Ex 32

1) A principal, $I \subseteq A$.

Soit $\tilde{J}$ idéal de A/I : <u>But</u> $\tilde{J}$ principal.

Notons : $\pi : A \longrightarrow A/_I$ le morphisme canonique (surjectif).

Soit $J = \pi^{-1}(\tilde{J})$.

<u>Idée n°1</u> : Soit x générateur de J. Montrer $\langle \bar{x} \rangle = \tilde{J}$

Problème : $\bar{x}$ peut être nul.

<u>Remarque</u> : $\ker(\pi) = I$ et π inject. $\Leftrightarrow I = \{0\}$

<u>Idée n°2</u> : Soit x générateur de $I + J$. Montrons $\langle \bar{x} \rangle = \tilde{J}$

- $\langle \bar{x} \rangle \subseteq \tilde{J}$ car $\bar{x} \in \tilde{J}$ car $x = a + b$ avec $a \in I$, $b \in J$ et donc $\bar{x} = \bar{a} + \bar{b} = \bar{0} + \bar{b} \in \tilde{J}$
- $\supseteq$: Soit $\alpha \in \tilde{J}$. $\exists a \in J$ tq $\bar{a} = \pi(a) = \alpha$
  $a \in J \subseteq I + J = \langle x \rangle$ donc $\exists b \in A$, $a = bx$
  et donc $\alpha = \bar{a} = \bar{b}\,\bar{x}$

2) (a) $A = \mathbb{Z}$ $I = n\mathbb{Z}$

Soit $m \in \mathbb{Z}$. Notons $I_m = \langle m, n \rangle \left(= \langle m \rangle + I\right)$

Notons $d_m = \mathrm{pgcd}(m, n)$.

<u>Montrons</u> que les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont les $\langle \overline{d_m} \rangle$ avec $m \in \mathbb{Z}$

$\hookrightarrow$ la question 1 le dit.

Montrons que : $\{d_m \mid m \in \mathbb{Z}\} = \{d \in \mathbb{Z} \mid d \mid n\}$

$\subseteq$ trivial

$\supseteq$ Soit d diviseur de n. alors $\mathrm{pgcd}(d, n) = d$ donc $d_d = d$.

(b) c'est idem.

3) Montrons que : l'ens. des idéaux max de $\mathbb{Z}/n\mathbb{Z}$ sont les $\langle \bar{p} \rangle$ avec p diviseur premier de n.

$n = \cdot\cdot\underbrace{\cdot\,\cdot\,\cdot}_{d}$

$\uparrow$
p

- Soit p premier avec $p \mid n$. <u>But</u> $\langle \bar{p} \rangle$ max.

  Soit $\tilde{J}$ idéal de $\mathbb{Z}/n\mathbb{Z}$ tq $\langle \bar{p} \rangle \subsetneq \tilde{J} \subseteq \mathbb{Z}/n\mathbb{Z}$

  $\tilde{J} = \langle \bar{d} \rangle$ avec $d \mid n$. <u>Deux cas</u> cas $p \mid d$. ie. $d = kp$

  $\Rightarrow \bar{d} = \bar{k}\,\bar{p} \in \langle \bar{p} \rangle$ ie $\tilde{J} \subseteq \langle \bar{p} \rangle$

  Absurde.

<u>Cas $(p, d) = 1$</u>. Bézout $1 = kp + ld$.

$\bar{1} = \bar{k}\bar{p} + \bar{l}\bar{d} \in \tilde{J}$ ie $\tilde{J} = \mathbb{Z}/n\mathbb{Z}$ | $\langle \bar{p} \rangle$ est bien maximal.

Ex 32

3) Réciproquement soit $\tilde{J} \subseteq \mathbb{Z}/n\mathbb{Z}$ maximal. But $\exists p$ premier $| n$ tq $\tilde{J} = \langle \bar{p} \rangle$.

Par (2) $\exists d$ diviseur de n tq $\tilde{J} = \langle \bar{d} \rangle$.

supposons (par l'absurde) que d n'est pas premier.

$\exists p$ premier avec $p \neq d$ tq $d = p.k$

On a $p | d$ donc $p | n$. Donc $\langle \bar{p} \rangle$ idéal de $\mathbb{Z}/n\mathbb{Z}$.

et $\bar{d} = \bar{k} \cdot \bar{p} \in \langle \bar{p} \rangle$ donc $\tilde{J} \subseteq \langle \bar{p} \rangle$.

Vérifions que $\tilde{J} \neq \langle \bar{p} \rangle$. Si on avait égalité : $\bar{p} = \bar{l}\,\bar{d}$

donc $\exists m \in \mathbb{Z}$ tq $p = ld + mn$

or $d | n$ ie $n = a \times d$

$p = ld + mad = d \times (l + ma)$

donc $d = \pm p$ ou $d = \pm 1$ Absurde.

- Pour $\mathbb{Q}[X]/\langle f \rangle$: les idéaux max sont les $\langle \bar{g} \rangle$ où g est un divis. irr. de f.

Ex 34 A intègre. $\mathbb{K} = Fr(A)$

- $x \in \mathbb{K}$ entier sur A : $\exists P \in A[X]$ unitaire, $P(x) = 0$
- A int. clos : $\forall x \in \mathbb{K}$, si x entier sur A alors $x \in A$

1) Soit A factoriel.

Soit $x \in \mathbb{K}$. On le suppose entier sur A. But $x \in A$.

$x = \frac{\alpha}{\beta}$, $\alpha \in A$, $\beta \in A \setminus \{0\}$.

$\exists a_0, a_1, \dots, a_{n-1} \in A$ tq $x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0$ $\quad a_0 = \frac{a_0}{1}$

On a : $\frac{\alpha^n}{\beta^n} + a_{n-1} \frac{\alpha^{n-1}}{\beta^{n-1}} + \dots + a_1 \frac{\alpha}{\beta} + a_0 = 0$ $\quad \times \beta^n$

$$\alpha^n + a_{n-1}\beta\alpha^{n-1} + a_{n-2}\beta^2\alpha^{n-2} + \dots + a_1\beta^{n-1}\alpha + a_0\beta^n = 0$$

On peut supposer $pgcd(\alpha, \beta) = 1$. (ie $\frac{\alpha}{\beta}$ est "simplifiée").

$\alpha^n = \beta \times (\ ----\ )$. Si β n'est pas inversible alors on considère un facteur irréd. de β. Alors il est dans α. Absurde car $pgcd(\alpha, \beta) = 1$

Ainsi $x \in A$.

Ex 34

(2) $d \in \mathbb{Z}$ sans facteur carré.

$$A = \mathbb{Z}[X]/\langle X^2 - d \rangle .$$

Pourquoi A est-il intègre ? (pour pouvoir considérer son corps de fraction)

$X^2 - d$ irréd. dans $\mathbb{Z}[X]$?

$X^2 - d = \alpha(aX+b)(cX+d)$ ou $X^2 - d = \alpha(aX^2 + bX + c)$

$\hookrightarrow -\frac{b}{a}$ racine, avec $-\frac{b}{a} \in \mathbb{Q}$ Absurde car les racines sont $\sqrt{d}$ et $-\sqrt{d}$

$\hookrightarrow \alpha a = 1$ ie $\alpha = 1$ et $a = 1$ et $b = 0$ et $c = -d$

$$\delta = \overline{X} \in \mathbb{Z}[X]/\langle X^2 - d \rangle$$

On suppose : $d \equiv 1 \mod 4$ ie $\exists k \in \mathbb{Z}$ tq $d = 1 + 4k$

Soit $x = \frac{1+\delta}{2}$. Montrons que x est entier sur A mais $x \notin A$

$$x^2 = \left(\frac{\overline{1}+\overline{X}}{2}\right)^2 = \frac{1}{4}\left(\overline{1} + 2\overline{X} + \overline{X}^2\right) \quad \left(\text{ici } \overline{X^2 - d} = \overline{0}\right)$$

$$= \frac{1}{4}\left(\overline{1} + 2\overline{X} + \overline{d}\right)$$

$$= \frac{1}{4}\left(\overline{1} + 2\overline{X} + 1 + 4\overline{k}\right)$$

$$= \frac{1+\overline{X}}{2} + \overline{k} = x + \overline{k}$$

Ainsi $x^2 - x - \overline{k} = \overline{0}$ ie x est racine de $\overline{1}T^2 - \overline{1}T - \overline{k} \in A[T]$

x est entier sur A.

Montrons que $x \notin A$.

Par l'absurde $x = \frac{\overline{P}}{\overline{1}}$ où $P \in \mathbb{Z}[X]$

$\frac{1+\overline{X}}{2} = \frac{\overline{P}}{\overline{1}}$ donc $1 + \overline{X} = 2 \times \overline{P}$

donc $1 + X - 2P \in \langle X^2 - d \rangle$

ie $\exists Q \in \mathbb{Z}[X]$ tq $1 + X - 2P = Q(X) \times (X^2 - d)$

On divise : $P = T(X)(X^2 - d) + aX + b$ $\quad T(X) \in \mathbb{Z}[X]$, $a, b \in \mathbb{Z}$.

$$1 + X - 2(aX + b) = \left(Q(X) + 2T(X)\right)(X^2 - d)$$

$\Rightarrow \begin{cases} 1 = 2a \\ 1 = 2b \end{cases}$ Absurde car $a, b \in \mathbb{Z}$. [si non nul alors à gauche $\deg \leq 1$ et à droite $\deg \geq 2$]

Ex 35

$\alpha \in \mathbb{C}$ est alg. sur $\mathbb{Q}$: est racine d'un polyn. dans $\mathbb{Q}[X] \setminus \{0\}$.

$\alpha \in \mathbb{C}$ est un entier alg. : $\exists P \in \mathbb{Z}[X]$ unitaire tq $P(\alpha) = 0$.

1) $\alpha \in \mathbb{C}$ alg. sur $\mathbb{Q}$

$I = \{P \in \mathbb{Q}[X] \mid P(\alpha) = 0\} \neq \{0\}$ car α alg.

$I = \langle \mu_\alpha \rangle$

But α entier alg. $\Longleftrightarrow \mu_\alpha \in \mathbb{Z}[X]$

$\Leftarrow$ trivial par définition

$\Rightarrow$ Par hyp. $\exists P \in \mathbb{Z}[X]$ unitaire tq $P(\alpha)$.

$\exists Q \in \mathbb{Q}[X]$ tq $P = Q \times \mu_\alpha$

P : $\in \mathbb{Z}[X]$ et unitaire ; μ_α : $\in \mathbb{Q}[X]$ et unitaire

Q est nécessairement unitaire.

On écrit $Q = \frac{Q_0}{a}$ et $\mu_\alpha = \frac{\mu_0}{b}$ avec $Q_0, \mu_0 \in \mathbb{Z}[X]$ et $a, b \in \mathbb{Z}$. et $c(Q_0) = c(\mu_0) = 1$

$ab P = Q_0 \mu_0$

$c(abP) = c(Q_0)\, c(\mu_0) = 1$

$c(abP) = ab\, c(P)$

$\Rightarrow a, b = \pm 1$

$\Rightarrow \mu_\alpha \in \mathbb{Z}[X]$

2) Soit $r \in \mathbb{Q}$. But $r \in \mathbb{Z} \Leftrightarrow r$ entier alg.

$\Rightarrow$. si $r \in \mathbb{Z}$ alors r est racine de $X - r$

$\Leftarrow$ Par $\exists a_0, \dots, a_{n-1} \in \mathbb{Z}$ tq $x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$ ($x = r$)

$r = \frac{p}{q}$ $p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}, (p, q) = 1$

$\frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_0 = 0$

$\times q^n$

$p^n + a_{n-1} q p^{n-1} + \dots + a_0 q^n = 0$

$p^n = q \times (\dots)$

Absurde car $(p, q) = 1$ sauf si $q = 1$. Donc $r \in \mathbb{Z}$

Indication :

3) Trouver explicitement le polyn. unitaire dans $\mathbb{Z}[X]$ qui annulle $a_n \alpha$

4) Utiliser question 1

$\boxed{\begin{array}{ll} X-i \mid \mu & i \text{ racine donc } \bar{i} \\ X+i \mid \mu & X^2+1 \mid \mu \text{ et } \mu \mid X^2+1 \end{array}}$

exemple pour i : son polyn. min. est X^2+1 et $X^2+1 \in \mathbb{Z}[X]$ donc par 1) i est entier alg.

5) • Calcul explicite
  • Utiliser question 1

6) Utiliser question 5

7)

8)

Ex 35

3) Par hypothèse $\exists a_0, \dots, a_n \in \mathbb{Z}$ avec $a_n \neq 0$ tq $a_n \alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$

On multiplie par a_n^{n-1} :

$$(a_n\alpha)^n + a_{n-1}(a_n\alpha)^{n-1} + a_{n-2}a_n(a_n\alpha)^{n-2} + \dots + a_1 a_n^{n-2}(a_n\alpha) + a_n^{n-1}a_0 = 0$$

Ainsi $a_n\alpha$ est racine de $P = X^n + a_{n-1}X^{n-1} + a_{n-2}a_n X^{n-2} + \dots + a_1 a_n^{n-2} X + a_n^{n-1}a_0$

4) Montrons que le polynôme minimal de i, noté μ, est X^2+1.

$\mu(i) = 0$ et $\mu \in \mathbb{Q}[X]$ donc $\bar{i} = -i$ est aussi racine

donc $X^2+1 \mid \mu$ mais μ divise tout polynôme de $\mathbb{Q}[X]$ dont i est racine ie $\mu \mid X^2+1$. Ainsi μ et X^2+1 sont égaux à une constante près. Or μ et X^2+1 sont unitaires donc cette constante est 1 i.e. $\mu = X^2+1$.

Variante : μ ne peut pas être de degré car sinon ce serait $X - i$ donc μ est de degré ≥ 2. Or X^2+1 annulle i et est unitaire c'est donc le polynôme (unitaire) de degré minimal parmi ceux qui s'annulle en i, μ est donc égal à X^2+1

Par la question 1, i est un entier algébrique.

- Etude de $\frac{i}{2}$:

  le polynôme minimal est $\mu = X^2 + \frac{1}{4} \notin \mathbb{Z}[X]$ donc $i/2$ n'est pas un entier algébrique.

- Etude de $\alpha = \frac{1}{2}(1+\sqrt{2})$

$$\alpha^2 = \frac{1}{4}(1 + 2\sqrt{2} + 2) = \frac{1}{4}(3 + 2\sqrt{2}) = \frac{1}{4}(1 + 2(1+2\sqrt{2}))$$
$$= \frac{1}{4} + \frac{1}{2}(1+2\sqrt{2}) = \alpha + \frac{1}{4}$$

Ainsi $\alpha^2 - \alpha - \frac{1}{4} = 0$ ie $P(\alpha) = 0$ où $P = X^2 - X - \frac{1}{4}$.

$\mu_\alpha \mid X^2 - X - \frac{1}{4}$. Si μ_α était de degré 1 alors $\frac{1}{2}(1+\sqrt{2})$ serait dans $\mathbb{Q}$ donc $\deg(\mu_\alpha) \geq 2$ et donc $\mu_\alpha = X^2 - X - \frac{1}{4} \notin \mathbb{Z}[X]$ et donc α n'est pas un entier alg.

- Etude de $\alpha = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

$$\alpha^2 = \frac{1}{4}(-1+i\sqrt{3})^2 = \frac{1}{4}(1 - 2i\sqrt{3} - 3) = \frac{1}{4}(-2 - 2i\sqrt{3}) = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$$
$$= -1 + \frac{1}{2} - i\frac{\sqrt{3}}{2} = -1 - \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = -1 - \alpha$$

Ainsi $\alpha^2 + \alpha + 1 = 0$. On montre alors que $\mu_\alpha = X^2 + X + 1 \in \mathbb{Z}[X]$ et donc α est bien un entier algébrique

Ex 35

5) Un calcul explicite montre que $a+b\delta$ est racine de $X^2-2aX+a^2-db^2=P$

Notons $\alpha = a+b\delta$.

Le polyn. minimal de α est P (car il ne peut pas être de degré 1 sinon $\alpha \in \mathbb{Q}$). Par la question 1, $P \in \mathbb{Z}[X] \Leftrightarrow \alpha$ entier alg.

ie α entier alg. $\Leftrightarrow a^2-db^2,\ 2a \in \mathbb{Z}$.

6) Ici $d=-1$ et $a+ib$ est entier alg. si et s. si $\begin{cases} a^2-b^2 \in \mathbb{Z} \\ 2a \in \mathbb{Z} \end{cases}$ $(*)$

Supposons $(*)$ satisfait :

$\exists k \in \mathbb{Z}$ tq $a = \frac{k}{2}$ et $\exists m \in \mathbb{Z}$ tq $a^2-b^2=m$

D'où $\frac{k^2}{4} = b^2+m$ et $k^2 = 4(b^2+m)$. Donc $2 \mid k$.

Ainsi $a \in \mathbb{Z}$. et $b^2 = a^2-m$ d'où $b^2 \in \mathbb{Z}$.

Si on écrit $b = \frac{p}{q}$ alors $b^2 = \frac{p^2}{q^2}$ et si p,q sont premiers entre eux alors la condition $b^2 \in \mathbb{Z}$ entraine $q^2=1$ et donc $b \in \mathbb{Z}$.

Ainsi on a : $(*) \Rightarrow a,b \in \mathbb{Z}$

on a trivialement l'implication inverse et donc $a+ib$, avec $a,b \in \mathbb{Q}$, est un entier alg. si et s. si $a,b \in \mathbb{Z}$.

7) Ici $d=2$ et : $a+b\sqrt{2}$ entier alg $\Leftrightarrow \begin{cases} a^2-2b^2 \\ 2a \end{cases} \in \mathbb{Z}$ $(*)$

Supposons $(*)$. Alors $a = \frac{k}{2}$ avec $k \in \mathbb{Z}$

et $a^2-2b^2 = m$ avec $m \in \mathbb{Z}$

D'où $\frac{k^2}{4} - 2b^2 = m$ D'où $k^2 = 4(2b^2+m)$

$2 \mid k$ et donc $a \in \mathbb{Z}$. Ainsi $2b^2 = a^2-m \in \mathbb{Z}$

Ecrivons $b = \frac{p}{q}$ avec $(p,q)=1$ alors $2b^2 = \frac{2p^2}{q^2}$

Si $2 \mid q$ alors $q = 2q'$ et $b^2 = \frac{p^2}{2q'^2}$ avec $(p^2, 2q'^2) = 1$

donc c'est absurde (b^2 ne peut pas être dans $\mathbb{Z}$)

sinon $(2p^2, q^2) = 1$ entraine $q^2=1$ et donc $b \in \mathbb{Z}$

Ainsi $(*) \Leftrightarrow a,b \in \mathbb{Z}$ et on peut conclure.

8) La réponse devrait être non mais les calculs semblent mener à une réponse positive...