Solution de TD N^0 1

Exercice 1 ***Solution*** *Soit*

$$\mathbb{Z}[i] = \{a + ib \mid (a;b) \in \mathbb{Z}^2 et i^2 = -1\}$$

Remarquons que $\mathbb{Z}[i]$ est sous ensemble de $\mathbb{C}$.

1. *Montrons que $\mathbb{Z}[i]$ est un sous anneau de $\mathbb{C}$.*
   (a) *$\mathbb{Z}[i]$ est non vide (On voit que $0 = 0 + i0 \in \mathbb{Z}[i]$).*
   (b) *Soient $z_1 = a_1 + ib_1$ et $z_2 = a_2 + ib_2$ deux éléments de $\mathbb{Z}[i]$. on a $z_1 - z_2 = (a_1 + ib_1) - (a_2 + ib_2) = (a_1 - a_2) + i(b_1 - b_2) \in \mathbb{Z}[i]$.*
   (c) *Soient $z_1 = a_1 + ib_1$ et $z_2 = a_2 + ib_2$ deux éléments de $\mathbb{Z}[i]$. on a $z_1.z_2 = (a_1 + ib_1).(a_2 + ib_2) = (a_1.a_2) - (b_1.b_2) + i[a_1b_2 + a_2b_1] \in \mathbb{Z}[i]$.*
2. *SoitN une application de $\mathbb{Z}[i]$ dans $\mathbb{N}$ tel que $N(a + ib) = a^2 + b^2$. On a*

$$N[(a + ib)(c + id)] = N[(ac - bd) + i(bc + ad)] = (ac - bd)^2 + (bc + ad)^2.$$

   Et on a

$$N(a + ib)N(c + id) = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (bc + ad)^2.$$

   Donc

$$\mathrm{N}[(a + ib)(c + id)] = N[(a + ib)N(c + id)].$$

   Cherchons maintenant les éléments inversibles de $\mathbb{Z}[i]$.
   Soit $a + ib$ un élément inversible de $\mathbb{Z}[i]$, donc il existe un élément $c + id$ de $\mathbb{Z}[i]$ tel que $(a + ib)(c + id) = 1$ donc $N((a + ib)(c + id)) = N(1) = 1$, alors $(a^2 + b^2)(c^2 + d^2) = 1$.
   Et comme a, b, c et d sont des nombres relatifs ($\in \mathbb{Z}$) alors $a^2 + b^2 = 1$.
   Donc

$$b = 0 \Longrightarrow a = \pm 1.$$

   Ou

$$a = 0 \Longrightarrow b = \pm 1.$$

   Alors l'ensemble des éléments inversibles de $\mathbb{Z}[i]$ est $\{1, -1, i, -i\}$.

Exercice 2 ***Indication pou la solution*** *Soit l'ensemble $\mathbb{Z}\left[\sqrt{2}\right]$ le sous-ensemble de $\mathbb{R}$ donné par*

$$\mathbb{Z}\left[\sqrt{2}\right] = \{a + \sqrt{2}b \mid (a;b) \in \mathbb{Z}^2\}$$

1. *Montrer que $\mathbb{Z}\left[\sqrt{2}\right]$ est un anneau. Il suffit de montrer que $\mathbb{Z}\left[\sqrt{2}\right]$ est un sous-anneau de $\mathbb{R}$.*
2. *On note $N(a + \sqrt{2}b) = a^2 - 2b^2$. Montrer que*

$$\forall x, y \in \mathbb{Z}\left[\sqrt{2}\right] : N(xy) = N(x)N(y).$$

   Voir l'exercice 1, la question 2.
3. *En déduire que les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$ sont les $a + b\sqrt{2}$ tels que $a^2 - 2b^2 \in [-1, +1]$.*

Exercice 3 ***Solution.*** *Soit A un anneau tel que tout élément de A soit idempotent (i.e. $\forall x \in A$, $x^2 = x$).*

1. *Si $x \in A$, alors $(2x)^2 = 2x$ donc $4x^2 = 2x$, ce qui entraine $4x = 2x$ puis $2x = 0$. Ceci s'écrit encore $x = -x$.*
   Montrons maintenant que A est commutatif. Si$x, y \in A$, $(x+y)^2 = x+y$ donc $x^2+xy+yx+y^2 = x + y$, d'où en tire $xy + yx = 0$ donc$xy = -yx = yx$.
2. *Si $x, y \in A$ alors $xy(x + y) = xyx + xy^2 = x^2y + xy^2 = xy + xy = 2xy = 0$.*
   Si A est intègre, alors A a au plus deux éléments. En effet, sinon il existe $x, y \in A$ distincts et différents de 0. Donc $(x + y) \neq 0$ (sinon $x = -y = y$) et A étant intègre $xy(x + y) \neq 0$, absurde.

Exercice 4 ***Solution.*** *Soit A un anneau commutatif et x ; y deux éléments nilpotents de A.*
x est nilpotent ssi il existe un entier n strictement positif tel que $x^n = 0$.
y est nilpotent ssi il existe un entier m strictement positif tel que $y^m = 0$.

1. *Montrons que l'élément $x.y$ est aussi nilpotent.*
   On a $(xy)^n = x^n y^n = 0y^n = 0$ (car A un anneau commutatif).
2. *L'élément $x + y$ est nilpotent car :*
   $(x + y)^{n+m-1} = \sum_{k=0}^{n+m-1} C_{n+m-1}^k x^k y^{n+m-1-k}$
   $= y^m(\sum_{k=0}^{n-1} C_{n+m-1}^k x^k y^{n-1-k}) + x^n(\sum_{k=n}^{n+m-1} C_{n+m-1}^k x^{k-n} y^{n+m-1-k})$
   $= 0(\sum_{k=0}^{n-1} C_{n+m-1}^k x^k y^{n-1-k}) + 0(\sum_{k=n}^{n+m-1} C_{n+m-1}^k x^{k-n} y^{n+m-1-k}) = 0$
3. *Montrons que l'élément $1 - x$ est inversible :*
   On a $1 = 1 - x^n = (1 - x)(1 + x + x^2 + \ldots + x^{n-1})$.
   Donc $1 - x$ est inversible, et son inverse est $(1 + x + x^2 + \ldots + x^{n-1})$.

Exercice 5 ***Solution.***

1. *Effectuons la division euclidienne de $4X^5 - 2X^4 + 5X^3 + 4X + 2$ par $X^2 + 1$.*

$$
\begin{array}{l|l}
4X^5 - 2X^4 + 5X^3 + 4X + 2 & X^2 + 1 \\ \cline{2-2}
\underline{-4X^5 - 0X^4 - 4X^3 - 0X^2 - 0X - 0} & 4X^3 - 2X^2 + X + 2 \\
-2X^4 + X^3 + 04X^2 + 4X + 2 & \\
\underline{2X^4 - 0X^3 + 2X^2 - 0X - 0} & \\
X^3 + 2X^2 + 4X + 2 & \\
\underline{-X^3 - 0X^2 - X - 0} & \\
2X^2 + 3X + 2 & \\
\underline{-2X^2 - 0X - 2} & \\
3X &
\end{array}
$$

   Donc : $4X^5 - 2X^4 + 5X^3 + 4X + 2 = (X^2 + 1)Q(X) + R(X)$, avec $Q(X) = 4X^3 - 2X^2 + X + 2$ et $R(X) = 3X$.

2. *La division euclidienne de $4X^5 - 2X^4 + 5X^3 + X^2$ par $4X^3 - 2X^2 + X + 2$ donne :*
   $4X^5 - 2X^4 + 5X^3 + X^2 = (4X^3 - 2X^2 + X + 2)Q(X) + R(X)$, avec $Q(X) = X^2 + 1$ et $R(X) = -X^2 - X - 2$.

3. *$-2X^5 - 2X^4 - X^3 + 4X^2 + 4X + 2$ par $X^2 + X + 1$.*

Exercice 6 *Déterminer le $PGCD(P; Q)$ dans chaque cas :*

1. *$P(X) = X^4 - 3X^3 + X^2 + 4$ et $Q(X) = X^3 - 3X^2 + 3X - 2$.*
   On recherche le PGCD des polynômes $P(X)$ et $Q(X)$ par l'algorithme d'Euclide, utilisant

les divisions euclidiennes des polynômes : le PGCD est alors le dernier reste non nul à une constante multiplicative près :

$$\begin{array}{l|l} X^4-3X^3+X^2+4 & X^3-3X^2+3X-2 \\ \underline{-X^4+3X^3-3X^2-2X-0} & \overline{X} \\ -2X^2+2X+4 & \end{array}$$

On obtient $P(X)=Q(X)Q_1(X)+R_1(X)$, *avec* $Q_1(X)=X$ *et* $R_1(X)=-2X^2+2X+4$.
On fait ensuite la division euclidienne de $Q(X)$ *par* $R_1(X)$ *:*

$$\begin{array}{l|l} X^3-3X^2+3X-2 & \underline{-2X^2+2X+4} \\ \underline{-X^3+X^2+2X-0} & 4X^3-2X^2+X+2 \\ -2X^2+5X-2 & \\ \underline{2X^2-2X-4} & \\ 3X-6 & \end{array}$$

On obtient $Q(X)=R(X)_1Q_2(X)+R_2(X)$, *avec* $Q_2(X)=-\frac{1}{2}X+1$ *et* $R_2X)=3X-6$.

On fait la division euclidienne de $R_1(X)$ *par* $R_2(X)$ *:*

$$\begin{array}{l|l} -2X^2+2X+4 & \underline{3X-6} \\ \underline{2X^2+4X-0} & -\frac{2}{3}X+\frac{2}{3} \\ -2X+4 & \\ \underline{2X-4} & \\ 0 & \end{array}$$

Donc $3X-6$ *est le dernier reste non nul, c'est donc le PGCD de* $X^4-3X^3+X^2+4$ *et* X^3-3X^2+3X-2.

2. $P(X)=X^5-X^4+2X^3-2X^2+2X-1$ *et* $Q(X)=X^5-X^4+2X^2-2X+1$.
3. $P(X)=X^n-1$ *et* $Q(X)=(X-1)^n$ *;* $n\geq 1$.

Exercice 7 *On considère dans* $\mathbb{K}[X]$ *(*$\mathbb{K}$ *étant* $\mathbb{R}$ *ou* $\mathbb{C}$ *), les trois polynômes A, B et C suivants :*
$A(X)=X^3+6X^2+11X+6$
$B(X)=X^3+4X^2+X-6$
$C(X)=X^3+X^2-X-1$
Calculer $pgcd(A,B)$, $pgcd(A,C)$, $pgcd(B,C)$, $pgcd(A,B,C)$.

Indication *Par définition, le PGCD, noté D, des polynômes* $P_1,P_2,\ldots,P_n$ *non tous nuls est le polynôme satisfaisant aux conditions a) et b) suivantes :*
a) Le polynôme D divise tous les polynômes P_i *,*
b) Tout polynôme divisant chacun des P_i *divise D.*
Remarquer que le PGCD de plusieurs polynômes divise le PGCD de deux d'entre eux.

Exercice 8 *Trouver le PGCD, noté D, dans*$\mathbb{K}[X]$ *(*$\mathbb{K}$ *étant* $\mathbb{R}$ *ou* $\mathbb{C}$*), des polynômes et suivants :*

$A(X)=X^6+X^5+4X^2+2X-2$
$B(X)=X^5+2X^4+X^3+5X+5$

On recherche le PGCD des polynômes $A(X)$ et $B(X)$ par l'algorithme d'Euclide, utilisant les divisions euclidiennes des polynômes : le PGCD est alors le dernier reste non nul à une constante multiplicative près. On fait la division euclidienne de $A(X)$ par $B(X)$ et on obtient $A(X) = B(X)Q_1(X)+R_1(X)$, avec $Q_1(X) = X-1$ et $R_1(X) = X^4+X^3-X^2+2X+3$.

On fait ensuite la division euclidienne de $B(X)$ par $R_1(X)$, on obtient $B(X) = R_1(X)Q_2(X) + R_2(X)$, avec $Q_2(X) = X+1$ et $R_2(X) = X^3-X^2+2$.

On fait la division euclidienne de $R_1(X)$ par $R_2(X)$, on obtient $R_1(X) = R_2(X)Q_3(X)+R_3(X)$, avec $Q_3(X) = X+2$ et $R_3(X) = X^2-1$.

On fait la division euclidienne de $R_2(X)$ par $R_3(X)$, on obtient $R_2(X) = R_3(X)Q_4(X)+R_4(X)$, avec $Q_4(X) = X-1$ et $R_4(X) = X+1$. Et $R_4(X)$ est le dernier reste non nul, c'est donc le PGCD de $A(X)$ et $B(X)$.

Pour déterminer un couple (U,V) de polynômes vérifiant l'identité de Bézout $AU+BV = D$, On regroupe les résultats obtenus.
$A = Q_1B+R_1$ *avec* $Q_1(X) = X-1$.
$B = Q_2R_1+R_2$ *avec* $Q_2(X) = X+1$.
$R_1 = Q_3R_2+R_3$ *avec* $Q_3(X) = X+2$.
$R_2 = Q_4R_3+R_4$ *avec* $Q_4(X) = X-1$.
On a $R_1(X) = A(X)-Q_1(X)B(X)$ *donc* $R_1(X) = A(X)-(X-1)B(X)$.
On a $R_2(X) = B(X)-Q_2(X)R_1(X)$ *donc* $R_2(X) = B(X)-(X+1)(A(X)-(X-1)B(X))$ *donc* $R_2(X) = -(X+1)A(X)+X^2B(X)$.
On a $R_3 = R_1-(X+2)R_2$ *et* $R_4 = R_2-(X-1)R_3$ *donc* $R_4 = R_2-(X-1)[R_1-(X+2)R_2]$.
Alors $R_4(X) = (-X^3-2X^2-X+2)A(X)+(X^4+X^3-2X+1)B(X)$.
Donc on a déterminé un couple (U,V) de polynômes vérifiant l'égalité $AU+BV = D$, avec $U(X) = -X^3-2X^2-X+2$, $V(X) = X^4+X^3-2X+1$ et $D(X) = R_4(X) = X+1$.

Exercice 9 *Trouver le PGCD, noté D, dans$\mathbb{K}[X]$ ($\mathbb{K}$ étant $\mathbb{R}$ ou $\mathbb{C}$), des polynômes et suivants :*

$$A(X) = X^4+1 \text{ et } B(X) = X^3-X^2+1$$

et déterminer tous les couples (U,V) de polynômes vérifiant l'identité de Bézout $AU+BV = D$.

Exercice 10 ***Solution.*** *Déterminons l'ensemble des polynômes $P \in \mathbb{R}[X]$ tels que $P \equiv 1(mod(X-1)^3)$ et $P \equiv -1(mod(X+1)^3)$.*
Notons Γ cet ensemble. On a

$$P \in \Gamma \Longleftrightarrow \exists U,V \in \mathbb{R}[X], P = 1+U(X-1)^3 \text{ et } P = -1+V(X+1)^3$$

$$\Longleftrightarrow \exists U,V \in \mathbb{R}[X], P = 1+U(X-1)^3 \text{ et} 1+U(X-1)^3 - 1+V(X+1)^3.$$

En d'autres termes, Γ représente l'ensemble des polynômes de la forme $1+U(X-1)^3$ où U appartient à l'ensemble

$$\{U \in \mathbb{R}[X] \mid \exists V \in \mathbb{R}[X], U(X-1)^3+V(X+1)^3 = 2\}.$$

On est ramené au problème suivant : quels sont les couples (U,V) tel que $U(X-1)^3+V(X+1)^3 = 2$?
Les polynômes $X-1$ et $X+1$ étant premiers entre eux, il en est de même pour les polynômes $(X-1)^3$ et $(X+1)^3$, donc et d'après le théorème de Bezout il existe (U_0,V_0) de $\mathbb{R}[X]$ tel que $U_0(X-1)^3+V_0(X+1)^3 = 1$.

Théorème de Bezout *: Soient P et Q deux de $\mathbb{R}[X]$, premiers entre eux. Alors il existe (U_0, V_0) tel que $U_0P+V_0Q = 1$, et l'ensemble des couples (U, V) vérifiant $UP+VQ = 1$ est $\Gamma' = (U_0 + KQ, V_0 + KP); K \in \mathbb{R}$*
On a :
$(X+1)^3 = (X-1)^3 + (6X^2+2)$ *et* $(X-1)^3 = (6X^2+2)(\frac{X}{6}-\frac{1}{2}) + (\frac{8}{3}X)$, $(6X^2+2) = (\frac{8}{3}X)(\frac{9}{4}X)+2.$
Maintenant on remonte

$$2 = (6X^2+2) - (\frac{8}{3}X)(\frac{9}{4}X) = 6X^2+2) - [(X-1)^3 - (6X^2+2)(\frac{X}{6}-\frac{1}{2})](\frac{9}{4}X).$$

$$= (-\frac{9}{4}X)(X-1)^3 + (6X^2+2)[(\frac{X}{6}-\frac{1}{2})(\frac{9}{4}X)+1]$$

$$= (-\frac{9}{4}X)(X-1)^3 + [(X+1)^3 - (X-1)^3](\frac{3X^2}{8} - \frac{9X}{8} + 1)$$

$$= (-\frac{3X^2}{8} - \frac{9X}{8} + 1)(X-1)^3 + (\frac{3X^2}{8} - \frac{9X}{8} + 1)(X+1)^3$$

Si $U_0 = -\frac{3X^2}{16} - \frac{9X}{16} + \frac{1}{2}$ *et* $V_0 = \frac{3X^2}{16} - \frac{9X}{16} + \frac{1}{2}$, *on donc* $U_0(X-1)^3 + V_0(X+1)^3 = 1$. *D'après le théorème de Bezout, on a donc :*

$$\Gamma = \{1 + [2U_0 + K(X+1)^3](X-1)^3, K \in \mathbb{R}[X]\}.$$

Exercice 11 ***Solution.***

1. *Décomposons en produit de facteurs irréductibles dans $\mathbb{R}[X]$ les polynômes suivants 1. X^4+1.*
   On commence par chercher les racines complexes pour factoriser dans $\mathbb{C}[X]$, puis on regroupe les racines complexes conjuguées

$$X^4 + 1 = (X - e^{i\frac{\pi}{4}})(X - e^{3i\frac{\pi}{4}})(X - e^{5i\frac{\pi}{4}})(X - e^{7i\frac{\pi}{4}})$$
$$= ((X - e^{i\frac{\pi}{4}})(X - e^{7i\frac{\pi}{4}}))((X - e^{3i\frac{\pi}{4}})(X - e^{5i\frac{\pi}{4}}))$$
$$= (X^2 - X(e^{7i\frac{\pi}{4}} + e^{i\frac{\pi}{4}}) + 1)(X^2 - X(e^{5i\frac{\pi}{4}} + e^{3i\frac{\pi}{4}}) + 1)$$
$$= (X^2 - \sqrt{2} + 1)(X^2 + \sqrt{2} + 1)$$

Les deux polynômes de degré 2 que l'on obtient non pas de racines réelles, ils sont irréductibles dans $\mathbb{R}[X]$.
2. $X^8 - 1$

$$X^8 - 1 = (X^4 - 1)(X^4 + 1)$$
$$= (X^2 - 1)(X^2 + 1)(X^2 - \sqrt{2} + 1)(X^2 + \sqrt{2} + 1)$$
$$= (X - 1)(X + 1)(X^2 + 1)(X^2 - \sqrt{2} + 1)(X^2 + \sqrt{2} + 1).$$

3. $X^4 - 6X^3 + 9X^2$

$$X^4 - 6X^3 + 9X^2 = X^2(X^2 - 6X + 9) = X^2(X + 3)(X + 3).$$

4. $(X^2 - X + 1)^2 + 1$.

$$(X^2-X+1)^2+1=(X^2-X+1)^2-i=(X^2-X+1-i)(X^2-X+1+i)$$

On factorise alors chacun des polynômes de degré 2 dans $\mathbb{C}$ *:*

$$\begin{aligned}(X^2-X+1)^2+1&=(X+i)(X-1-i)(X-i)(X-1+i)\\&=(X^2+1)((X-1)^2+1)\\&=(X^2+1)((X)^2-2X+2)\end{aligned}$$

2. *On a :* $9=-(3i)^2$ *donc*

$$\begin{aligned}X^4-6X^3+9X^2+9&=(X(X-3))^2-(3i)^2\\&=(X(X-3)-3i)(X(X-3)+3i)\\&=(X^2-3X-3i)(X^2-3X+3i)\end{aligned}$$

On factorise chacun de ces deux polynômes. Le discriminant du premier est $9+12i=(\sqrt{3}(2+i))^2$ *ses racines sont* $\alpha_1=\frac{3}{2}+\sqrt{3}+i\frac{\sqrt{3}}{2}$ *et* $\alpha_2=\frac{3}{2}-\sqrt{3}-i\frac{\sqrt{3}}{2}$.
Le discriminant du premier est $9-12i=(\sqrt{3}(2-i))^2$. *Ses racines sont* $\beta_1=\frac{3}{2}+\sqrt{3}-i\frac{\sqrt{3}}{2}$ *et* $\beta_2=\frac{3}{2}-\sqrt{3}+i\frac{\sqrt{3}}{2}$.
La décomposition en produit de facteurs irréductibles de $\mathbb{C}[X]$ *est donc :*

$$(X-\alpha_1)(X-\alpha_2)(X-\beta_1)(X-\beta_2)$$

Pour obtenir la décomposition dans $\mathbb{R}[X]$, *on regroupe les racines complexes conjuguées à savoir* α_1 *et* β_1 *d'une part et* α_2 *et* β_2 *d'autre part. On trouve*

$$X^4-6X^3+9X^2+9=(X^2-(2\sqrt{3}+3)X+3\sqrt{3}+6)(X^2+(2\sqrt{3}+3)X-3\sqrt{3}+6)$$