MAT 3543 : Examen mi-session (solutions)

[5] 1) (a) Soient $R = \mathbb{Z}_3 = \mathbb{Z}/3\mathbb{Z}$, $f = 2x^3 + 2x \in \mathbb{Z}_3[x]$ et $g = 2x^2 + x + 1$. Trouver $q, r \in \mathbb{Z}_3[x]$ tels que $f = qg + r$ et $\deg r < 2$.

Solution : On fait une division avec reste :

$$\begin{array}{rl|l} 2x^3 + 2x & 2x^2 + x + 1 & = x + 1 \\ \underline{2x^3 + x^2 + x} & & \\ 2x^2 + x & & \\ \underline{2x^2 + x + 1} & & \\ -1 & & \end{array}$$

Donc $q = x + 1$, et $r = 2$

[5] (b) Montrer que $x^3 - 8x^2 + 5x + 3 = 0$ n'a pas de solutions dans $\mathbb{Z}$.

Solution Soit $a \in \mathbb{Z}$ une solution de $x^3 - 8x^2 + 5x + 3$, donc $a^3 - 8a^2 + 5a + 3 = 0$. Alors, dans $\mathbb{Z}_2$ on obtient $\bar{a}^3 + \bar{a} + \bar{1} = \bar{0}$

Mais pour $\bar{a} \in \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ on a toujours $\bar{a}^3 + \bar{a} + \bar{1} = \bar{1} + \bar{0}$.

Autre solution : On applique le critère de la racine rationelle.

[6] (c) Est-ce que $x^3 - 8x^2 + 5x + 3$ est un polynôme irréductible dans $\mathbb{Q}[x]$? Dans $\mathbb{R}[x]$?

Solution Dans $\mathbb{Q}[x]$ oui, car toutes les racines rationelles de $f = x^3 - 8x^2 + 5x + 3$ sont des diviseurs de 3 dans $\mathbb{Z}$, mais il n'y en a pas d'après (b)

Dans $\mathbb{R}[x]$ non, car un polynôme irréductible dans $\mathbb{R}[x]$ a toujours un degré ≤ 2.

3) a) Donner la définition d'un élément irréductible dans $F[x]$ pour F un corps. [3]

Solution: Un polynôme $p \in F[x]$ est irréductible si $\deg p \geq 1$ et si $p = fg$ avec $f, g \in F[x]$ implique $f \in F$ ou $g \in F$

b) Donner un exemple d'un polynôme irréductible et un exemple d'un polynôme non-irréductible dans $F[x]$, F corps arbitraire. (Sans justification) [4]

Solution $p = x$ est irréductible et $p = x^2$ ne l'est pas.

c) Prouver: Si $p \in F[x]$ est irréductible, alors $F[x]/\langle p \rangle$ est un corps. [8]

Solution: Soit $0 \neq f + \langle p \rangle \in F[x]$, i.e. $f \notin \langle p \rangle$. Il faut montrer qu'il y a $g \in F[x]$ tel que $fg + \langle p \rangle = 1 + \langle p \rangle$, i.e. $1 - fg \in \langle p \rangle$. Soit $d = pgcd(f, p)$. Vu que $d \mid p$, il y a $q \in F[x]$ t.q. $dq = p$. Alors, soit $q \in F$, soit $d \in F$. Supposons que $q \in F$. Vu que d et p sont unitaires on obtient $q = 1$, donc $d = p$. Alors $p \mid f$ car $d \mid f$. Mais $p \mid f$ implique $f \in \langle p \rangle$, contradiction. Donc $d \in F$. Alors $d = 1$ car d est unitaire. Donc, il y a $r, g \in F[x]$ t.q. $fg + rp = 1$. Ensuite $(f + \langle p \rangle)(g + \langle p \rangle) = fg + \langle p \rangle = 1 + \langle p \rangle$.

4) Soit R un anneau intègre.

[3] (a) Pour $a, b \in R$ définir la relation $a \sim b$.

Solution: Pour $a, b \in R$, les 3 conditions suivantes sont équivalentes.

(1) $a|b$ et $b|a$,

(2) $a = ub$ pour un $u \in R^\times$,

(3) $\langle a \rangle = \langle b \rangle$.

Si l'une, donc toutes ces conditions sont remplies, on dit que a est associé à b.

[7] (b) Soient $a, b, a', b' \in R$ tels que $a \sim a'$ et $b \sim b'$. Montrer:

$$a|b \iff a'|b'$$

Solution $a|b \iff ac = b$ pour un $c \in R \iff b \in \langle a \rangle \iff \langle b \rangle \subset \langle a \rangle$

$\iff \langle b' \rangle \subset \langle a' \rangle$ (car $\langle b \rangle = \langle b' \rangle$ et $\langle a \rangle = \langle a' \rangle$)

$\iff b' \in \langle a' \rangle \iff a'|b'$

[6] (c) Soit $R = \{a+ib : a, b \in \mathbb{Z}\}$

Montrer: (i) $R^\times = \{\pm 1, \pm i\}$ [2]

(ii) $(2+i) \sim (1-2i)$, mais $(1+2i) \not\sim (2+i)$

Solution: (i) L'inclusion $\{\pm i, \pm 1\} \subset R^\times$ est claire. Pour l'autre inclusion soit $r = a+ib \in R^\times$. Donc $r^{-1} = \frac{1}{a+ib} = \frac{a-ib}{a^2+b^2} \in R$, c'est-à-dire $\frac{a}{a^2+b^2} \in \mathbb{Z}$ et $\frac{b}{a^2+b^2} \in \mathbb{Z}$. Il s'ensuit que $a^2+b^2 = 1$ donc $a^2 = 1, b^2 = 0$, ou $a^2 = 0, b^2 = 1$. Alors $r \in \{\pm i, \pm 1\}$.

(ii) On a $(-i)(2+i) = -2i - i^2 = 1-2i$

Mais $\frac{1+2i}{2+i} = \frac{(1+2i)(2-i)}{4-i^2} = \frac{1}{5}(2 - 2i^2 + i(4-1)) = \frac{1}{5}(4+3i) \notin R$

donc $(1+2i) \not\sim (2+i)$.

Autre preuve: Montrer que $2+i \notin \{u(1+2i) : u = \pm 1, \pm i\}$.

[3 ½] a) Donner la définition d'un idéal maximal M dans un anneau R

[5] b) Donner un exemple d'un idéal maximal dans l'anneau R

(i) $R = \mathbb{Z}$ (ii) $R = \mathbb{Z}_8$

(sans justification)

[10] c) Prouver qu'un idéal I dans un anneau R est un idéal maximal si et seulement si R/I est un anneau simple

Solution a) Un idéal M est maximal si $M \neq R$ et si pour chaque ideal I qui contient M on a soit $I = M$, soit $I = R$.

b) (i) $M = p\mathbb{Z}$, p nombre premier

(ii) $M = \langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ (maximal car $\mathbb{Z}_8/\langle \bar{2} \rangle \cong \mathbb{Z}/2\mathbb{Z}$)

c) On appelle R un anneau simple si $R \neq \{0\}$ et si $\{0\}$ et R sont les seuls idéaux de R.

Soit $M \lhd R$ un idéal maximal. Alors $R/M \neq \{0\}$ car $M \neq R$. Si $J \lhd R/M$ on a $J = I/M$ par un idéal I de R qui contient M. Alors, vu que M est maximal, soit $I = M$, donc $I/M = M/M = \{0\}$, soit $I = R$ et $J = R/M$.

Supposons que R/I est un anneau simple. Le fait que $R/I \neq \{0\}$ implique $I \neq R$. Soit $J \lhd R$ tel que $I \subset J$. Donc $J/I \lhd R/I$, alors soit $J/I = \{0\}$, soit $J/I = R/I$. Dans le premier cas on obtient $J = I$, et dans le deuxième cas on a $J = R$. Donc I est un idéal maximal.