Fiche n°5 sur les anneaux.

Exercice 17.

Pgcd dans $\mathbb{Q}[X]$ de $P(X)=X^4+X^3-3X^2-4X-1$ et $Q(X)=X^3+X^2-X-1$

Rappel : si $P=BQ+R$ alors $\text{pgcd}(P,Q)=\text{pgcd}(Q,R)$.

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

$P(X)=(X+1)(X^3-3X-1)$

Or X^3-3X-1 est irréductible sur $\mathbb{Q}$.

$\Rightarrow \text{pgcd}(P,Q)=X+1$.

Avec l'algorithme d'Euclide.

$P=QX-2X^2-3X-1$

$Q=(-2X^2-3X-1)\left(-\frac{X}{2}+\frac{1}{4}\right)\underbrace{-3\frac{X}{4}-\frac{3}{4}}_{-\frac{3}{4}(X+1)}$

$-2X^2-3X-1=(X+1)(-2X-1)+0$

$\Rightarrow \text{pgcd}\,(P,Q)=X+1$.

Exercice 18.

$A=\mathbb{Z}[i\sqrt{3}]=\mathbb{Z}+i\sqrt{3}\mathbb{Z}$, $K=\mathbb{Q}(i\sqrt{3})$

1) $X^2-X+1=\left(X-\frac{1+i\sqrt{3}}{2}\right)\left(X-\frac{1-i\sqrt{3}}{2}\right)$ dans $K[X]$

$\Delta=1-4=-3=(i\sqrt{3})^2$

2) $\frac{1\pm i\sqrt{3}}{2}\notin\mathbb{Z}+i\sqrt{3}\mathbb{Z}=A\Rightarrow$ pas de racines dans A

3)rappel :

Théorème. A factoriel$\Rightarrow A[X]$ est factoriel

et de plus, dans ce cas, les irréductibles de $A[X]$sont les polynômes $P(X)\epsilon A[X]$ tels que $P(X)$ est irréductible sur $K = \mathrm{Frac}(A)$ et pgcd des coefficients de P(X)=1.

En particulier $A = \mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel$\Rightarrow$pas principal $\Rightarrow$ pas euclidien.

(on aurait pu le voir en remarquant que $4 = 2 \times 2 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ et 2, $1 \pm i\sqrt{3}$ sont irréductibles).

En revanche, l'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ est factoriel.

Exercice 19.

$P(X)\epsilon\mathbb{Z}[X]$

1) $P(0), P(1)$ sont impairs$\Leftrightarrow P(0) = P(1) = 1 \bmod 2$

Si $x\epsilon\mathbb{Z}, P(x) = P(\bar{x}) \bmod 2$ où $\bar{x} = x \bmod 2$

car $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ $x \mapsto x \bmod 2$

estun morphisme d'anneaux.

(donc: si $P(X) = a_0 + a_1X + \cdots + a_dX^d$, alors :

$P(\bar{x}) = a_0 + a_1\bar{x} + \cdots + a_d\bar{x}^d = \overline{a_0 + a_1x + \cdots + a_dx^d}$).

D'où : $P(x) = P(0)$ ou $P(1) \bmod 2 = 1 \neq 0 \bmod 2$.

2) $P(0), \ldots, P(n-1) \neq 0 \bmod n$

Raisonner dans $\mathbb{Z}/n\mathbb{Z}$.

Soit $x\epsilon\mathbb{Z}$. Alors $P(x) \bmod n = P(\bar{x})$. Or $\bar{x} = 0, 1, \ldots,$ ou $n-1 \bmod n$.

$\Rightarrow \forall x\,\epsilon\mathbb{Z}, P(x) \neq 0 \bmod n \Rightarrow P(x) \neq 0$.

.

Exercice 20.

Proposition. *Critère d'Eisenstein.*

Soit $P(X) = a_0 + a_1X + \cdots + a_dX^d \epsilon \mathbb{Z}[X]$.

Si p, nombre premier, vérifie :

$1°) p | a_{0,} a_{1,\ldots,} a_{d-1}$

$2°) p \nmid a_d$

$3°) p^2 \nmid a_0$

ALORS : $P(X)$ est irréductible sur $\mathbb{Q}$.

démonstration. On raisonne dans $\mathbb{Z}/p\mathbb{Z}[X]$.

$P(X) = \bar{a_d}X^d$ si $P(X) = Q_1(X)Q_2(X)$ avec $Q_1, Q_2 \epsilon \mathbb{Z}[X]$ et deg $Q_{1,}$deg $Q_2 < d$ alors : $\bar{a_d}X^d = \overline{Q_1}\,\overline{Q_2} \underset{\text{car } l'\text{anneau } \mathbb{Z}/p\mathbb{Z}[X] \text{ est factoriel}}{\Rightarrow} \overline{Q_1}, \overline{Q_2} =$ une puissance de X dans

$\mathbb{Z}/p\mathbb{Z}[X] \Rightarrow Q_1(0) = Q_2(0) = 0 \bmod p \Rightarrow p^2$divise $P(0) = Q_1(0)Q_2(0)$ contradiction.

Si $P(X) = Q_1(X)Q_2(X)$, avec $Q_1, Q_2 \epsilon \mathbb{Q}[X]$, alors il existe q_1, q_2 entiers non nuls tels que $q_iQ_i \epsilon \mathbb{Z}[X] \Rightarrow q_1q_2P = q_1Q_1q_2Q_2 \Rightarrow c(q_1q_2P) = q_1q_2c(P) = c(q_1Q_1)c(q_2Q_2)$

$=> \frac{P}{c(P)} = \underbrace{\frac{q_1Q_1}{c(q_1Q_1)}\frac{q_2Q_2}{c(q_2Q_2)}}_{\epsilon \mathbb{Z}[X]} \Rightarrow P = c(P)\frac{q_1Q_1}{c(q_1Q_1)}\frac{q_2Q_2}{c(q_2Q_2)}$ et on est ramené au cas où P s'écrit comme produit de polynômes à coefficients entiers et de degrés $<$deg P.

Rappel sur le contenu.

Si $P(X) = a_0 + a_1X + \cdots + a_dX^d$, *on pose* $c(P) = \text{pgcd}(a_0, a_1, \ldots, a_d)$ *c'est le contenu de* P .

Lemme de Gauss. *Si* $R, S \epsilon \mathbb{Z}[X]$, *alors* $c(RS) = c(R)c(S)$.

démonstration. Il suffit de montrer que si $c(R) = c(S) = 1$, *alors* $c(RS) = 1$.

En effet, sinon, il existe p, *nombre premier, qui divise* $c(RS)$.

Alors $RS = 0$ *dans* $\mathbb{Z}/p\mathbb{Z}[X]$. *Mais l'anneau*

$\mathbb{Z}/p\mathbb{Z}[X]$ est intègre. Donc R ou S $=0$ dans $Z/p\mathbb{Z}[X] \Rightarrow p | c(R)$ ou $c(S)$ absurde !

Application du critère d'Eisenstein :

$\forall n, X^n - 2$ est irréductible sur $\mathbb{Q}$.

1) $X^4 - 8X^3 + 12X^2 - 6X + 2$ est irréductible par le critère d'Eisenstein avec $p = 2$: Q_1

2 divise tous les coefficients sauf le coefficient dominant, $2^2 = 4$ ne divise pas le coefficient constant$\Rightarrow$irréductible sur $\mathbb{Q}$.

2) $X^5 - 12X^3 + 36X - 12$

irréductible par Eisenstein avec $p = 3$.

3) $X^4 - X^3 + 2X + 1$

Modulo 2 : $X^4 + X^3 + 1$

dans $\mathbb{Z}/2\mathbb{Z}[X]$, $X^2 + X + 1$ est le seul polynôme irréductible de degré 2.

$X^2 + X + 1 \nmid X^4 + X^3 + 1$ (par exemple : faire division euclidienne)

Donc pas de facteur irréductible de degré 1 ou $2 \Rightarrow$ irréductible sur $\mathbb{Z}/2\mathbb{Z} \Rightarrow$ irréductible sur $\mathbb{Q}$.

Exercice 21.

$P(X) \in \mathbb{Z}[X]$, soient a, b entiers premiers entre eux tels que $P\left(\frac{a}{b}\right) = 0$.

1) $\forall k \in \mathbb{Z}, a - bk \mid \quad P(k)$

c-à-d, $P(k) = 0 \bmod a - bk =: m$

$P(X) = a_n X^n + \cdots + a_0$ où a_i sont entiers.

$P\left(\frac{a}{b}\right) = 0 \Rightarrow a_n a^n + a_{n-1} a^{n-1} b + \cdots + a_0 b^n = 0$

Modulo m, $a = bk \Rightarrow a_n (bk)^n + a_{n-1} (bk)^{n-1} b + \cdots + a_0 b^n = 0$

$\Leftrightarrow b^n (a_n k^n + \cdots + a_0) = 0$ ($\clubsuit$)

Or b est premier avec $a - bk \Rightarrow b$inversible dans $\mathbb{Z}/m\mathbb{Z}$.

Donc dans ($\clubsuit$) on peut diviser par b^n : $\Rightarrow P(k) = 0 \bmod m$.

2) $f(x) = x^3 - 6x^2 + 15x - 14$

$f(0) = -14, f(1) = -4 \Rightarrow f\left(\frac{a}{b}\right) = 0 \Rightarrow a \mid 14, a - b \mid -4$

$f(2)=0 \Rightarrow f(x)=(x-2) \quad \underbrace{(x^2-4x+7)}_{\text{pas de racine rationnelle car le discriminant est } <0}$

2 est la seule racine rationnelle

$g(x)=2x^3+3x^2+6x-4=(2x-1)(x^2+2x+4)$

$f(0)=-4, f(1)=7, f(-1)=-9 \Rightarrow$ si $\frac{a}{b}$ racine alors $a|-4$,

$g\left(\frac{a}{b}\right)=0 \Rightarrow 2\times a^3+3a^2b+6ab^2-4b^3=0 \Rightarrow b|2a^3 \Rightarrow b|2 \Rightarrow b=1$ ou 2

Pas de racine entière car $g(\pm 1), g(\pm 2), g(\pm 4) \neq 0$ et si $b=2$, comme a est premier à b, on a $a=\pm 1$.

$g\left(\frac{a}{2}\right)=\frac{a^3+3a^2+12a-16}{4}=0 \Rightarrow a=\pm 1 \Leftarrow$ oui si $\frac{a}{b}=\frac{1}{2}$.

On factorise : $g(x)=(2x-1)\underbrace{(x^2+2x+4)}_{\text{discriminant}<0}$

Donc $x=\frac{1}{2}$ est la seule racine rationnelle.

Exercice 22.

1) $P(n+km)=P(n) \bmod m = m \bmod m = 0 \bmod m$.

2) Si $\forall n$, $P(n)$ est premier, alors $p=P(0)$ divise $P(kp)$ pour tout $k \Rightarrow p=\pm P(kp) \Rightarrow \forall k, P(kp)=\pm p \Rightarrow P$ constant (car sinon $\lim_{k\to\infty} P(kp)=\pm\infty$)