Arithmétique des polynômes.

1 Divise, pgcd, Bezout.

1.1 Divise

Définition 1.
Soit A, B deux polynômes.

On dit que le polynôme B divise le polynôme A le polynôme P

Ssi il existe une polynôme Q tel que $A = B.Q$

On note $div_+(A)$ l'ensemble des diviseur `unitaire` de $A(X)$

Exemple : Soit le polynômes $A = A(X) = 2(X-1)(X-2)^2$

$$\text{Ainsi } div_+(A) = \left\{ 1\,,\ \underbrace{(X-1)\,,\ (X-2)}_{\textit{Les poly de degré 1}}\,,\ \underbrace{(X-1)(X-2)\,,\ (X-2)^2}_{\textit{Les poly de degré 2}}\,,\ (X-1)(X-2)^2 \right\}$$
$$= \{1, ..., (X-1)(X-2)^2\}$$

De plus il y a 2 situations particulières $div_+(1) = \{1\}$ et $div_+(\mathscr{O}) = \{$ *Tous les poly unitaires* $\}$

On remarquera que $div_+(K_{\neq 0}) = \{1\}$

Théorème 2. Du bon sens
Soit A et B deux polynômes non-nuls.

On suppose que B divise A, on a alors $A(X) = B(X).Q(X)$ ainsi

> $\deg(B) \leqslant \deg(A)$

> Les racines de B sont aussi des racines de A

et la multiplicité dans B est inférieur à celle dans A.

1.2 pgcd, ppcm.

Définition 3. pgcd, ppcm
Soit A et B deux polynômes.

> D est le Plus Grand Commun Diviseur de A et B, noté $PGCD(A,B)$,

Ssi D le polynôme **unitaire** de plus grand degré qui divise A et qui divise B.

> M est le Plus Petit Commun Multiple de A et B, noté $PPCM(A,B)$,

Ssi M le polynôme **unitaire** de plus petit degré qui est un multiple de A et B.

Théorème 4. Comment calculer le pgcd (et bonus le ppcm)

> Il y a l'algorithme d'Euclide (MAIS pas glop)

> Il y a les factorisations (MAIS glop-glop)

Complément : $PGCD(A,B).PPCM(A,B) = AB$

> Bézout.

Il existe 2 polynômes U, V tel que $D = PGCD(A,B) = AU + BV$

Exemple : Soit le polynômes $A = A(X) = 2(X-1)(X-2)^2$ et $B = B(X) = 3(X-1)^3(X-2)$

2 Polynômes premiers entre eux, Gauss, etc ....

Définition 5. Polynômes premiers entre eux

On dit que le polynômes A et B sont premiers entre eux

Ssi $PGCD(A,B) = 1$

Ssi le seul diviseur **unitaire** commun de A et B, c'est $X^0 = 1$

Propriété de Bézout. Soit A, B deux polynômes.

On suppose que A et B sont premiers entre eux.

Alors (Ssi) il existe 2 polynômes U, V tel que $A(X)\,U(X) + B(X)\,V(X) = 1$

Théorème 6. Racines communes

> A et B n'ont pas de racine commune (dans $\mathbb{C}$)

Alors (Ssi) les polynômes A et B sont premiers entre eux

Complément : r est une racine commune de A et B Ssi r est une racine de $D = PGCD(A,B)$

> *Application classique* :

On sait que : r est une racine multiple (double, triple,...) du poly A

Ssi r est une racine commune de de A et de A'

Ssi r est une solution du système $\left\{\begin{array}{l} A(X) = 0 \\ A'(X) = 0 \end{array}\right.$

Ainsi le poly A n'a pas de racine multiple Ssi A et A' sont premiers entre eux.

Théorème 7. Théorème de Gauss et copain

Soit A, B, C des polynômes.

$$\left.\begin{array}{c} A \text{ divise } BC \\ A \text{ et } B \text{ sont premiers entre eux} \end{array}\right\} \Longrightarrow A \text{ divise } C$$

$$\left.\begin{array}{c} A \text{ divisent } C \text{ et } B \text{ divisent } C \\ A \text{ et } B \text{ sont premiers entre eux} \end{array}\right\} \Longrightarrow AB \text{ divise } C$$

3 Polynômes irréductible et factorisation.

Définition 8. Polynômes irréductible

Soit P un polynôme.

On dit que le polynôme P est irréductible

Ssi | le polynôme P est **unitaire**
| *et*
| P admet exactement 2 diviseurs unitaires : 1 et P, CàD $div_+(P) = \{1, P\}$

Théorème 9. Polynômes irréductibles de $\mathbb{C}[X]$ et factorisation.

> P est un polynôme irréductible de $\mathbb{C}[X]$

Ssi $P = X - r$ avec $r \in \mathbb{C}$

> P est un polynôme irréductible de $\mathbb{R}[X]$

Ssi $P = X - r$ OU $P = X^2 + aX + b$

$= (X - r)(X - \overline{r})$

> Soit A est un polynôme. Je note $n = \deg(A)$

alors A se factorise dans $\mathbb{C}[X]$ en produit de facteurs irréductibles,

CàD $A = a\,(X - r_1)\cdots(X - r_n)$

Pour déterminer la factorisation dans $\mathbb{R}[X]$, on regroupe les facteurs conjuguées.

4 Exercice.

Exercice 1. [Correction] *Calcul à finir.*

Soient $a, b \in \mathbb{R}$ et $P = X^3 - aX + b$ avec $a \geqslant 0$

On a le raisonnement suivant (à finir)

$$\begin{aligned} r \textit{ est une racine double de } P \textit{ dans } \mathbb{R} \text{ Ssi } & \begin{cases} P(r) = 0 \\ P'(r) = 0 \iff 3r^2 - a = 0 \iff r = \pm\sqrt{a/3} \end{cases} \\ & \text{Ssi } r = +\sqrt{a/3} \textit{ ou } r = -\sqrt{a/3} \text{ est une racine de } P \\ & \text{Ssi } P\left(\sqrt{a/3}\right) = 0 \textit{ ou } P\left(-\sqrt{a/3}\right) = 0 \\ & \text{Ssi } P\left(\sqrt{a/3}\right) \times P\left(-\sqrt{a/3}\right) = 0 \end{aligned}$$

Calculer et simplifier $P\left(\sqrt{a/3}\right) \times P\left(-\sqrt{a/3}\right)$

et trouver une condition pour que $P = X^3 - aX + b$ ait une racine double (dans $\mathbb{R}$)

Exercice 2. [Correction] Première partie de CCP-MP 2016

Soit n un entier naturel non nul.

I.1. Soit P et Q deux polynômes non nuls à coefficients complexes.

I.1.a. Démontrer que si P et Q n'ont aucune racine complexe commune, alors P et Q sont premiers entre eux (on pourra raisonner par l'absurde).

I.1.b. On suppose que P et Q sont premiers entre eux.

En utilisant le théorème de Gauss, démontrer que si P et Q divisent un troisième polynôme R à coefficients complexes,

alors il en est de même pour le polynôme PQ.

I.2. Soit $(P_i)_{1 \leqslant i \leqslant n}$ une famille de polynôme non nuls de $\mathbb{R}[X]$. On considère le polynôme $P \in \mathbb{R}[X]$ et la fraction rationnelle $Q \in \mathbb{R}(X)$ définis par $P = \prod_{i=1}^{n} P_i$ et $Q = \dfrac{P'}{P}$.

Démontrer par récurrence que $Q = \sum_{i=1}^{n} \dfrac{P_i'}{P_i}$.

Exercice 3. [Correction]

1. Déterminer la factorisation de $X^3 - 1$ et $X^4 - 1$ dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.
2. Déterminer la factorisation de $X^4 + 1$ dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.
3. Déterminer la factorisation de $X^{2n} - 1$ dans $\mathbb{C}[X]$ puis dans $\mathbb{R}[X]$.

Exercice 4. [Correction] Montrer (à l'aide d'un RA) que le polynôme $P = X^3 + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

Exercice 5. [Correction] *Polynôme scindé (et le retour de Rolle)*

Les questions sont indépendantes

1. Trouver la définition de "Polynôme scindé"
2. Soit $P \in \mathbb{R}[X]$ un polynôme scindé à racines simples dans $\mathbb{R}$

   Montrer que pour tout $a \in \mathbb{R}^*$, les racines de $P^2 + a^2$ dans $\mathbb{C}$ sont toutes simples.
3. (difficile) Soit $P \in \mathbb{R}[X]$ un polynôme scindé sur $\mathbb{R}$

   Montrer que pour tout réel a, le polynôme $P' + aP$ est scindé sur $\mathbb{R}$.

   Indication/Remarqua : $P' + aP$ n'est pas une dérivée mais presque.

Correction.

Solution de l'exercice 1 (Énoncé) Le polynôme $P = X^3 - aX + b$ a une racine double (dans $\mathbb{R}$) Ssi $-4a^3 + 27b^2 = 0$

Solution de l'exercice 2 (Énoncé)

I.1. Soit P et Q deux polynômes non nuls à coefficients complexes.

I.1.a. C'est du cours

I.1.b. C'est du cours

I.2. par récurrence

Solution de l'exercice 3 (Énoncé) On a

$$X^3 - 1 = 1(X-1)\underbrace{(X-j)(X-j^2)}_{\text{facteur conjugué}} = (X-1)(X^2+X+1)$$

$$\begin{aligned} X^4 - 1 &= 1(X-1)(X-i)(X+1)(X+i) \\ &= (X-1)(X+1)\underbrace{(X-i)(X+i)}_{\text{facteur conjugué}} = (X-1)(X+1)(X^2+1) \end{aligned}$$

$$\begin{aligned} X^4 + 1 &= 1(X-z_0)(X-z_1)(X-z_2)(X-z_3) \\ &= \underbrace{(X-z_0)(X-z_3)}_{\text{facteur conjugué}}\underbrace{(X-z_1)(X-z_2)}_{\text{facteur conjugué}} \\ &= \left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right) \end{aligned}$$

$$\begin{aligned} X^{2n} - 1 &= 1\prod_{k=0}^{2n-1}(X - w_k) \\ &= (X-1)(X+1)\prod_{k=0}^{n-1}\left(X^2 - 2\cos(\ldots.)X + 1\right) \end{aligned}$$

Solution de l'exercice 4 (Énoncé)

On fait un RA. On suppose : le polynôme $P = X^3 + X + 1$ n'est pas irréductible dans $\mathbb{Q}[X]$.

> Comme P n'est pas irréductible dans $\mathbb{Q}[X]$,

il est possible de le factoriser comme produit de deux polynômes *non constants* à coefficients dans $\mathbb{Q}$.

L'un d'eux est de degré 1, CàD dire de la forme $aX + b = a(X - r)$, ainsi le polynôme P admet une racine $r \in \mathbb{Q}$

On traduit $r \in \mathbb{Q}$ sous forme d'une fraction *irréductible* $r = {}^{p}/_{q}$

> l'égalité $P(r) = 0$ devient, après réduction au même dénominateur, $p^3 + pq^2 + q^3 = 0$

- Or p divise $p^3 + pq^2$ donc p divise $-q^3$

Or p et q sont premiers entre donc (théorème de Gauss) p divise -1 donc $p = \pm 1$

- De même q divise $q^3 + pq^2$ donc q divise $-p^3$

Or p et q sont premiers entre donc (théorème de Gauss) q divise -1 donc $q = \pm 1$

> Conclusion $r = {}^{p}/_{q}$ est égale à 1 ou -1

Or $P(1) = 3 \neq 0$ et $P(-1) = -1 \neq 0$ Oups

Solution de l'exercice 5 (Énoncé)

1. Voir internet
2. Le théorème de Rolle assure que les racines de P' sont réelles (et simples)
   Les racines multiples de $P^2 + a^2$ sont aussi racines de $\left[P^2 + a^2\right]' = 2PP'$.
   Or les racines de $P^2 + a^2$ ne peuvent être réelles et les racines de PP' sont toutes réelles.
   Conclusion : Il n'y a donc pas de racines multiples au polynôme $P^2 + a^2$.
   Montrer que pour tout $a \in \mathbb{R}^*$, les racines de $P^2 + a^2$ dans $\mathbb{C}$ sont toutes simples.
3. On note $f(x) = P(x)e^{ax}$ et on remarque que $f'(x) = [P(x)e^{ax}]' = \left(P'(x) + aP(x)\right)e^{ax}$.
   De plus Comme l'exponentielle ne s'annule pas,
   on a $f(X) = 0 \iff P(X) = 0$ et $f'(X) = 0 \iff P'(X) + aP(X) = 0$.
   Comme P est scindé sur $\mathbb{R}$, il admet exactement n racine distincte ou confondu dans R, *avec* $\deg(P) = n$ ainsi f n'annule n fois (avec multiplicité) dans R
   On applique Rolle ainsi f n'annule $n-1$ fois (avec multiplicité) dans R.
   Ainsi $P'(X) + aP(X) = 0$ admet $n-1$ racines dans R.
   On justifie que la dernière racine (car $\deg(P' - aP) = n$) est dans $\mathbb{R}$ avec le lien coef racine