# DM1 - Résultant et théorème de Wedderburn

L. Tintinaglia

Ce devoir est votre premier devoir à me rendre. Il n'y a aucune obligation, mais je vous demande d'essayer de faire le maximum de ce devoir.
Avoir une copie supplémentaire corrigée est un avantage supplémentaire pour identifier ses erreurs, lacunes et s'améliorer en vue des concours.
Vous pouvez évidemment vous aider entre vous, mais il est inutile de se copier... Ce devoir sera noté, mais la note est indicative (elle ne compte pas dans votre moyenne, c'est juste pour vous donner un repère).
La difficulté de chaque partie est indiquée (entre ⋆ et ⋆⋆⋆), mais cela ne doit pas vous freiner : essayez ! Vous ne perdez rien, et avez tout à gagner à vous confronter à quelque chose de plus difficile.

## Pendant les congés

- ◁ Apprenez votre cours et surtout les **démonstrations**. Inutile de les apprendre par coeur, il suffit de se rappeler de l'idée générale ; en vue de l'interro de la rentrée et des colles de la première semaine. Si vous vous sentez en difficulté, révisez en priorité le cours de première année, puis les parties ⋆⋆⋆⋆ et ⋆⋆⋆. Si au contraire vous vous sentez à l'aise, lisez et travaillez les paragraphes que je n'ai pas fait en classe (⋆). Maîtriser ces exercices classiques que je mets dans le cours permet de se forger une intuition pour résoudre ceux qui sont plus difficiles : il ne s'agit pas d'apprendre par coeur ou de bachoter, seulement de retenir les idées de résolution.
- ◁ Ensuite, entraînez vous sur le TD, faites d'abord les exercices ⋆ puis ⋆⋆ et éventuellement ⋆⋆⋆.
  N'hésitez pas à me poser des questions par mail : *luigi.tintinaglia@polytechnique.edu*
- ◁ Enfin, entraînez vous sur ce devoir. Faites vous confiance !

Evidemment, reposez-vous ; il vaut mieux revenir en forme à la rentrée en n'ayant pas fini le DM, que revenir fatigué. Les 6 semaines suivantes avant les congés de Noël seront intenses (colles, DM, DS, ...).

# I) Problème 1 - Résultant de polynômes

Dans tout ce problème, $\mathbb{K}$ désigne un corps commutatif quelconque.

Soient $m$, $n$ deux entiers naturels non-nuls. Si $P(X) = \sum_{i=0}^{n} a_i X^i$ et $Q(X) = \sum_{j=0}^{m} b_j X^j$ sont

deux éléments de $\mathbb{K}[X]$ de degrés respectifs $n$ et $m$, on appelle le **résultant de $P$ et $Q$**, noté $\mathrm{Res}_{\mathbb{K}}(P,Q)$ (ou bien $\mathrm{Res}(P,Q)$ si aucune confusion n'est possible) le déterminant de la matrice carré à coefficients dans $\mathbb{K}$ de taille $(n+m, n+m)$ :

$$\begin{vmatrix}
a_0 & 0 & \cdots & \cdots & 0 & b_0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 & 0 \\
a_1 & a_0 & \ddots & & & b_1 & \ddots & \ddots & & & & \vdots & \vdots \\
\vdots & \ddots & \ddots & \ddots & & \vdots & \ddots & \ddots & \ddots & & & \vdots & \vdots \\
\vdots & & \ddots & \ddots & 0 & \vdots & & \ddots & \ddots & \ddots & & \vdots & \vdots \\
\vdots & & & \ddots & a_0 & b_{m-1} & & & \ddots & \ddots & \ddots & \vdots & \vdots \\
\vdots & & & & a_1 & b_m & & & & \ddots & \ddots & 0 & \vdots \\
\vdots & & & & \vdots & 0 & \ddots & & & & \ddots & b_0 & 0 \\
a_{n-1} & a_{n-2} & \cdots & \cdots & a_{n-m} & \vdots & \ddots & \ddots & & & & b_1 & b_0 \\
a_n & a_{n-1} & & & \vdots & \vdots & & \ddots & \ddots & & & b_2 & b_1 \\
0 & \ddots & & & \vdots & \vdots & & & \ddots & \ddots & & \vdots & \vdots \\
\vdots & \ddots & \ddots & & \vdots & \vdots & & & & \ddots & \ddots & \vdots & \vdots \\
\vdots & & \ddots & \ddots & \vdots & \vdots & & & & & \ddots & b_m & b_{m-1} \\
0 & \cdots & \cdots & 0 & a_n & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & b_m
\end{vmatrix}$$

La matrice dont le résultant est le déterminant est appelée *résultante*. On la notera $R(P,Q)$. Ses $m$ premières colonnes contiennent les coefficients de $P$ (décalés vers le bas à chaque colonne) ; les $n$ colonnes suivantes contienne tles coefficients de $Q$ (décalés vers le bas à chaque colonne).
Par exemple si $P = 1 - 2X + 5X^2 + 4X^3$ et $Q = -1 + 3X + 2X^2$,

$$\mathrm{Res} = \begin{vmatrix}
1 & 0 & -1 & 0 & 0 \\
-2 & 1 & 3 & -1 & 0 \\
5 & -2 & 2 & 3 & -1 \\
4 & 5 & 0 & 2 & 3 \\
0 & 4 & 0 & 0 & 2
\end{vmatrix}$$

Enfin, si $A$ est un sous-anneau de $\mathbb{K}$, on notera $A[X]$ le sous-anneau de l'anneau des polynômes $\mathbb{K}[X]$, constitué des polynômes dont tous les coefficients sont dans $A$.

## A) Résultats préliminaires ⋆

Soit $A$ un sous-anneau d'un corps commutatif $k$.

1. Vérifier que $A[X]$ est bien un sous-anneau de $k[X]$.
2. Montrer que si $P, Q$ sont deux éléments de $A[X]$, $\mathrm{Res}_k(P,Q)$ est un élément de $A$.
3. On se place dans le cas particulier $A = \mathbb{K}[X]$ et $k = \mathbb{K}(X)$ avec $\mathbb{K}$ un corps. On considère donc $\mathbb{K}[X][Y]$ le sous-anneau de l'anneau $\mathbb{K}(X)[Y]$ des polynômes sur le corps des fractions rationnelles $\mathbb{K}(X)$. Montrer que tout élément $P$ de $\mathbb{K}[X][Y]$ s'écrit de façon unique sous la forme $P(X,Y) = \sum_{i,j\geqslant 0} a_{i,j}X^iY^j$ avec $a_{i,j} \in \mathbb{K}$ nul sauf pour un nombre fini de couples $(i,j)$.
4. En déduire que si $P \neq 0$ est un élément de $k[X][Y]$ s'écrivant comme ci-dessus, alors le nombre $d(P) = \max\{i+j, a_{i,j} \neq 0\}$ est un entier naturel bien défini, appelé degré total de $P$.

## B) Propriété fondamentale du résultant ⋆

Soient $P(X) = \sum_{i=0}^{n} a_iX^i$ et $Q(X) = \sum_{j=0}^{m} b_jX^j$ deux polynômes de $\mathbb{K}[X]$ de degrés $n$ et $m$.

1. Montrer que les polynômes $P$ et $Q$ ne sont pas premiers entre eux dans $\mathbb{K}[X]$ *si et seulement si* il existe deux polynômes $A$ et $B$ non-nuls de $\mathbb{K}[X]$, de degrés $\deg A < m$ et $\deg B < n$ tels que $AP = BQ$.

On note $\mathbb{K}_d[X]$ le sous-espace vectoriel de $\mathbb{K}[X]$ constitué des polynômes de degré inférieur ou égal à $d$.
On pose $\phi$ l'application

$$\phi : \begin{cases} E = \mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X] & \longrightarrow & \mathbb{K}_{m+n-1}[X] \\ (A,B) & \longmapsto & AP+BQ \end{cases}$$

2. Montrer que $\phi$ est une application linéaire.
3. On note $\mathfrak{B} = ((1,0),(X,0),\ldots,(X^{m-1},0),(0,1),(0,X),\ldots,(0,X^{n-1}))$ base de $E$. Quelle est la matrice de $\phi$ dans les bases $\mathfrak{B}$ et $\mathfrak{B}_0$ (la base canonique de $\mathbb{K}_{m+n-1}[X]$) si $\phi$ est bijective.
4. En déduire que $P$ et $Q$ sont premiers entre eux dans $\mathbb{K}[X]$ *si et seulement si* $\mathrm{Res}_{\mathbb{K}}(P,Q) \neq 0$.

## C) Autres expressions du résultant ⋆⋆

1. Que vaut $\mathrm{Res}(\alpha, Q)$ pour $\alpha \in \mathbb{K}^*$ ?
2. Relier $\mathrm{Res}(P,Q)$ et $\mathrm{Res}(Q,P)$.
3. On suppose les deux polynômes scindés : $P = \alpha\prod_{i=1}^{n}(X-\lambda_i)$ et $Q = \beta\prod_{j=1}^{m}(X-\mu_j)$.

   Montrer que

$$\mathrm{Res}(P,Q) = \beta^m\prod_{j=1}^{n}P(\mu_j) = \alpha^n\beta^m\prod_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}}(\mu_j-\lambda_i)$$

4. Montrer que pour tout $\lambda \neq 0$, on a :

$$\text{Res}\left(\lambda^n P\left(\frac{X}{\lambda}\right), \lambda^Q\left(\frac{X}{\lambda}\right)\right) = \lambda^{mn}\text{Res}_{\mathbb{C}}(P(X), Q(X))$$

## D) Entiers algébriques ⋆⋆

On note $\mathcal{O}$ l'ensemble des nombres complexes $z$ pour lesquels il existe un polynôme non-nul $P \in \mathbb{Z}[X]$ (l'anneau des polynômes à coefficients dans $\mathbb{Z}$), qui soit *unitaire*), et vérifiant $P(z) = 0$.

1. Soient $z_1$ et $z_2$ des éléments de $\mathcal{O}$, annulant les polynômes $P_1$ et $P_2$ de degrés respectifs $n_1$ et $n_2$. Montrer que le polynôme (en $X$)

$$R(X) = \text{Res}_{\mathbb{Q}(X)}(P_1(X - Y), P_2(Y))$$

est un élément de $\mathbb{Z}[X]$, unitaire de degré $n_1 n_2$.

2. Montrer que $R$ annule la somme $z_1 + z_2$.
3. Procéder de même pour trouver un polynôme de $\mathbb{Z}[X]$ qui annule $z_1 z_2$.
4. En déduire que $\mathcal{O}$ est un sous-anneau de $\mathbb{C}$.
5. Déterminer un polynôme à coefficients entiers de degré 4 ayant pour racine $\sqrt{3} + \sqrt{7}$. Quelles sont les autres racines de ce polynôme ?

# II) Problème 2 - Théorème de WEDDERBURN

## A) Action d'un groupe sur un ensemble ⋆⋆

Soit $X$ un ensemble fini non-vide et $G$ un groupe. On considère une action du groupe $G$ sur l'ensemble $X$ *id est*un morphisme de groupes de $G$ vers l'ensemble des permutations de $X$ :

$$\rho : \begin{cases} G & \longrightarrow & \mathfrak{S}(X) \\ g & \longmapsto & \rho_g \end{cases}$$

On définit une relation sur $X$ : pour tout $(a, b) \in X^2$, $a \sim b$ *si et seulement si* il existe $g \in G$ tel que $b = \rho_g(a)$.

1. Montrer que l'on définit ainsi une relation d'équivalence.
Pour tout $a \in X$, on appelle orbite de $a$, $\text{Orb}(a)$ la classe d'équivalence de $a$ pour cette relation.
2. Soit $a \in X$. On appelle stabilisateur de $X$ : $\text{Stab}(a) = \{g \in G, \rho_g(a) = a\}$. Montrer qu'il s'agit d'un sous-groupe de $G$.
3. Soit $a \in G$. Soit $b \in \text{Orb}(a)$. Soit $h \in G$ tel que $b = \rho_h(a)$. Montrer que $\text{Stab}(b) = h\text{Stab}(a)h^{-1}$.
4. Montrer que pour tout $a \in X$, $|\text{Stab}(a)||\text{Orb}(a)| = |G|$.
5. On note $O = \{\text{Orb}(a), a \in G\} = \{\text{Orb}(a_j), 1 \leqslant j \leqslant N\}$, avec $N = |O|$ (en choisissant des représentants $(a_j)$). Montrer que $|X| = \sum_{j=1}^{N} \frac{|G|}{|\text{Stab}(a_j)|}$.

6. *Formule de* BURNSIDE. En dénombrant de deux manières différentes $\{(g,x) \in G \times X, \rho_g(x) = x\}$, montrer que le nombre d'orbites vaut :

$$N = |O| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

où $\mathrm{Fix}(g) = \{x \in X, \rho_g(x) = x\}$.

## B) Application à l'études de groupes ⋆⋆⋆

1. Expliquer le groupe symétrique $\mathfrak{S}_n$ agit naturellement sur $[\![1\,,n]\!]$.
2. Montrer que tout groupe $G$ agit sur lui-même par translation à gauche en posant pour $g \in G$, $\rho_g : x \in G \longmapsto gx$. En déduire que si $G$ a pour cardinal $n$, $G$ est isomorphe à un sous-groupe de $\mathfrak{S}_n$.
3. Montrer que tout groupe $G$ agit sur lui-même par conjugaison en posant pour $g \in G$, $\rho_g : x \in G \longmapsto gxg^{-1}$.
4. On appelle centre d'un groupe $Z(G)$ l'ensemble des éléments qui commutent avec tous les autres. Vérifier qu'il s'agit d'un sous-groupe de $G$.
5. Soit $p$ premier. En faisant agir le groupe $G$ sur lui-même par conjugaison, montrer que le centre d'un $p$-groupe (*id est*d'un groupe de cardinal $p^d$) n'est jamais trivial.
6. On considère un groupe de cardinal $p^2$. On suppose qu'il n'est pas abélien. En considérant un élément $a \in G \backslash Z(G)$ et en étudiant son stabilisateur (pour l'action par conjugaison), aboutir à une contradiction. Et en déduire que tout groupe de cardinal $p^2$ est abélien.

## C) Démonstration du théorème ⋆⋆⋆

**Théorème II.C.1: WEDDERBURN**

Tout corps fini est commutatif.

Soit $(\mathbb{K}, +, .)$ un anneau vérifiant toutes les hypothèses d'un corps sauf la commutativité de la multiplication. On le suppose fini (de cardinal $q \geqslant 3$).
Notons $Z = \{z \in \mathbb{K}, \forall x \in \mathbb{K}, z.x = x.z\}$. On souhaite montrer que $Z = \mathbb{K}$.

1. Montrer que $Z$ est un sous-anneau de $\mathbb{K}$, et que $Z$ est un corps commutatif (*id est*un corps au sens du cours).
2. En déduire que $\mathbb{K}$ peut être muni d'une structure d'espace vectoriel sur $Z$ ; et que donc si $p = |Z|$, le cardinal de $\mathbb{K}$ est de la forme $q = p^n$ avec $n \geqslant 1$. On souhaite montrer que $n = 1$.
3. Pour tout $a \in \mathbb{K}$, notons $Z_a = \{g \in \mathbb{K}, ga = ag\}$ (le normalisateur de $a$). Expliquer que $Z_a$ est un $Z$-sous espace vectoriel de $\mathbb{K}$ et donc qu'il existe $d_a \geqslant 1$ tel que $|Z_a| = p^{d_a}$.

Par ailleurs $G = (\mathbb{K}^*, +)$ est un groupe fini de cardinal $q - 1$. On fait agir $G$ sur lui-même par conjugaison : pour tout $a \in G$, pour tout $g \in G$, $\rho_g(a) = gag^{-1}$.

4. Expliquer qu'il s'agit bien d'une action de groupe.

On obtient ainsi la relation d'équivalence sur $\mathbb{K}^* = G$ :

$$\forall (a,b) \in G^2, a \sim b \iff \exists g \in G, b = gag^{-1}$$

Pour tout $a \in G$, on note $\tilde{a} = \text{Orb}(a)$ la classe d'équivalence de $a$ et $\tilde{G}$ l'ensemble des classes d'équivalence.

5. Pour tout $a \in G$, expliquer que $\text{Stab}(a) = Z_a^* = Z_a \backslash \{0\}$. On notera $H_a$ ce sous-groupe de $G$. Donner $|H_a|$, puis $|\text{Orb}(a)|$.
6. Dans le cas où $a \in Z^*$, donner $Z_a$, $H_a$ et $\tilde{a}$.
7. Dans le cas général, comme $|H_a| \mid |G|$ (on admettra le théroème de LAGRANGE : le cardinal d'un sous-groupe divise celui du groupe), en déduire que $d_a \mid n$ ; expliquer que si $a \notin Z^*$, $d_a \neq n$.
8. Expliquer que $|G| = \displaystyle\sum_{a \in G} |\tilde{a}| = |Z^*| + \sum_{\tilde{a} \in \tilde{G}, a \notin Z^*} |\tilde{a}|$, et donc que :

$$p^n - 1 = p - 1 + \sum_{\tilde{a} \in \tilde{G}, z \notin Z^*} \frac{p^n - 1}{p^{d_a} - 1}$$

On note $\Phi_n$ le $n$-ième polynôme cyclotomique

$$\Phi_n = \prod_{\omega \in \mathbb{V}_n} (X - \omega)$$

où $\mathbb{V}_n$ sont les racines primitives $n$-ièmes de l'unité. On admet la proposition suivante :

$$X^n - 1 = \prod_{d \mid n} \Phi_d$$

9. Par l'absurde, si $n > 1$, montrer que $\Phi_n(p) \mid (p-1)$. Expliquer nécessairement que $p \geqslant 2$ et que l'on aboutit à une contradiction.
10. Conclure.