MAT 3543 : Examen mi-session (solutions)

1) [2] (a) Donner la définition d'un idéal premier P dans un anneau commutatif R.

Solution : P est un idéal premier, si P est un idéal de R tel que $P \neq R$ et si $rs \in P$ alors $r \in P$ ou $s \in P$, quels que soient $r, s \in R$.

[6] (b) Soit P un idéal dans un anneau commutatif. Prouver : P est un idéal premier si et seulement si R/P est un anneau intègre.

Solution "$\Rightarrow$" Soit P un idéal premier. Alors, $P \neq R$ implique $R/P \neq \{0\}$, donc $1 \neq 0$ dans R/P. Aussi, supposons que $ab = 0$ pour $a, b \in R/P$, disons $a = r + P$, $b = s + P$. On a $0 = ab = rs + P$, i.e. $rs \in P$. Donc $r \in P$, i.e. $a = 0$, ou $s \in P$, i.e., $b = s + P = 0$. CQFD.

"$\Leftarrow$" Vu que $1 \neq 0$ dans R/P, on a $P \neq R$. Supposons que $rs \in P$, i.e. $(r+P)(s+P) = 0_{R/P}$. Donc $r + P = 0$, ie $r \in P$, ou $s + P = 0$, ie $s \in P$. Ceci montre que P est un idéal premier.

[2] (c) Donner (sans preuve) tous les idéaux premiers dans $\mathbb{Z}$.

Solution $\{0\}$ et $p\mathbb{Z}$, p premier.

[3] (d) Soit P un idéal premier et soit $a \in R$ un élément nilpotent. Montrer $a \in P$.

Solution Il y a $n \in \mathbb{N}$ tel que $a^n = 0$, car a est nilpotent. Alors, $a^n = a\,a^{n-1} = 0 \in P$, donc $a \in P$ ou $a^{n-1} \in P$. Si $a \notin P$, on obtient $a^{n-1} \in P$. On répète cet argument et l'on obtient $a^{n-i} \in P$ pour $i \in \mathbb{N}$, $i \leq n$, en particulier $a \in P$, pour $i = n-1$! Donc $a \in P$.

2) Soient A, B deux idéaux dans un anneau R tels que $A \subset B$.

Montrer :

[3] (a) L'application $\Theta : R/A \to R/B$, $r+A \mapsto r+B$, est bien définie.

[4] (b) Θ est un épimorphisme d'anneaux

[2] (c) le noyau de Θ est B/A

[2] (d) $R/A \,/\, B/A \cong R/B$.

Solution : (a) Soit $r+A = s+A$, i.e. $r-s \in A$, donc aussi $r-s \in B$.

Alors : $\Theta(r) = r+B = s+B = \Theta(s)$.

(b) $\Theta(1_{R/A}) = \Theta(1+A) = 1+B = 1_{R/B}$, et $\Theta((r+A)+(s+A)) = \Theta(r+s+A) =$

$r+s+B = (r+B)+(s+B) = \Theta(r+A) + \Theta(s+A)$; $\Theta((r+A)\cdot(s+A)) =$

$= \Theta(rs+A) = rs+B = (r+B)(s+B) = \Theta(r+A)\,\Theta(s+A)$

Surjectivité : Pour chaque classe de R/B, à savoir $r+B$, on a $\Theta(r+A) = r+B$.

(c) Soit $r+A \in R/A$. Alors $\Theta(r+A) = 0_{R/B} \Leftrightarrow r+B = B \Leftrightarrow$

$r \in B$. Donc $\operatorname{Ker}\Theta = B/A$.

(d) Cette une conséquence du théorème d'isomorphisme.

3) [2] (a) Soit F un corps. Donner la définition d'un polynôme irréductible dans $F[x]$.

Solution: Un polynôme $p \in F[x]$ est irréductible, si $\deg p \geq 1$ et si $p = fg$ avec $f, g \in F[x]$ entraîne $\deg f = 0$ ou $\deg g = 0$.

(5) Énoncer le test d'irréductibilité modulaire

[3] Solution Soit $f \in \mathbb{Z}[x]$ et soit $p \in \mathbb{Z}$ un nombre premier tel que

(i) p ne divise pas le coefficient dominant de f, et

(ii) le polynôme $\overline{f} \in \mathbb{Z}_p[x]$, obtenu de f par réduction modulo p, est irréductible

Alors, f est irréductible dans $\mathbb{Q}[x]$.

(c) Montrer que $2x^3 - x^2 + 3x + 1$ est irréductible dans $\mathbb{Q}[x]$

[4] Solution On applique le test d'irréductibilité modulaire avec $p = 3$.
On obtient $\overline{f} = 2x^3 - x^2 + 1 \in \mathbb{Z}_3[x]$. $\overline{f}$ est irréductible, car $\overline{f}$ n'a pas de racines dans $\mathbb{Z}_3$: $\overline{f}(0) = 1$, $\overline{f}(1) = 2 - 1 + 1 = 2$, $\overline{f}(2) = 16 - 4 + 1 = 1$
Alors, $f \in \mathbb{Q}[x]$ est irréductible.
2° solution D'après le critère de la racine rationelle, les racines rationnelles de f sont $\frac{c}{d}$ avec $c \mid 1$ et $d \mid 2$, i.e. $\pm 1, \pm \frac{1}{2}$.
On vérifie que $f(\pm 1) \neq 0 \neq f(\pm \frac{1}{2})$. Donc (Th 1, §4.2), f est irréductible

(d) Construire un corps K d'ordre 4 et donner la table de

[6] multiplication de K.

Solution: le polynôme $f = x^2 + x + 1$ est irréductible dans $\mathbb{Z}_2[x]$, car f n'a pas de racines dans $\mathbb{Z}_2$. Alors (§4.3 Th 3), $K = \mathbb{Z}_2[x]/\langle f \rangle$ est un corps. D'après le Th 2 de §4.3 on a

$K = \{0, 1, t, t+1\}$ avec $t = x + \langle f \rangle$.

	0	1	t	$t+1$
0	0	0	0	0
1	0	1	t	$t+1$
t	0	t	$t+1$	1
$t+1$	0	$t+1$	1	t

Raison: $t^2 = t+1$, car $t^2 + t + 1 = 0$

$t(t+1) = t^2 + t = 1$

$(t+1)^2 = t^2 + 2t + 1 = t^2 + 1 = t$

4)(a) Soit F un corps, $0 \neq I$ un idéal dans $F[x]$. Prouver qu'il y a un polynôme h unitaire et un seul tel que $I = \langle h \rangle$.

[10] Solution Vu que $I \neq 0$, il y a des polynômes non-nuls dans I. Après multiplication avec un constant on voit qu'il y a des polynômes unitaires dans I. Soit m le plus petit degré de tous les polynômes unitaires dans I et soit $h \in I$ un polynôme unitaire de degré m. Vu que $h \in I$, on a $\langle h \rangle \subset I$. Pour montrer l'autre direction, soit $f \in I$. Après division avec reste, on a $f = qh + r$ avec $q, r \in F[x]$ et $r = 0$ ou $\deg r < \deg h$. Supposons que $0 \neq r$. Donc $r = f - qh \in I$. Après division par le coefficient dominant, on obtient un polynôme unitaire $\tilde{r} \in I$ avec $\deg \tilde{r} = \deg r$. Ceci contredit le choix de h. Donc $r = 0$ et $f = qh \in \langle h \rangle$.

Unicité: Soit $I = \langle h \rangle = \langle \tilde{h} \rangle$, où h et $\tilde{h}$ sont unitaires. Alors $h \mid \tilde{h}$ et $\tilde{h} \mid h$. Donc, d'après le Th. 9, §4.2, on a $h = \tilde{h}$.

[3] (b) Soit $I = \{ f \in F[x] : f(0) = 0 \}$. Trouver un polynôme unitaire $h \in F[x]$ tel que $I = \langle h \rangle$.

Solution: On cherche un polynôme unitaire $h \in I$ avec un degré minimale. h ne peut pas être un constant, donc $\deg h \geq 1$. Mais $x \in I$, donc $h = x$ et $I = \langle x \rangle$.