Introduction et construction du corps $\mathbb{C}$ des complexes. Propriétés.

Pré-requis:

- ◇ Définition de l'anneau $\mathbb{R}[X]$ des polynômes à coefficients réels.
- ◇ Connaissance de la division euclidienne des polynômes: Pour tout couple (P, P') de $\mathbb{R}[X]$ tel que P' soit unitaire (le monôme de plus haut degré est 1), alors il existe un unique couple (Q, R) de $\mathbb{R}[X]$ vérifiant:

$$P = QP' + R, \quad \text{avec } \mathrm{d}^\circ R \leq \mathrm{d}^\circ P'.$$

  On dira que Q est le quotient et R le reste de la division de P par P'.
- ◇ Définition d'un groupe quotient et toutes les notions sous-jacentes à celle-ci (relation d'équivalence, classe d'equivalence, ensemble quotient, sytème de représentants)

0.1 Construction de $\mathbb{C}$.

Soit $M(X) = 1 + X^2 \in \mathbb{R}[X]$, remarquons immédiatement que le choix de ce polynôme n'est pas anodin puisqu'on ne peut pas l'écrire comme produit de deux polynômes du premier degré à coefficients dans $\mathbb{R}$ (en effet, l'équation $M(X) = 0$ n'a pas de solution dans $\mathbb{R}$).

Proposition 0.1.1.
La relation définie sur $\mathbb{R}[X]$ par: $\forall (P, P') \in \mathbb{R}[X] \times \mathbb{R}[X]$,

$$P \mathcal{R} P' \Leftrightarrow (X^2+1) | (P'(X) - P(X))$$

est une relation d'équivalence.

Démonstration.

– $\forall P \in \mathbb{R}[X]$,

$$P \mathcal{R} P \Leftrightarrow (X^2+1) | 0$$

ce qui est toujours vrai.

– $\forall (P, Q) \in \mathbb{R}[X]^2$,

$$P \mathcal{R} Q \Leftrightarrow (X^2+1) | (P - Q)(X)$$

, c'est-à-dire qu'il existe $R \in \mathbb{R}[X]$ tel que $P(X) - Q(X) = R(X)(X^2+1)$, soit encore $Q(X) - P(X) = -R(X)(X^2+1)$ d'où $(X^2+1) | (Q - P)(X)$. Donc

$$P \mathcal{R} Q \Leftrightarrow Q \mathcal{R} P.$$

– $\forall (P, Q, R) \in \mathbb{R}[X]^3$,

$$\begin{cases} P \mathcal{R} Q \\ Q \mathcal{R} R \end{cases} \Leftrightarrow \begin{cases} (X^2+1) | (P - Q)(X) \\ (X^2+1) | (Q - R)(X) \end{cases},$$

donc $(X^2+1) | (P - Q + Q - R)(X) = (P - R)(X)$ c'est-à-dire $P \mathcal{R} R$.

■

Notation: On note cette relation

$$P \equiv P' \ [X^2+1]$$

et on dit que P est congru à P' modulo X^2+1.

Proposition 0.1.2.
La relation de congruence est compatible avec l'addition et la multiplication dans $\mathbb{R}[X]$, c'est-à-dire: Soit $(P,Q,P',Q') \in \mathbb{R}[X]^4$,

$$\text{si} \quad \begin{cases} P \equiv P' \ [X^2+1] \\ Q \equiv Q' \ [X^2+1] \end{cases} \quad \text{alors} \quad \begin{cases} P+Q \equiv P'+Q' \ [X^2+1] \\ PQ \equiv P'Q' \ [X^2+1] \end{cases}$$

Démonstration. Si $P \equiv P' \, [X^2+1]$, alors il existe $R \in \mathbb{R}[X]$ tel que $P(X) = P'(X) + R(X)(X^2+1)$.
Si $Q \equiv Q' \, [X^2+1]$, alors il existe $R' \in \mathbb{R}[X]$ tel que $Q(X) = Q'(X) + R'(X)(X^2+1)$.
Ainsi, $(P+Q)(X) = (P'+Q')(X)+(R+R')(X)(X^2+1)$ c'est-à-dire $P+Q \equiv P'+Q' \, [X^2+1]$ et

$$\begin{aligned} (PQ)(X) &= (P'(X) + R(X)(X^2+1)) \cdot (Q'(X) + R'(X)(X^2+1)) \\ &= (P'Q')(X) + ((P'R')(X) + (Q'R)(X) + (RR')(X)(X^2+1))(X^2+1) \end{aligned}$$

donc $PQ \equiv P'Q' \, [X^2+1]$. ∎

Notations:
- Pour $P \in \mathbb{R}[X]$, on note $Z(P) := \{Q \in \mathbb{R}[X] | Q \equiv P \ [X^2+1]\}$ la classe d'équivalence de P.
- On note $\mathbb{C}$ l'ensemble quotient $\mathbb{R}[X]/(X^2+1) := \{Z(P) | P \in \mathbb{R}[X]\}$

Proposition 0.1.3.
On peut définir sur $\mathbb{C}$ une addition et une multiplication de la façon suivante: $\forall (P,Q) \in \mathbb{C}$, $\exists (R,S) \in \mathbb{R}[X]^2$ tels que $P = Z(R)$ et $Q = Z(S)$, on pose alors

$$P+Q = Z(R) + Z(S) := Z(R+S)$$

et

$$PQ = Z(R) \cdot Z(S) := Z(RS).$$

Démonstration. Montrons que ces deux opérations sont bien définies: prenons R', S' deux autres représentants vérifiant, $P = Z(R) = Z(R')$ et $Q = Z(S) = Z(S')$ alors

$$\begin{cases} R \equiv R' \ [X^2+1] \\ S \equiv S' \ [X^2+1] \end{cases} \implies \begin{cases} R+S \equiv R'+S' \ [X^2+1] \\ RS \equiv R'S' \ [X^2+1] \end{cases}$$

ainsi

$$\begin{cases} Z(R+S) = Z(R'+S') \\ Z(RS) = Z(R'S') \end{cases}.$$

Ainsi on trouve le même résultat pour $P+Q$ et PQ, quels que soient les représentants choisis. ∎

Théorème 0.1.4.
L'ensemble $(\mathbb{C}, +, .)$ est un anneau commutatif.

Démonstration. Avec la définition précédente des opérations, nous avons immédiatement:
- $+$ est commutative, associative sur $\mathbb{C}$ car elle l'est dans $\mathbb{R}[X]$.
- $Z(0)$ est l'élément neutre pour $+$.
- L'opposé de $Z(P)$ est $Z(-P)$.
- $\cdot$ est commutative, associative et distributive par rapport à $+$ sur $\mathbb{C}$ car elle possède ces propriétés dans $\mathbb{R}[X]$.
- $Z(1)$ est l'élément neutre pour $\cdot$.

■

Proposition 0.1.5.
Soient P et Q dans $\mathbb{R}[X]$, alors $P \equiv Q\ [X^2+1]$ si, et seulement si P est Q ont le même reste dans la division euclidienne par X^2+1.

Démonstration.
$\boxed{\Rightarrow}$ Si $P \equiv Q\,[X^2+1]$; effectuons les divisions euclidiennes de P et Q par X^2+1:

$$P(X) = P'(X)(X^2+1) + R(X) \quad \text{avec } 0 \leq \mathrm{d}^\circ R \leq 1$$

et

$$Q(X) = Q'(X)(X^2+1) + R'(X) \quad \text{avec } 0 \leq \mathrm{d}^\circ R' \leq 1.$$

Par hypothèse, il existe $T \in \mathbb{R}[X]$ tel que $(P-Q)(X) = T(X)(X^2+1)$ or

$$(P-Q)(X) = (P'-Q')(X)(X^2+1) + (R-R')(X).$$

Comme $(X^2+1)|(P-Q)(X)$, alors $(X^2+1)|(R-R')(X)$ et donc $\mathrm{d}^\circ(R-R') \geq 2$ ou $R-R'$ est le polynôme nul. Mais $\mathrm{d}^\circ(R-R') \leq 1$ donc $(R-R')(X) \equiv 0$.
$\boxed{\Leftarrow}$ Si $R = R'$, alors $(P-Q)(X) = (P'-Q')(X)(X^2+1)$ et donc $P \equiv Q\,[X^2+1]$.

■

Proposition 0.1.6.
L'ensemble quotient $\mathbb{C}$ admet pour système de représentants $a+bX$ où a et b sont réels. Ainsi,

$$\mathbb{C} = \left\{ Z(a+bX) | (a,b) \in \mathbb{R}^2 \right\}.$$

Démonstration. Soit $P \in \mathbb{R}[X]$, la division euclidienne par X^2+1 nous donne un unique polynôme R de degré inférieur ou égal à 2 tel que $P \equiv R\,[X^2+1]$, c'est-à-dire $P \in Z(R)$. Donc les polynômes de la forme $aX+b$ où a, b sont des réels forment un système de représentants de $\mathbb{C}$. Or, $Z(aX+b) = Z(a)Z(X) + Z(b)$ donc la connaissance de $Z(a)$ pour a réel et $Z(X)$ suffit pour déterminer cette classe, d'où le résultat annoncé. ■

Remarque et notations: On va maintenant identifier la classe du réel a et la classede X. Avec ce qui précède, il est facile de vérifier que l'application $\begin{array}{rccc} f: & \mathbb{R} & \longrightarrow & \mathbb{R}[X]/(X^2+1) \\ & a & \longmapsto & Z(a) \end{array}$ est un homomorphisme d'anneau injectif, et on peut alors identifier $Z(a)$ au réel a.

En effet, pour a, b des réels, $f(a+b) = Z(a+b) = Z(a) + Z(b) = f(a)f(b)$, $f(ab) = Z(ab) = Z(a)Z(b) = f(a)f(b)$ et $f(1) = 1$, donc f est un homomorphisme d'anneau et

$\mathrm{Ker} f = \{a \in \mathbb{R} | f(a) = Z(0)\} = \{0\}$ puisque 0 est le seul réel divisible par X^2+1, ce qui signifie que f est injective.

De plus, un polynôme de $Z(X)$ s'écrit: $P(X) = Q(X)(X^2+1)+X$ où P et Q sont dans $\mathbb{R}[X]$. Donc

$$\begin{aligned}
[Z(X)]^2 &= (Q(X)(X^2+1)+X)\cdot(Q'(X)(X^2+1)+X) \\
&= (Q(X)Q'(X)(X^2+1)+Q(X)X+Q'(X)X)(X^2+1)+X^2 \\
&= (Q(X)Q'(X)(X^2+1)+Q(X)X+Q'(X)X)(X^2+1)+X^2+1-1 \\
&= (Q(X)Q'(X)(X^2+1)+Q(X)X+Q'(X)X+1)(X^2+1)-1 \\
[Z(X)]^2 &= Z(-1)
\end{aligned}$$

Il est alors légitime d'identifier i à $Z(X)$, ainsi tout polynôme $P \in \mathbb{R}[X]$ on peut écrire,

$$Z(P) = a+ib, \quad (a,b) \in \mathbb{R}^2$$

avec $i^2 = -1$. On dira alors que $a+ib$ est un nombre complexe.

Afin de savoir si $\mathbb{C}$ est un corps, nous allons étudier l'inverse d'un tel nombre:

0.2 La conjugaison et le calcul d'inverse.

Définition 0.2.1.
On appelle conjugé du nombre complexe $z = a+ib$, le nombre complexe $\overline{z} = a-ib$.

Remarque: Le passage au conjugué est un isomorphisme d'anneau ($\overline{z+z'} = \overline{z}+\overline{z'}$ et $\overline{zz'} = \overline{z}\cdot\overline{z'}$) involutif.

Propriété 0.2.2.
Pour tout nombre complexe $z = a+ib$, on a

$$z\overline{z} = a^2+b^2.$$

Démonstration.

$$\begin{aligned}
z\overline{z} &= (a+ib)(a-ib) \\
&= a^2 - iab + iab - i^2b^2 \\
&= a^2+b^2
\end{aligned}$$

■

Définition 0.2.3.
Le nombre $\sqrt{a^2+b^2}$ est appelé le module de z et est noté $|z|$.

Conséquence: Si $|z| \neq 0$ (autrement dit si $z \neq 0$), alors

$$\frac{z\overline{z}}{z\overline{z}} = 1 \Leftrightarrow z\cdot\left(\frac{\overline{z}}{|z|^2}\right) = 1.$$

Ainsi tout élément non nul de l'anneau $\mathbb{C}$ est inversible pour la multiplication; $\mathbb{C}$ est donc un corps.

0.3 Propriété algèbrique de $\mathbb{C}$.

Résolution d'une équation du second degré.
Résoudre dans $\mathbb{C}$, pour $(a,b,c) \in \mathbb{C}^3$, $a \neq 0$ l'équation:

$$az^2 + bz + c = 0.$$

Démonstration. Commençons par montrer que:

Lemme 0.3.1.
Soit $a \in \mathbb{C}^*$. L'équation $z^2 = a$ admet deux solutions dans $\mathbb{C}$.

Démonstration. On écrit $z = x + iy$ où x et y sont des réels et $a = b + ic$ où a et b sont des réels. Alors $z^2 = x^2 + 2ixy - y^2$, ainsi $x^2 - y^2 = b$ et $2xy = c$ et en remarquant que $z^2 = a \Leftrightarrow (z\overline{z})^2 = a\overline{a} \Leftrightarrow x^2 + y^2 = \sqrt{b^2 + c^2}$ et en résolvant le sytème de trois équations ainsi trouvé, on trouve les deux solutions souhaitées. ■

$$\begin{aligned}
az^2 + bz + c = 0 &\Leftrightarrow a\left(z^2 + \frac{b}{a}z + \frac{c}{a}\right) = 0 \\
&\Leftrightarrow \left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a} = 0 \\
&\Leftrightarrow \left(z + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2} \quad \text{où } \Delta = b^2 - 4ac \\
&\Leftrightarrow \begin{cases} z + \frac{b}{2a} = \frac{\delta}{2a} \\ z + \frac{b}{2a} = \frac{\delta'}{2a} \\ z + \frac{b}{2a} = 0, \end{cases} \begin{array}{l} , \quad \text{si } \Delta \neq 0 \\ \\ \quad \text{si } \Delta = 0 \end{array}
\end{aligned}$$

où δ et δ' sont les solutions de l'équation $z^2 = \Delta$.

$$az^2 + bz + c = 0 \Leftrightarrow \begin{cases} z = \frac{-b+\delta}{2a} \\ z = \frac{-b+\delta'}{2a} \\ z = -\frac{b}{2a}, \end{cases} \begin{array}{l} , \quad \text{si } \Delta \neq 0 \\ \\ \quad \text{si } \Delta = 0 \end{array}$$

■

Remarque: En particulier, toute équation du second degré à coefficients réels n'ayant pas de racines réelles admet deux racines complexes conjuguées.

Le résultat précédent nous amène à penser au théorème suivant:

Théorème 0.3.2.
Théorème de d'Alembert
Tout polynôme P de $\mathbb{C}[X]$, non constant, admet une racine dans $\mathbb{C}$.

Conséquence: $\mathbb{C}$ est algèbriquement clos.

Néanmoins, la démonstration de ce théorème nécessitant l'utilisation de l'analyse, elle ne doit pas figurer dans cette leçon;

Démonstration. Soit f définie par $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ $(n \in \mathbb{N}^*)$. Nous supposons que $a_n \neq 0$ (sinon 0 est racine).

On organise la démonstration en deux temps:

(i) Prouver que $\inf_{z\in\mathbb{C}} |f(z)|$ est atteint en un point z_0 de $\mathbb{C}$.
(ii) Montrer que $f(z_0) = 0$.
(i) Pour $z \in \mathbb{C}^*$,

$$f(z) = z^n \left(1 + \frac{a_1}{z} + \ldots + \frac{a_n}{z^n}\right).$$

Ainsi

$$\lim_{|z|\to+\infty} |f(z)| = +\infty.$$

Il existe $R > 0$ tel que $|z| > R$, $|f(z)| > |f(0)|$, ce qui prouve que

$$\inf_{z\in\mathbb{C}} |f(z)| = \inf_{|z|\leq R} |f(z)|.$$

Mais $|f|$ est continue sur $\mathbb{C}$ et à valeurs dans $\mathbb{R}$: elle atteint son minimum sur la boule fermée de rayon R, donc il existe $z_0 \in \mathbb{C}$ tel que

$$\inf_{z\in\mathbb{C}} |f(z)| = |f(z_0)|.$$

(ii) Si $f(z_0) \neq 0$, soit alors la fonction polynôme g définie par

$$g(z) = \frac{f(z_0 + z)}{f(z_0)},$$

elle est de degré n;

$$g(z) = \sum_{i=0}^{n} b_i z^i \quad \text{avec} \quad b_n \neq 0 \quad \text{et} \quad b_0 = g(0) = 1.$$

Soit alors

$$k = \inf\{i \in [\![1, n]\!] | b_i \neq 0\},$$

on a

$$g(z) = 1 + \sum_{i=k}^{n} b_i z^i = 1 + b_k z^k (1 + \varphi(z))$$

où

$$\varphi(z) = \sum_{i=k+1}^{n} \frac{b_i}{b_k} z^{i-k}$$

d'où

$$\lim_{z\to 0} \varphi(z) = 0,$$

il existe alors $r > 0$ tel que, pour $|z| < r$, $|\varphi(z)| < \frac{1}{2}$. Pour z tel que $|z| < r$, on a donc

$$|g(z)| \leq \left|1 + b_k z^k\right| + \frac{1}{2} \left|b_k z^k\right|.$$

Posons $b_k = |b_k| e^{i\theta}$ et particularisons z sous la forme $Z = \rho e^{-i\frac{\theta+\pi}{k}}$ avec $\rho \in]0, 1[$ suffisamment voisin de 0 pour que $\rho < r$ et que $1 + b_k Z^k = 1 - |b_k| \rho^k$ soit positif.
Alors $|g(Z)| \leq 1 - |b_k|\rho^k + \frac{1}{2}|b_k|\rho^k < 1$ soit $|f(z_0 + Z)| < |f(z_0)|$ ce qui est absurde.

■