Fiche 1 exerce 1 : Discriminant

Soit $P = z^3 + pz + q = (z - z_1)(z - z_2)(z - z_3)$. On pose :

$$\Delta = (z_1 - z_2)^2(z_2 - z_3)^3(z_1 - z_3)^2 \ .$$

C'est le discriminant de P.

On a :

$$\begin{aligned}\Delta &= -P'(z_1)P'(z_2)P'(z_3)\\ &= -(3z_1^2 + p)(3z_2^2 + p)(3z_3^2 + p)\\ &= -27(z_1z_2z_3)^2 - 9(z_1^2z_2^2 + z_2^2z_3^2 + z_1^2z_3^2)p - 3(z_1^2 + z_2^2 + z_3^2)p^2 - p^3\\ &= -27q^2 - 9(p^2 + 2q(z_1 + z_2 + z_3))p - 3((z_1 + z_2 + z_3)^2 - 2p)p^2 - p^3\\ &= -27q^2 - 4p^3 \ .\end{aligned}$$

Si $p, q \in \mathbb{R}$ et si $\Delta > 0$, c'est le *casus irreducibilis* :

les trois racines sont réelles mais s'expriment avec des radicaux de nombres complexes non réelles.

Par exemple, les trois racines de

$$z^3 - 3z + 1 = 0$$

sont :

$$2\cos\frac{2\pi}{9},\ 2\cos\frac{4\pi}{9},\ 2\cos\frac{8\pi}{9}$$

et par exemple :

$$2\cos\frac{2\pi}{9} = \sqrt[3]{j} + \sqrt[3]{j^2}$$

pour certaines racines cubiques de j et j^2.

Fiche 1 exercice 2 : Méthode de Lagrange

Soient z_1, z_2, z_3 les trois racines du polynôme $z^3 + pz + q$.

On pose $A := (z_1 + jz_2 + j^2z_3)^3$, $B := (z_1 + j^2z_2 + jz_3)^3$.

On a :

$$A+B = 2(z_1^3+z_2^3+z_3^3)-3(z_1z_2(z_1+z_2)+z_2z_3(z_2+z_3)+z_3z_1(z_3+z_1))+12z_1z_2z_3$$

Posons :

$$s_1 := z_1 + z_2 + z_3,\ s_2 := z_1z_2 + z_2z_3 + z_1z_3,\ s_3 := z_1z_2z_3$$

on a :

$$s_1 = 0,\ s_2 = p,\ s_3 = -q \ .$$

On a donc :

$$A + B = 2(s_1^3 - 3s_1s_2 + 3s_3) - 3(s_1s_2 - 3s_3) + 12s_3$$
$$= -27q \ .$$

On a aussi :

$$AB = -27p^3$$

car :

$$(z_1 + jz_2 + j^2z_3)(z_1 + j^2z_2 + jz_3) = -3p \ .$$

Donc A, B sont les racines du polynôme :

$$X^2 + 27qX - 27p^3 \ .$$

On a donc :

$$\begin{cases} z_1 + z_2 + z_3 & = & 0 \ \ (l1) \\ z_1 + jz_2 + j^2z_3 & = & u \ \ (l2) \\ z_1 + j^2z_2 + jz_3 & = & v \ \ (l3) \end{cases}$$

où u est une racine cubique de A et v la racine cubique de B telle que $uv = -3p$.

Le système ci-dessus se résout par exemple avec les opérations suivantes sur les lignes : $l1 + l2 + l3$, $l1 + jl2 + j^2l3$, $l1 + j^2l2 + jl3$. On obtient :

$$\begin{cases} z_1 = \frac{u+v}{3} \\ z_2 = \frac{j^2u+jv}{3} \\ z_3 = \frac{ju+j^2v}{3} \end{cases} \ .$$

Fiche 2 exercice 1

Soit $\mathbb{H}$ l'algèbre des quaternions sur $\mathbb{R}$. C'est l'algèbre des matrices complexes de la forme :

$$\begin{pmatrix} a & -b \\ \overline{b} & \overline{a} \end{pmatrix}$$

où $a, b \in \mathbb{C}$. On a $\mathbb{H} = \mathbb{R}e + \mathbb{R}I + \mathbb{R}J + \mathbb{R}K$ si on note :

$$e := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ I := \begin{pmatrix} i & \\ & -i \end{pmatrix} \ J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \ .$$

L'algèbre $\mathbb{H}$ n'est pas commutative et tous ses éléments non nuls sont inversibles (on dit que c'est une *algèbre à divisions* ou un *corps gauche*.

Dans un corps commutatif une équation polynomiale de degré $n > 0$ a au plus n racines. Ce n'est plus vrai sur une algèbre à divisions ! Par exemple l'équation $X^2 = -1$ a une infinité de solutions dans $\mathbb{H}$ puisque si $x_0, x_1, x_2, x_3 \in \mathbb{R}$, on a :

$$(x_0 e + x_1 I + x_J + x_3 K)^2 = -1 \Leftrightarrow x_0 = 0 \text{ et } x_1^2 + x_2^2 + x_3^2 = 1$$

(c'est l'équation d'une sphère réelle de dimension 2).

Fiche 2 exercice 2

Soit G un sous-groupe fini d'un $k^\times := k\backslash\{0\}$ où k est un corps commutatif. Soit n l'ordre de G. On note N_d le nombre d'éléments de G d'ordre d. (On dit que g est d'ordre d si d est le plus petit entier > 0 tel que $g^d = 1$).

Tout élément de G a un ordre qui divise n. Donc :

$$\sum_{d|n} N_d = n \ .$$

Soit $\varphi(d) :=$ le nombre d'entiers $1 \leq k \leq d$ premiers à d (c'est *l'indicateur d'Euler*).

En comptant de deux façons le nombre d'éléments de l'ensemble :

$$\left\{\frac{1}{n}, ..., \frac{n-1}{n}, \frac{n}{n}\right\} ,$$

on voit que :

$$\sum_{d|n} \varphi(d) = n \ .$$

Montrons que pour tout d, $N_d \leq \varphi(d)$.

Si G n'a pas d'élément d'ordre d, c'est évident. Sinon, il existe $g \in G$ d'ordre d. On a alors :

$$(g^k)^d = 1$$

pour tout $1 \leq k \leq d$. Cela fait au moins d solutions :

$$g, g^2, ..., g^d$$

à l'équation $X^d = 1$ dans le corps k. Cette équation a au plus d solutions puisqu'on est dans un corps.

Donc les éléments $x \in k^\times$ tels que $x^d = 1$ sont exactement les g^k. En particulier, les éléments de G d'ordre d sont de la forme :

$$g^k$$

avec $1 \leq k \leq d$. Or, comme g est d'ordre d, on voit facilement que l'ordre de g^k est $\frac{d}{\text{pgcd}(k,d)}$. Donc les éléments de G d'ordre d sont les g^k avec $1 \leq k \leq d$ et k premier à d. Cela fait $\varphi(d)$ éléments.

En résumé, dans tous les cas, $N_d \leq \varphi(d)$.

Or :

$$n = \sum_{d|n} \varphi(d) = \sum_{d|n} N_d$$

$$\Rightarrow \sum_{d|n} \underbrace{\varphi(d) - N_d}_{\geq 0} = 0$$

donc forcément $N_d = \varphi(d)$ pour tout d. En particulier, $N_n = \varphi(n) > 0$ et G possède au moins un élément d'ordre n *i.e.* G est cyclique.

En particulier si k est un corps fini, alors $k^\times$ est cyclique.

Fiche 2 exercice 3 Soient $k \subseteq K$ deux corps. Soit $z \in K$. Montrons que i),ii),iii) sont équivalentes :

i) l'algèbre $k[z]$ est un corps ;

ii) il existe un polynôme non nul $P \in k[T]$ qui annule z ;

iii) le $k-$espace vectoriel $k[z]$ est de dimension finie.

i) $\Rightarrow$ ii) : le morphisme d'anneaux $k[T] \to k[z]$, $a_0 + ... + a_n T^n \mapsto a_0 + ... + a_n z^n$ est surjectif de noyau l'idéal $I = \{P \in k[T] \ : \ P(z) = 0\}$.

Donc $k[T]/I \simeq k[z]$. En particulier, si $k[z]$ est un corps, I est un idéal maximal de $k[T]$ et donc $I \neq 0$.

ii) $\Rightarrow$ iii) : Supposons que $P(z) = 0$ pour un certain $0 \neq P \in k[T]$. Si $f \in k[T]$, alors $f = PQ + r$ pour des polynômes $Q, r \in k[T]$ avec $\deg r < \deg P$. On a alors $f(z) = P(z)Q(z) + r(z) = r(z)$. Donc l'espace $k[z]$ est engendré par $1, z, ..., z^{\deg P - 1}$ et $k[z]$ est de dimension finie.

iii) $\Rightarrow$ i) : Supposons que l'espace $k[z]$ est de dimension finie. Soit $0 \neq f \in k[z]$. L'endomorphisme :

$$k[z] \to k[z] \ , \ g \mapsto fg$$

est injectif car $k[z] \subseteq K$ et K est un corps. Comme on est en dimension finie, cet endomorphisme est aussi surjectif. En particulier, il existe $g \in k[z]$ tel que $fg = 1$. Ainsi $k[z]$ est un corps.

*

Plus généralement si $x_1, ..., x_n \in K$ et si l'algèbre engendrée $k[x_1, ..., x_n]$ est un corps, alors tous les x_i sont algébriques sur k (mais c'est plus difficile à démontrer). C'est une version du célèbre théorème des zéros de Hilbert.