Feuille d'exercices $n^0 5$.

Anneaux et idéaux

Exercice 10.

(1) Polynômes irréductibles sur $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} = \{-1, 0, 1\}$.

indications : les irréductibles de degrés 2,3 sont ceux qui n'ont pas de racines ...

$\pm(X^2+1)$

$\pm(X^2+X-1)$, $\pm(X^2-X-1)$

sont les polynômes irréductibles de degré 2 sur $\mathbb{F}_3$.

Degré 3 :

$\pm(X^3-X+1), \pm(X^3-X^2+1), \pm(X^3+X^2-X+1), \pm(X^3-X-1), \pm(X^3+X^2-1), \pm(X^3+X^2+X-1), \pm(X^3-X^2-X-1)$

sont les polynômes irréductibles de degré 3 sur $\mathbb{F}_3$.

$P = X^3 + aX^2 + bX + c$ irréductible $\Leftrightarrow P(0), P(1), P(-1) \neq 0$.

c-à-d $c=\pm 1, a+b+c\neq -1, a-b+c\neq -1$

puis distinguer les cas si $c=1$ ou -1.

(2)Factoriser $X^2+X+1=(X-1)^2$(dans $\mathbb{F}_3[X]$)

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

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

X^3+1	$X+1$
X^3+X^2	X^2-X+1
$-X^2+1$	
$-X^2-X$	
$X+1$	
$X+1$	
0	

Exercice 11.

$P(X)=X^5-6X^3+2X^2-4X+5\epsilon\mathbb{Z}[X]$.

Mod 2 : $P(X)=X^5+1$dans $\mathbb{F}_2[X]$réductible.

Mod 3 : $P(X)=X^5-X^2-X-1$ dans $\mathbb{F}_3[X]$.

$P \bmod 3$ n'a pas de racines dans $\mathbb{F}_3$

Pmod 3 a-t-il un facteur de degré 2 ?

Dans $\mathbb{F}_3[X]$, $P(X)$ n'est pas divisible par X^2+1,ni par X^2-X-1 ni par X^2+X-1.

En effet : par exemple

$$P(X)=(X^2-X-1)(X^3+X^2-X-1)\underbrace{+1}_{\neq 0}.$$

Conclusion = mod 3, $P(X)$ n'a pas de racine et n'est pas divisible par un polynôme irréductible de degré 2. Donc comme deg P=5, $P(X)$ est irréductible sur $\mathbb{F}_3 \Rightarrow P(X)$ irréductible sur $\mathbb{Q}$ donc sur $\mathbb{Z}$.

Rappel : si $P(X)=Q(X)R(X)$ avec $Q, R \epsilon \mathbb{Z}[X]$ et $\deg Q, \deg R < \deg P$, alors en réduisant mod p: $\bar{P}(X)=\bar{Q}(X)\bar{R}(X)$où $\bar{P}=$ polynôme obtenu en prenant les classes des coefficients mod p.

$\mathbb{Z}[X] \rightarrow \mathbb{Z}/p\mathbb{Z}[X] a_0+a_1X+\cdots+a_nX^n \mapsto \bar{a_0}+\bar{a_1}X+\cdots+\overline{a_n}X^n$ est un morphisme d'anneaux.

Remarque P de contenu $1 \Rightarrow$ si P est réductible sur $\mathbb{Q}$ alors P est réductible sur $\mathbb{Z}$.

contenu de $P := c(P) =$ pgcd des coefficients de P.

Lemme de Gauss : $c(PQ) = c(P)c(Q)$.

$\Rightarrow$Proposition: $P \epsilon \mathbb{Z}[X]$ alors P irréductible sur $\mathbb{Z} \Leftrightarrow P$ irréductible sur $\mathbb{Q}$ et $c(P) = 1$.

Même question pour $P(X) = 7X^4 + 8X^3 + 11X^2 - 24X - 455$.

$P(X) = X^4 + X^2 + 1 = (X^2 + X + 1)^2$ dans $\mathbb{F}_2[X]$.

$P(X) = X^4 - X^3 - X^2 + 1$ dans $\mathbb{F}_3[X]$.

$P(X) = (X-1)\underbrace{(X^3 - X - 1)}_{\text{irréductible}}$ dans $\mathbb{F}_3[X]$

Si P était réductible sur $\mathbb{Z}$, alors

$$\underbrace{P = \underbrace{Q \quad R}_{\text{de degrés } 1,3} \text{ avec } Q, R \epsilon \mathbb{Z}[X]}_{\text{impossible car pas de facteur de degré 1 mod 2}}$$

ou bien $2,2$.

Remarques : les coefficients dominants de Q, R sont premiers à 2 et à 3.

Donc $P = QR$ avec deg Q=deg R =2. Donc mod 3:

$\bar{P} = \bar{Q}\,\bar{R}$=$(X-1)(X^3-X-1)$=>

$X^3-X-1|\bar{Q}$ ou $\bar{R}$ absurde !

Conclusion : P irréductible sur $\mathbb{Z}$.

$P(X) = 5X^3+8X^2+3X+15$

$=X^3+X+1 \bmod 2$ irréductible sur $\mathbb{F}_2$. Donc

irréductible sur $\mathbb{Z}$.

$P(X) = X^5+2X^3+3X^2-6X-5$

$=X^5+X^2+1 \bmod 2$ irréductiblesur $\mathbb{F}_2$

car pas de racine et non divisible par X^2+X+1(unique polynôme irréductible sur $\mathbb{F}_2$)

(division euclidienne $\Rightarrow$ $X^5+X^2+1=(X^2+X+1)(X^3+X^2)+1$)

donc $P(X)=X^5+2X^3+3X^2-6X-5$ irréductible sur $\mathbb{Z}$.

ATTENTION. par exemple X^4+1 est irréductible sur $\mathbb{Z}$ mais réductible mod p pour tout p premier.

Exercice 12.

$f(x)=(x-a_1)\ldots(x-a_n)-1$ où les $a_i\epsilon\mathbb{Z}$ sont deux à deux distincts.

Indication : si $f=gh$ avec $g,h\epsilon\mathbb{Z}[x]$ et deg g, $\deg h<n$,

Considérer $g(a_i),h(a_i)$.

$-1=f(a_1)=g(a_1)h(a_1)\Rightarrow g(a_1)=\pm1,h(a_1)=\pm1$. De plus $g(a_1)=-h(a_1)$.

$\forall i,\ g(a_i)=-h(a_i)$

$\ldots$

$\forall i, (g+h)(a_i) = 0.$

Or, $\deg(g+h) \leqslant \max\{\deg g, \deg h\} < n$

Contradiction car $g+h$s'annule n fois $\ldots$

On a montré : f irréductible dans $\mathbb{Z}[x]$ montrons que f est irréductible sur $\mathbb{Q}$.

Si $f = gh$ avec $g, h \in \mathbb{Q}[x]$, alors il existe $0 \neq a$, $b \in \mathbb{Z}$ tels que $ag, bh \epsilon \mathbb{Z}[x]$. Alors $abf = (ag)(bh)$.

Donc $c(abf) = ab = c(ag)c(bh)$

$$\Rightarrow f = \frac{abf}{ab} = \frac{(ag)(bh)}{c(ag)c(bh)} = \underbrace{\frac{ag}{c(ag)}}_{\epsilon \mathbb{Z}[x]} \times \underbrace{\frac{bh}{c(bh)}}_{\epsilon \mathbb{Z}[x]} \ldots$$

Même raisonnement avec

$g(x) = (x-a_1)^2 \ldots (x-a_n)^2 + 1.$

Si $g(x) = p(x)q(x)$ avec $p, q \in \mathbb{Z}[x]$ et $\deg p$, $\deg q < 2n$.

Alors $\forall i, g(a_i) = 1 = p(a_i)\, q(a_i) \Rightarrow p(a_i) = q(a_i) = \pm 1$.

Remarque g ne s'annule pas sur $\mathbb{R}$ donc p, q non plus. Donc p, q sont de signe constant. Supposons p, q unitaires, alors $\forall x \epsilon \mathbb{R}, p(x), q(x) > 0$. Supposons p, q non constants ....

Donc $\forall i, p(a_i) = q(a_i) = 1 \Rightarrow \deg p, \deg q \geqslant n$

$\Rightarrow$deg $p =$ deg $q = n$. Comme p, q unitaires, $\deg(p - q) < n$ et pourtant $p - q$ s'annule n fois ... contradiction.

Donc g irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.