

**Corrigé de l'examen terminal (première session)**

**Exercice 1**

1. Résoudre le système de congruences d'inconnue  $x \in \mathbf{Z}$  :  $\begin{cases} x \equiv 5 [7] \\ x \equiv 7 [13] \end{cases}$ .

On note que  $\text{pgcd}(7, 13) = 1$ .

Déterminons une solution particulière du système. Calculons tout d'abord une relation de Bezout pour 7 et 13. Si on ne la voit pas directement, on peut écrire  $13 = 7 + 6$ ,  $7 = 6 + 1$  d'où

$$1 = 7 - 1 \times 6 = 7 - (13 - 7) = 2 \times 7 - 13$$

Ainsi  $1 \equiv -13 [7]$  et  $1 \equiv 2 \times 7 [13]$  d'où  $5 \equiv (-5) \times 13 [7]$  et  $7 \equiv 14 \times 7 [13]$ . Ainsi

$$x_0 = (-5) \times 13 + 14 \times 7 = 33$$

est une solution particulière du système. Le système proposé est donc équivalent à  $\begin{cases} x \equiv x_0 [7] \\ x \equiv x_0 [13] \end{cases}$ .

Comme 7 et 13 sont premiers entre eux, on peut écrire

$$\begin{cases} x \equiv x_0 [7] \\ x \equiv x_0 [13] \end{cases} \iff (7|(x-x_0)) \text{ et } (13|(x-x_0)) \iff 7 \times 13|(x-x_0) \iff x \equiv x_0 [7 \times 13].$$

L'ensemble des solutions du système proposé est donc l'ensemble  $33 + 91\mathbf{Z}$ .

2. Résoudre l'équation  $x^3 = 5$ ,  $x \in A$  pour les anneaux  $A$  suivants :  $\mathbf{Z}/11\mathbf{Z}$ ,  $\mathbf{Z}/121\mathbf{Z}$ .

Supposons d'abord  $A = \mathbf{Z}/11\mathbf{Z}$ . Dans  $\mathbf{Z}/11\mathbf{Z}$ , on a  $[0]_{11}^3 = [0]_{11} \neq [5]_{11}$ . Par ailleurs 11 est premier donc  $\mathbf{Z}/11\mathbf{Z}$  est un corps. Ainsi

$$\{x \in \mathbf{Z}/11\mathbf{Z}, x^3 = [5]_{11}\} = \{x \in (\mathbf{Z}/11\mathbf{Z})^\times, x^3 = [5]_{11}\}.$$

Or  $(\mathbf{Z}/11\mathbf{Z})^\times$  est un groupe de cardinal 10, et comme  $7 \times 3 \equiv 1 [10]$ , l'application  $x \mapsto x^3$  est un isomorphisme du groupe  $(\mathbf{Z}/11\mathbf{Z})^\times$  sur lui-même, de réciproque  $x \mapsto x^7$ .

Ainsi

$$\{x \in (\mathbf{Z}/11\mathbf{Z})^\times, x^3 = [5]_{11}\} = \{[5]_{11}^7\}.$$

Par ailleurs

$$\begin{aligned} [5]_{11}^7 &= (([5]_{11})^2)^2 \times ([5]_{11})^2 \times [5]_{11} = ([25]_{11})^2 \times [25]_{11} \times [5]_{11} = ([3]_{11})^2 \times [3]_{11} \times [5]_{11} \\ &= [9]_{11} \times [3]_{11} \times [5]_{11} = [5]_{11} \times [5]_{11} = [3]_{11} \end{aligned}$$

Donc l'ensemble des solutions de l'équation proposée est  $\{[3]_{11}\}$ .

Considérons à présent le cas où  $A = \mathbf{Z}/121\mathbf{Z}$ . On note que  $121 = 11^2$ .

Soit  $a \in \mathbf{Z}$  tel que  $[a]_{121}^3 = [5]_{121}$ , autrement dit  $a^3 \equiv 5 [121]$ . Comme 11 divise 121, on a en particulier  $[a]_{11}^3 = [5]_{11}$ . D'après ce qui précède, on a donc nécessairement  $a \equiv 3 [11]$ . Ainsi

$$\{a \in \mathbf{Z}, [a]_{121}^3 = [5]_{121}\} = \{a \in 3 + 11\mathbf{Z}, [a]_{121}^3 = [5]_{121}\}.$$

Pour  $k \in \mathbf{Z}$ , considérons  $a = 3 + 11k$ . D'après la formule du binôme de Newton et comme  $121 = 11^2$ , on a

$$(3 + 11k)^3 - 3 \equiv 3^3 + 3 \cdot 3^2 \cdot 11 \cdot k - 3 [121] \equiv 11(2 + 3 \cdot 3^2 \cdot k) [121]$$

Ainsi

$$(3 + 11k)^3 - 3 \equiv 0 [121] \iff 2 + 3 \cdot 3^2 \cdot k \equiv 0 [11] \iff 2 + 5 \cdot k \equiv 0 [11]$$

Or 5 est inversible modulo 11, d'inverse  $-2$ , d'où

$$2 + 5 \cdot k \equiv 0 [11] \iff -2 \times (2 + 5 \cdot k) \equiv 0 [11] \iff -4 + k \equiv 0 [11]$$

Ceci montre que

$$\{a \in 3 + 11\mathbf{Z}, [a]_{121}^3 = [5]_{121}\} = 3 + 11(4 + 11\mathbf{Z}) = 47 + 121\mathbf{Z}.$$

Ainsi l'ensemble des solutions de l'équation proposée est  $\{[47]_{121}\}$ .

### Exercice 2

Soit  $\mathbf{K}$  un corps à 4 éléments. On note 0 l'élément neutre pour l'addition, 1 l'élément neutre pour la multiplication, et  $\mathbf{K} \setminus \{0, 1\} = \{\alpha, \beta\}$ . En respectant ces notations, donner les tables d'addition et de multiplication de  $\mathbf{K}$ . Aucune justification, aucun calcul annexe n'est demandé sur la copie.

+	0	1	$\alpha$	$\beta$
0	0	1	$\alpha$	$\beta$
1	1	0	$\beta$	$\alpha$
$\alpha$	$\alpha$	$\beta$	0	1
$\beta$	$\beta$	$\alpha$	1	0

$\times$	0	1	$\alpha$	$\beta$
0	0	0	0	0
1	0	1	$\alpha$	$\beta$
$\alpha$	0	$\alpha$	$\beta$	1
$\beta$	0	$\beta$	1	$\alpha$

### Exercice 3

Pour chacune des assertions  $(\mathbf{A}_1)$  à  $(\mathbf{A}_{10})$  ci-dessous, indiquer si elle est vraie ou fausse. On rappelle que toutes les réponses doivent être justifiées !

1. Soit  $B$  un anneau et  $A$  un sous-anneau de  $B$ .

(a)  $(\mathbf{A}_1)$  On a  $A^\times = B^\times \cap A$ .

FAUX : Prenons  $A = \mathbf{Z}$  et  $B = \mathbf{Q}$ ; alors  $2 \in \mathbf{Z}$  est non nul donc inversible dans  $\mathbf{Q}$  (qui est un corps) mais n'est pas un élément de  $\mathbf{Z}^\times = \{1, -1\}$ .

(b)  $(\mathbf{A}_2)$  Soit  $a \in A$  un élément irréductible de  $A$ ; alors  $a$  est un élément irréductible de  $B$ .

FAUX : Prenons  $A = \mathbf{R}[X]$ ,  $B = \mathbf{C}[X]$ , et  $a = X^2 + 1$ ;  $a$  est de degré 2 et n'a pas de racine dans  $\mathbf{R}$ , donc est irréductible dans  $\mathbf{R}[X]$ ; cependant dans  $\mathbf{C}[X]$ , on peut écrire  $a = (X + i)(X - i)$  comme produit de deux polynômes de degré 1, donc  $a$  n'est pas irréductible dans  $\mathbf{C}[X]$ .

2.  $(\mathbf{A}_3)$  Soit  $A$  et  $B$  des anneaux et  $\varphi: A \rightarrow B$  un morphisme d'anneaux surjectif. NB :  $(\mathbf{A}_3)$  n'était bien sûr pas une assertion, désolé pour la coquille.

(a) (**A<sub>4</sub>**) Soit  $\mathfrak{p}$  un idéal premier de  $A$ ; alors  $\varphi(\mathfrak{p})$  est un idéal premier de  $B$ .

FAUX : Prenons  $A = \mathbf{Z}$ ,  $B = \mathbf{Z}/4\mathbf{Z}$ ,  $\mathfrak{p} = \{0\}$  et  $\varphi$  le morphisme quotient;  $\varphi$  est bien surjectif et comme  $\mathbf{Z}$  est intègre,  $\{0\}$  est bien un idéal premier de  $\mathbf{Z}$ ; cependant  $\varphi(\{0\}) = \{0\}$  n'est pas un idéal premier de  $\mathbf{Z}/4\mathbf{Z}$  car  $\mathbf{Z}/4\mathbf{Z}$  n'est pas intègre.

(b) (**A<sub>5</sub>**) Soit  $\mathfrak{p}$  un idéal maximal de  $B$ ; alors  $\varphi^{-1}(\mathfrak{p})$  est un idéal maximal de  $A$ .

VRAI : Considérons  $\psi: A \rightarrow B/\mathfrak{p}$  la composée de  $\varphi$  avec le morphisme quotient  $\pi: B \rightarrow B/\mathfrak{p}$ ; comme composée de deux morphismes surjectifs,  $\psi$  est surjectif; comme le noyau de  $\pi$  est  $\mathfrak{p}$ , le noyau de  $\psi$  est  $\varphi^{-1}(\mathfrak{p})$ ; par le théorème d'isomorphisme,  $A/\varphi^{-1}(\mathfrak{p})$  est isomorphe à  $B/\mathfrak{p}$ ; comme  $\mathfrak{p}$  est maximal,  $B/\mathfrak{p}$  est un corps, donc  $A/\varphi^{-1}(\mathfrak{p})$  est un corps et donc  $\varphi^{-1}(\mathfrak{p})$  est maximal.

3. (**A<sub>6</sub>**) Le polynôme  $X^4 + X^2 + 1 \in \mathbf{F}_2[X]$  est l'unique polynôme de  $\mathbf{F}_2[X]$  de degré 4, réductible et sans racine dans  $\mathbf{F}_2$ .

VRAI : Soit  $P \in \mathbf{F}_2[X]$  un polynôme de  $\mathbf{F}_2[X]$  de degré 4, réductible et sans racine dans  $\mathbf{F}_2$ ; comme  $P$  est réductible,  $P$  s'écrit  $QR$ , avec  $Q, R \in \mathbf{F}_2[X]$  et  $\deg(Q), \deg(R) < \deg(P)$ ; comme  $P$  est sans racine dans  $\mathbf{F}_2$ ,  $Q$  et  $R$  sont également sans racine dans  $\mathbf{F}_2$ , donc  $\deg(Q), \deg(R) \geq 2$ ; comme  $4 = \deg(P) = \deg(Q) + \deg(R)$ , on a donc nécessairement  $\deg(Q) = \deg(R) = 2$ . Or les quatre polynômes de degré 2 sur  $\mathbf{F}_2[X]$  sont  $X^2, X^2 + 1, X^2 + X, X^2 + X + 1$  et on vérifie aussitôt que parmi eux seul  $X^2 + X + 1$  n'a pas de racine dans  $\mathbf{F}_2$ . Donc  $Q = R = X^2 + X + 1$  et  $P = (X^2 + X + 1)^2 = X^4 + X^2 + 1$ . Réciproquement, comme  $X^2 + X + 1$  n'a pas de racine dans  $\mathbf{F}_2$ ,  $(X^2 + X + 1)^2$  est bien réductible et sans racine dans  $\mathbf{F}_2$ .

4. (**A<sub>7</sub>**) Le polynôme  $X^4 + 3X^3 - 6X^2 + 12X + 21$  est un élément irréductible de  $\mathbf{Z}[X]$ .

VRAI : 3 est un élément irréductible de l'anneau factoriel  $\mathbf{Z}$ , qui ne divise pas 1 et divise 3, -6, 12, 21, et par ailleurs  $3^2$  ne divise pas 21; le critère d'Eisenstein permet donc de dire que  $X^4 + 3X^3 - 6X^2 + 12X + 21$  est irréductible dans  $\mathbf{Q}[X]$ , donc dans  $\mathbf{Z}[X]$  car il est unitaire donc primitif.

5. (**A<sub>8</sub>**) Le polynôme  $X^4 + 3X^3 - 6X^2 + 12X - 10$  est un élément irréductible de  $\mathbf{Z}[X]$ .

FAUX : Le polynôme en question s'annule en 1; comme il est de degré strictement supérieur à 1, c'est donc un élément réductible de  $\mathbf{Q}[X]$ , et donc de  $\mathbf{Z}[X]$  d'après le cours.

6. Soit  $A$  un anneau,  $S$  une partie multiplicative de  $A$  ne contenant pas 0 et  $\iota: A \rightarrow S^{-1}A$  le morphisme de localisation.

(a) (**A<sub>9</sub>**) Le morphisme  $\iota$  est injectif.

FAUX : Prenons  $A = \mathbf{Q} \times \mathbf{Q}$  et  $S = \mathbf{Q}^\times \times \{0, 1\}$ , dont on vérifie facilement que c'est une partie multiplicative ne contenant pas 0. Comme  $(1, 0) \times (0, 1) = 0$ , on a  $0 = \iota((1, 0) \times (0, 1)) = \iota((1, 0))\iota((0, 1))$ . Or  $(1, 0) \in S$  donc  $\iota((1, 0))$  est inversible, donc  $\iota((0, 1)) = 0$  et  $\iota$  n'est pas injectif.

(b) (**A<sub>10</sub>**) (\*) L'application  $\mathcal{I} \mapsto \iota^{-1}(\mathcal{I})$  est une bijection de l'ensemble des idéaux propres de  $S^{-1}A$  sur l'ensemble des idéaux  $\mathcal{J}$  de  $A$  tels que  $\mathcal{J} \cap S = \emptyset$ .

FAUX : Prenons  $A = \mathbf{Z}$ ,  $S = \mathbf{Z} \setminus 2\mathbf{Z}$  et montrons que l'application en question n'est pas surjective. L'idéal  $\mathcal{J} := 6\mathbf{Z}$  est contenu dans  $2\mathbf{Z}$  et donc ne rencontre pas  $S$ . Supposons qu'il existe un idéal propre  $\mathcal{I}$  de  $S^{-1}\mathbf{Z}$  tel que  $\iota^{-1}(\mathcal{I}) = \mathcal{J}$ . Alors  $\mathcal{I}$  contient  $\iota(6) = \iota(3) \times \iota(2)$  et comme  $\iota(3)$  est inversible,  $\mathcal{I}$  contient  $\iota(2)$ ; donc  $2 \in \iota^{-1}(\mathcal{I})$ , or  $2 \notin \mathcal{J}$ , contradiction.

#### Exercice 4

Soit  $\mathbf{K}$  un corps et  $n$  un entier positif tel que  $\text{pgcd}(3, n) = 1$ .

1. Soit  $R_0, R_1, R_2$  des éléments de  $\mathbf{K}[T]$  ( $\mathbf{K}$ -algèbre des polynômes en une variable  $T$  à coefficients dans  $\mathbf{K}$ ). On suppose qu'on a la relation

$$R_0(T^3) + R_1(T^3)T^n + R_2(T^3)T^{2n} = 0.$$

Montrer que  $R_0 = R_1 = R_2 = 0$ .

Si  $R_0 = R_1 = 0$ , il vient aussitôt  $R_2(T^3) = 0$  d'où  $R_2 = 0$ .

Supposons à présent  $R_0 \neq 0$  ou  $R_1 \neq 0$ . Alors  $3 \deg(R_0)$  et  $3 \deg(R_1) + n$  sont distincts : c'est clair si  $R_0$  ou  $R_1$  est nul, et sinon l'égalité  $3 \deg(R_0) = 3 \deg(R_1) + n$  entraîne que 3 divise  $n$  ce qui contredit  $\text{pgcd}(3, n) = 1$ . On en déduit que

$$\deg(R_0(T^3) + R_1(T^3)T^n) = \text{Max}(3 \deg(R_0), 3 \deg(R_1) + n) \in \mathbf{N}$$

puis que (utilisant la relation de l'énoncé)

$$3 \deg(R_2) + 2n = \text{Max}(3 \deg(R_0), 3 \deg(R_1) + n).$$

En particulier  $\deg(R_2) \in \mathbf{N}$ . Si  $3 \deg(R_2) + 2n = 3 \deg(R_0)$ , on en déduit donc que 3 divise  $2n$ , donc  $n$  car  $\text{pgcd}(2, 3) = 1$ , ce qui contredit  $\text{pgcd}(3, n) = 1$ . Si  $3 \deg(R_2) + 2n = 3 \deg(R_1) + n$ , on en déduit que 3 divise  $n$ , ce qui là encore contredit  $\text{pgcd}(3, n) = 1$ .

On a donc bien  $R_0 = R_1 = R_2 = 0$ .

2. Soit  $\varphi: \mathbf{K}[X, Y] \rightarrow \mathbf{K}[T]$  l'unique morphisme de  $\mathbf{K}$ -algèbres qui envoie  $X$  sur  $T^n$  et  $Y$  sur  $T^3$ . Montrer que  $\text{Ker}(\varphi) = \langle X^3 - Y^n \rangle$ . En déduire que l'idéal  $\langle X^3 - Y^n \rangle$  est premier, puis que  $X^3 - Y^n$  est un élément irréductible de  $\mathbf{K}[X, Y]$ .

On a  $\varphi(X^3 - Y^n) = (T^n)^3 - (T^3)^n = T^{3n} - T^{3n} = 0$  donc  $X^3 - Y^n \in \text{Ker}(\varphi)$ . Comme  $\text{Ker}(\varphi)$  est un idéal de  $\mathbf{K}[X, Y]$ , on a l'inclusion  $\langle X^3 - Y^n \rangle \subset \text{Ker}(\varphi)$ .

Montrons l'inclusion réciproque. Soit  $P \in \text{Ker}(\varphi)$ . Vu comme polynôme en l'indéterminée  $X$  à coefficients dans  $\mathbf{K}[Y]$ ,  $X^3 - Y^n$  est unitaire de degré 3. On sait donc qu'il existe  $Q \in \mathbf{K}[X, Y]$  et  $R \in \mathbf{K}[X, Y]$ , avec  $\deg_X(R) \leq 2$  tel que  $P = (X^3 - Y^n)Q + R$ . Il existe en particulier  $R_0, R_1, R_2 \in \mathbf{K}[Y]$  tels que  $R = R_0(Y) + R_1(Y)X + R_2(Y)X^2$ . On a par ailleurs

$$0 = \varphi(P) = \varphi(X^3 - Y^n)\varphi(Q) + \varphi(R_0(Y)) + \varphi(R_1(Y))\varphi(X) + \varphi(R_2(Y))\varphi(X^2)$$

soit

$$0 = 0 \cdot \varphi(Q) + R_0(T^3) + R_1(T^3)T^n + R_2(T^3)T^{2n}.$$

D'après la question précédente, on a  $R_0 = R_1 = R_2 = 0$ , donc  $R = 0$  d'où  $P = (X^3 - Y^n)Q$  soit finalement  $P \in \langle X^3 - Y^n \rangle$ .

Donc  $\text{Ker}(\varphi) \subset \langle X^3 - Y^n \rangle$  et finalement  $\text{Ker}(\varphi) = \langle X^3 - Y^n \rangle$ .

Par le théorème d'isomorphisme, les anneaux  $\mathbf{K}[X, Y]/\text{Ker}(\varphi)$  et  $\text{Im}(\varphi)$  sont isomorphes. Or  $\text{Im}(\varphi)$  est un sous-anneau de  $\mathbf{K}[T]$ , qui est intègre. Donc  $\text{Im}(\varphi)$  est intègre, et finalement  $\mathbf{K}[X, Y]/\text{Ker}(\varphi)$  est intègre. Donc  $\text{Ker}(\varphi) = \langle X^3 - Y^n \rangle$  est premier.

On sait que dans n'importe quel anneau intègre, un élément non nul qui engendre un idéal premier est irréductible. Donc  $X^3 - Y^n$  est irréductible.

3. En considérant  $X^3 - Y^n$  comme un élément de  $\mathbf{K}(Y)[X]$ , donner une autre démonstration du fait que  $X^3 - Y^n$  est un élément irréductible de  $\mathbf{K}[X, Y]$ ; pourquoi peut-on en déduire que  $\langle X^3 - Y^n \rangle$  est un idéal premier de  $\mathbf{K}[X, Y]$  ?

Vu comme élément de  $\mathbf{K}(Y)[X]$ ,  $P := X^3 - Y^n$  est de degré 3 ; il est donc irréductible dans  $\mathbf{K}(Y)[X]$  si et seulement s'il n'a pas de racine dans  $\mathbf{K}(Y)$ . Soit  $A, B \in \mathbf{K}[Y]$ , avec  $B \neq 0$ , tels que  $P(\frac{A}{B}) = 0$ . On a donc  $\frac{A^3}{B^3} = Y^n$ , d'où  $A^3 = B^3 Y^n$ . Ainsi  $A$  est non nul et en prenant les degrés on trouve  $3 \deg(A) = 3 \deg(B) + n$ , donc 3 divise  $n$ , contradiction. On en conclut que  $P$  est bien irréductible dans  $\mathbf{K}(Y)[X]$ . Vu comme polynôme en l'indéterminée  $X$  à coefficients dans  $\mathbf{K}[Y]$ ,  $P$  est unitaire donc primitif. Donc  $P$  est un élément irréductible de  $\mathbf{K}[Y][X] = \mathbf{K}[X, Y]$ .

Comme  $\mathbf{K}[X, Y]$  est factoriel, tout élément irréductible engendre un idéal premier.

### Exercice 5

Soit  $p$  un nombre premier et  $\mathbf{Z}_{(p)}$  le localisé de l'anneau  $\mathbf{Z}$  par rapport au système multiplicatif  $\mathbf{Z} \setminus p\mathbf{Z}$ . Soit  $\mathfrak{M}_p := p\mathbf{Z}_{(p)}$  l'idéal engendré par  $p$  dans  $\mathbf{Z}_{(p)}$ .

1. Montrer que  $\mathbf{Z}_{(p)} \setminus \mathfrak{M}_p$  ne contient que des éléments inversibles de  $\mathbf{Z}_{(p)}$ .

Soit  $x \in \mathbf{Z}_{(p)} \setminus \mathfrak{M}_p$ , que l'on écrit  $x = \frac{a}{b}$  avec  $a \in \mathbf{Z}$  et  $b \in \mathbf{Z} \setminus p\mathbf{Z}$ . Si  $a \in p\mathbf{Z}$ , on voit aussitôt que  $x \in \mathfrak{M}_p$ .

Supposons à présent  $x \in \mathbf{Z}_{(p)} \setminus \mathfrak{M}_p$ . En particulier  $a \notin p\mathbf{Z}$ , donc  $\frac{b}{a}$  est un élément de  $\mathbf{Z}_{(p)}$ . Comme  $\frac{a}{b} \frac{b}{a} = 1$ , ceci montre que  $x$  est inversible dans  $\mathbf{Z}_{(p)}$ .

2. En déduire que  $\mathfrak{M}_p$  est l'unique idéal maximal de  $\mathbf{Z}_{(p)}$ .

Montrons que  $\mathfrak{M}_p$  est un idéal maximal de  $\mathbf{Z}_{(p)}$ . Comme  $1 \notin \mathfrak{M}_p$ ,  $\mathfrak{M}_p$  est un idéal propre de  $\mathbf{Z}_{(p)}$ . Soit  $\mathcal{I}$  un idéal de  $\mathbf{Z}_{(p)}$  contenant strictement  $\mathfrak{M}_p$ . En particulier  $\mathcal{I}$  rencontre  $\mathbf{Z}_{(p)} \setminus \mathfrak{M}_p$ , donc  $\mathbf{Z}_{(p)}^\times$  d'après la question précédente. Donc  $\mathcal{I} = \mathbf{Z}_{(p)}$ . Ceci achève de montrer que  $\mathfrak{M}_p$  est un idéal maximal de  $\mathbf{Z}_{(p)}$ .

Soit  $\mathcal{I}$  un idéal maximal de  $\mathbf{Z}_{(p)}$ . En particulier,  $\mathcal{I}$  est propre, donc  $\mathcal{I}$  ne rencontre pas  $\mathbf{Z}_{(p)}^\times$ . D'après la question précédente,  $\mathcal{I}$  est inclus dans  $\mathfrak{M}_p$ . Comme  $\mathfrak{M}_p$  est propre et  $\mathcal{I}$  est maximal, on a  $\mathcal{I} = \mathfrak{M}_p$ .

Ainsi  $\mathfrak{M}_p$  est bien l'unique idéal maximal de  $\mathbf{Z}_{(p)}$ .

3. Montrer que le morphisme quotient  $\mathbf{Z} \rightarrow \mathbf{F}_p$  se factorise de manière unique par le morphisme de localisation  $\mathbf{Z} \rightarrow \mathbf{Z}_{(p)}$ .

Par la propriété universelle du localisé, il suffit de montrer que le morphisme quotient envoie  $\mathbf{Z} \setminus p\mathbf{Z}$  dans  $\mathbf{F}_p^\times$ . Mais ceci n'est rien d'autre que le fait que,  $p$  étant premier, un entier est inversible modulo  $p$  si et seulement s'il est non divisible par  $p$ .

4. (\*) En déduire que  $\mathbf{Z}_{(p)}/\mathfrak{M}_p$  est isomorphe à  $\mathbf{F}_p$ .

Notons  $\varphi_p: \mathbf{Z}_{(p)} \rightarrow \mathbf{F}_p$  le morphisme obtenu à la question précédente. Comme le morphisme quotient  $\mathbf{Z} \rightarrow \mathbf{F}_p$  est surjectif,  $\varphi_p$  l'est également. En particulier  $\mathbf{Z}_{(p)}/\text{Ker}(\varphi_p)$  est isomorphe à  $\mathbf{F}_p$ . Comme  $\mathbf{F}_p$  est un corps,  $\text{Ker}(\varphi_p)$  est un idéal maximal de  $\mathbf{Z}_{(p)}$ . D'après la question 2,  $\text{Ker}(\varphi_p) = \mathfrak{M}_p$ , ce qui conclut.

5. (\*) Soit  $q$  un nombre premier distinct de  $p$ . Montrer que les anneaux  $\mathbf{Z}_{(p)}$  et  $\mathbf{Z}_{(q)}$  ne sont pas isomorphes.

Supposons qu'il existe un isomorphisme  $\psi: \mathbf{Z}_{(q)} \rightarrow \mathbf{Z}_{(p)}$ . Composant  $\psi$  avec le morphisme  $\varphi_p$  (cf. question précédente), on obtient un morphisme surjectif  $\psi_p: \mathbf{Z}_{(q)} \rightarrow \mathbf{F}_p$ . Comme  $\mathbf{F}_p$  est un corps, le noyau de  $\psi_p$  est nécessairement  $\mathfrak{M}_q$ . Donc  $\mathbf{Z}_{(q)}/\mathfrak{M}_q$  est isomorphe à  $\mathbf{F}_p$ , et d'après la question précédente, on en déduit que  $\mathbf{F}_q$  est isomorphe à  $\mathbf{F}_p$ . Pour des raisons de cardinal, ceci est contradictoire si  $q$  est distinct de  $p$ .

