteur. Il est cependant assez difficile d'analyser cette somme, dès que p est au moins 5, à cause de la condition portant sur les couples $(\underline{\ell}, \sigma)$ qui indicent la somme :

$$\text{« } p \text{ ne divise pas } \sum_{i=1}^{p-1} i\ell_{\sigma(i)} \text{ » } .$$

C'est sur cette condition que nous nous concentrons maintenant.

2.4. **Permutation de partitions.** Lorsque $p = 3$, la situation est très simple car on n'a que trois partitions à considérer :

$$\begin{aligned} 3 &= 3+0+0 \\ &= 2+1+0 \\ &= 1+1+1 \ , \end{aligned}$$

et l'on voit aisément que pour tout $\sigma \in \mathfrak{S}_3$, $\sum_{i=1}^{2} i\ell_{\sigma(i)}$ est toujours divisible par 3 quand $\underline{\ell} = (3,0,0)$ ou $(1,1,1)$, jamais quand $\underline{\ell} = (2,1,0)$. La condition « 3 ne divise pas $\sum_{i=1}^{2} i\ell_{\sigma(i)}$ » équivaut donc à $\underline{\ell} = (2,1,0)$, c'est-à-dire qu'elle ne porte pas sur σ, ce qui entraîne que la deuxième somme de l'égalité ci-dessus est une expression invariante par toute permutation des racines (on retrouve d'ailleurs le résultat obtenu dans la première section en continuant le calcul).

Quand $p = 5$, les choses se compliquent. Les partitions sont :

$$\begin{aligned} 5 &= 5+0+0+0+0 \\ &= 4+1+0+0+0 \\ &= 3+2+0+0+0 \\ &= 3+1+1+0+0 \\ &= 2+2+1+0+0 \\ &= 2+1+1+1+0 \\ &= 1+1+1+1+1 \ , \end{aligned}$$

et $\sum_{i=1}^{4} i\ell_{\sigma(i)}$ est toujours divisible par 5 lorsque $\underline{\ell} = (5,0,\ldots,0)$ ou $(1,\ldots,1)$, jamais lorsque $\underline{\ell} = (2,1,1,1,0)$, ni lorsque $\underline{\ell} = (4,1,0,0,0)$ ou $(3,2,0,0,0)$. Par contre, si $\underline{\ell} = (3,1,1,0,0)$ ou $(2,2,1,0,0)$, la condition de divisibilité dépend de $\sigma \in \mathfrak{S}_5$:

$$0\times 3 + 1\times 1 + 2\times 1 = 3 \ , \quad 0\times 3 + 1\times 1 + 4\times 1 = 5 \ .$$

La deuxième somme n'est alors plus invariante par permutation des racines et ne peut plus être exprimée à l'aide des fonctions symétriques élémentaires. (Il en ira de même pour tout premier $p \geq 5$, puisqu'on a vu que $y_1^p + \cdots + y_{p-1}^p$ n'est pas invariant par les transpositions dans ce cas.)

Pour espérer analyser cette deuxième somme, il faut donc comprendre un peu mieux la condition qui la définit. On remarque, pour $p = 5$, que les partitions pour lesquelles la condition dépend de la permutation considérée sont celles qui ont au plus 2 ($< 5-2$) parts nulles et au plus 2 parts égales à 1. Ceci mène au critère général suivant.

Théorème. *Soit $\underline{\ell} = (\ell_0,\ldots,\ell_{p-1})$ une partition de p à p parts (éventuellement nulles). Les deux conditions suivantes sont équivalentes :*

(i) il existe $\sigma,\tau \in \mathfrak{S}_p$ tels que p divise $\sum_{i=1}^{p-1} i\ell_{\sigma(i)}$ et p ne divise pas $\sum_{i=1}^{p-1} i\ell_{\tau(i)}$;

(ii) $\max\{e_k(\underline{\ell}),\ 0 \leq k \leq p\} < p-2$.

La preuve de (i)⇒(ii) se fait par contraposée ; celle de (ii)⇒(i) se fait en considérant deux cas, selon que le nombre s de parts non nulles de $\underline{\ell}$ vérifie $3 \leq s \leq \frac{p-3}{2}$ (on fait alors une récurrence sur s, en utilisant le théorème de Bézout) ou qu'il vérifie $\frac{p-1}{2} \leq s \leq p-2$, auquel cas on a suffisamment de latitude pour modifier la somme

$$0\times\ell_0 + 1\times\ell_1 + \cdots + (s-1)\ell_{s-1} \ ,$$

en augmentant les cœfficients affectés aux parts égales à 1, pour la rendre divisible par p. Ceci prouve l'existence de $\sigma \in \mathfrak{S}_p$ tel que p divise $\sum_i i\ell_{\sigma(i)}$, pour les partitions $\underline{\ell}$ vérifiant (ii). On termine la démonstration du théorème en observant qu'alors p ne divise pas $\sum_i i\ell_{\tau(i)}$, où τ est obtenu en composant σ avec une transposition qui échange deux parts distinctes.

Remarque. D'après ce qu'on a vu plus haut, si $\underline{m}$ est une partition de p à p parts distincte de $(p, 0, \ldots, 0)$, alors

$$\sum_{k=0}^{p-1} k e_k(\underline{m}) = \sum_{k=0}^{p-1} m_k = p \ .$$

Il s'ensuit que la propriété (i) est immédiate pour les partitions $\underline{\ell}$ qui sont de la forme $\underline{\ell} = \tau\big(e_0(\underline{m}), \ldots, e_{p-1}(\underline{m})\big)$, pour une permutation τ. Mais ceci n'est pas toujours le cas, par exemple pour la partition $(2,2,2,1,0,0,0)$ de 7. Par contre, celle-ci peut être mise sous cette forme en utilisant une partition $\underline{m}$ de 14 à 7 parts[(3)].

De fait, $\sigma \in \mathfrak{S}_p$ et $\underline{\ell} \neq (p, 0, \ldots, 0)$ étant fixés, l'égalité $\sum_{i=0}^{p-1} i\ell_{\sigma(i)} = np$ pour $n \in \mathbf{N}$ équivaut à l'existence d'une partition $\underline{m}$ de np à p parts telle que $\sigma(\underline{\ell}) = \big(e_0(\underline{m}), \ldots, e_{p-1}(\underline{m})\big)$. Il s'agit de la partition dans laquelle chaque $i \in \{0, \ldots, p-1\}$ apparaît $\ell_{\sigma(i)}$ fois. Noter que toutes les parts de $\underline{m}$ sont nécessairement $\leq p-1$.

La question se pose alors de savoir si on peut démontrer directement que toute partition $\underline{\ell}$ satisfaisant (ii) peut s'écrire sous la forme $\underline{\ell} = \sigma^{-1}\big(e_0(\underline{m}), \ldots, e_{p-1}(\underline{m})\big)$ pour une permutation $\sigma \in \mathfrak{S}_p$ et une partition $\underline{m}$ d'un multiple de p à p parts, ce qui donnerait une autre preuve du théorème.

XLIM UMR 6172 CNRS / UNIVERSITÉ DE LIMOGES — Faculté des Sciences et Techniques de Limoges, 123 avenue Albert Thomas, 87060 Limoges cedex, France — http://www.unilim.fr/pages_perso/stephane.vinatier/

(3) Trouvez-la ! (Directement, ou à l'aide de ce qui suit.)